UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS
NÍVEL MESTRADO

ROSANE MACHADO

ANÁLISE DA RELAÇÃO ENTRE A GESTÃO DE RISCOS DA TECNOLOGIA DA INFORMAÇÃO (TI) E A GESTÃO DE RISCOS CORPORATIVOS

São Leopoldo
2012

ROSANE MACHADO

ANÁLISE DA RELAÇÃO ENTRE A GESTÃO DE RISCOS DA TECNOLOGIA DA INFORMAÇÃO (TI) E A GESTÃO DE RISCOS CORPORATIVOS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciências Contábeis, pelo Programa de Pós Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos - UNISINOS.

Orientador: Prof. Dr. Adolfo Alberto Vanti

São Leopoldo

2012

Ficha Catalográfica

M149a Machado, Rosane

Análise da relação entre a gestão de riscos da tecnologia da informação (TI) e a gestão de riscos corporativos. / por Rosane Machado. – 2012.

201 f. : il. ; 30cm.

Dissertação (mestrado) — Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Ciências Contábeis, São Leopoldo, RS, 2012.

"Orientação: Prof. Dr. Adolfo Alberto Vanti, Ciências econômicas".

1. Administração - Empresa - Análise - Risco. 2. Gestão - Risco. 3. Tecnologia - Informação. 4. ISO 31000 - COBIT. I. Título.

CDU 658.011.7

Catalogação na Publicação:
Bibliotecária Camila Quaresma Martins - CRB 10/1790

ROSANE MACHADO

ANÁLISE DA RELAÇÃO ENTRE A GESTÃO DE RISCOS DA TECNOLOGIA DA INFORMAÇÃO (TI) E A GESTÃO DE RISCOS CORPORATIVOS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciências Contábeis, pelo Programa de Pós Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos - UNISINOS.

Aprovado em _____/_____/_____.

BANCA EXAMINADORA

_____

Componente da Banca Examinadora

_____

Componente da Banca Examinadora

_____

Componente da Banca Examinadora

Dedico este trabalho aos meus pais Adão e Angelina, ao meu esposo Clóvis e minha filha Milene, por terem me proporcionado suporte familiar nesta trajetória.

AGRADECIMENTOS

Existem pessoas que contribuem de forma efetiva na nossa jornada, aquela palavra que se precisa escutar para que os desafios sejam vencidos. Quero agradecer aos meus familiares, em especial ao meu amor Clóvis e minha filha Milene. Vocês foram decisivos para o caminho até a materialização deste sonho.

Ao meu orientador Professor Dr. Adolfo Alberto Vanti, pelos desafios instigados e as valiosas contribuições para esta dissertação. Bem como, por me proporcionar exemplo de dedicação e qualidade na prestação da atividade da docência.

A companhia SLC Agrícola e aos gestores entrevistados, por possibilitar acesso às informações para que esta pesquisa pudesse ser realizada. Destaco agradecimento especial ao Sr. Frederico Logemann por incentivar esta pesquisa.

Aos meus colegas de mestrado, que nestes últimos anos foram muito mais que apenas colegas de aula, foram parceiros de caminhada. Jornada esta que contemplou diversos meios de comunicação na qual a distância não foi limitador e sim nos aproximou na busca dos conhecimentos instigados por este programa.

Realizo um agradecimento a todos os professores deste PPGA/UNISINOS, em especial aos professores Marcos Antônio de Souza, Clóvis Kronbauer, Carlos Alberto Diehl e Tiago Wickstrom Alves, pelo aprendizado obtido nas aulas deste mestrado.

Aos meus queridos alunos das Faculdades Monteiro Lobato (FATO), que me estimulam a cada aula dada a acreditar na evolução através do conhecimento, bem como me ensinam o valor de ser professor.

Enfim, agradeço a todos aqueles que de forma direta ou indireta, contribuíram para o desenvolvimento desse estudo e principalmente para o meu desenvolvimento no programa de mestrado.

A todos vocês, meu sincero e afetuoso obrigado.

“Mudam-se os tempos, mudam-se as vontades, Muda-se o ser, muda-se a confiança; Todo o mundo é composto de mudança, Tomando sempre novas qualidades..”

(Luis de Camões)

RESUMO

A crescente utilização da tecnologia e dos sistemas de informação, tornou a tecnologia um aliado na gestão das organizações. Neste ambiente, os riscos inerentes à tecnologia da informação (TI) e aos processos de negócios (riscos corporativos) podem impactar de forma negativa os resultados das corporações. É mediante a gestão destes riscos que as organizações podem explorar suas oportunidades e reduzir suas fraquezas, evitando assim perdas desnecessárias. O foco deste trabalho se concentrou em analisar a relação entre a gestão de riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos, mediante um estudo fundamentado teoricamente que foi aprofundado em um estudo de caso único. Evidenciou-se o tipo de pesquisa metodológica como um estudo de caso exploratório de natureza aplicada, com abordagem qualitativa. 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 não existe um processo formal de gerenciamento de riscos de TI, apesar de existirem iniciativas pontuais. Já em se tratando dos riscos corporativos a atuação do comitê de riscos foi identificada, porém a estrutura instaurada não contempla a gestão do risco do tipo operacional, neste prisma os dados indicaram oportunidades de melhorias da relação entre a gestão dos riscos de TI e riscos corporativos.

Palavras-chave: Gestão de riscos. Tecnologia da Informação. ISO 31000. COBIT.

ABSTRACT

The increasing use of technology and information systems became the technology an ally in the management of organizations. In this environment, the risks of information technology (IT) and business processes (enterprise risk) may impact in a negative way the results of the corporations. It is through the management of these risks that organizations can exploit opportunities and reduce their weaknesses, thus avoiding unnecessary losses. The focus of this work is concerned on analyzing the relationship between the risk management of information technology (IT) and management of corporative risk, it is a study based upon a theory that was detailed in a single case study. It became evident the kind of research methodology as an exploratory case study of an applied nature, with a qualitative approach. Data collection was performed from multiple sources such as interviews, questionnaires and documents, interviews were treated by use of software for the lexical analyzer. The results arising from this research indicated that in the case investigated there is no formal process for managing IT risks, although there are specific initiatives. Already in the case of corporate risk committee of the performance of risk has been identified, but the structure does not include established risk management of the type operating, in this perspective the data indicated opportunities for improvement of the relationship between IT risk management and corporate risk.

Keywords: Risk Management. Information Technology. ISO 31000. COBIT.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

A crescente utilização da tecnologia e dos sistemas de informação, tornou a tecnologia da informação um aliado na gestão das organizações. Com a complexidade dos processos, sistemas e operações produzir informações seguras e tempestivas passou a ser fator de sucesso. Neste ambiente, os riscos inerentes a tecnologia da informação (TI) e aos processos de negócios (riscos corporativos) podem impactar de forma negativa os resultados das corporações. Sendo assim, estes riscos necessitam ser gerenciados, afim de sustentar que as práticas decorrentes destes processos não gerem perdas de recursos.

Mediante a gestão de riscos e suas ferramentas, as organizações podem explorar suas oportunidades e reduzir suas fraquezas, evitando assim perdas desnecessárias. Esta pode contemplar a gestão de riscos em tecnologia da informação (TI) e a gestão de riscos corporativos, descritas a seguir.

Para gestão dos riscos da tecnologia da informação (TI) destaca-se a utilização do COBIT representado pela ISACA (*Information Systems Audit and Control Association*), como modelo que 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 descreve em seu processo nº9 maneiras de avaliar e gerenciar os riscos de tecnologia da informação (TI) 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, a recomendações de planos de ação para remediação, e o monitoramento dos riscos (ITGI, 2007) .

Para a gestão dos riscos corporativos preocupa-se com todos os riscos que possam afetar a organização em seu ambiente corporativo, sejam eles estratégicos, financeiros ou operacionais. Para a gestão destes riscos destaca-se a norma ISO 31000 que busca de forma genérica descrever os componentes necessários para uma estrutura de gestão de riscos. Cabe destacar que a avaliação estratégica do risco pode complementar e alavancar a execução de processos ocasionando a melhoria da governança (FRIGO E ANDERSON, 2011).

Em função destes aspectos, o foco deste trabalho se concentrou em analisar a relação existente entre a gestão de riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos, mediante um estudo fundamentado teoricamente que foi aprofundado em um estudo de caso. Para tanto o problema de pesquisa definido foi o seguinte: Como ocorre a relação entre a gestão dos riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Uma vez que se tem o problema de pesquisa, objetivos foram traçados para a busca de sua resposta. O objetivo geral proposto neste estudo é de analisar da relação entre a gestão de riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos.

1.2.2 Objetivos Específicos

Para consecução do objetivo geral definido, foram propostos os seguintes objetivos específicos:

- Identificar requisitos de negócio relacionados à gestão dos riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos;

- Analisar a relação entre os modelos de gestão de riscos de tecnologia da informação (TI) e de gestão de riscos corporativos. Esta análise é contemplada mediante comparação do COBIT (através de seu processo nº9-PO9) e da ISO 31000.
- Analisar as práticas da gestão de riscos de TI e da gestão riscos corporativos, em relação aos processos organizacionais.

1.3 DELIMITAÇÃO DO TEMA

Neste trabalho o foco central concentra-se na análise da relação entre a gestão de riscos da tecnologia da informação (TI) e gerenciamento dos riscos corporativos. Neste sentido, este estudo delimita-se em análises voltadas ao tema gestão de riscos em TI como parte integrante da GTI, e sua relação com a gestão de riscos corporativos.

Não sendo neste prisma objeto deste estudo, a análise do nível de adequação de práticas relacionadas à GTI identificadas na literatura, bem como o grau de probabilidade ou impacto dos tipos de riscos.

1.4 JUSTIFICATIVA

A recente crise mundial levou as empresas a potencializarem a implantação de mecanismos de governança, capazes de garantir os objetivos da companhia e o bom relacionamento com as partes interessadas do negócio.

Neste cenário, a tecnologia da informação (TI) se insere como fator-chave para a tomada de decisão, pois possibilita além de avanços tecnológicos a gestão das informações que subsidiarão este processo. A contribuição da GTI se destaca na garantia de informações adequadas, tempestivas e seguras, características possíveis mediante a utilização de seus instrumentos e modelos.

Estudos sobre a gestão de Riscos de TI e a GTI e sua implantação nas organizações podem ser identificados, como por exemplo: SILVA NETTO e SILVEIRA (2007); RODRIGUES, MACCARI, e SIMÕES (2009); BULGURCU, CAVUSOGLU, e BENBASAT (2010); SPEARS e BARKI (2010); MARINHO DA SILVA, e MORAES (2011); KNORST, *et al.* (2011); e SANTANA e VERAS (2011). Estes estudos estão detalhados nos estudos relacionados da próxima seção.

Cabe destacar que a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando assim o risco, e maximizando o retorno sobre o investimento e as oportunidades, ISO/IEC 27002 (2005). Desta forma, para que as informações sejam seguras é preciso encontrar maneiras de minimizar os riscos inerentes ao negócio e ao ambiente de TI. Uma das formas de buscar a redução desta vulnerabilidade é mediante a gestão destes diferentes riscos.

A gestão dos riscos dentro do ambiente corporativo das organizações tem sido tema de diversos estudos, como por exemplo: LOURENSI *et al.* (2008), GUIMARÃES, *et al.* (2009); DANTAS, *et al.* (2010); ZONATTO e BAUREN (2010); CUNHA, SILVA, e FERNANDES (2011); AVEN (2011); FRIGO e ANDERSOS (2011); e GERIGK e CORBARI (2011). Estes estudos estão detalhados nos estudos relacionados da próxima seção.

Para a ISO 31000 (2009), a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação, considerando a incerteza, a natureza desta incerteza, e como ela pode ser tratada. Esta norma se aplica como uma estrutura genérica para gestão de riscos corporativos.

Neste contexto este estudo contribui com a ampliação da pesquisa em torno dos temas gestão de riscos da tecnologia da informação (TI), e gestão dos riscos corporativos tornando-se relevante para o meio acadêmico e profissional, já que visou à análise da teoria encontrada no âmbito do tema de pesquisa e a aplicação prática dos conceitos mediante verificação no caso de estudo. Este estudo empírico comprova sua relevância ao realizar a análise da relação entre a gestão dos riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos, possibilitando entender como estes afetam o ambiente empresarial, bem como a gestão dos riscos a que a corporação está exposta.

1.5 ESTUDOS RELACIONADOS

Com o intuito de embasar esta pesquisa, e justificar sua relevância, realizou-se uma pesquisa bibliográfica objetivando identificar a ocorrência de publicações específicas sobre gestão de riscos de TI (mediante a GTI) e a gestão dos riscos corporativos.

Buscou-se identificar estudos relacionados publicados em revistas científicas de programas de pós-graduação *stricto sensu* em Ciências contábeis. Com os dados da CAPES (2012) mapeou-se os programas de mestrado em contabilidade, ciências contábeis e controladoria, conforme apresentado no Quadro 1.

Quadro 1: Programas de Pós Graduação Stricto Senso em Ciências Contábeis

PROGRAMA	IES	UF
CIÊNCIAS CONTÁBEIS	FUCAPE	ES
CIÊNCIAS CONTÁBEIS	FURB	SC
CIÊNCIAS CONTÁBEIS E ATUARIAIS	PUC/SP	SP
CIÊNCIAS CONTÁBEIS	UERJ	RJ
CONTABILIDADE E CONTROLADORIA	UFAM	AM
CONTABILIDADE	UFBA	BA
CIÊNCIAS CONTÁBEIS	UFES	ES
CIÊNCIAS CONTÁBEIS	UFMG	MG
CIÊNCIAS CONTÁBEIS	UFPE	PE
CONTABILIDADE	UFPR	PR
CIÊNCIAS CONTÁBEIS	UFRJ	RJ
CONTABILIDADE	UFSC	SC
CONTABILIDADE - UNB - UFPB - UFRN	UNB	DF
CIÊNCIAS CONTÁBEIS	UNIFECAP	SP
CIÊNCIAS CONTÁBEIS	UNISINOS	RS
CIÊNCIAS CONTÁBEIS	UPM	SP
CONTROLADORIA E CONTABILIDADE	USP	SP
CONTROLADORIA E CONTABILIDADE	USP/RP	SP

Fonte: Capes (2012)

Nos dezoito programas identificados na relação da Capes, localizaram-se dezesseis revistas científicas. A lista das revistas é apresentada no Quadro 2.

Quadro 2: Revistas Ligadas à Programas de Pós Graduação *Stricto Senso* em Ciências Contábeis

INSTITUIÇÃO	REVISTA
FUCAPE	Brazilian Business Review – BBR

INSTITUIÇÃO	REVISTA
FURB	Revista Universo Contábil
PUC/SP	Revista Pensamento e Realidade
UERJ	Revista de Contabilidade do Mestrado de Ciências Contábeis da UERJ
UFAM	**o programa não possui revista científica**
UFBA	Revista de Contabilidade da UFBA
UFES	**o programa não possui revista científica**
UFMG	Contabilidade Vista & Revista
UFPE	Revista de Informação Contábil
UFPR	Revista de Contabilidade e Controladoria RC&C
UFRJ	Sociedade, Contabilidade e Gestão
UFSC	Revista Contemporânea de Contabilidade
UNB	UNB Contábil (antiga Contabilidade, Gestão e Governança)
UNIFECAP	Revista Brasileira de Gestão de Negócios – RBGN
UNISINOS	Revista de Administração e Contabilidade da UNISINOS - BASE
UPM	Revista de Administração Mackenzi
USP	Revista de Gestão da Tecnologia e Sistemas de Informação
USP/RP	Revista de Contabilidade e Organizações

Fonte: Elaborado pela autora

Nas revistas citadas no Quadro 2 buscaram-se artigos que continham nas palavras chaves, resumo ou título as seguintes palavras ou expressões: riscos, *risks*, ISO 31000, COSO, Segurança, GTI, Informação, Tecnologia, Governança, COBIT. A escolha das palavras para a busca considerou a relação com os temas gestão de riscos de TI e gestão dos riscos corporativos.

O período considerado foi de seis anos (2007 à 2012) , optou-se por este corte de tempo com o intuito de refletir os estudos recentes sobre o tema. O período selecionado resultou na busca em 229 edições, considerando a soma das edições de todas as revistas científicas listadas no Quadro 2.

Nos artigos encontrados que continham as palavras/expressões procuradas realizou-se uma leitura do resumo, selecionando aqueles que tratavam da gestão de riscos de forma ampla (sem foco em um único tipo de risco), e nos que tratavam de riscos de TI no âmbito da governança de TI. Os artigos encontrados nos periódicos foram organizados em forma de quadro sendo relacionado nos Quadros 3 e 4. Utilizando os mesmos critérios de busca e palavras chaves procedeu-se a pesquisa nos seguintes congressos brasileiros: Congresso de controladoria e contabilidade da Universidade de São Paulo – USP e CONTECSI (Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação).

Quadro 3: Estudos Relacionados ao tema Riscos de TI

ANO	AUTORES	TÍTULO	OBJETIVO	FONTE
2007	SILVA NETTO, e SILVEIRA.	Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas	Verificar em que medida as pequenas e médias empresas realizam gestão da segurança da informação e identificar fatores que influenciam pequenas e médias empresas a adotarem medidas de gestão da segurança da informação.	Periódico
2009	RODRIGUES, MACCARI, e SIMÕES.	O desenho da gestão da tecnologia da informação nas 100 maiores empresas na visão dos executivos de TI	Identificar o desenho do gerenciamento da TI nas 100 maiores empresas brasileiras	Periódico
2010	BULGURCU, CAVUSOGLU, e BENBASAT.	*Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*	Ampliar o conhecimento sobre o cumprimento dos funcionários com as Políticas de Segurança da Informação (PSIs), identificando fatores de racionalidade baseado na teoria da escolha racional.	Periódico
	SPEARS e BARKI	*User participation in information systems security risk management*	Identificar como os usuários participam do Gerenciamento de Riscos de segurança nos processos de negócios, e como a sua participação é percebida e qual é o impacto da participação na segurança do negócio.	Periódico
2011	MARINHO DA SILVA, e MORAES.	Influencia dos direcionadores do Uso da TI na Governança de TI	Analisar como as dimensões tipificam o ambiente organizacional, e influenciam na estruturação de sua governança.	Periódico
	SANTANA e VERAS	Gerenciamento de riscos de TI e suas práticas nas organizações brasileiras: um estudo de casos múltiplos.	Investigar como as organizações gerenciam esses riscos decorrentes do uso da TI e que afetam os seus negócios.	Congresso CONTECSI
	KNORST, *et al.*	*Aligning Information security with the image of The organization and prioritization based on*	Desenvolver o alinhamento estratégico do comportamento organizacional, mediante a priorização das praticas de	Periódico

		Fuzzy logic for the industrial Automation sector	segurança das informações nas organizações.	

Fonte: Elaborado pela autora

O estudo de Silva Netto e Silveira (2007) relevou que 59% das empresas pesquisadas possuíam um nível de segurança satisfatório e que o principal fator motivador para adoção de gestão da segurança da informação é "evitar possíveis perdas financeiras". Todos os fatores inibidores se mostraram importantes para as empresas pesquisadas: falta de conhecimento, valor do investimento, dificuldade em mensurar custo/ benefício e cultura organizacional.

Rodrigues, Maccari e Simões (2009) identificaram que: a GTI é conduzida essencialmente com base nas metodologias padrões de gestão de TI, muito mais dentro da lógica de fornecedora de soluções do que dentro dos princípios da inovação ou quebra de regras dos negócios. Assim, apesar de alinhar-se e responder às demandas básicas dos negócios, a gestão da TI mostras claros avanços de aderência à natureza evolutiva dos modelos de negócios necessária à sustentação de desempenho desses.

Bulgurcu, Cavusoglu, e Benbasat, (2010), observaram que os efeitos da atitude, crenças normativas e auto-eficácia para dar cumprimento a PSI foram significativas. Verificaram que três crenças (percepção do benefício de conformidade, custo percebido de conformidade e custo percebido de descumprimento) sobre a avaliação global das consequências, exerceram influência significativa sobre a atitude do funcionário para com o cumprimento. A Conscientização da Segurança da Informação (CSI) de um funcionário tem um impacto significativo e influencia sobre a atitude em relação à conformidade. Os impactos do benefício de conformidade e custos de abandono da intenção de cumprir com o PSI foram totalmente medidas pela atitude de um funcionário para o seu cumprimento.

Spears e Barki (2010) confirmaram a função importante dos usuários de negócios na contribuição para reduzir riscos de segurança e controles quando a conformidade regulamentar tem uma orientação de processos de negócios. A participação do usuário aumenta quando os mesmos fazem parte do Gerenciamento de Riscos e Segurança do Sistema.

Marinho da Silva e Moraes (2011) encontraram que as características de investimentos em TI influenciam positivamente as principais decisões sobre sua governança, por meio dos direcionadores de uso que envolvem a instituição e que estão presentes em fatores externos que impactam decisões criticas da área, influenciando-as, exceto as relacionadas aos princípios de TI. O contexto interno não influencia diretamente os aspectos de decisões sobre a governança. A TI não é vista como um elemento capaz de estruturar os arquétipos de governança pelo seu uso, ficando definidos pela hierarquia organizacional da instituição.

Santana e Veras (2011), constataram que o conceito de governança de riscos de TI é pouco compreendido e implementado nos casos estudados e que essas não possuem metodologias de gestão de riscos de TI definidas, tampouco executadas. No entanto, exercem a maior parte das práticas indicadas pela referência central da pesquisa, sem alinhamento com um processo de gerenciamento de riscos.

Knorst *et al.* (2011), ao desenvolver o alinhamento estratégico do comportamento organizacional, por meio da priorização das práticas de segurança das informações nas organizações, encontraram que a priorização das estratégias indica de forma significativa os serviços de novos negócios e mercados internacionais. Quanto à proteção da informação, segurança ficou entre "mínimo" e "razoável" e no domínio 8 (RH) da norma ISO/IEC27002, considerada de proteção de 71% como “inadequada” e mínima” no Contexto da governança de TI.

Quadro 4: Estudos Nacionais sobre o tema Riscos Corporativos

ANO	AUTORES	TÍTULO	OBJETIVO	FONTE
2008	LOURENSI, *et al.*	*Risk assessment* nas empresas do estado do Rio Grande do Sul e Santa Catarina: uma visão dos auditores independentes	Identificar se as empresas auditadas no Estado do RS e SC estão observando a Gestão de Riscos	Congresso CONTECSI
2009	GUIMARÃES, *et al.*	A importância da controladoria na gestão de riscos das empresas não financeiras: um estudo da percepção de gestores de riscos e *controllers*	Analisar a importância da controladoria como apoio à gestão de riscos em empresas não financeiras, na percepção dos gestores de riscos e *controllers*	Periódico
2010	DANTAS, *et al.*	Custo-benefício do controle: proposta de um método para avaliação com base no COSO	Propor um método que possibilite a avaliação do custo versus benefício do controle, utilizando como referência os preceitos de gerenciamento de risco e de controle interno divulgados pelo COSO	Periódico

	ZONATTO, e BAUREN.	Categoria de riscos evidenciados nos relatórios de administração de empresas Brasileiras com ADRs	Identificar as categorias de riscos evidenciados nos relatórios de administração (RA)	Periódico
2011	CUNHA, SILVA, e FERNANDES.	Riscos empresariais divulgados em ofertas públicas de ações no Brasil	Investigar o nível de evidenciação dos riscos empresariais informados nos prospectos de oferta pública de ações	Periódico
	GERIGK, e CORBARI.	Risco no ambiente público municipal: um estudo exploratório nos pequenos municípios da região sul do Brasil	Aplicar, junto às administrações públicas municipais, os clássicos conceitos de mensuração de riscos utilizados no ambiente empresarial, com o objetivo de verificar se a vigência da Lei de Responsabilidade Fiscal – LRF impactou positivamente sobre as organizações públicas municipais e se estas estão menos expostas aos riscos do seu ambiente.	Periódico

Fonte: Elaborado pela autora

Lourensi *et al.* (2008) concluíram que de forma geral, não existe conhecimento disseminado sobre o modelo COSO nas empresas pesquisadas. Porém, de alguma forma, os gestores aplicam partes do *Risk Assessment* para avaliar os riscos das organizações, principalmente com relação ao risco do negócio e sua capacidade de solvência. Deste modo, as organizações tentam reduzir a um nível aceitável, a possibilidade de ocorrência dos riscos apresentados em cada atividade inerente a seus negócios.

Os resultados da pesquisa de Guimarães, *et al.* (2009) apontam que a controladoria fornece suporte à gestão de riscos por meio de informações que contribuem para a mitigação dos riscos nas empresas não financeiras. Já Cunha Silva e Fernandes (2011), constataram que o nível de evidenciação de riscos nos prospectos de ofertas de ações ainda não é satisfatório.

Dantas, *et al.* (2010), demonstraram por meio de seu estudo que a utilização de metodologia de avaliação de riscos e a construção de metodologia que relacione a importância do risco e a eficácia do controle já instituído foram importantes para possibilitar: o fortalecimento dos controles atrelados aos riscos de maior relevância; o direcionamento dos recursos às atividades que mais agregam valor; e o amadurecimento do ambiente de controle.

Zonatto e Bauren (2010), identificaram que 19 empresas dentre as pesquisadas evidenciaram algum tipo de risco a que a empresa está exposta, o que representou 67,86% da amostra. Nove empresas, 32,14% não evidenciaram nenhum tipo de estudo. Cunha, Silva e Fernandes (2011), contataram que o nível de evidenciação dos riscos nos prospectos de oferta de ações ainda não é satisfatório.

Gerigk e Corbari (2011), identificaram que os municípios estudados estão menos expostos aos riscos de seu ambiente após a vigência da Lei de Responsabilidade Fiscal – LRF, podendo assim propiciar mais retorno à sociedade na forma de bens e serviços públicos.

No próximo capítulo a estrutura da dissertação é apresentada.

1.6 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está estruturada em cinco capítulos. No primeiro capítulo, consta a introdução, onde se apresenta a contextualização, o problema de pesquisa, os objetivos, a delimitação do tema, a justificativa e os estudos relacionados.

O segundo capítulo é destinado a revisão da literatura, no qual foram tratados aspectos teóricos relacionados com o tema de pesquisa. Inicialmente aborda-se a Gestão de riscos em TI, para tanto, reflexões quanto a governança corporativa Governança de TI, e o modelo COBIT se tornam necessárias. Posteriormente a revisão da literatura concentra-se na gestão dos riscos corporativos, possível mediante a ISO 31000. Na parte final da revisão da literatura é realizada uma reflexão sobre a relação entre gestão de riscos de TI e a gestão dos riscos corporativos, com base na pesquisa teórica realizada.

No terceiro capítulo a metodologia da pesquisa é descrita detalhadamente. Compõem este capítulo: o delineamento da pesquisa, os critérios para seleção da unidade de estudo, plano de coleta e tratamento dos dados,o plano de análise dos dados, e as limitações do método.

o estudo de caso – SLC Agrícola S.A. é o quarto capítulo, neste a análise de dados coletados na fase de campo é descrita, foram demonstrados os resultados obtidos, e as análises do caso estudado; e no quinto capítulo se apresentam a conclusão do estudo e a sugestão para trabalhos futuros, seguido de referências, apêndices e anexos.

2 REVISÃO DA LITERATURA

Neste capítulo será explanado sobre a gestão de riscos em tecnologia da informação (TI) e a gestão dos riscos corporativos. Neste prisma, cabe primeiramente o entendimento do conceito de risco, que segundo a AS / NZS 4360 (1999) é a probabilidade de acontecer algo que vai ter um impacto sobre os objetivos predefinidos, sendo este medido em termos de consequências e de verossimilhança. Já para Aven (2011) significa a incerteza sobre a gravidade das consequências de uma atividade. Conforme a ISO 31000 (2009) o efeito que a incerteza tem sobre os objetivos da organização é chamado de risco.

Enquanto o Risco de Tecnologia da Informação está vinculado aos sistemas computacionais, e a infraestrutura tecnológica da corporação, os riscos corporativos são ameaças relacionadas aos processos de negócio, voltadas a aspectos estratégicos, financeiros e operacionais.

2.1 GESTÃO DE RISCOS EM TECNOLOGIA DA INFORMAÇÃO (TI)

Com o passar dos anos, a abertura das fronteiras e a tecnologia cada vez mais presente no cenário dos negócios, ampliaram a necessidade de informações precisas e a tempo real. Neste sentido, gerenciar os recursos tecnológicos e as informações de forma eficiente passou a ser fator de geração de resultados.

A grande utilização pelas empresas da TI oferece grandes oportunidades no aproveitamento dos benefícios oferecidos por este uso (ALBERTIN e ALBERTIN, 2012). Neste sentido, a TI precisa estar próxima da gestão dos negócios e sua governança mediante a GTI. Isso porque ela é parte integrante da governança corporativa e explora as melhores práticas de TI, focando no apoio à tomada de decisão. Para um melhor entendimento da GTI, cabe inicialmente discorrer primeiramente sobre o tema Governança Corporativa (GC).

A GC pode ser entendida como o sistema mediante o qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas, Conselho de administração, Diretoria, Auditoria Independente e Conselho Fiscal, IBGC (2009). A necessidade do aprimoramento dos mecanismos de Governança Corporativa emergiu devido à separação entre propriedade e controle.

Dentro deste contexto, os acionistas, afastados do controle, deveriam de alguma forma assegurar que o interesse dos administradores estivesse alinhado com os seus interesses (JUNIOR, JUNQUEIRA e BERTUCCI, 2010). Desta forma, a preocupação com a governança corporativa está associada à criação de mecanismos de controle e monitoramento, para assegurar que as decisões dos executivos estejam alinhadas com as dos acionistas.

A adoção dos mecanismos da governança corporativa incorre na adequação das companhias aos seus conceitos, o que repercute na forma que conduzem sua gestão, já que envolve a criação de mecanismos de controle. As discussões quanto ao tema governança da tecnologia da informação (GTI) se utilizam de outros dois temas, a governança corporativa e do planejamento estratégico de TI, ambos tem como foco as estratégias da organização (WEBB, POLLARD e RIDLEY, 2006).

O *link* estabelecido entre TI e negócio gera resultado a partir do momento em que os objetivos da GTI vão sendo alcançados. Para que isso seja possível, as organizações estão exigindo que seus departamentos de TI estejam cada vez mais estruturados de modo a serem flexíveis, eficientes, padronizados e com elevada qualidade nos produtos e no nível de serviço, além de estarem constantemente buscando por redução de custos e tempo (LUCIANO e TESTA, 2011).

A necessidade da avaliação do valor de TI e da gestão dos riscos relacionados a TI, sejam relacionados a infraestrutura ou a sistemas, e as crescentes necessidades de controle sobre as informações são agora entendidos como elementos-chave da governança corporativa. Valor, risco e controle constituem a essência da governança de TI (ITGI, 2007).

Neste 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.

Segundo Albertin e Albertin (2012), a GTI pode ser entendida como a autoridade e responsabilidade pelas decisões referentes ao uso de TI. Já para Weill e Ross (2006), a GTI é um processo pelo qual as empresas alinham TI com suas ações, desempenho, metas e as atribuem responsabilidade, mantendo o foco em atingir os objetivos da empresa alinhando-os com os de TI e com o planejamento empresarial.

Os mesmos autores afirmam ainda que as decisões de TI estão inter-relacionadas a alguns arranjos, entre eles, os principais foram: princípios de TI; arquitetura de TI; infraestrutura de TI; necessidade de aplicações de negócio; investimentos e priorização de TI. Desta forma, quando estabelecidos estes inter-relacionamentos, as decisões de TI buscam ser definidas do encontro ao objetivo do negócio.

O ITGI (2007) descreve as áreas de foco na Governança de TI, à saber: alinhamento estratégico, entrega de valor, gestão de recursos, gestão de riscos, e mensuração de desempenho, no Quadro 5 é possível identificar qual a relação de cada área de foco com a GTI.

Quadro 5: Áreas de foco na GTI

ÀREA DE FOCO DA GTI	RELAÇÃO DA ÁREA COM A GTI
Alinhamento estratégico	Foco em garantir a ligação entre os planos de negócio de TI, definindo mantendo e avaliando a proposta de valor de TI.
Entrega de valor	È a execução da proposta de valor de TI mediante o ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização concentrando-se em otimizar custos.
Gestão de recursos	Melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas.
Gestão de risco	Preocupação com os riscos, requerimento de conformidades, transparência sobre os riscos significantes para a organização e a inserção do gerenciamento dos riscos nas atividades da companhia.
Mensuração do desempenho	Acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos, e entrega dos serviços.

Fonte: Adaptado de ITGI (2007, P.8)

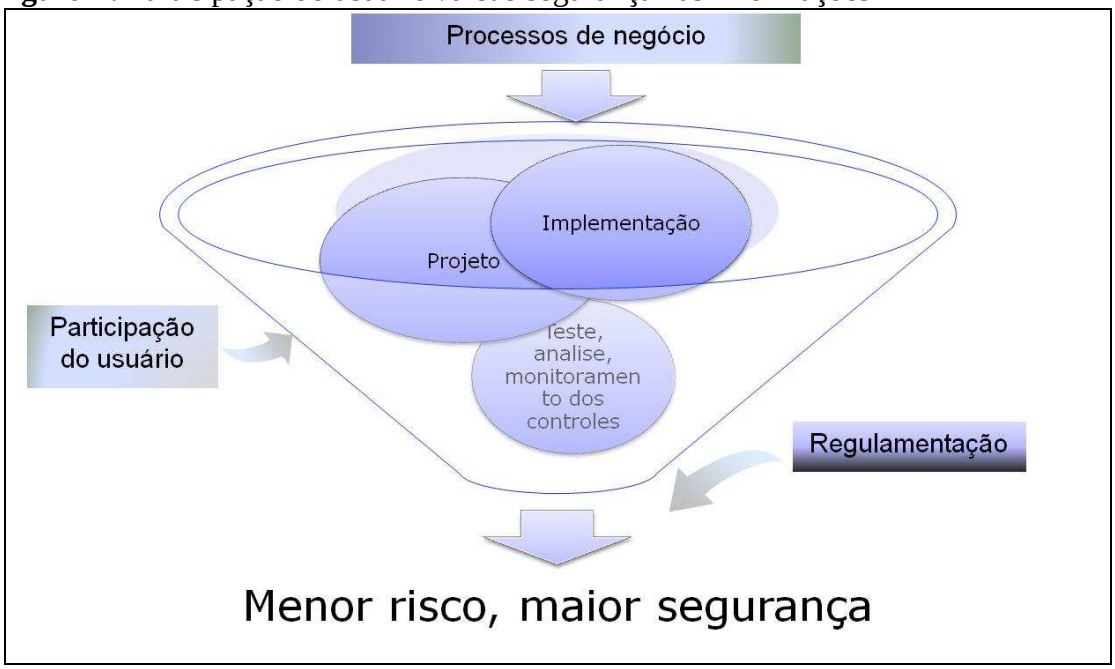
Estas áreas de foco em GTI descrevem os tópicos que os executivos precisam atentar para direcionar a área de TI dentro das organizações (ITGI, 2007). Para Albertin e Albertin (2012, p.128), “os executivos de negócio devem ter uma atitude em relação à TI adequada ao que se espera desta tecnologia, de forma crítica e realista, permitindo que suas inovações sejam aproveitadas.”

O alinhamento estratégico dos negócios e da TI deve, portanto, ser utilizado como ferramenta de gestão, focando nas atividades que a gerência deve executar para atingir coesão entre os esforços desenvolvidos pela área de TI e pelas áreas funcionais e de negócio (TAROUCO e GRAEML, 2011). Este alinhamento deve ocorrer de forma a evitar os riscos gerados tanto no ambiente de TI quanto nos demais ambientes de negócio.

Cabe salientar que, as organizações precisam investir um alto volume de recursos em TI, sendo estes investimentos justificados pela necessidade de se fornecer informações corretas e precisas em tempo adequado (COHAN, 2005; LUCHT, HOPPEN e MAÇADA, 2007). Estes investimentos precisam ser suficientes para garantir que potenciais riscos não afetem o sistema operacional e os controles, visando evitar erros e falhas.

O envolvimento dos usuários nestes investimentos e na identificação da real necessidade destes investimentos podem gerar bons resultados. 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 têm sido positivos nas organizações, gerando satisfação e comprometimento. A Figura 1 ilustra esta participação.

Figura 1: Participação do usuário *versus* segurança nas informações



Fonte: Adaptado de Spears e Barki (2010).

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. É mediante a GTI, por meio de seus processos e mecanismos, que se alcança uma maior transparência e segurança nas informações. Sendo que 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 a realização de planos de segurança, que buscam contemplar os processos de toda a organização.

Conforme Bulgurcu, Cavusoglu e Benbasat (2010), 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, já citados no tema teoria da agência.

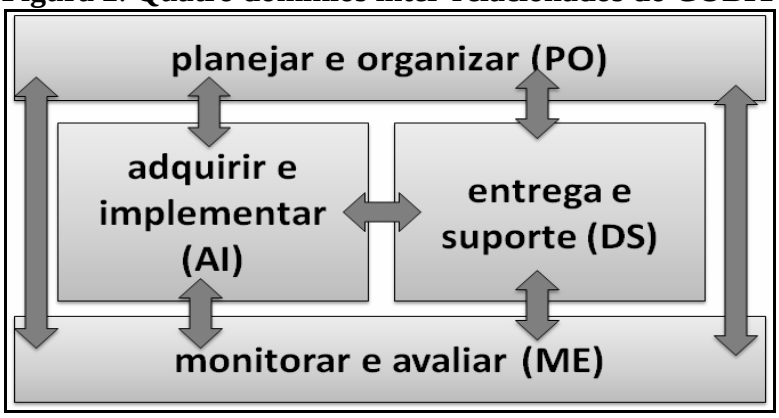
Tarouco e Graeml (2011, p.10) afirmam que, nas últimas décadas, surgiram diversos modelos de melhores práticas para TI que buscam em geral, garantir que as ações de TI estejam alinhadas com as estratégias, contribuindo para os objetivos dos investidores.

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, 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 é um *framework* modelo de melhores práticas de governança de TI (TUGAS, 2010). Já para Luciano e Testa (2010), os objetivos de controle do COBIT procuram atestar como cada processo faz uso dos recursos de TI para atender de forma primária ou secundária cada requisito do negócio em termos de informação, cobrindo todos os aspectos. Estes autores, ainda destacam que o COBIT independe da plataforma de TI adotada pela organização, uma vez que seu uso é voltado para o negócio.

O COBIT define atividades de TI em um modelo de processos genéricos, que possui quatro domínios e trinta e quatro processos genéricos de controle. O ITGI (2007) relaciona os domínios de TI e sua interligação, sendo eles identificados na Figura 2:

Figura 2: **Quatro domínios inter-relacionados do COBIT**



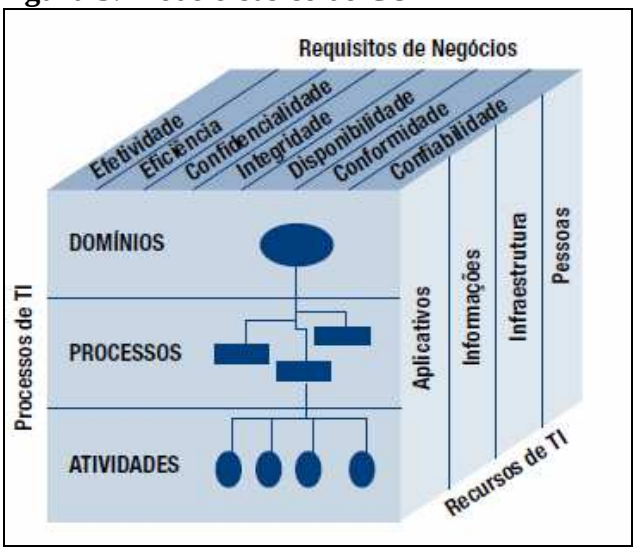
Fonte: ITGI (2007, P.14)

Sendo que os domínios identificados na Figura 2 foram descritos por Tugas (2010), como: 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, foram identificados trinta e quatro processos de TI, nos quais as ligações são realizadas. A visão dos domínios se dá em três dimensões, a saber: processo de TI, os Recursos de TI, e os requisitos de negócio.

Os recursos de TI são gerenciados pelos processos de TI que respondem aos requisitos do negócio, sendo este o princípio básico do COBIT (ITGI, 2007), conforme é ilustrado na Figura 3.

Figura 3: Modelo básico do COBIT



Fonte: ITGI (2007, P.27)

Segundo o modelo básico do COBIT, os requisitos do negócio são**:**

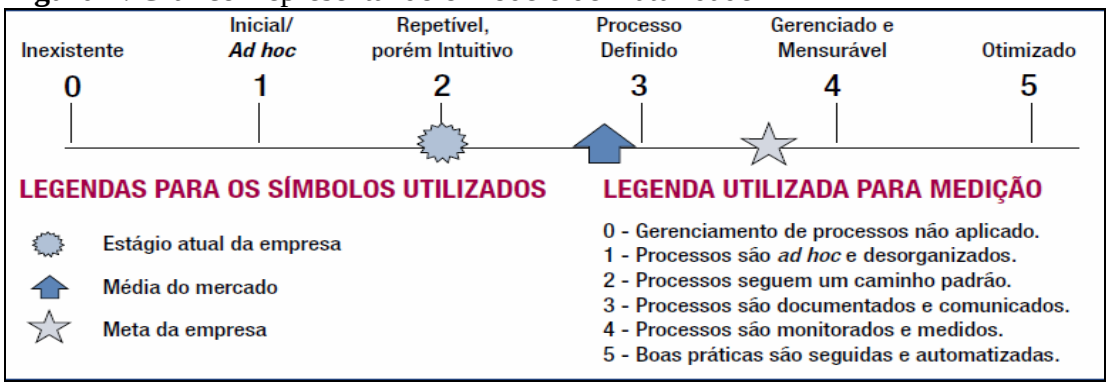
- **Efetividade**: trabalha com as informações relevantes e pertinentes para o processo de negócio bem como a sua entrega de forma correta e em tempo;
- **Eficiência**: entrega da informação com o melhor uso possível dos recursos;
- **Confidencialidade:** proteção da informação a fim de que não haja mau uso das mesmas;
- **Integridade:** fidedignidade, validade da informação de acordo com os valores de negócios e expectativas;
- **Disponibilidade**: informações disponíveis para o negócio quando requeridas, ligada a salvaguarda dos recursos necessários e capacidades associadas;

- **Conformidade:** cumprimento das Leis, contratos e regulamentações; e confiabilidade: entrega de informações apropriadas aos gestores para tomada de decisão.
- **Confiabilidade:** entrega da informação apropriada aos executivos para administrar a entidade e exercer suas responsabilidades fiduciárias e de governança.

O COBIT descreve um modelo de maturidade denominado CMM *(Capability Maturity Model)*, sendo que o COBIT 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.

Para esta avaliação o modelo de maturidade apresenta alguns níveis de classificação, apresentados na Figura 4.

Figura 4: Gráfico Representando o modelo de maturidade



Fonte: ITGI (2007, P.20)

Neste modelo de avaliação da maturidade existem seis níveis, que variam de 0 (inexistente) até 5 (Otimizando). Além dos níveis de maturidade, a Figura 4 contempla uma legenda, que descreve um a um os níveis utilizados para medição segundo o CMM. Para Rafeq (2010) a medição dos níveis de maturidade é necessária para identificar *gaps* em processos específicos, avaliar o estado atual do uso da TI na empresa e desenvolver planos de ação para alcançar os níveis desejados.

Melhorar a maturidade reduz riscos e aprimora a eficiência, levando a uma menor quantidade de erros, processos mais previsíveis e uso eficiente dos recursos sob o ponto de vista de custos (ITGI , 2007). Para a gestão de riscos em TI o COBIT incorpora dentro de seu primeiro domínio (planejar e organizar) o processo P09 - Avaliar e gerenciar os riscos de TI.

O P09 do COBIT é 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.

Sugere ainda que estratégias de mitigação de risco devem 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).

No Quadro 6 é possível identificar os objetivos de controle e boas práticas para que este controle seja alcançado.

Quadro 6: Boas práticas para a gestão de riscos em TI

OBJETIVO DE CONTROLE	BOAS PRÁTICAS PARA O CONTROLE
Que satisfaça aos requisitos do negócio para a TI	Analisar e comunicar os riscos de TI e seus possíveis impactos nos processos e objetivos de negócio
Com foco em	Desenvolver uma estrutura de gerenciamento de risco integrada às estruturas corporativa e operacional de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual
É alcançado por	Garantia de que o gerenciamento de risco esteja completamente integrado aos processos gerenciais, interna e externamente, e seja aplicado de forma consistente; Realização de avaliações de risco; Recomendação e comunicação de planos de ação de remediação dos riscos.
É medido por	Percentual de objetivos críticos de TI cobertos pela avaliação de risco; Percentual de riscos críticos de TI identificados que tenham planos de ação desenvolvidos; Percentual dos planos de ação de gestão de risco aprovados para implementação

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

Cabe destacar que para este processo do COBIT 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 gerenciamento dos riscos de TI, objetivos de controle foram detalhados no P09 do COBIT, sendo eles segundo o ITGI (2007, p.66):

- **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.

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:

Quadro 7: Graus de maturidade segundo o P09 do Cobit

GRAU DE MATURIDADE	DESCRIÇÃO
0 – Inexistente	Quando não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.
1 – Inicial	Os riscos de TI são considerados de forma inicial. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes. Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.
2 – Repetitivo, mas intuitivo	Quando Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.
3 – Definido	Quando Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.
4 – Gerenciado	Quando a avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os cenários de riscos relacionados a TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, e o comitê executivo e a Diretoria de TI

GRAU DE MATURIDADE	DESCRIÇÃO
	estabeleceram os níveis de risco que a organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.
5 – Otimizado	Quando O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A Direção de TI avalia continuamente as estratégias de mitigação de risco.

Fonte: Adaptado de ITGI (2007, p.68)

No Quadro 7 é possível identificar os níveis de maturidade para avaliação da gestão de riscos de TI segundo o COBIT. Sendo o ponto 5-Otimizado o grau mais elevado onde boas práticas para este gerenciamento foram aplicadas em toda a organização.

Depois de abordado sobre o tema Riscos de TI, os principais aspectos encontrado na literatura foram categorizados no Quadro 8, afim de subsidiar o entendimento sobre o tema e dar suporte a análise dos dados.

Quadro 8: Categorização das temáticas da Gestão de Riscos em TI

CATEGORIA	AUTORES
Planejamento estratégico de TI – Planejar e organizar	Webb, Pollard e Ridley (2006) - ITGI (2007) - Simonson, Johnson e Ekstedt (2010) - Tarouco e Graeml (2011) – Tugas (2010)
Requisitos de negócio (efetividade, eficiência, confidencialidade, Integridade, disponibilidade, conformidade, confiabilidade) primários para a gestão de riscos em TI	ITGI (2007)
Investimentos e Recursos de TI – Adquirir e implementar	Cohan (2005) - Lucht, Hoppen e Maçada (2007)- ITGI (2007)
Segurança nas informações - Uso de TI – Usuários	ITGI (2007) - Albertin e Pinochet (2010) - Albertin e Albertin (2012) - Simonson, Johnson e Ekstedt (2010) - Bulgurcu, Cavusoglu e Benbasat (2010) - Spears e Barki (2010)
Processos de TI – Entrega e suporte	ITGI (2007)
Boas Práticas para Gestão Riscos em TI	ITGI (2007)
Processos de controle para a gestão dos riscos de TI (estabelecimento do contexto, identificação, avaliação, resposta, manutenção e monitoramento)	ITGI (2007)

Monitoramento da gestão de TI	ITGI (2007)

Fonte: Elaborado pela autora.

Na próxima seção aborda-se a gestão de riscos corporativos como ferramenta de apoio a gestão da organização, possibilitando boas práticas para redução destes riscos no contexto empresarial.

2.2 GESTÃO DOS RISCOS CORPORATIVOS

As organizações operam na busca de seus objetivos, neste caminho elas precisam estabelecer um sistema para a gestão de seus riscos, já que os riscos podem afetar negativamente ou positivamente esta caminhada.

GERIGK e CORBARI (2011) destacam que diversos fatores pressionam os gestores a tomarem decisões cada vez mais rápidas sobre assuntos cada vez mais complexos, fazendo com que os riscos assumidos sejam significativamente mais desafiadores e com consequências extremamente drásticas caso a decisão tomada tenha sido errada. Diferentes percepções sobre a importância da gestão de riscos para as organizações podem ser encontradas na literatura.

Quadro 9: Percepções quanto à gestão de riscos

AUTOR	PERCEPÇÃO SOBRE A GESTÃO DE RISCOS
COSO (2007)	Possibilita a redução da perda de recursos pelas organizações já que contribui para assegurar comunicação eficaz e o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas consequências.
ISO 31000 (2009)	Auxilia aos tomadores de decisão a fazerem escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação, levando em consideração a incerteza, a natureza desta incerteza, e como ela pode ser tratada.
AVEN (2011)	Fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro.
GERIGK e CORBARI (2011)	Procura identificar os eventos que possam ter consequências operacionais, financeiras e estratégicas adversas e, então, encontrar salvaguardas para prevenir ou minimizar o perigo causado por tais eventos.

Fonte: Elaborado pela autora.

No Quadro 9 é destacada a percepção de alguns autores quanto à gestão de riscos, para estes ela fornece benefícios às organizações já que busca prevenir eventuais perdas que podem ocorrer. Para Frigo e Anderson (2011), a avaliação estratégica do risco pode complementar e alavancar a execução de processos em uma organização, ocasionando a melhoria da governança. Esta avaliação estratégica dos riscos permite o fortalecimento de mecanismos de controle.

Segundo o COSO (2007) a gestão dos riscos corporativos tem por finalidade:

- **Alinhar o impulso ao risco com a estratégia adotada** – os administradores avaliam o impulso ao risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos.
- **Fortalecer as decisões em resposta aos riscos** – o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos – como evitar, reduzir, compartilhar e aceitar os riscos.
- **Reduzir as surpresas e prejuízos operacionais** – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados.
- **Identificar e administrar riscos múltiplos e entre empreendimentos** – toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos.
- **Aproveitar oportunidades** – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa.

- **Otimizar o capital** – a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

As finalidades da gestão dos riscos corporativos evidenciam vantagens para a organização, como por exemplo reduzir as surpresas e prejuízos operacionais. Para alcance desta finalidade eventos potenciais precisam ser identificados, isto pode ocorrer mediante categorização dos tipos de riscos.

Categorizar os riscos segundo sua natureza permite sua agregação de uma forma organizada. Quanto à natureza os riscos podem ser classificados em: estratégicos, financeiros e operacionais (IBGC, 2007).

Os riscos estratégicos estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico das organizações, IBGC (2007). Cabe destacar sua relação com os fatores externos a organização. Os tipos de riscos estratégicos mais comuns foram ilustrados no Quadro 10.

Quadro 10: Tipos de Riscos Estratégicos

RISCOS ESTRATÉGICOS		
TIPO DE RISCO	***DESCRIÇÃO***	***AUTOR***
Econômicos	Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.	COSO (2007)
Políticos	Eleição de agentes do governo com novas agendas políticas, novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.	COSO (2007)
Ambiental	Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.	IBGC (2007); FENKER (2009);
Risco de Marca, de imagem ou reputação	É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e consequentemente, a consecução de transações com estes clientes.	BRITO (2003)
Sociais	São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.	COSO (2007)
Tecnológicos	São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infraestrutura e aumento da demanda de serviços com base em tecnologia.	COSO (2007)

Fonte: Elaborado pela autora.

Os riscos financeiros foram àqueles associados à exposição das operações financeiras da organização, IBGC (2007). Os tipos de riscos financeiros mais comuns, são demonstrados no Quadro 11.

Quadro 11: Tipos de Riscos Financeiros

RISCOS FINANCEIROS		
RISCOS	***DESCRIÇÃO***	***AUTOR***
Mercado	A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).	BCB (2000)
Crédito	É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação	MARSHALL (2002); BCB (2000)
Liquidez	Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.	BCB (2000)

Fonte: Elaborado pela autora.

Os riscos operacionais geralmente acarretam na redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais, IBGC (2007). Os tipos de riscos operacionais mais comuns, são demonstrados no Quadro 12.

Quadro 12: Tipos de Riscos Operacionais

RISCOS OPERACIONAIS		
RISCOS	***DESCRIÇÃO***	***AUTOR***
Pessoal	Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.	MARSHALL (2002), COSO (2007)
Processos	Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.	COSO (2007)
Tecnologia	Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).	IBGC (2007)

RISCOS OPERACIONAIS		
RISCOS	***DESCRIÇÃO***	***AUTOR***
Riscos de *compliance*	Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.	IBGC (2007)

Fonte: Elaborado pela autora.

É válido destacar que mesmo havendo tipos de riscos diferenciados, cabe às organizações que realizem uma gestão integrada destes riscos. Segundo o COSO (2007) um evento pode desencadear o outro, ou ainda vários eventos podem ocorrer concomitantemente.

Coimbra (2011, p.38) cita alguns exemplos da inter-relação entre os tipos de riscos: "... uma mudança na taxa de juros afeta as taxas de câmbio; a decisão de reduzir o investimento em capital pode postergar um aperfeiçoamento dos sistemas de gestão de distribuição e ocasionar um tempo de paralisação adicional e uma elevação dos custos operacionais."

Diversos tipos de riscos podem ser identificados nas organizações, porém identificar este não é tarefa suficiente, torna-se preciso construir uma estrutura para seu gerenciamento. Para tanto, diferentes padrões e modelos têm sido desenvolvidos para identificar, avaliar e gerenciar eficazmente os riscos, entre eles a norma Australiana **AS/ NZS 4360** e a norma **ISO 31000**.

A estrutura e padrões apresentados por estas duas normas apresentam grande semelhança (AVEN, 2011). A ISO 31000, tema destaque na próxima subseção trata de princípios e diretrizes genéricas para que a gestão eficaz dos riscos possa ocorrer.

A ISO 31000 surgiu com a intenção de harmonizar padrões, regulamentações e frameworks que a antecederam e que estão relacionados à gestão de riscos. Prevê os princípios e as diretrizes genéricas para a gestão dos riscos, não sendo destinada a uma certificação, mas sim, a diretrizes para que os processos das organizações estejam em harmonia com o gerenciamento de seus riscos.

Salienta-se que a aplicação da norma ISO 31000 (2009) deve ser considerada ao longo da vida útil da organização, podendo ser aplicada a qualquer tipo de riscos independente de sua natureza, ou consequência.

Os **Princípios para a gestão de riscos** estabelecidos pela ISO 31000 vislumbram uma gestão de riscos eficaz às empresas em todos os níveis. Os seguintes princípios, quanto à gestão de riscos são citados:

1) Cria e protege valor;

2) É parte integrante de todos os processos organizacionais;

3) É parte da tomada de decisão;

4) Aborda explicitamente a incerteza;

5) É sistemática, estruturada e oportuna;

6) Baseia-se nas melhores informações possíveis;

7) É realizada sob medida;

8) Considera fatores humanos e culturais;

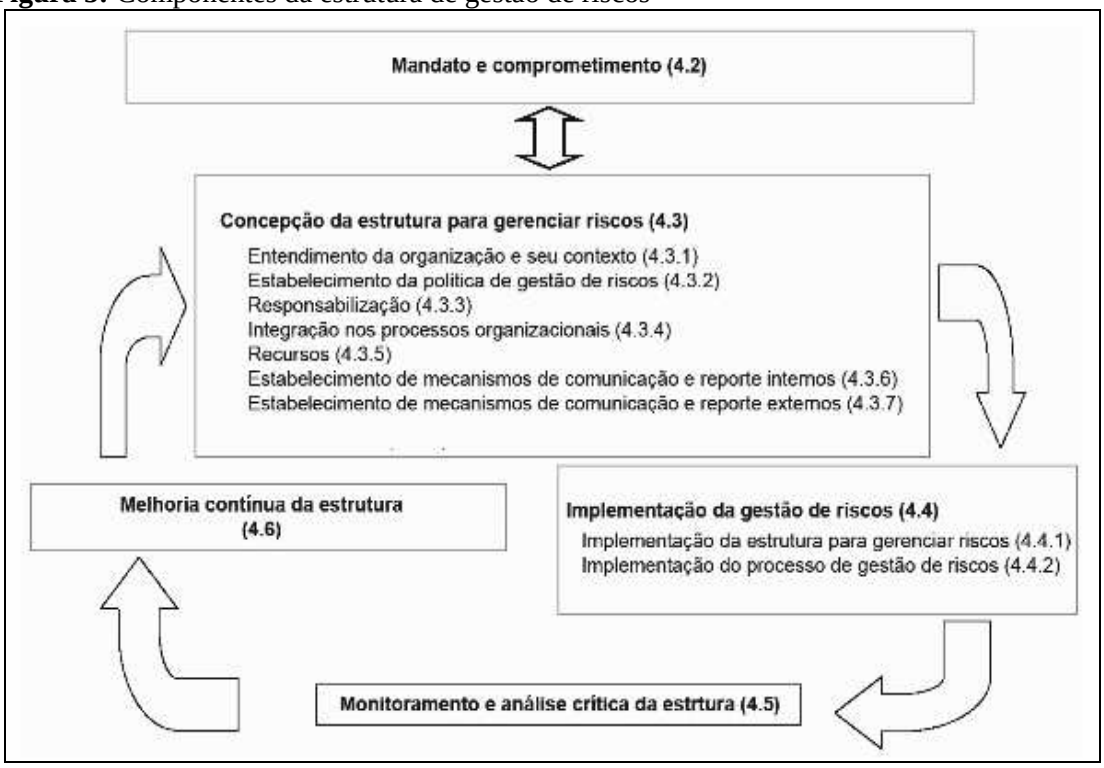
9) É transparente e inclusiva;

10) É dinâmica e interativa, capaz de reagir a mudanças; e

11) Facilita a melhoria contínua da organização.

Segundo a ISO 31000 (2009), o sucesso da gestão de riscos depende da eficácia e da estrutura de gestão que fornece os fundamentos e os arranjos que irão incorporá-la mediante toda organização e em todos os níveis. A norma descreve os componentes necessários de estrutura para gerenciar riscos e a forma como estes se inter-relacionam conforme expresso na Figura 5.

Figura 5: Componentes da estrutura de gestão de riscos



Fonte: ISO 31000 (2009, p.15)

Cabe salientar que a estrutura proposta pretende auxiliar na gestão de riscos, e é importante que cada organização busque adaptar os componentes da estrutura às suas necessidades. A estrutura para gestão de riscos demonstrada na Figura 5 é composta pelos seguintes componentes: Mandado e comprometimento, Concepção da estrutura para gerenciar riscos, Implementação da gestão de riscos, Monitoramento e análise crítica da estrutura, Melhoria contínua da estrutura.

Para melhor entendimento da estrutura da gestão de riscos, cada um dos componentes propostos pela ISO 31000:2009 é detalhado a seguir:

Mandado e comprometimento: busca garantir a contínua eficácia da gestão de riscos salientando a importância do comprometimento da administração das companhias, mediante planejamento rigoroso e estratégico em todos os níveis operacionais.

Concepção da estrutura para gerenciar riscos: para conceber a estrutura necessária ao gerenciamento dos riscos, é preciso uma compreensão do contexto (externo e interno) da organização, já que este pode afetar os riscos.

Convém a adoção de políticas de gestão de riscos afim de estabelecer claramente os objetivos, e o comprometimento de todos com a gestão destes riscos, atribuindo responsabilidades, autoridade e competências apropriadas para gerenciar os riscos.

A integração dos processos organizacionais prevê que a gestão de riscos seja incorporada em todas as práticas e processos organizacionais, tornando-se assim parte integrante destes. Torna-se assim em alguns momentos necessária a alocação de recursos apropriados à gestão de riscos.

Sugere-se que as organizações estabeleçam mecanismos de comunicação interna e externa, responsáveis pelos reportes inerentes à gestão de riscos.

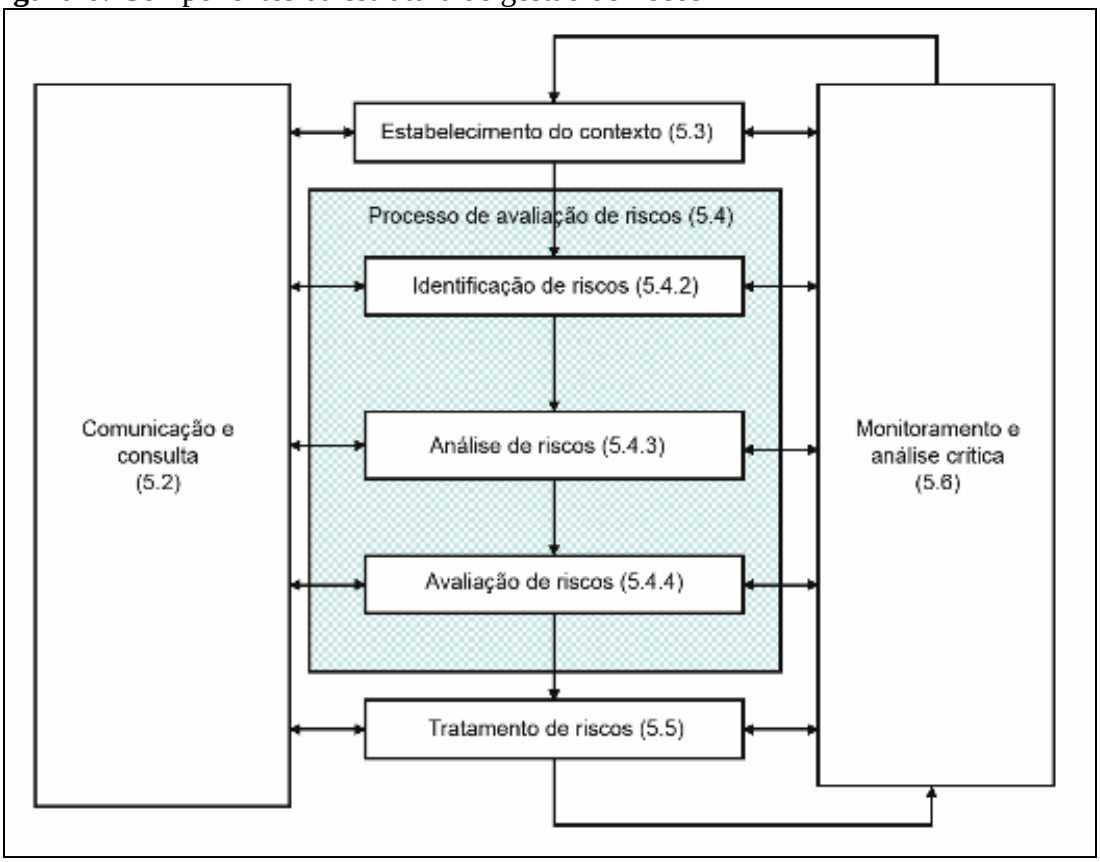
Implementação da gestão de riscos: Para a implementação, a estrutura e os processos devem ser aplicados em um plano envolvendo todos os níveis e funções da organização sendo parte integrante de suas práticas.

Monitoramento e análise crítica da estrutura: Esta etapa sugere que as empresas em relação à gestão de riscos: 1) meçam o desempenho mediante indicadores, analisados de forma periódica e crítica; 2) avaliem o progresso obtido e seus desvios; 3) avaliem periodicamente a política, o plano e a estrutura estabelecida; 4) análisem a eficácia da estrutura adotada.

Melhoria contínua da estrutura: decisões devem ser tomadas/avaliadas sobre como a política, o plano, e a estrutura da gestão de riscos podem ser melhorados continuamente.

Quanto aos processos para a gestão de riscos, a norma ISO 31000 (2009) estabelece que o processo para gestão de riscos deva ser considerado como parte integrante da gestão, incorporada na cultura e nas práticas, e adaptado aos processos de negócio organizacionais. Neste contexto, na Figura 6 podem ser observadas, as etapas deste processo e seus inter-relacionamentos:

Figura 6: Componentes da estrutura de gestão de riscos



Fonte: ISO 31000 (2009, p.20)

Os componentes ilustrados na Figura 6 foram descritos de forma detalhada a seguir, segundo a ISO 31000 (2009):

Comunicação e consulta: esta etapa trata que a comunicação e consulta às partes interessadas (internas e externas) devem ocorrer durante todas as fases da gestão de riscos. Para tanto, estabelece que planos de comunicação e consulta, sejam elaborados e que estes abordem questões relacionadas ao risco, suas causas, suas consequências e as medidas tomadas para tratá-los.

Esta relação com as partes interessadas se faz importante porque elas fazem julgamentos sobre os riscos, baseadas em suas percepções.

Estabelecimento do contexto: neste processo, foram articulados os objetivos e os parâmetros internos e externos que precisam ser levados em consideração. É estabelecido o escopo e os critérios de riscos com riqueza de detalhes, para que estes orientem as demais etapas do processo.

A norma divide o estabelecimento do contexto em externo e interno. O contexto externo é o ambiente externo no qual a organização busca atingir seus objetivos, já o contexto interno é o ambiente interno no qual ela busca seus objetivos, ISO 31000 (2009). Os fatores a serem considerado em cada contexto, podem ser observados no Quadro 13:

Quadro 13: Contexto interno e externo na gestão de riscos

CONTEXTO EXTERNO PODE INCLUIR	CONTEXTO INTERNO PODE INCLUIR
- Ambiente cultural, social, político, legal, regulamentador, financeiro, tecnológico, econômico, natural, e competitivo, quer seja internacional, nacional, regional ou local; - Os fatores- chave e as tendências que tenham impacto sobre os objetivos organizacionais; e - As relações com as partes interessadas externas e suas percepções e valores.	- à governança, estrutura organizacional, funções e responsabilidades; - às políticas, objetivos e estratégias implementadas para atingi-los; - às capacidades, entendidas em termos de recursos e conhecimentos; - aos sistemas de informações, fluxos de informações, e processo de tomada de decisão; - às relações com as partes interessadas internas, suas percepções e valores; - às normas, diretrizes e modelos adotados pela organização; e - a forma de extensão das relações contratuais.

Fonte: Adaptado de ISO 31000 (2009, p.22)

O contexto no qual as organizações estão inseridas varia de acordo com as suas necessidades e relações, podendo envolver diversos fatores, que iniciam com a definição dos objetivos da gestão de riscos e vão até a melhoria continua deste processo.

Cabe salientar que neste processo serão definidos os critérios de risco, e estes segundo a ISO 31000 (2009) devem considerar os seguintes aspectos:

a) A natureza, os tipos de causas e consequências, como serão medidas;

b) Como a probabilidade será definida;

c) A evolução do tempo da probabilidade ou consequência (s);

d) Como deve ser determinado o nível de riscos;

e) Os pontos de vistas das partes interessadas;

f) O nível em que o risco se torna aceitável ou tolerável; e

g) Se as combinações de múltiplos riscos sejam levadas em consideração.

Avaliação dos Riscos: o processo de avaliação dos riscos se preocupa com a identificação, análise e avaliação dos riscos.

Na etapa de ***identificação dos riscos*** as fontes de riscos, áreas de impacto, eventos, causas e consequências potenciais foram identificadas, com a finalidade de gerar uma lista abrangente de riscos com base nestes eventos.

Nesta etapa a ISO 31000:2009 sugere que a organização: a) Identifique e inclua todos os riscos estando suas fontes sob o controle ou não; b) aplique ferramentas e técnicas para identificação adequadas aos seus objetivos e capacidades, bem como aos riscos enfrentados; c) que ao processo sejam alocadas pessoas de conhecimento adequado.

Uma vez identificados os riscos necessitam ser analisados**.** É na ***etapa de análise*** dos riscos que desenvolve a compreensão dos riscos, além de fornecer uma entrada para a avaliação dos riscos, e para decisões quanto ao tratamento do risco, ISO 31000 (2009).

Nesta etapa ocorre: a) apreciação das causas e riscos e suas fontes de incerteza, consequências positivas ou negativas, e a probabilidade que estas consequências possam ocorrer; b) as causas, consequências, e a probabilidade de ocorrência do risco combinadas precisam refletir o nível dos riscos, os tipos de riscos, as informações disponíveis ; c) deve levar em consideração a existência de controles, e a compatibilidade com os critérios dos riscos; e d) devem considerar a confiança na determinação do nível de risco e sua sensibilidade.

Para Aven (2011, p.725) a probabilidade é uma medida para representar ou expressar incerteza, seguindo o regras de cálculo de probabilidade. Segundo o COSO (2005, p.54), “a probabilidade representa a possibilidade de que um determinado evento ocorrerá, enquanto o impacto representa o seu efeito”.

Na Figura 7, a relação entre impacto e probabilidade é demonstrada de forma gráfica, denominada matriz para análise do risco.

Figura 7: Matriz para análise de riscos.

	PROBABILIDADE

		IMPROVÁVEL	BAIXA	MÉDIA	ALTA	MUITO ALTA
	MUITO ALTO	RA	RA	RMA	RMA	RMA
	ALTO	RM	RM	RA	RMA	RMA
	MÉDIO	RB	RM	RM	RA	RA
	BAIXO	RMB	RB	RB	RM	RM
	NULO	RMB	RMB	RMB	RMB	RMB
Legenda: RMA= Risco Muito Alto; RA = Risco Alto; RM= Risco Médio; RB= Risco Baixo; RMB= Risco Muito Baixo						

Fonte: Adaptado de COSO (2005); Dantas *et.al* (2010).

Segundo a AS/NZS 4360 (1999) as consequências e probabilidade foram combinadas para produzir um nível de risco, sendo que estas podem ser determinadas por meio de análise estatística e cálculos. A mesma norma ainda destaca que alternativamente, quando não há dados anteriores, as estimativas podem ser realizadas de forma subjetiva, refletindo o grau de convicção de um indivíduo ou grupo. Para evitar o viés subjetivo ao analisar conseqüências e probabilidade, deve ser utilizado as melhores técnicas e fontes de informação disponíveis.

Neste sentido a AS/NZS 4360 (1999) menciona que as fontes de informações podem incluir: a) registros anteriores; b) experiência comprovada; c) Prática e experiência na indústria; d) literatura pertinente; e) marketing e pesquisa de mercado; f) os experimentos e protótipos; g) os modelos econômicos de engenharia, ou outra; h) as opiniões e julgamentos de especialistas e peritos.

Quanto à **avaliação dos riscos** a ISO 31000 (2009) estabelece sua finalidade como sendo de auxiliar na tomada de decisão com base nos resultados na análise de riscos, sobre as quais riscos precisam de tratamento e prioridade para a implementação deste.

Conforme, Vanti, Ortega e Blanco (2011) a avaliação de riscos é um dos principais temas atuais nas organizações e o mesmo necessita ser avaliado contemplando a subjetividade dos itens avaliados, bem como considerar determinada incerteza na relação entre os mesmos itens avaliados, para assim realizar efetivo alinhamento estratégico.

As decisões quanto à avaliação dos riscos devem levar em consideração o contexto mais amplo, e levem em considerações os requisitos legais ou regulamentares.

Tratamento dos Riscos: envolve o processo de seleção das opções que modificarão os riscos, e a implementação destas, já que uma vez implementado o tratamento fornece novos controles ou modifica os já existentes, ISO 31000 (2009).

Segundo a ISO 31000 (2009), o tratamento dos riscos se dá mediante um processo cíclico composto por: 1) a avaliação do tratamento dos riscos já realizados; 2) a decisão se os níveis de risco residuais são toleráveis; 3) caso não sejam toleráveis, deve ser implantado novo tratamento; 4) a avaliação da eficácia dos tratamentos.

Estas opções elas buscam soluções para que os riscos sejam minimizados ou excluídos.

Monitoramento e análise crítica dos Riscos: Nesta etapa os riscos são vigiados regularmente, mediante ações pré-definidas no escopo da gestão de riscos.

Conforme a ISO 31000 (2009), os progressos na implantação dos planos de tratamento dos riscos proporcionam uma medida de desempenho, que pode ser incorporada na gestão, na mensuração e na apresentação das informações.

Depois de abordado sobre o tema Riscos Corporativo, os principais aspectos encontrados na literatura foram categorizados no Quadro 14, afim de subsidiar o entendimento sobre o tema e dar suporte a análise dos dados.

Quadro 14: Categorização das temáticas da Gestão de Riscos Corporativos

Categoria	Autores
Avaliação estratégica do risco – Aproveitar oportunidades	IBGC (2007) – COSO (2007) - ISO 31000 (2009) - Frigo e Anderson (2011)
Perda de Recursos (custos ou prejuízos associados) – Danos – Consequências negativas	IBGC (2007) – COSO (2007) - ISO 31000 (2009) - Aven (2011) – Gerigk e Corbari (2011)
Identificação dos eventos e categorização dos riscos (estratégicos, financeiros e operacionais)	IBGC (2007) – COSO (2007) - ISO 31000 (2009)
Inter-relação entre os tipos de riscos	ISO 31000 (2009) – Coimbra (2011)
Princípios para a gestão de riscos	ISO 31000 (2009)
Estrutura para gerenciamento dos riscos (concepção, implementação, monitoramento e melhoria contínua) - mandado e comprometimento	IBGC (2007) – COSO (2007) - ISO 31000 (2009) – Aven (2011)
Processos para a gestão de riscos (estabelecimento do contexto, identificação dos riscos, análise dos riscos, avaliação dos riscos e tratamento dos riscos)	ISO 31000 (2009)
Conscientização e Resposta ao risco (evitar, reduzir, compartilhar e aceitar riscos)	COSO (2007) - Bulgurcu, Cavusoglu e Benbasat (2010) -

Fonte: Elaborado pela autora

Na seção seguinte é realizada uma comparação entre a gestão de riscos de TI e gestão de riscos corporativos, com base no que foi encontrado na literatura.

2.3 GESTÃO DE RISCOS EM TI *versus* GESTÃO DOS RISCOS CORPORATIVOS

O processo de gestão de riscos atua nas organizações com o objetivo de reduzir custos ou maximizar oportunidades com eventos não previstos. Enquanto a gestão de riscos corporativos procura instituir práticas para todos os riscos inerentes à governança das corporações, a gestão de riscos em TI busca proporcionar um ambiente de segurança, propiciando controle sobre as informações e processos de TI.

Os riscos para o negócio podem ser potencialmente impactados pela segurança das informações produzidas em um ambiente de TI vulnerável a riscos. Dependendo do valor que TI tem para o negócio a segurança das informações precisa ser alcançada de maneira mais eficiente (ITGI, 2007). A tecnologia da Informação, como provedora de serviços participa cada vez mais nos processos organizacionais, com uma atuação que pode variar, em termos de complexidade, desde o suporte até a habilitação, podendo até contribuir para o redesenho dos processos de negócio, (WEILL e ROSS, 2006; SANTANA e VERAS, 2011).

Sob o prisma destas reflexões, cabe destacar que a atuação da TI como responsável pela estrutura tecnológica e os sistemas operacionais necessita atuar de forma a responder às perspectivas do negócio, esta atuação visa garantir que requisitos de negócio como: confidencialidade, integridade e disponibilidade das informações, sejam alcançados.

Esta interação entre as perspectivas de negócios e os riscos relacionados a sistemas ou infraestrutura de TI, vislumbra da mesma forma a proteção da companhia dos riscos corporativos, principalmente aqueles dos tipos estratégico tecnológico e operacionais de tecnologia. Spears e Barki (2010) justificam a participação dos usuários na gestão de riscos de segurança dos sistemas de informações mediante o alinhamento dos controles de segurança com os objetivos do negócio. Os autores ainda destacam a compreensão do valor da informação e da participação do usuário no negócio como parte do desenvolvimento das estratégias voltadas para a segurança da informação.

Outro aspecto sobre a relação objetivada neste estudo é a governança corporativa, fruto do processo de maior transparência nas organizações, que com suas regras impõem um modelo de gestão ligado principalmente a bons controles internos, a qualidade das informações transmitida aos investidores, obrigando de certa forma aos administradores a um alto padrão quanto às suas gestões empresariais, (SILVEIRA, DUCA e MARIO, 2010).

A adoção de melhores controles internos proporciona um ambiente cada vez mais seguro. Isto é possível mediante o estabelecimento de sistemas ou processos de controles voltados ao monitoramento dos diversos riscos inerentes as atividades. Em uma estrutura de gestão focada na melhoria dos processos e em sua governança corporativa foram os conselheiros que decidem sobre os melhores rumos a serem tomados.

Neste sentido o IBGC (2009) destaca que a o Conselho de Administração deve assegurar-se de que a Diretoria identifique preventivamente (por meio de sistema de informações adequado) e liste os principais riscos aos quais a sociedade está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização. Esta recomendação permite perceber a contemplação dos sistemas de informações a gestão de riscos inerentes ao negócio, mediante atuação do conselho de administração. A interação destes sistemas sua integridade e confianças nas informações por eles produzidas podem possibilitar a redução de erros e falhas, sendo possível assim à redução de riscos corporativos e riscos de TI.

Outro aspecto recomendado pelo IBGC (2009) é a criação de comitês para atendimento dos interesses dos conselheiros. Neste sentido a adoção de um comitê para a gestão de riscos que contemple uma visão integrada sobre os diversos tipos oriundos dos processos organizacionais é recomendada.

A melhoria dos processos, a adoção de sistemas íntegros, e a busca pela melhoria da governança, exigem padrões para a mitigação dos riscos. Sob este aspecto, destaca-se a norma ISO 31000 (2009) como sendo uma norma genérica para construção de uma estrutura de gestão dos riscos corporativos e o COBIT como modelo de melhores práticas de gerenciamento de riscos de TI. Da análise destes dois instrumentos de gerenciamento é possível traçar uma comparação entre tais modelos com diferentes finalidades. A comparação entre estas duas ferramentas pode ser observada no Quadro 15.

Quadro 15: Comparação entre o COBIT e a ISO 31000

ETAPA	COBIT 4.1 (Riscos de TI)	ISO 31000 (Riscos Corporativos)
Princípios para gestão de riscos	Não deixa claros os princípios para a gestão de riscos.	Estabelece onze princípios para a gestão de riscos eficaz as empresas em todos os níveis
Estabelecimento do contexto	(PO9.2) definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos foram avaliados.	Estabelecimento do contexto em externo e interno. A norma apresenta os fatores que podem ser considerados em cada contexto.
Comunicação e Consulta	Não trata especificamente deste ponto	Trata que a comunicação e consulta às partes interessadas (internas e externas) devem ocorrer durante todas as fases da gestão de riscos.
Identificação dos eventos	(PO9.3): Identificar eventos (importante ameaça real que explora significativas vulnerabilidades) com potencial impacto negativo nos objetivos ou nas operações da organização. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.	Nesta etapa as fontes de riscos, áreas de impacto, eventos, causas e consequências potenciais foram identificadas, com a finalidade de gerar uma lista abrangente de riscos com base nestes eventos.
Análise do risco	Ocorre no P09 – etapa de identificação dos riscos	Desenvolve a compreensão dos riscos, além de fornecer uma entrada para a avaliação dos riscos, e para decisões quanto ao tratamento do risco
Avaliação do 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.	A finalidade desta etapa é de auxiliar na tomada de decisão com base nos resultados na análise de riscos, sobre as quais riscos precisam de tratamento e prioridade para a implementação deste.
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.	Esta etapa é chamada de Tratamento do risco e identificada como o processo de seleção das opções que modificarão os riscos, e a implementação destas, já que uma vez implementado o tratamento fornece novos controles ou modifica os já existentes.

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 e 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.	Denomina esta etapa de Monitoramento e análise crítica dos Riscos. Nesta etapa os riscos são vigiados regularmente, mediante ações pré-definidas no escopo da gestão de riscos.

Fonte: Elaborado pela autora

Os modelos comparados no Quadro 15 possuem uma estrutura próxima, apesar de algumas diferenças. A Norma ISO 31000 (2009) estabelece princípios para a gestão de riscos corporativos, e o processo de comunicação e consulta as partes interessadas, tais aspectos não foram abrangidos na estrutura para a gestão de riscos de TI proposta pelo COBIT. Adicionalmente salienta-se a participação de auditorias capazes de monitorar as ações relacionadas à manutenção e monitoramento de planos de ações de riscos.

Na comparação entre os modelos foi percebido que enquanto o COBIT apresenta-se como um modelo mais focado na gestão e monitoramento dos riscos de TI a ISO 31000(2009) busca operacionalizar de forma genérica desde os princípios a serem estabelecidos até a realização do monitoramento de toda a estrutura para gestão de riscos. Neste âmbito, concluí-se que as normas não são excludentes, elas acabam de certa forma se complementando não sendo percebidos motivos para elas não serem utilizadas em conjunto pelas corporações.

Depois de abordado sobre a relação entre gestão riscos de TI e gestão dos riscos corporativos, os principais aspectos encontrados na literatura foram categorizados no Quadro 16, afim de subsidiar o entendimento sobre o tema e dar suporte a análise dos dados. Posteriormente o Quadro 17 consolida os três quadros (Quadro8, Quadro14, e Quadro 16).

Quadro 16: Categorização Gestão de Riscos de TI *versus* Gestão de Riscos Corporativos

Categoria / Relação	Autores
Atuação de TI *versus* perspectiva de negócio	ITGI (2007)
Governança corporativa *versus* gestão de riscos em TI e Riscos corporativos	IBGC (2009)
Criação de mecanismos de controle *versus* redução de riscos em TI e Riscos corporativos	JUNIOR, JUNQUEIRA e BERTUCCI (2010)
Atuação dos usuários *versus* segurança nos processos de	BULGURCU, CAVUSOGLU E BENBASAT

negócio	(2010), SPEARS E BARKI (2010)
Estabelecimento de controles internos	IBGC (2009); FRIGO E ANDERSON (2011)
Atuação Comitê de riscos *versus* prevenção de riscos de TI e Corporativos	IBGC (2009)

Fonte: Elaborado pela autora

No capítulo seguinte, aborda-se a metodologia de pesquisa utilizada, que apresenta os procedimentos metodológicos adotados neste estudo a fim de que o objetivo desta pesquisa fosse concluído.

3 METODOLOGIA

Esta pesquisa teve por objetivo gerar conhecimento sobre a relação existente entre a gestão de riscos corporativos e riscos de TI. Desta forma, seu objetivo envolve o tratamento do assunto sob o foco do que ocorre na realidade. Portanto, de acordo com o conceito de Silva e Menezes (2001), classifica-se quanto a sua natureza, como uma pesquisa aplicada.

Existem dois tipos de abordagem da pesquisa, a qualitativa e a quantitativa. Este estudo tem característica qualitativa, pois busca descrever a percepções sobre o problema de pesquisa. A pesquisa qualitativa é caracterizada pela descrição, considera a relação entre o mundo real e o sujeito, realizando análises não possíveis de serem quantificadas (SILVA E MENEZES, 2001; GIL, 2009; YIN, 2010).

A estratégia de pesquisa adotada é a do estudo de caso, que para Eisenhardt e Graebner (2007) envolvem a utilização de um ou mais casos para criar construções teóricas, proposições ou teorias. Estes autores afirmam que esta modalidade de estudo pode acomodar uma rica variedade de fontes de dados. Considerando que estuda um único caso em profundidade.

A escolha por um estudo de caso único ocorreu devido à busca de identificação da resposta ao problema de pesquisa de forma ampla e aprofundada, visando adquirir conhecimento detalhado sobre o tema em questão. Segundo Yin (2010), os projetos de caso único exigem uma investigação cuidadosa do caso potencial a fim de minimizar equívocos e maximizar o acesso necessário à coleta de evidências do estudo de caso.

Um protocolo de estudo de caso foi construído e utilizado na pesquisa (apêndice A), com o intuito de apoiar o processo de coleta e análise de dados. Segundo Yin (2010), o protocolo de estudo de caso tem por finalidade dar confiabilidade à pesquisa, dar foco e servir de suporte ao pesquisador na realização da coleta de dados.

Do ponto de vista de abordagem a pesquisa se classifica como exploratória, já que proporciona familiaridade com o problema, uma vez que tratou das associações entre a gestão de riscos de TI e a gestão de riscos corporativos. Do ponto de vista de seus objetivos é descritiva pois visou descrever as características da relação explorada mediante o estudo de caso (SILVA e MENEZES, 2001).

As próximas seções que tratam do processo de coleta e análise dos dados foram construídas a partir das categorias estabelecidas na revisão da literatura. Para tanto os Quadros 8 (Categorização das temáticas da Gestão de Riscos em TI); Quadro 14 (Categorização das temáticas da Gestão de Riscos Corporativos) e Quadro 16 (Categorização Gestão de Riscos de TI versus Gestão de Riscos Corporativos), foram consolidados no *Framework* metodológico para análise da relação objeto do estudo (Quadro 17), o qual direcionou a aplicação do caso prático.

Quadro 17: *Framework* metodológico para análise da relação objeto do estudo

GESTÃO DE RISCOS DA TECNOLOGIA DA INFORMAÇÃO (TI)	**Relação**	**GESTÃO DE RISCOS CORPORATIVOS**
Categoria		**Categoria**
Planejamento estratégico de TI – Planejar e organizar	Atuação de TI *versus* perspectiva de negócio	Avaliação estratégica do risco – Aproveitar oportunidades
Requisitos de negócio (confidencialidade, Integridade, disponibilidade) primários para a gestão de riscos em TI	Governança corporativa *versus* gestão de riscos em TI e Riscos corporativos	Princípios para a gestão de riscos corporativos
Investimentos e Recursos de TI – Adquirir e implementar	Criação de mecanismos de controle *versus* redução de riscos em TI e Riscos corporativos	Identificação dos eventos e categorização dos riscos (estratégicos, financeiros e operacionais)
Segurança nas informações - Uso de TI – Usuários	Atuação dos usuários *versus* segurança nos processos de negócio	Inter-relação entre os tipos de riscos
Processos de TI – Entrega e suporte	Estabelecimento de controles internos	Perda de Recursos (custos ou prejuízos associados) – Danos – Consequências negativas
Boas Práticas para Gestão Riscos em TI	Atuação Comitê de riscos *versus* prevenção de riscos de TI e Corporativos	Estrutura para gestão dos riscos (concepção, implementação, monitoramento e melhoria contínua) mandado e comprometimento
Processos de controle para a gestão dos riscos de TI (estabelecimento do contexto, identificação, avaliação, resposta, manutenção e monitoramento)	COBIT PO9	Processos para a gestão de riscos (estabelecimento do contexto, identificação dos riscos, análise dos riscos, avaliação dos riscos e tratamento dos riscos)
Monitoramento da gestão de TI	Aproximação entre riscos corporativos e riscos de TI	Conscientização e Resposta ao risco (evitar, reduzir, compartilhar e aceitar

		riscos)

Fonte: Elaborado pela autora

As próximas seções tratam dos procedimentos para coleta, tratamento e análise dos dados, seguidos das limitações do método.

3.1 PROCEDIMENTOS PARA COLETA DE DADOS

Uma vez que a opção de pesquisa foi o estudo de caso, cabe destacar os critérios utilizados para a seleção da organização participante da pesquisa, bem como os cuidados necessários em relação ao caso estudado.

Segundo Yin (2010, p. 100) o pesquisador é responsável pela condução do seu estudo de caso e deve ter cuidados e sensibilidade especiais, envolvendo geralmente os seguintes aspectos: a) obter o consentimento informado de todos os envolvidos no estudo de caso, b) proteger os participantes, sua a privacidade e confidencialidade dos que participaram, e c) tomar precauções especiais para proteção de grupos específicos que possam ser vulneráveis. Neste sentido um pedido de autorização para realização do estudo foi encaminhado à empresa objeto do estudo (Apêndice A).

Para seleção da organização a ser estudada, foi considerado:

a. 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.

b. Interesse e disponibilidade por parte da empresa em participar da pesquisa, fornecendo assim as informações necessárias ao estudo;

c. O acesso à empresa (sede situada no estado do Rio Grande do Sul).

O caso selecionado para estudo com base nos critérios descritos anteriormente nessa seção é a SLC Agrícola, empresa do ramo de *commodities* agrícola, fundada em 1945, com sede administrativa em Porto Alegre/RS.

Os procedimentos para coleta e tratamento dos dados utilizaram como base de apoio o protocolo de estudo de caso (Apêndice A). Para coleta dos dados, diferentes instrumentos foram utilizados, com o intuito de gerar evidencias suficientes para suportar os achados. Utilizou-se como instrumentos de coleta:

1. Documentos;

2. Entrevistas;

3. Questionários.

Os instrumentos de coleta de dados foram posteriormente descritos de forma detalhada.

1. Documentos: a utilização de documentos na pesquisa teve como objetivo buscar evidências que pudessem ser cruzadas com as respostas obtidas nas entrevistas e no questionário. Os documentos utilizados na pesquisa foram aqueles disponibilizados no portal do investidor da empresa (relatórios trimestrais, demonstrações financeiras, comunicados, e documentos entregues a CVM – Comissão de valores mobiliários).

Os documentos foram lidos e analisados a fim de identificar informações sobre as categorias que direcionaram a aplicação do caso de estudo consolidadas no *Framework* metodológico para análise da relação objeto do estudo (Quadro 17). Foram selecionados após esta análise os seguintes documentos:

- Apresentação para o Investidor, (SLC 2012a).

- Código de Ética e Conduta SLC Agrícola, (SLC 2012b).

- Demonstrações Financeiras 2011, (SLC 2012c).

- Fatores de Risco. (SLC, 2012d).

2. Entrevistas: o processo de coleta de dados através de entrevistas contemplou a seleção dos respondentes, o agendamento prévio das entrevistas, a elaboração do roteiro, e a aplicação das entrevistas. Cada uma destas etapas é descrita a seguir.

Seleção dos entrevistados: A seleção dos participantes considerou sua atuação vinculada à gestão de riscos de TI e gestão de riscos corporativos, bem como a disponibilidade e interesse em participar da pesquisa. Foram selecionados como respondentes: um Membro do comitê de riscos, o Gerente Corporativo de TI, e o Coordenador de sistemas.

Agendamento prévio das entrevistas: A correspondência formal para realização da pesquisa, constante no protocolo de estudo de caso, foi enviada previamente aos participantes por meio de correio eletrônico (*e-mail)*, para que estes tivessem entendimento quanto aos objetivos do estudo. Depois de confirmada a participação realizou-se um contato telefônico para agendamento das entrevistas. Em alguns casos as entrevistas precisaram ser reagendadas, devido a imprevistos que surgiram na agenda dos entrevistados. Contatos posteriores foram realizados para complementar as respostas obtidas.

Roteiro para a entrevista: mediante a associação entre as temáticas de estudo foi possível gerar um roteiro para as entrevistas (Apêndice B). Este foi elaborado com base nas categorias de cada seção identificadas na revisão da literatura, e consolidadas no *Framework* metodológico para análise da relação objeto do estudo (Quadro 17), o qual direcionou a aplicação do caso prático.

Para facilitar as análises, o roteiro foi organizado em blocos. Os títulos e as questões de cada bloco, bem como a categoria correspondente ao *framework* metodológico (Quadro 17) foram detalhados a seguir:

Bloco I – Caracterização do respondente:

- Cargo (ocupação);

- Tempo na função e na empresa;

- Formação acadêmica;

- Idade; e

- Principais Responsabilidades.

Bloco II – Gestão dos Riscos de TI

- Categoria 1 – Planejamento estratégico de TI – Planejar e organizar: Na sua percepção, como o modo que TI é gerenciado na organização permite o desenvolvimento do planejamento estratégico, planejamento de TI, e gestão de riscos? Este gerenciamento ocorre de forma crítica e realista? SIMONSON, JOHNSON e EKSTEDT (2010).

- Categoria 2- Requisitos de negócio: De que forma a confidencialidade, integridade e disponibilidade das informações atuam dentro da organização em relação aos riscos? Na sua percepção, como estes requisitos de negócio atendem as necessidades de informações da empresa? ITGI (2007).

- Categoria 3- Investimentos e Recursos de TI – adquirir e implementar: Os investimentos realizados em TI são suficientes para permitir que as informações sejam corretas, precisas e estejam disponíveis no tempo adequado? Como isso é validado pelos usuários? De que forma estes investimentos podem proteger a empresa de riscos? COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).

Como a estrutura de TI presente na organização possibilita a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas)? De que maneira esta estrutura interage com a prevenção dos riscos? ITGI (2007).

- Categoria 4- Segurança das Informações, uso de TI e Usuários: Quais as vantagens ou desvantagens que a Tecnologia da Informação – TI oferece decorrentes de seu uso? Qual a sua percepção da relação desta utilização com os riscos? ALBERTIN e ALBERTIN (2012).

Como a empresa implanta planos de segurança para reduzir os riscos relacionados à segurança das informações? Qual o envolvimento funcional dos usuários? De que maneira eles participam da gestão de riscos e segurança? BULGURCU, CAVUSOGLU E BENBASAT (2010); SPEARS E BARKI (2010).

- Categoria 5- Processos de TI – Entrega e Suporte: De que maneira os processos de TI possibilitam que a entrega e suporte dos serviços de TI atendam as necessidades dos usuários? Como a prestação de serviços de TI atua para minimizar os riscos? ITGI (2007).

- (Categoria 6) Como a recomendação e comunicação de planos de ação de remediação dos riscos consideram a participação dos usuários para a gestão de riscos e segurança? Como esta gestão se integra aos processos gerenciais? SPEARS E BARKI (2010); ITGI (2007).

- Categoria 7- Processo de controle para a gestão de riscos em TI: Como a estrutura para gestão de riscos de TI é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? BULGURCU, CAVUSOGLU E BENBASAT (2010).

- Categoria 8- Monitoramento da gestão de TI: Que tipos de esforços são realizados pela corporação para manutenção e monitoramento de planos de ação para os riscos? Como estes esforços contemplam o desenvolvimento e a performance de controles? ITGI (2007); SPEARS E BARKI (2010).

Bloco III – Gestão dos Riscos Corporativos

- Categoria 1 – Avaliação estratégica dos riscos: Como a organização realiza a avaliação estratégica de seus riscos? Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança ? FRIGO E ANDERSON (2011).

- Categoria 2 – Perda de recursos, danos e consequências negativas: De que forma o gerenciamento dos riscos corporativos possibilitam evitar, reduzir, compartilhar ou aceitar os riscos? Na sua percepção este gerenciamento estabelecer respostas a estes, reduzindo surpresas, custos ou prejuízos associados? IBGC (2007); COSO (2007); ISO 31000 (2009); AVEN (2011); GERIGK E CORBARI (2011).

- Categoria 3 – Identificação dos eventos e categorização dos riscos: A organização procura identificar os eventos que possam ter consequências operacionais, financeiras ou estratégicas adversas? Caso afirmativo, como são prevenidos ou minimizados tais eventos? COSO (2007); IBGC (2007); GERIGK e CORBARI (2011).

- Categoria 4 – Avaliação estratégica dos Riscos: Como a gestão de riscos corporativos possibilitam uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos? Como isto ocorre? COSO (2007); IBGC (2007)

- Categoria 5 – Princípios para a gestão de riscos corporativos: Você considera que os seguintes princípios são atendidos pela empresa, quanto à gestão de riscos. Explique como isso ocorre. 1)Cria e protege valor; 2) Participa de todos os processos organizacionais; 3) Participa da tomada de decisão; 4) Aborda explicitamente a incerteza; 5) Atua de forma Sistemática, estruturada e oportuna; 6) Baseia-se nas melhores informações possíveis; 7) Se adéqua a realidade da organização; 8) Considera fatores humanos e culturais; 9) Atua de forma transparente e inclusiva; 10) Atua de forma dinâmica e interativa, capaz de reagir a mudanças; 11) Facilita a melhoria contínua da organização. ISO 31000(2009)

- Categoria 6 – Estrutura para o gerenciamento dos riscos: Como a estrutura para gestão de riscos corporativos é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? BULGURCU, CAVUSOGLU E BENBASAT (2010).

A gestão dos riscos realizada na organização fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro? AVEN (2011).

- Categoria 7 – Processos para a gestão de riscos: Como os seguintes processos são considerados em relação aos processos de negócio organizacionais? 1)Comunicação e consulta às partes interessadas (internas e externas); 2) Estabelecimento do contexto (parâmetros internos e externos que precisam ser levados em consideração); 3) Avaliação dos Riscos (identificação, análise e avaliação dos riscos); 4) Tratamento dos Riscos; 5) Monitoramento e análise crítica dos Riscos, ISO 31000(2009)

- Categoria 8 – Monitoramento da gestão de riscos de TI: Como a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações? Estas decisões consideram a incerteza, a natureza desta incerteza, e como ela pode ser tratada? ISO 31000 (2009)

Bloco IV – Relação entre a gestão de riscos de TI e a gestão dos Riscos Corporativos.

- Categoria 1– Atuação de TI *versus* perspectivas de negócio: Como a TI atua para prevenir riscos inerentes ao negócio? Esta atuação pode ser considerada satisfatória dentro de uma perspectiva de negócio? ITGI (2007)

- Categoria 2 – Governança corporativa *versus* gestão de riscos de TI e gestão de riscos corporativos: Como a práticas de governança corporativa orientam o dia a dia do trabalho da organização? De que forma elas contribuem para a gestão de riscos em TI e gestão dos riscos corporativos? (IBGC 2009).

- Categoria 3– Criação de mecanismos de controle versus redução de riscos em TI e riscos corporativos: De que forma a adoção de mecanismos de controle possibilita redução dos riscos corporativos e riscos de TI? JUNIOR, JUNQUEIRA e BERTUCCI (2010).

- Categoria 4– Atuação dos usuários versus segurança nos processos de negócio: De que maneira os usuários participam do gerenciamento de riscos de segurança nos processos de negócios? Como a sua participação é percebida e qual é o impacto da participação na segurança do negócio? SPEARS E BARKI (2010).

- Categoria 5– Estabelecimento de controles internos: Como os controles internos protegem as informações financeiras ? Esta proteção é capaz de produzir informações contábeis financeiras confiáveis? SPEARS E BARKI (2010).

- Categoria 6– Atuação Comitê de riscos versus prevenção de riscos de TI e Corporativos: De que maneira a atuação do comitê para a gestão de riscos ocorre? Como sua atuação contempla a prevenção de riscos de TI e risco corporativos? (IBGC 2009).

O último item do roteiro da entrevista buscou identificar a opinião do entrevistado sobre a aproximação dos riscos de TI e riscos corporativos, contemplando a seguinte questão: Em sua opinião existe uma aproximação entre os riscos de TI e riscos corporativos? Como isso seria possível?

Aplicação das entrevistas: As entrevistas foram realizadas com profundidade, e realizadas em separado com cada um dos entrevistados e foram conduzidas pela pesquisadora, que buscou esclarecer aos respondentes quaisquer dúvidas que surgissem frente às perguntas. O primeiro entrevistado foi o Coordenador coorporativo de TI, posteriormente com o Gerente de sistemas e por fim o profissional atuante no comitê de riscos (Gerente de RI- relação com o investidor). As entrevistas duraram em média 2 horas e 30 minutos.

Cabe destacar que todas as entrevistas foram gravadas em arquivo digital e transcritas (ver Apêndice D). Como complemento às entrevistas, após a transcrição, os entrevistados receberam por *e-mail* suas respostas, que foram validadas, sendo possível desta maneira a correção de erros oriundos do processo de transcrição.

3. Questionário: O questionário foi construído à luz das categorias demonstradas no Quadro *Framework* Metodológico (Quadro 17), que foi elaborado com base no referencial teórico. Cabe destacar duas etapas neste processo: a elaboração e a aplicação do questionário.

Elaboração: O questionário foi dividido em duas partes com diferentes objetivos: 1) entender as ações que foram tomadas pela corporação para a gestão dos riscos de TI, e 2) Identificar a importância dos diferentes tipos de riscos corporativos nas atividades da organização.

Parte 1- Entendimento das ações que são tomadas pela corporação para a gestão dos riscos de TI. A elaboração desta etapa foi realizada com base no processo nº 9 do COBIT que trata exclusivamente da execução e avaliação da gestão de riscos em TI. Neste sentido, os respondentes precisavam escolher o nível de maturidade para os processos listados, utilizando a linha vazia para explicar ações que são tomadas pela corporação nestes processos. Os níveis de maturidade utilizados são específicos para a gestão de riscos em TI e podem ser observados no Quadro 18.

Quadro 18: Níveis de maturidade do PO9 do COBIT

Grau de maturidade	Descrição
0 – Inexistente	Quando não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.
1 – Inicial	Os riscos de TI são considerados de forma inicial. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes. Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.
2 – Repetitivo, mas intuitivo	Quando Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.
3 – Definido	Quando Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.
4 – Gerenciado	Quando A avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os cenários de riscos relacionados a TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, o comitê executivo e a Diretoria de TI estabelecem os níveis de risco que a

	organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.
5 – Otimizado	Quando o gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A Direção de TI avalia continuamente as estratégias de mitigação de risco.

Fonte: ITGI (2007, p.68)

O respondente precisava selecionar os níveis de maturidade de acordo com cada processo listado. Foram listados no instrumento os seguintes processos: *1) Alinhamento da gestão de riscos de TI e de Negócios; 2) Estabelecimento do Contexto de Risco; 3) Identificação de Eventos; 4) Avaliação de Risco; 5) Resposta ao Risco; 6) Manutenção e Monitoramento do Plano de Ação de Risco.* Cabe destacar que abaixo de cada processo, foi acrescentada uma breve explicação sobre o que contemplaria cada etapa, a fim de subsidiar o respondente na sua escolha. No Quadro 19 pode ser obervado esta etapa do questionário.

Quadro 19: Questionário – Etapa 1 Avalia e Gerencia os Riscos de TI

Processos COBIT		**Nível de maturidade**					
		0 - Inexistente	**1 - Inicial**	**2 – Repetitivo**	**3 - Definido**	**4 - Gerenciado**	**5- Otimizado**
PO9 - Avalia e gerencia os riscos							
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).							
Explique:							
PO9.2 Estabelecimento do Contexto de Risco 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							

Processos COBIT		Nível de maturidade					
		0 - Inexistente	1 - Inicial	2 – Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
avaliação e os critérios pelos quais os riscos são avaliados.							
Explique:							
PO9.3 Identificação de Eventos 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 jurídicos, 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.							
Explique:							
PO9.4 Avaliação de Risco 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.							
Explique:							
PO9.5 Resposta ao Risco 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.							
Explique:							
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco 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 e 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.							
Explique:							

Fonte: Construído a partir de ITGI (2007, p.66)

O item “Explique” demonstrado no Quadro 19, permitiu aos entrevistados explanarem sobre sua opção, esta explanação possibilitou na etapa de análise dos dados a confirmação das informações fornecidas nas entrevistas e retiradas dos documentos, enriquecendo assim os achados.

Parte 2 – Identificação da importância dos diferentes tipos de riscos corporativos nas atividades da organização. Nesta etapa o respondente precisava responder a seguinte questão: *Qual a importância dos tipos de risco abaixo relacionados nas atividades organização?*

Para tanto precisava levar em consideração o grau de importância de cada tipo de riscos, estes foram identificados no Quadro 20.

Quadro 20: Graus de Importância Utilizados no Questionário

Grau de importância	Descrição
Igual	Igualmente importante ou preferido
Moderado	Levemente mais importante ou preferido
Forte	Medianamente mais importante ou preferido
Muito Forte	Fortemente mais importante ou preferido
Extrema	Extremamente mais importante ou preferido

Fonte: Saaty (1991).

Para este trabalho foi utilizado exclusivamente os graus de importância ilustrados no Quadro 20. As descrições estão relacionadas às comparações par a par, sendo que estas fazem parte de estudos futuros sugeridos por esta pesquisadora. Salienta-se que uma simulação de avaliação par a par mediante aplicação do método *analytic hierarchy process* (AHP) foi realizada neste estudo. Esta simulação foi ilustrada de forma gráfica no Apêndice F.

Nesta etapa foram considerados os seguintes tipos de riscos identificados na teoria: *1) Risco econômico; 2) Risco político;3) Risco ambiental; 4) Riscos de Marca, Imagem ou Reputação; 5) Riscos Sociais; 6) Riscos Tecnológicos (estratégicos); 7) Riscos de Mercado; 8) Riscos de Crédito; 9) Riscos de Liquidez; 10) Riscos de Pessoal; 11) Riscos de Processos; 12) Risco de Tecnologia (operacional); e 13) Riscos de compliance.* Abaixo de cada tipo de risco foi acrescentando um breve conceito, para apoio do respondente no momento da escolha de cada questão. O Quadro 21 demonstra a estrutura do questionário.

Quadro 21: Questionário – Etapa 1 Avalia e Gerencia os Riscos de TI

	Extrema	Muito forte	Forte	Moderada	Igual
Riscos Econômicos Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas					

	Extrema	Muito forte	Forte	Moderada	Igual
barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.					
Qual o significado de sua resposta:					
Riscos Políticos Eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.					
Qual o significado de sua resposta:					
Riscos Ambiental Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.					
Qual o significado de sua resposta:					
Riscos de Marca, Imagem ou Reputação É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e,consequentemente, a consecução de transações com estes clientes.					
Qual o significado de sua resposta:					
Riscos Sociais São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.					
Qual o significado de sua resposta:					
Riscos Tecnológicos (estratégicos) São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.					
Qual o significado de sua resposta:					
Riscos de Mercado A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).					
Qual o significado de sua resposta:					
Riscos de Crédito É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação					
Qual o significado de sua resposta:					
Riscos de Liquidez Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.					
Qual o significado de sua resposta:					
Riscos de Pessoal Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.					
Qual o significado de sua resposta:					

	Extrema	Muito forte	Forte	Moderada	Igual
Riscos de Processos Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.					
Qual o significado de sua resposta:					
Risco de Tecnologia (operacional) Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).					
Qual o significado de sua resposta:					
Riscos de compliance Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.					

Fonte: Elaborado pela autora

Ao final o respondente precisava justificar se alteraria os critérios de avaliação utilizados, e qual o motivo desta alteração. Esta avaliação permitiu validar se os critérios de seleção utilizados estavam de acordo com os itens questionados.

As aplicações de todos os instrumentos de coleta de dados proporcionaram subsídios juntamente com a revisão da literatura, para o entendimento da relação entre a gestão riscos de TI e a gestão dos riscos corporativos, ou seja, para ser possível proceder com a análise dos dados.

3.2 PROCEDIMENTOS PARA TRATAMENTO e ANÁLISE DOS DADOS

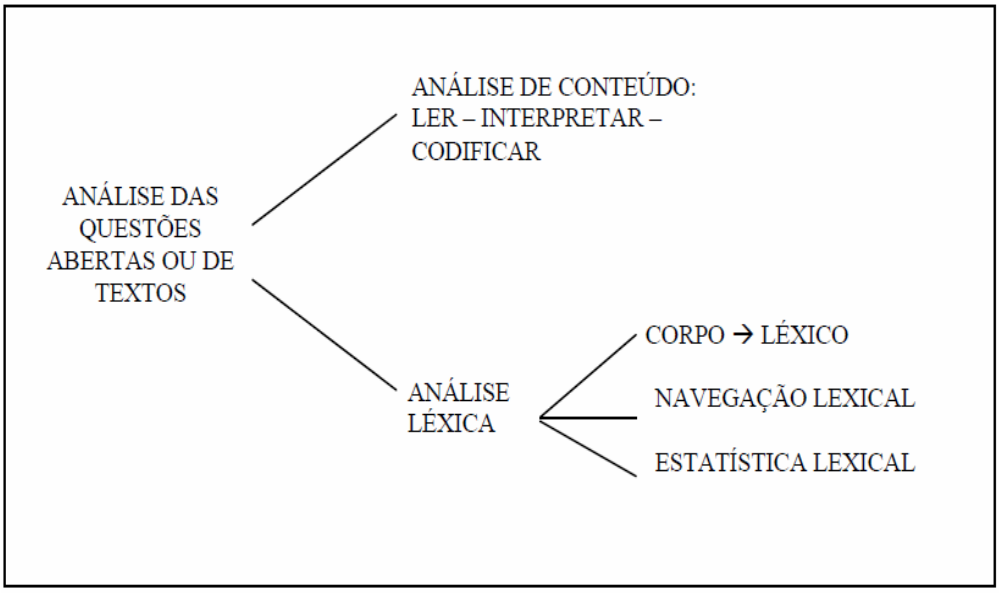
Após coletados os dados procedeu-se o tratamento e sua análise, a qual contemplou a refinação dos dados e a forma de apresentação das evidencias coletadas. De acordo com Yin (2010), a análise dos dados consiste em examinar, categorizar, tabular, testar ou recombinar as evidências para tratar as proposições iniciais do estudo.

Os dados obtidos com a aplicação das entrevistas foram analisados de forma comparativa entre as respostas dos entrevistados. Tal análise seguiu a mesma ordenação das categorias identificadas na literatura e consolidadas no *Framework* metodológico para análise da relação objeto do estudo (Quadro 17). Este panorama foi desenvolvido de forma qualitativa frente aos dados, e complementado com as informações obtidas na análise dos documentos utilizados na pesquisa.

Os dados coletados na entrevista foram tratados a partir do software *Sphinx* Léxica (versão 5.1), na tentativa de compreender as percepções dos entrevistados sobre riscos de TI e riscos corporativos, de acordo com as respostas obtidas. Através de um banco de dados composto pelas informações dos participantes, 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. A forma de utilização destas duas técnicas pode ser observada na Figura 8:

Figura 8: A análise de Conteúdo e a Análise Léxica.



Fonte: FREITAS; MOSCAROLA (2000, p.108)

Para Freitas (2011), o uso 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 descritas no *Framework* metodológico (Quadro 17), porém foram abreviadas para melhor disposição no mapa fatorial. No Quadro 22 foram apresentadas estas categorias e sua descrição reduzida utilizada no *software.*

Quadro 22: Categorias Utilizadas no *Sphinx*

***Framework* Metodológico**	***SPHINX***	***Framework* Metodológico**	***SPHINX***	***Framework* Metodológico**	***SPHINX***
GESTÃO DE RISCOS DE TI		**Relação**		**GESTÃO DE RISCOS CORPORATIVOS**	
Planejamento estratégico de TI – Planejar e organizar	Planejamento TI	Atuação de TI *versus* perspectiva de negócio	TI *X* Negócio	Avaliação estratégica do risco – Aproveitar oportunidades	Avaliação Estratégica RC
Requisitos de negócio (confidencialidade, Integridade, disponibilidade) primários para a gestão de riscos em TI	Requisitos TI	Governança corporativa *versus* gestão de riscos em TI e Riscos corporativos	GC X GR	Perda de Recursos (custos ou prejuízos associados) – Danos – Consequências negativas	Perdas de recursos
Investimentos e Recursos de TI – Adquirir e implementar	Investimento TI	Criação de mecanismos de controle *versus* redução de riscos em TI e Riscos corporativos	Controle interno X GR	Identificação dos eventos e categorização dos riscos (estratégicos, financeiros e operacionais)	Identificaçã o Eventos
Segurança nas informações - Uso de TI – Usuários	Segurança Uso e Usuários	Atuação dos usuários *versus* segurança nos processos de negócio	Usuários X negócio	Inter-relação entre os tipos de riscos	Inter-relação
Processos de TI – Entrega e suporte	Processos TI	Estabelecimento de controles internos	Controles Internos	Princípios para a gestão de riscos corporativos	Princípios GRC
Boas Práticas para Gestão Riscos em TI	Boas Práticas GRTI	Atuação Comitê de riscos *versus* prevenção de riscos de TI e Corporativos	Comitê	Estrutura para gerenciamento dos riscos (concepção, implementação, monitoramento e melhoria contínua) - mandado e comprometimento	Estrutura GRC

Framework Metodológico	*SPHINX*	*Framework* Metodológico	*SPHINX*	*Framework* Metodológico	*SPHINX*
GESTÃO DE RISCOS DE TI		**Relação**		**GESTÃO DE RISCOS CORPORATIVOS**	
Processos de controle para a gestão dos riscos de TI (estabelecimento do contexto, identificação, avaliação, resposta, manutenção e monitoramento)	Processos GRTI	Aproximação entre riscos corporativos e riscos de TI	Aproximação	Processos para a gestão de riscos (estabelecimento do contexto, identificação dos riscos, análise dos riscos, avaliação dos riscos e tratamento dos riscos)	Processos GRC
Monitoramento da gestão de TI	Monitoramento GRTI			Conscientização e Resposta ao risco (evitar, reduzir, compartilhar e aceitar riscos)	Resposta ao risco GRC

Fonte: Elaborado pela autora

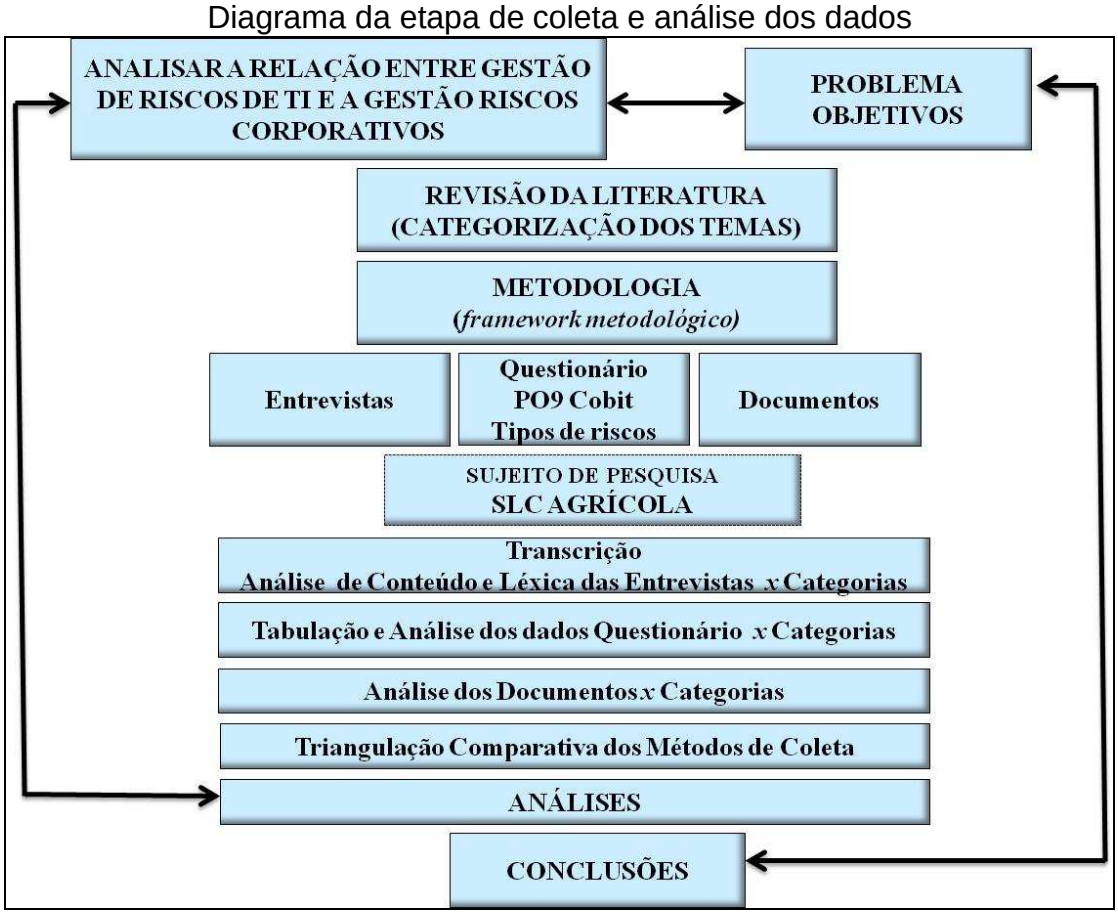
Depois de inclusa as categorias no *Sphinx* procederam-se a análise de conteúdo das respostas no software. Neste momento as respostas foram lidas, sendo atribuídas a elas uma ou mais categorias existentes no *framework* metodológico, e compatível ao texto da resposta.

Uma vez concluída a análise de conteúdo das respostas procedeu-se a análise léxica – AL das palavras mais frequentes na fala dos entrevistados. Em um primeiro instante a AL foi empregada para organizar o vocabulário, posteriormente houve o agrupamento das palavras que continham o mesmo sentido e a exclusão daquelas de menor relevância, considerando a essência do texto. Com as categorias e os léxicos relevantes foi possível gerar um mapa fatorial por categoria, afim de identificar a relação entre os léxicos mais frequentes na fala dos entrevistados.

Após análise dos dados coletados nas entrevistas, passou-se para análise das respostas do questionário. As opções marcadas no questionário foram tabuladas (com auxílio do software Excel) e analisadas com o objetivo de entender o processo de controle dos riscos de TI (processo nº9 do COBIT), e a identificação da importância dos riscos corporativos.

A análise dos documentos foi realizada de forma a encontrar evidencias que corroborassem com as informações localizadas nas demais técnicas. Na Figura 9 é ilustrada a etapa de coleta, análise e tratamento dos dados descritos nesta seção.

Figura 9: Diagrama da etapa de coleta e análise dos dados.



Fonte: Elaborado pela autora.

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 conclusões.

3.3 LIMITAÇÕES DO MÉTODO

Durante o processo de realização deste estudo algumas limitações puderam ser observadas. Uma das principais refere-se à utilização de entrevistas, principalmente devido à disponibilidade de tempo dos entrevistados para atendimento da pesquisadora, o que de certa forma pode comprometer a profundidade das respostas obtidas. Além deste, outro ponto de limitação identificado neste processo são as divergências que podem ocorrer da interpretação dos entrevistados e pesquisador. Contudo, conforme já exposto na sessão anterior, houve cuidado por parte da pesquisadora em esclarecer os pontos que pudessem gerar dúvidas no momento das entrevistas e os questionamentos feitos posteriormente para complementar as respostas.

Adicionalmente, identificou-se outra possível limitação, esta no sentido de que em função da estratégia de estudo ser um estudo de caso, seus resultados não podem ser generalizados, restringindo-se apenas ao caso de estudo. Portanto, não é possível generalizar os resultados para demais empresas. Apesar disto, este estudo pode ser usado como parâmetro em futuros estudos de forma comparativa (YIN, 2010).

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. O Caso se mostrou apropriado para resposta à questão problema e atendimento dos objetivos.

O objetivo deste capítulo é realizar a descrição e análise dos dados coletados junto à unidade de estudo. Primeiramente é realizada a caracterização da empresa estudada seguido da caracterização dos gestores participantes da pesquisa. Posteriormente, serão analisados os riscos de TI e riscos corporativos no caso de estudo. Por fim, é analisada a relação entre a gestão de riscos de TI e a gestão dos riscos corporativos com base no caso estudado.

4.1. CARACTERIZAÇÃO DA EMPRESA

Nesta seção, apresentam-se as principais características do caso de estudo. Sua atuação, seu porte, o quadro funcional, e o organograma da estrutura corporativa. Por fim, a localização dentro desta estrutura do Comitê de Gestão de Riscos e do Departamento de TI (áreas de atuação dos respondentes).

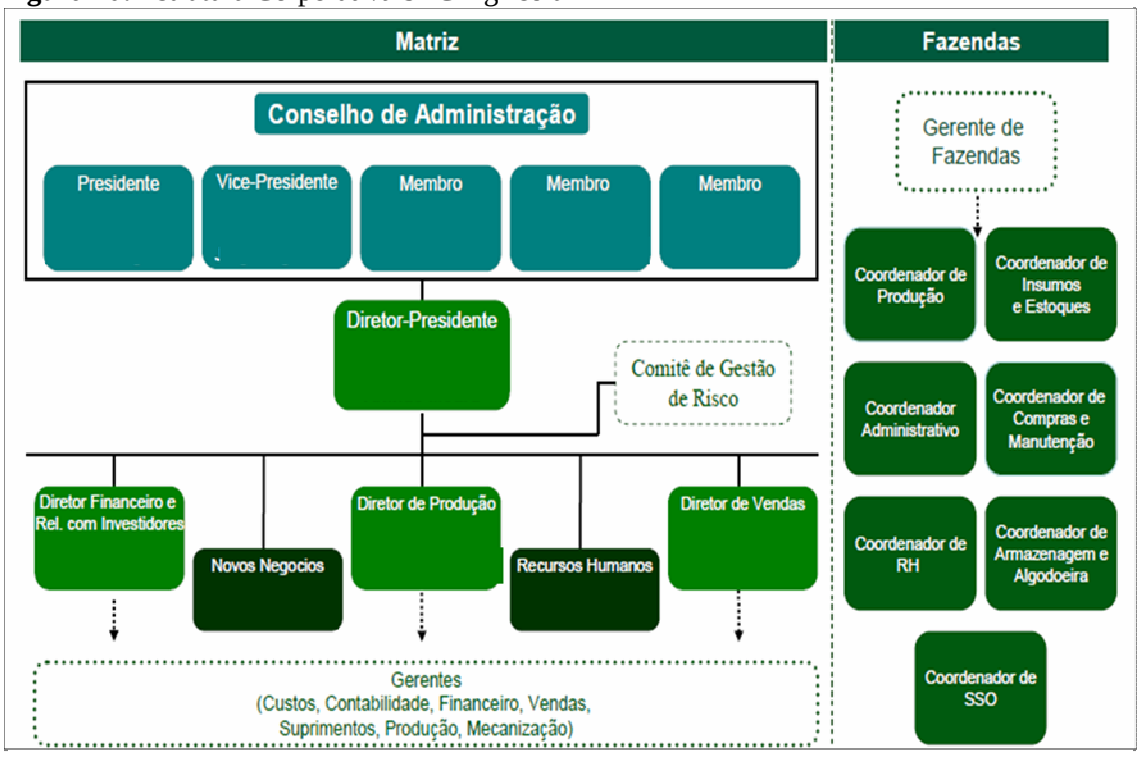
A empresa objeto deste estudo é SLC Agrícola S.A. Organização fundada em 1977, que têm atividades de agricultura e pecuária, como a produção e comercialização de milho, arroz, feijão soja e algodão, suprimentos para a indústria e revenda de maquinário agrícola. A organização é parte do Grupo SLC que 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).

Sua matriz está sediada na cidade de Porto Alegre/RS. Na safra 2010/11, iniciada em 1º de setembro de 2010, a Companhia operou com onze unidades de produção (fazendas), com uma área plantada total de 226,6 mil hectares, entre áreas próprias e arrendadas de terceiros, localizadas em cinco estados brasileiros: Mato Grosso, Mato Grosso do Sul, Goiás, Bahia e Maranhão (SLC, 2012c).

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. A composição hierárquica da gestão da companhia pode ser observada na Figura 10.

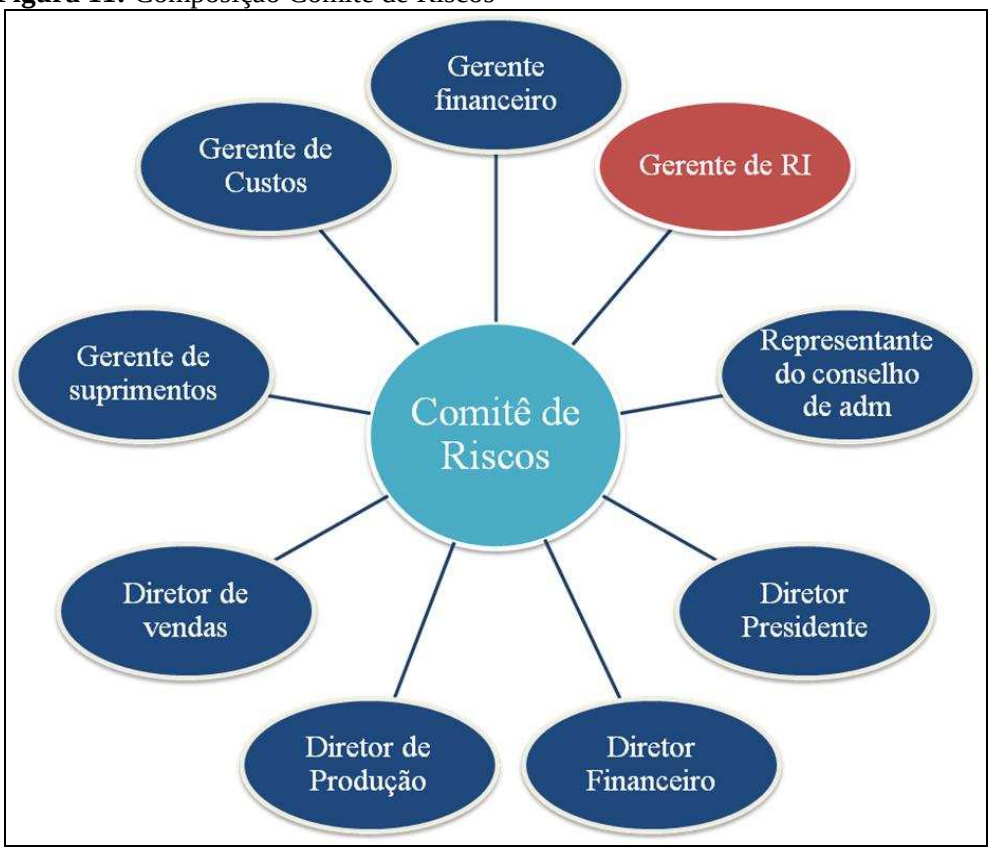
Figura 10: Estrutura Corporativa SLC Agrícola



Fonte: Adaptado de SLC (2012a, p.7)

Destaca-se na Figura 10 a existência do Comitê de Gestão de Riscos que está ligado ao Diretor-Presidente da companhia. Participam do Comitê de Gestão de Riscos: o Diretor- Presidente, um Conselheiro, três Diretores (Produção, Financeiro e Vendas) e quatro Gerentes, a composição completa do Comitê pode ser observada na Figura 11.

Figura 11: Composição Comitê de Riscos

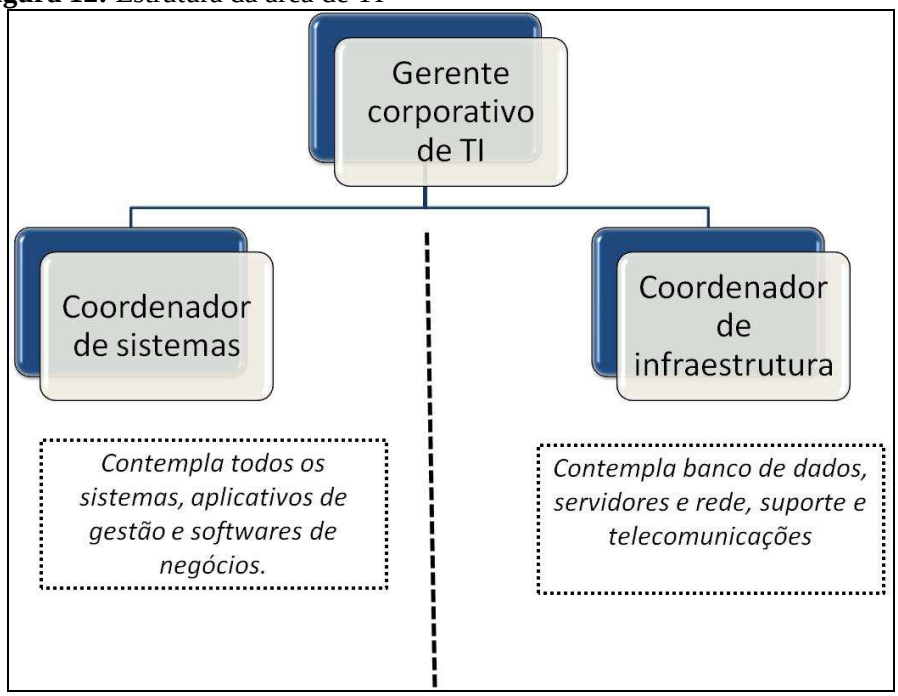


Fonte: Elaborado pela autora com base nas entrevistas

O Gerente de Relações com o Investidor - RI, destacado na Figura 11 foi o profissional atuante no Comitê que participou da pesquisa. Cabe salientar que não foi identificada na pesquisa a participação do departamento de Tecnologia da Informação – TI nas atividades do Comitê. Apesar da TI não estar apresentada na estrutura corporativa ilustrada na Figura 10, sua atuação está hierarquicamente ligada a Diretoria Financeira.

Ao departamento de TI estão diretamente 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. A estrutura completa de TI bem como as principais características de seus setores pode ser observada na Figura 12.

Figura 12: Estrutura da área de TI



Fonte: Elaborado pela autora com base nas entrevistas

Salienta-se a participação do Gerente Corporativo de TI e o Coordenador de sistemas no processo de coleta de dados.

Na próxima seção é realizada a caracterização dos participantes da pesquisa cuja atuação está ligada ao Comitê de Gestão de Riscos e ao departamento de TI.

4.2. CARACTERIZAÇÃO DOS PARTICIPANTES

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 23 as principais características dos respondentes foram descritas.

Quadro 23: Principais Características dos Participantes

	Gerente Corporativo de TI	**Coordenado de Sistemas**	**Membro do Comitê de Riscos**
Tempo na Função e na empresa	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.
Formação acadêmica	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.
Idade	46 anos	46 anos	30 anos

Fonte: Elaborado pela autora com base nas entrevistas

Dentre os entrevistados observa-se que o Gerente Coorporativo 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.

A seguir, descrevem-se as principais responsabilidades dos gestores participantes dos processos de coleta de dados:

- **Gerente corporativo de TI** – (i) Gerenciar toda a estrutura de TI (sistemas e infraestrutura) da corporação; (ii) Representar a área de TI em reuniões de Diretoria; (iii) Gerenciar a atuação dos coordenadores de sistemas e infraestrutura; (iv) Gerenciar a parte de telecomunicações do grupo.
- **Coordenador de Sistemas:** (i) Implementação e manutenção de sistemas de todas as fazendas e unidades do grupo; (ii) Coordenar a atuação dos analistas de negócio que cuidam da parte funcional, técnica de sistemas e processos da empresa, e também a equipe de analistas de sistemas desenvolvedores; (iii) Suporte e manutenção de sistemas; (iv) Coordenar atuação de empresas terceirizadas (especialistas nos sistemas utilizados pela empresa); (v) Homologação de alterações realizadas pelas terceirizadas e testes de desenvolvimentos internos.

- **Membro do Comitê de Riscos –** ***(i) no Comitê –*** 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. ***(ii) na Gerencia de RI-*** Produzir informações trimestrais e anuais para os investidores, informações trimestrais e anuais para a CVM[1]. Contato todo com o mercado financeiro (fornecedores). Relacionamento com os investidores (Brasil e Exterior), fundos de investimentos, gestores de fundos. Participar do Planejamento estratégico da Companhia.

As próximas três seções tratam de análises relativas aos Riscos de TI e Riscos Corporativos. Neste sentido a ordem de descrição dos achados se dará na sequencia das categorias identificadas na revisão da literatura. Cabe destacar que as entrevistas foram analisadas mediante Análise de Conteúdo combinada com a Análise Léxica a partir de informações extraídas do software *Sphinx*, que consiste em identificar a frequência das palavras para extrair, as que tenham conteúdo no texto.

4.3. GESTÃO DOS RISCOS EM TECNOLOGIA DA INFORMAÇÃO (TI)

Esta seção aborda análises quanto à gestão dos riscos de TI contemplando: o planejamento estratégico de TI; os requisitos de negócio; investimentos e recursos de TI; segurança nas informações, o uso de TI e usuários; processos de TI; boas práticas para a gestão de riscos de TI, processo de controle para a gestão de riscos de TI; e monitoramento da gestão de TI.

[1] CVM – Comissão de Valores Mobiliários – Instituição que tem poderes para disciplinar, normatizar e fiscalizar a atuação dos diversos integrantes do mercado. Seu poder normatizador abrange todas as matérias referentes ao mercado de valores mobiliários (CVM, 2012)

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.

> *[...] O planejamento estratégico, de TI e os riscos, pelo menos, leva em conta há questão de como incrementar isso, sistematicamente falando ter um ERP centralizado, para que as coisas funcionem de forma conectada, tudo tem que estar muito bem sincronizado, alicerçado, muito bem unido pra poder funcionar corretamente e evitar riscos.* ***[...] Coordenador de sistemas***
>
> *[...] O gerenciamento de TI hoje ocorre de forma crítica e busca contemplar as necessidades dos usuários sem por em risco as informações. [...]* ***Gerente Corporativo de TI***

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.

> *[...] Eu vejo que o planejamento estratégico em parte está voltado a TI, mas não todo, hoje eu entendo que aqui no grupo esta vinculação ainda é pouca, nós precisávamos ter um pouquinho mais de conhecimento, um pouquinho mais de informação do que a empresa quer saber praticamente, até para podermos saber suportar de forma mais eficiente o nosso trabalho, principalmente apoiando, ajudando no planejamento estratégico, neste ponto acredito que pecamos um pouquinho ainda como TI, acho que uma boa comunicação da estratégica para chegar à parte tática [...]* ***Coordenador de sistemas***
>
> *[...] a TI participa do planejamento estratégico, conhecendo o direcionamento que a empresa está dando para os seus negócios, a TI é envolvida em todas essas questões [...]* ***Gerente Corporativo de TI***

O membro do comitê de riscos elencou o gerenciamento de TI muito mais ligado à parte operacional do trabalho da TI, foi percebido desconhecimento deste entrevistado da vinculação do gerenciamento de TI com o planejamento estratégico.

A análise Léxica da categoria planejamento estratégica de TI contemplou a percepção dos entrevistados sobre o modo que TI é gerenciado para o desenvolvimento do planejamento estratégico, planejamento de TI e gestão de riscos. No mapa fatorial apresentado na Figura 13 se evidenciam as variáveis que permitem a análise entre os léxicos obtidos nas respostas dos entrevistados.

Figura 13: Planejamento Estratégico de TI – Planejar e organizar

Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na Figura 13 é 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, corroborando o que foi anteriormente explanado com os trechos das entrevistas, há uma preocupação com a participação dos usuários nos procedimentos vinculados ao planejamento estratégico e planejamento de TI.

Contudo, observa-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).

Outro aspecto de destaque na Figura 13 é a aproximação das variáveis: negócio, sistema, informações, e TI. Portanto, se evidencia que a área de TI na organização sinaliza uma integração entre os processos de negócio, colaborando com a percepção de Weill e Ross (2006), que salientam a necessidade de alinhamento da TI com os processos de negócio.

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:

- Investimento no último ano na implantação de um ERP totalmente integrado;
- Preparação de informações para divulgação a CVM e Investidores;
- Auditoria externa independente das informações contábeis e dos processos de TI;
- Implantação da gestão da mudança (modificações solicitadas são pré-aprovadas pelos usuários em um ambiente de teste);
- Atuação da Central de operações NOC (núcleo de operações e controle) que monitora todos os links e acessos;
- 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 a execução de processos inadequados pela TI, bem como o auxilio no monitoramento das ações relacionadas a manutenção de planos de ações de riscos.

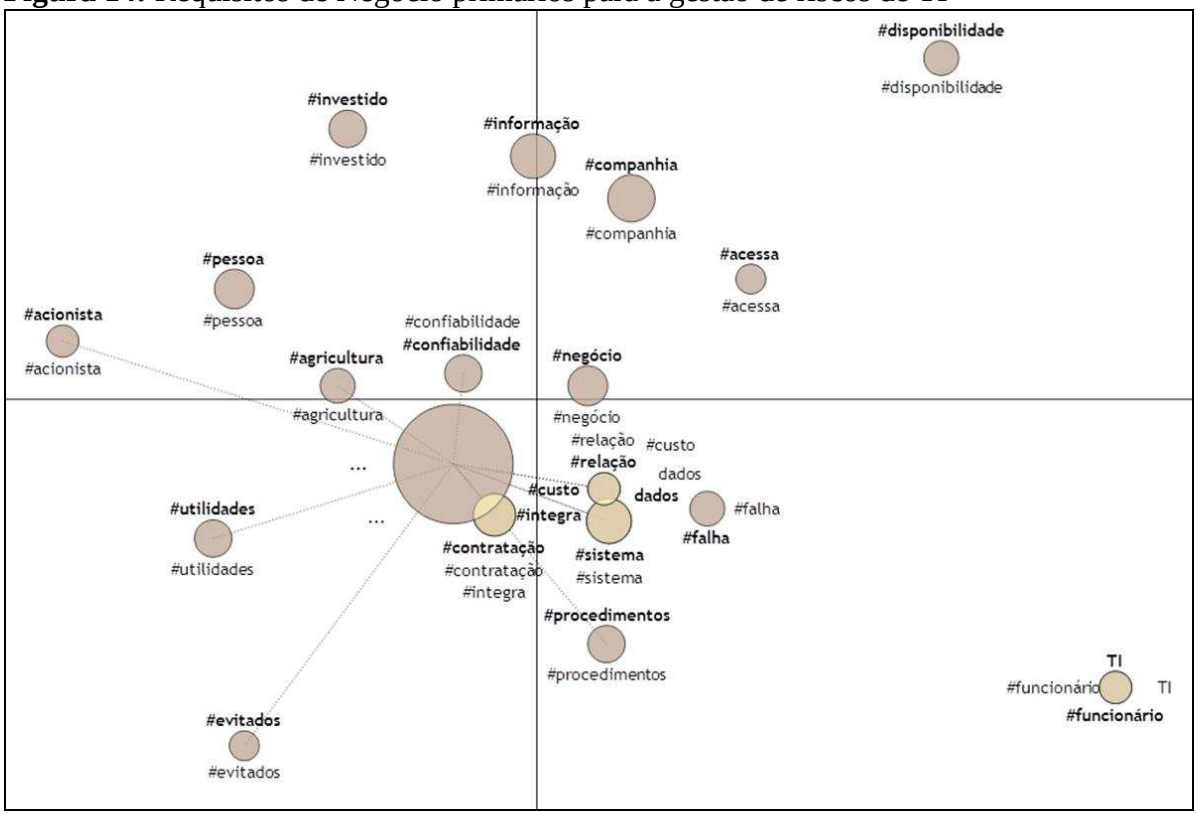
Foram identificadas adicionalmente em relação às ações para manutenção dos requisitos algumas vantagens para o caso de estudo, a saber:

- Redução de redigitações ou de reinformação de dados ao longo do processo, evitando a produção de informações errôneas;
- Melhora da confiança dos investidores nos números produzidos;
- Melhoria da segurança nos processos após utilização de sistema integrado;
- Disponibilidade da informação para acionistas de qualquer lugar do país; e
- Garantia da recuperação de informações em caso de possíveis perdas.

É identificado que tais vantagens decorrentes das ações implementadas demonstram a exigência da organização frente ao departamento de TI, afim de que o nível de serviços de TI busque redução de custo e tempo nos processos, colaborando com a percepção de LUCIANO e TESTA (2011).

A análise Léxica da categoria requisitos TI contemplou a percepção dos entrevistados sobre a forma que estes requisitos atuam na organização para redução dos riscos de TI. Na fala dos entrevistados o requisito disponibilidade foi o mais citado nas respostas que contemplavam estes requisitos.

Figura 14: Requisitos de Negócio primários para a gestão de riscos de TI



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na parte central do mapa fatorial apresentado na Figura 14, se evidenciam a aproximação entre as variáveis: negócio (processos de negócio), confiabilidade e custo. Desta forma, evidencia-se que a confiabilidade das informações pode ser obtida mediante melhoria nos processos de negócio, reduzindo assim os custos de manutenção das informações destes processos, por exemplo mediante redução das falhas ou erros.

Cabe destacar que além deste requisito (a confiabilidade) mediante a análise léxica identificou-se a variável disponibilidade como requisito frequente na fala dos entrevistados. Porém, este requisito não se mostrou próximo dos léxicos: investido (que remete a investimento), informação, companhia e acesso. Esta relação comprova a preocupação da companhia em investimentos para controle de acesso e disponibilidade de informações, como por exemplo, aqueles realizados em sistemas e *links,* para redução de seus riscos de TI.

Na categoria Investimentos em TI buscou-se identificar se estes foram realizados de forma suficiente para garantir informações corretas, precisas e disponíveis no tempo adequado. Neste aspecto, cabe destacar algumas percepções dos entrevistados:

> *[...] hoje está adequado, não é o melhor volume, com certeza tem oportunidades de haver mais investimentos. [...] Muitos investimentos continuam sendo feito em sistemas, e melhorias de sistemas, então com certeza ele cada vez mais protege a SLC Agrícola [...]* ***Coordenador de sistemas.***
>
> *[...] foram suficientes especialmente investimentos na questão da disponibilidade, a companhia optou por ter sistemas online, hoje todas as fazendas tem um link principal de rádio terrestre, um link de dados e um link de contingências por satélite, isto comprova o grande volume de investimento nesta questão. Estes investimentos geram maior conectividade entre as redes pra tornar disponíveis os sistemas para os usuários, inclusive àqueles que trabalham nas fazendas. [...]* ***Gerente Corporativo de TI.***
>
> *[...] Eu acho que a gente poderia melhorar um pouco ainda o investimento, por exemplo, em uma internet mais rápida, nos computadores melhores, em conexões mais modernas,para melhorar a comunicação. [...]* ***Membro do Comitê de Riscos.***

Identifica-se que os entrevistados atuantes na área de TI consideram os investimentos suficientes, estes objetivaram melhorias de sistemas e conectividade como protetores das informações. O membro do Comitê de riscos elencou a necessidade de investimentos em computadores e na comunicação (internet e conexões). A validação dos usuários dos recursos investidos segue o seguinte fluxo:

Fluxo da necessidade de Investimento: 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.

Adicionalmente foram citados exemplos de como os investimentos possibilitam proteger a empresa de riscos, os principais exemplos citados estão relacionados no Quadro 24. Estes investimentos foram justificados pela necessidade de se fornecer informações corretas e precisas em tempo adequado de acordo com a proposta de COHAN (2005), LUCHT, HOPPEN e MAÇADA (2007).

Quadro 24: Exemplos de investimentos que geram redução de riscos

ENTREVISTADO	EXEMPLO
Coordenador de Sistemas	Investimentos em sistemas possibilitam dados integrados, com muito mais agilidade nos fechamentos, realizar as apurações identificar falhas que por ventura acontecerem e consequentemente de ter mais agilidade, isso protege o negócio.
Gerente corporativo de TI	O investimento em torres transmissoras feito em casinhas de painel solar, com banco de baterias minimiza o risco de indisponibilidade naquele local /
Membro do Comitê de riscos	Os investimentos feitos em TI permitiram que as informações sejam corretas, e em tempo correto, de forma rápida, evitando riscos de divulgação das informações.

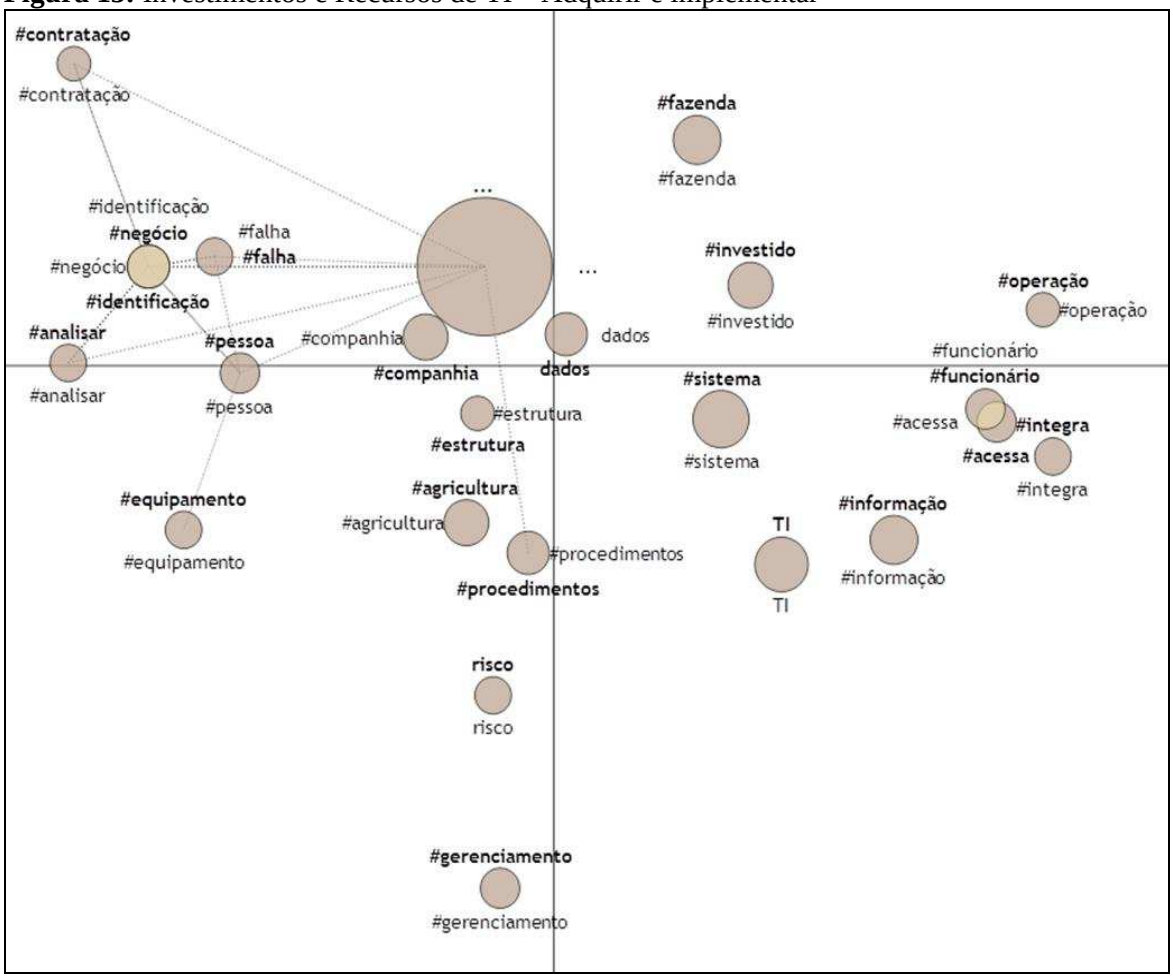
Fonte: Elaborado pela autora com base nas entrevistas

O investimento em sistema integrado também foi percebido na análise documental das demonstrações financeiras de 2011 da companhia, destacado como uma conquista naquele ano.

> *[...]* ***Conquistas importantes no ano:*** *implementação de um sistema operacional (ERP) que interligou todas as fazendas com a Matriz de forma on-line, aprimorando os nossos controles internos;. [...]* ***SLC (2012c).***

Para a categoria Investimentos em TI a análise léxica permitiu identificar a relação entre as variáveis selecionadas nas entrevistas mediante análise de conteúdo – AC. Esta análise possibilitou a geração do Mapa Fatorial apresentado na Figura 15.

Figura 15: Investimentos e Recursos de TI – Adquirir e implementar



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Ao analisar a Figura 15 é possível identificar uma aproximação com relativa significância entre as variáveis: falha, negócio (que remete a processos de negócio) e identificação. Desta forma evidencia-se a sinalização da necessidade de investimentos em processos de negócio para a identificação das falhas. Ao mesmo tempo esta identificação poderia contemplar análises quanto aos procedimentos adotados em tais processos, vislumbrando a manutenção dos requistos de negócio e a mitigação de riscos inerentes a tais processos. A falta de investimentos para redução de erros ou falhas pode acarretar em falhas no próprio sistema operacional ou nos controles internos, conforme alertado na literatura pelos autores: COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).

Contudo apesar de ter sido identificado investimento relevante pela companhia, principalmente em sistemas, foi identificado à necessidade de avaliações sobre ampliação de investimentos a procedimentos,processos de negócio, e controles internos.

Durante as entrevistas foram destacadas vantagens e desvantagem do uso da TI para a organização. Os principais pontos citados foram destacados a seguir:

Vantagens do uso da TI para a organização:

- Facilidade na integração de informações independente da localização geográfica;
- Disponibilização de informações para os controles dos negócios operacionais e análises estratégicas;
- Rapidez no processo de fechamento dos resultados;
- Agiliza controles internos;
- Possibilita cruzamento entre informações para melhores decisões;
- Uniformidade de informações;
- Padronização de alguns processos e controles;
- Possibilita acesso a conectividade com bancos, clientes, fornecedores e outras áreas internas dentro da fazenda.

Percebem-se nas vantagens as oportunidades no aproveitamento dos benefícios oferecidos pelo uso da TI, neste sentido a TI auxilia os negócios no caso estudado conforme destacado na literatura por ALBERTIN e ALBERTIN (2012).

Desvantagens do uso da TI para a organização:

- Quantidade de informações e interações necessárias para abastecer os sistemas;
- Cultura das pessoas relacionada a mudanças tecnológicas;
- Complexidade de uso de alguns recursos tecnológicos;
- O custo com treinamentos necessários para utilização dos recursos;
- Custo elevado para implantação e manutenção de novas tecnologias; e
- O engessamento de processos decorrentes de travas nos sistemas.

Cabe comparar as vantagens com as desvantagens encontradas no caso de estudo, relacionadas ao uso da TI. Ao mesmo tempo em que há a facilidade de integração, e disponibilização de informações, existe o custo com o volume de informações abastecidas nos sistemas. Outro aspecto a salientar é o custo elevado com novas tecnologias que geram rapidez nos fechamentos e agilidade nos controles internos.

A complexidade de uso de alguns recursos tecnológicos impulsiona outro aspecto negativo identificado, 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:

- Vazamento de informações confidenciais (por exemplo, preços e margens de lucro);
- As fraudes;
- A invasão de externos aos sistemas provocando instabilidade.

Como ações adotadas para prevenir estes riscos foram identificadas nas entrevistas:

- O controle de acessos externos aos sistemas;
- Treinamento dos funcionários em relação ao uso da TI;
- Restrição quanto ao uso do e-mail (correio eletrônico), controle de tamanhos e tipos de arquivos; e
- A criação de controles e políticas de acesso e uso dos recursos.

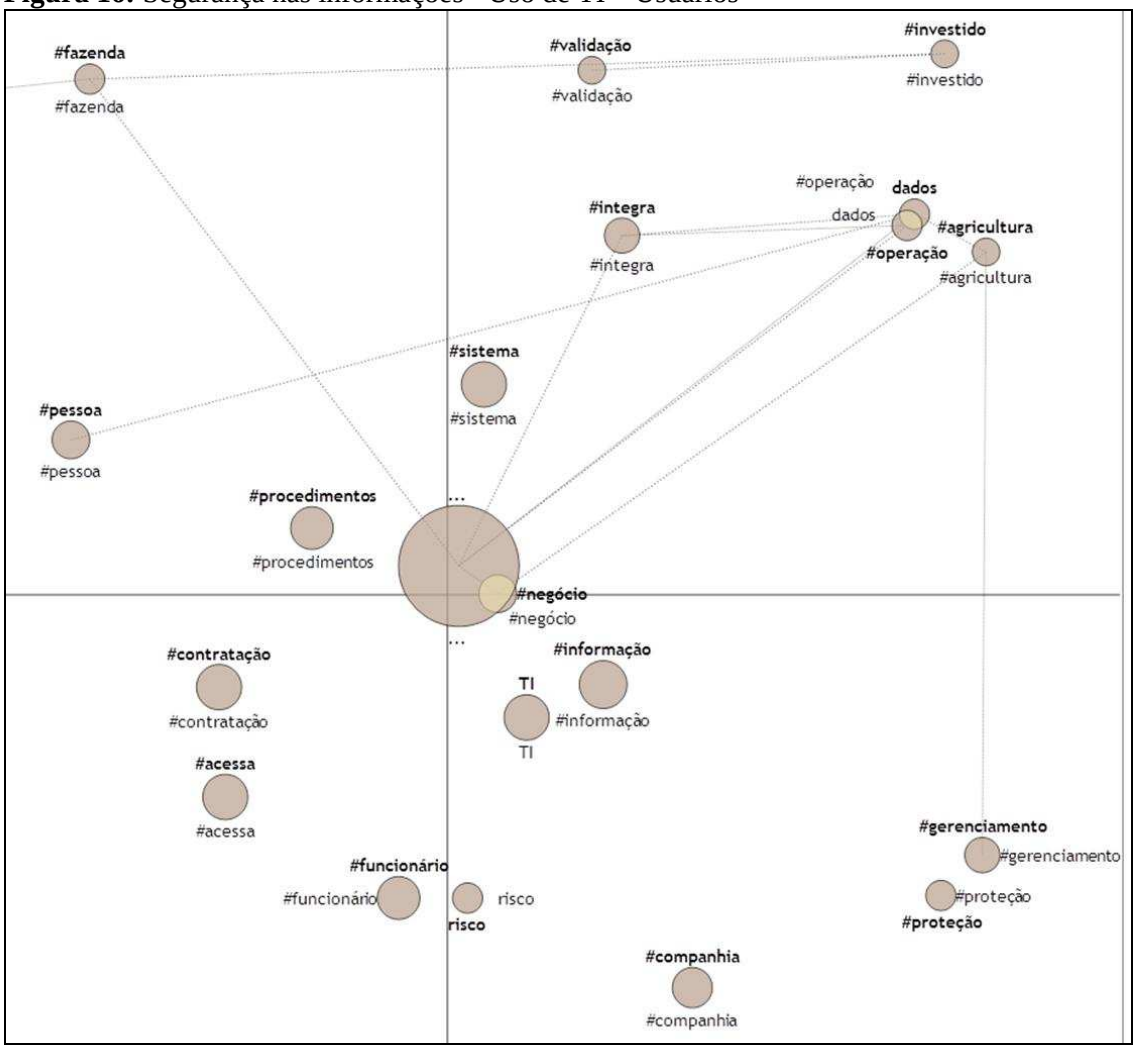
A criação de controles e políticas para a segurança das informações corrobora com a indicação de Bulgurcu, Cavusoglu e Benbasat (2010) no aspecto da participação dos usuários como aliados da organização nos esforços de reduzir os riscos. A gestão da informação pode ser eficaz quando aborda de forma integrada 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, esta foi citada 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 pelo caso de estudo, é identificada 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.. [...]* ***Coordenador de Sistemas.***

A análise Léxica da categoria: segurança nas informações, uso de TI e usuários, contemplou a percepção dos entrevistados sobre tais aspectos. No mapa fatorial apresentado na Figura 16 se evidenciam as variáveis que permitem a análise entre os léxicos obtidos nas respostas dos entrevistados.

Figura 16: Segurança nas informações - Uso de TI – Usuários



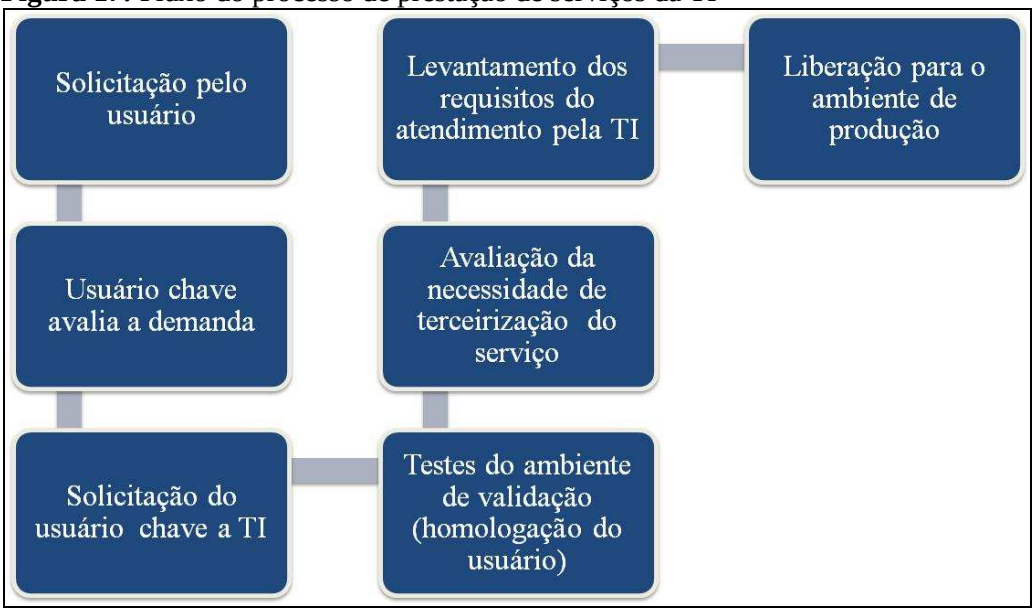
Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na Figura 16 identifica-se 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, afim 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 (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 levar 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.

Figura 17: Fluxo do processo de prestação de serviços da TI

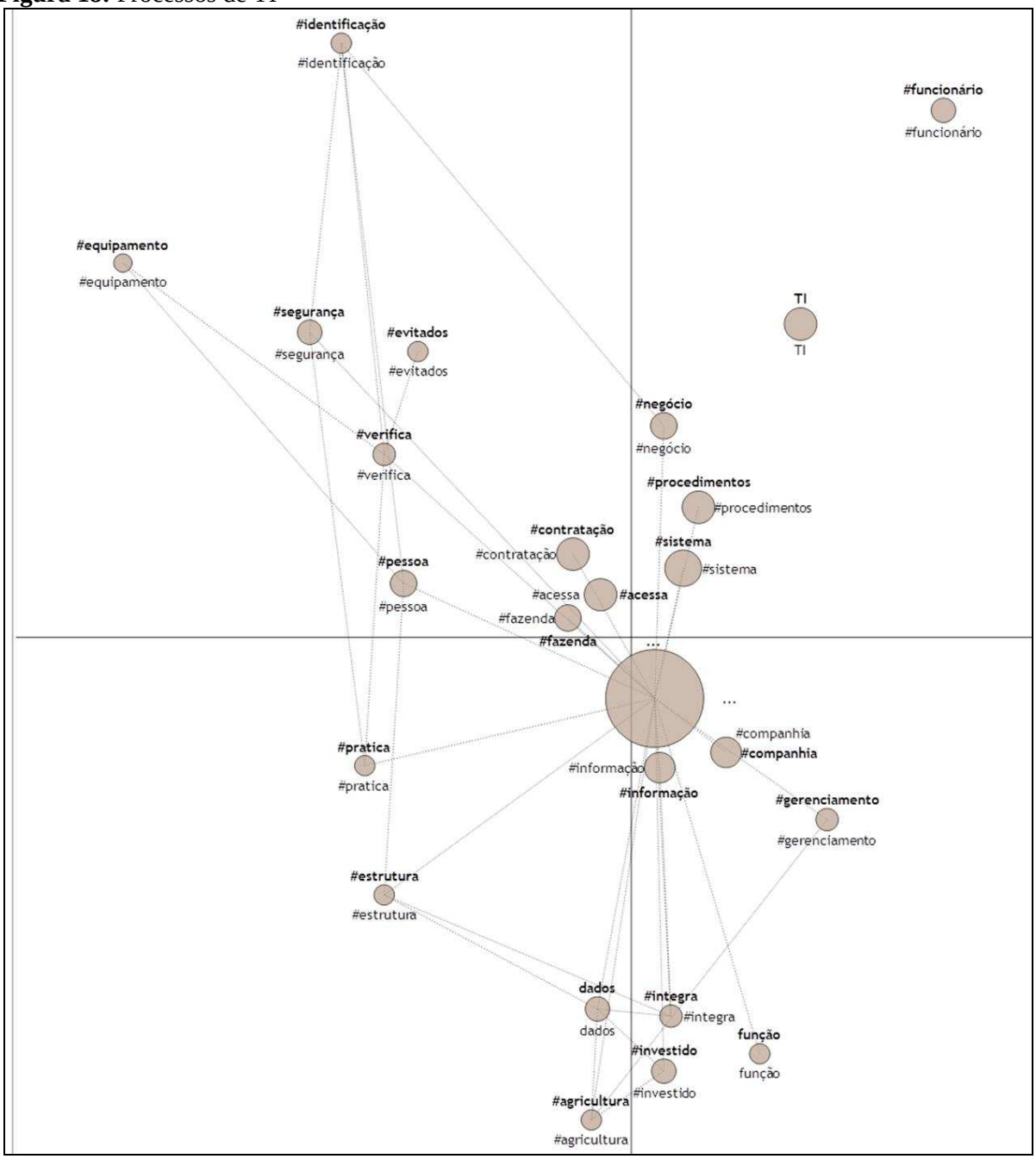


Fonte: Elaborado pela autora com base nas entrevistas

No fluxo de processo da prestação de serviços de TI é 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.

Na Figura 18 percebe-se, próximo ao ponto central do mapa fatorial obtido pela AC da categoria processos de TI, a forte relação entre os léxicos: informação, fazenda, acessa, sistema, companhia, procedimento, negócio, contratação e gerenciamento. Tais aspectos sinalizam a no caso de estudo a necessidade de um maior envolvimento dos usuários no processo de segurança das informações principalmente no acesso aos sistemas e recursos de TI utilizado nos processos das fazendas.

Figura 18: Processos de TI



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

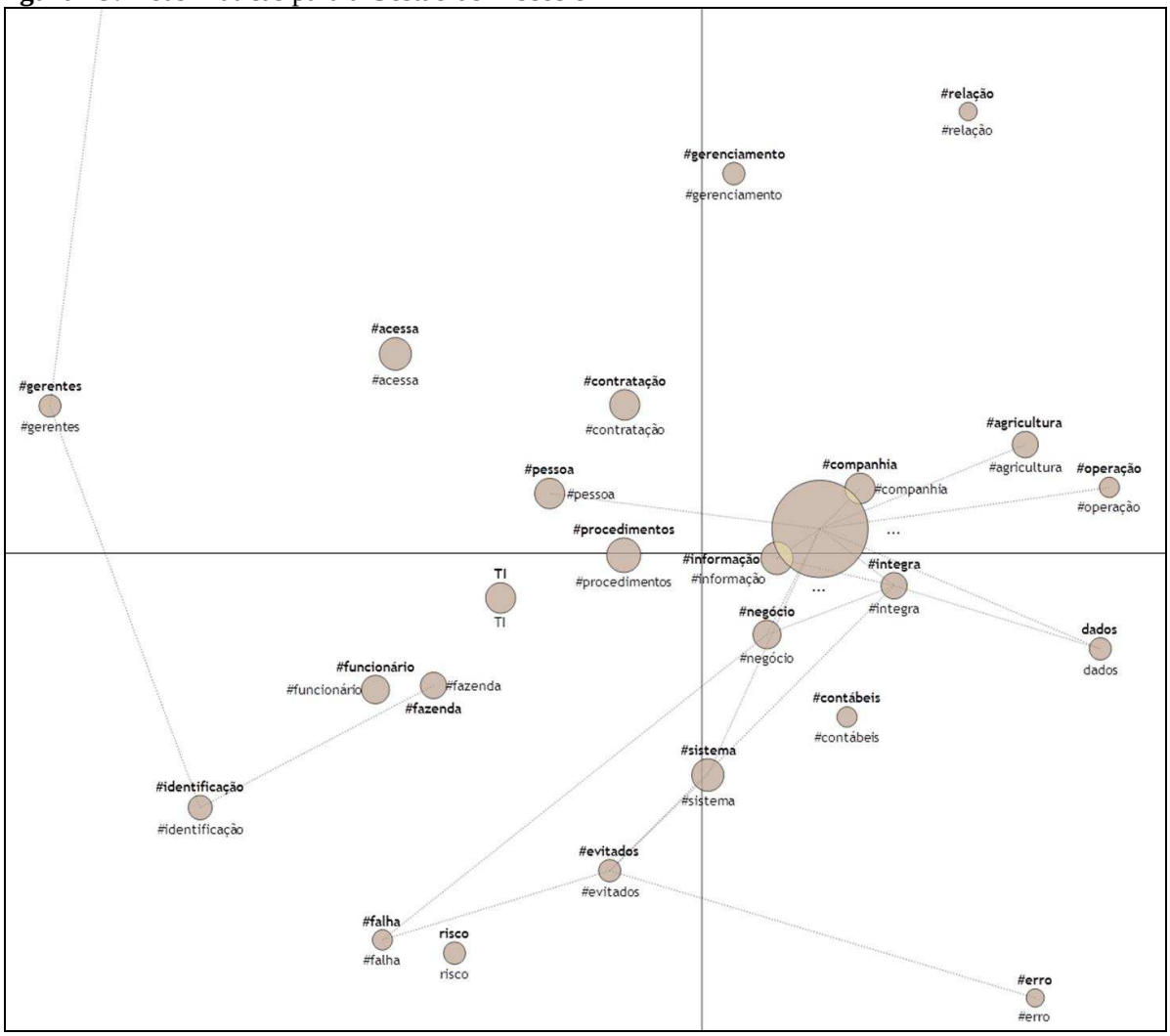
No que diz respeito aos processos de TI, apesar de ser identificada participação do usuário na homologação dos projetos realizados por TI (Figura 17), a participação destes nos processos de negócio vislumbrando o gerenciamento dos riscos de TI ainda carece de ampliação. Na Figura 18 isto se comprova, mediante visualização da relação entre as variáveis: pessoa (que remete a usuários), verifica e evitados (evitar riscos no ambiente de TI).

Os processos de TI contemplados pelo COBIT 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).

As boas práticas para a gestão de riscos em TI visam criar estratégias de mitigação para minimizar os riscos a níveis aceitáveis. A partir da visualização do mapa fatorial (Figura 19) evidenciam-se variáveis que permitem análises entre os léxicos relacionados às respostas dos entrevistados. Percebe-se por exemplo, a aproximação entre os léxicos: procedimento, acessa, funcionário, contratação, TI, Sistema e Informação.

Isto demonstra que no caso de estudo, 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 recomenta o ITGI (2007). Contudo, foi identificado que esta participação ainda precisa ser ampliada para haver uma disseminação de práticas que proporcionem redução efetiva de riscos.

Figura 19: Boas Práticas para a Gestão de Riscos em TI



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

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 internamento.

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. Na Tabela 1 é demonstrado o nível de maturidade selecionado por cada participante.

Tabela 1: Maturidade dos processos para avaliar e gerenciar riscos de TI

		Processos COBIT	Nível de maturidade					
			0 - Inexistente	1 - Inicial	2 – Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
Gerente de Sistemas	PO9.1	Alinhamento da gestão de riscos de TI e de Negócios		x				
	PO9.2	Estabelecimento do Contexto de Risco			x			
	PO9.3	Identificação de Eventos			x			
	PO9.4	Avaliação de Risco			x			
	PO9.5	Resposta ao Risco		x				
	PO9.6	Manutenção e Monitoramento do Plano de Ação de Risco		x				
Coordenador De TI	PO9.1	Alinhamento da gestão de riscos de TI e de Negócios		x				
	PO9.2	Estabelecimento do Contexto de Risco			x			
	PO9.3	Identificação de Eventos				x		
	PO9.4	Avaliação de Risco			x			
	PO9.5	Resposta ao Risco				x		
	PO9.6	Manutenção e Monitoramento do Plano de Ação de Risco		x				
Membro Comitê De Riscos	PO9.1	Alinhamento da gestão de riscos de TI e de Negócios		x				
	PO9.2	Estabelecimento do Contexto de Risco				x		
	PO9.3	Identificação de Eventos				x		
	PO9.4	Avaliação de Risco				x		
	PO9.5	Resposta ao Risco				x		
	PO9.6	Manutenção e Monitoramento do Plano de Ação de Risco			x			

Fonte: Elaborado pela autora com base nas respostas do questionário

Cabe destacar, que além de selecionar um nível de maturidade ilustrado na Tabela 1, os participantes explicavam o motivo desta escolha, a fim de que as análises realizadas contemplassem características qualitativas dos dados coletados, estas respostas foram evidenciadas no Apêndice E.

O alinhamento da gestão de riscos de TI (P09-1) ao negócio foi identificado segundo respostas de todos os entrevistados como 1-Inicial. Os gestores destacaram que a gestão de riscos de TI é realizada pela própria TI, sem conexão com a gestão de riscos da organização, coforme pode ser percebido no trecho seguinte, extraído do instrumento.

> *[...] No meu ponto de vista, os riscos de TI são avaliados de forma informal e quando solicitados em cada projeto sem haver maiores alinhamentos com a gestão de riscos da empresa. [...]* ***Coordenador de Sistemas.***
>
> *[...] A gestão de riscos de TI é feita pela Gestão de TI, enquanto a gestão de riscos da organização é feita pela área de RI (relação com Investidores) [...]* ***Coordenador de Sistemas.***
>
> *[...] Existe certo alinhamento entre riscos de TI e riscos de negócio, mas não muito formalizado [...]* ***Membro do Comitê de riscos.***

Dois dos questionados identificaram o estabelecimento do contexto de riscos (PO9.2) como 2- Repetitivo. Justificativas para esta escolha contemplam a abordagem algumas vezes superficial do contexto do risco. A identificação deste processo em estágio não evoluído prejudica o processo de mitigação dos riscos de TI já que o objetivo das avaliações e critérios de riscos não é estabelecido de forma ampla. Tais justificativas podem ser percebidas nos trechos seguintes, extraídos do Questionário respondido (Apêndice E).

> *[...] Quando definida a necessidade de definição e acompanhamento dos riscos inerentes ao projeto e/ou ações de negócio, existe uma abordagem superficial para identificação dos riscos, ações de mitigação, acompanhamento da efetividade das ações e readequação das ações de acordo com a necessidade e mudanças de cenário. [...]* ***Coordenador de Sistemas.***
>
> *[...] Em termos de risco de negócio, estão bem mapeados pela organização e há ações concretas. para mitigá-los. [...]* ***Membro do Comitê de riscos.***

A Identificação dos eventos (PO9.3), a Avaliação do Risco (PO9.4), e a resposta ao Risco (PO9.5) foram selecionada pela maioria como nível de maturidade 3-Definido. Segundo os respondentes os riscos-chaves podem ser identificados, mas a identificação através de procedimentos padronizados ainda não ocorre. Adicionalmente houve posicionamentos quanto a não existência de prática regular de avaliações de probabilidade e o impacto dos riscos, tampouco análise quanto à efetividade das ações de mitigação. Isto pode ser percebido nos trechos dos questionários respondidos (Apêndice E) abaixo listados.

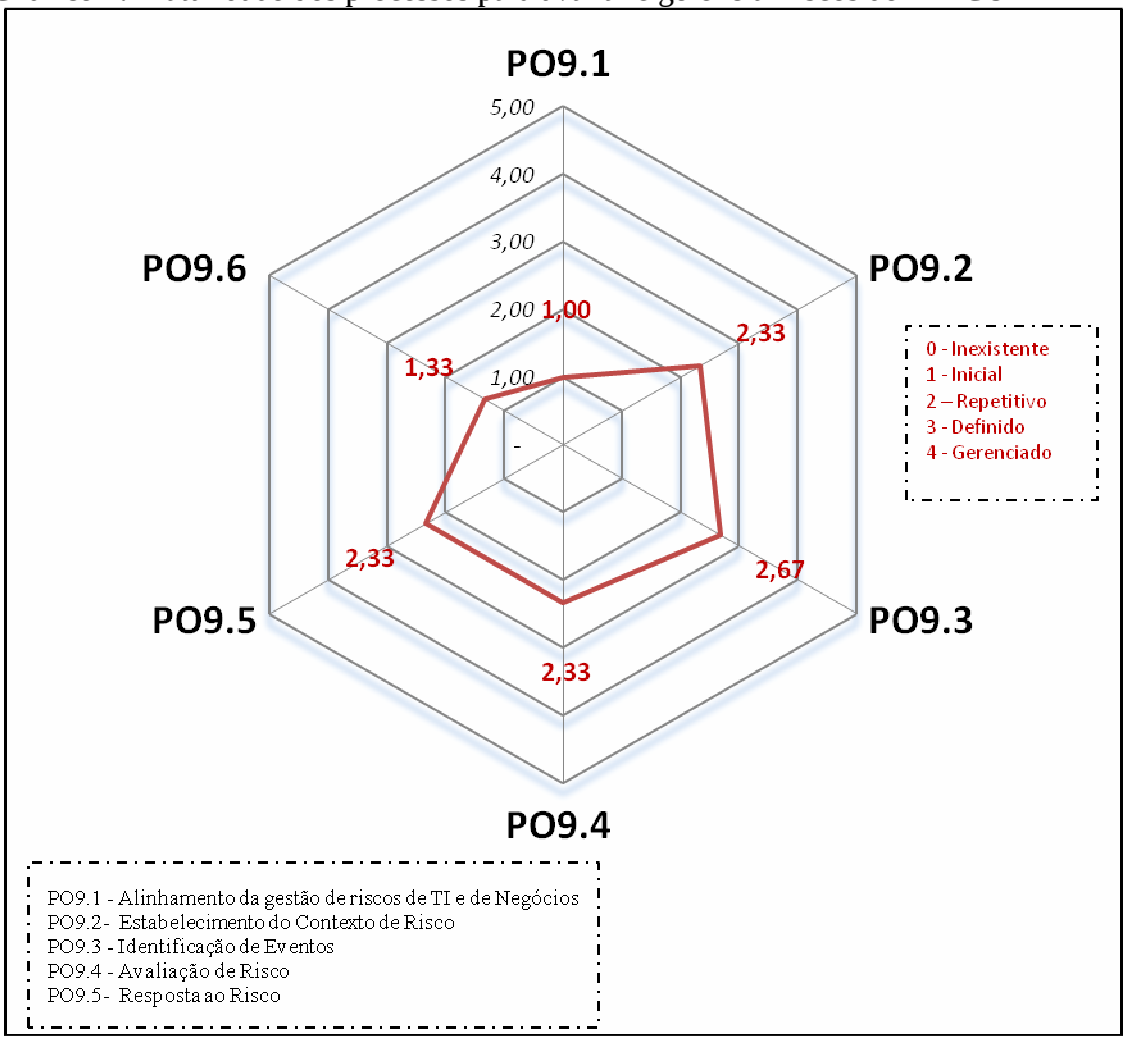
> *[...] No meu ponto de vista existe uma abordagem inicial e muitas vezes não muito aprofundada de avaliação de todos os riscos que envolvem as ações de projeto. Quando definida a necessidade de identificar os riscos, ainda não existe uma regularidade em avaliar a probabilidade e o impacto dos riscos, tampouco análise quanto à efetividade das ações de mitigação. Desconheço a existência de um processo de respostas a riscos nesta organização. [...]* ***Coordenador de Sistemas.***
>
> *[...] Existe uma boa identificação de eventos que possam ameaçar o bom funcionamento do negócio e a natureza e abrangência do impacto são bem mapeadas. Principalmente os riscos financeiros são mensurados em sua probabilidade e são delineados obedecendo a métodos quantitativos e qualitativos. Sim, entendo que existem respostas aos riscos e que há um processo para responder a eles. [...]* ***Membro do Comitê de riscos.***

O P09.6 que estabelece a Manutenção e Monitoramento do Plano de Ação de Risco, foi o quesito que mais gerou divergência de opiniões, estas permearam entre os níveis 0-Inexistente e 2-Repetitivo. O Coordenador de Sistemas desconhece a existência de processos para a manutenção e monitoramento dos planos de TI.

O Gerente de TI não justificou sua opinião, e o Membro do Comitê de Riscos entende que existem atividades de controle, no entanto não em todos os níveis da organização. Provavelmente estas divergências de opiniões estão associadas ao contato que cada um tem com ações que foram desenvolvidas para gerenciamentos dos riscos. Enquanto o coordenador de sistemas tem suas atividades mais voltadas a aspectos operacionais de TI o Membro do Comitê participa das decisões que envolvem os principais riscos. Neste sentido caberia um envolvimento maior de todos os gestores neste processo, concordando com a sugestão do COBIT, (ITGI, 2007).

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

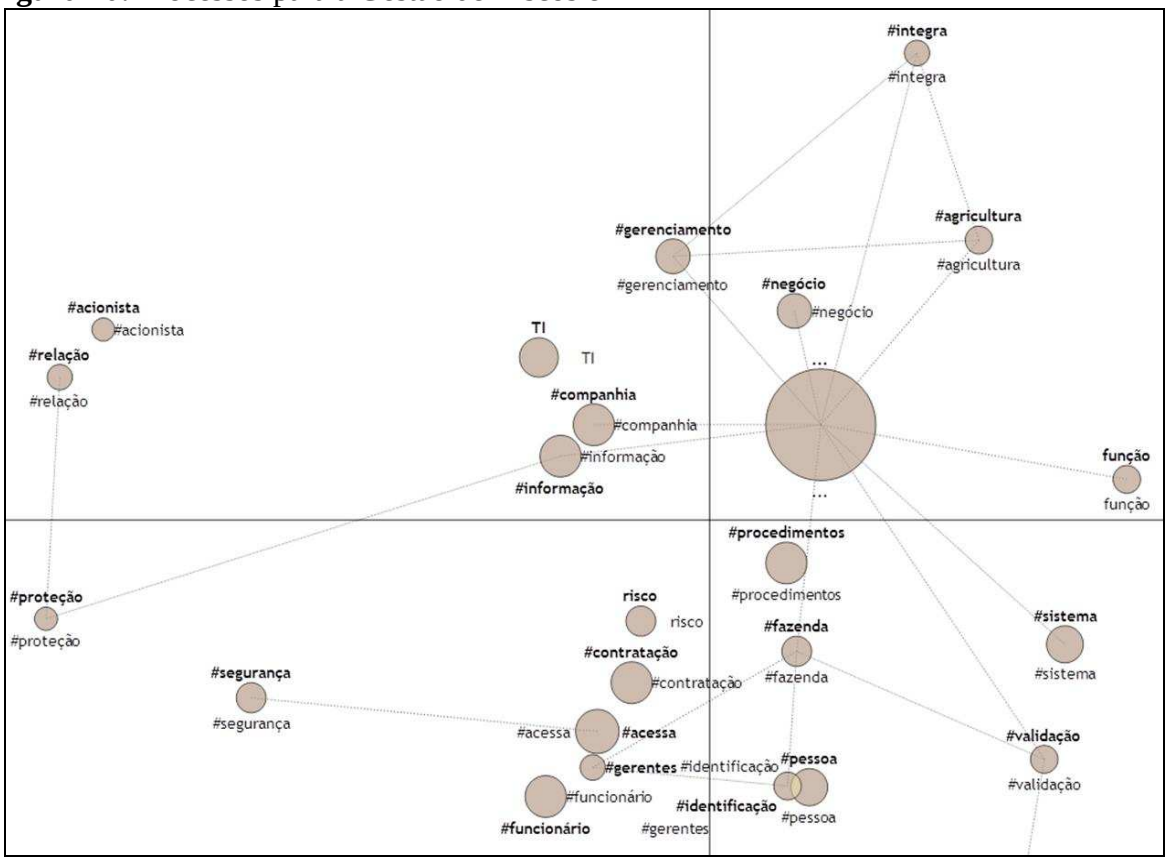


Fonte: Elaborado pela autora com base nas respostas do questionário

Para o ITGI (2007) O gerenciamento do processo de avaliar e gerenciar dos riscos de TI deve satisfazer aos requisitos do negócio para a TI, identificando assim os riscos de TI e seus potenciais impactos nos processos e objetivos de negócio. Esta recomendação da literatura foi analisada no caso de estudo a partir da visualização do mapa fatorial (Figura 20) no qual se evidenciam variáveis que permitem análises entre os léxicos relacionados às respostas dos entrevistados. Por exemplo, na relação entre os léxicos: informação, proteção e companhia, que possivelmente evidenciam a preocupação dos entrevistados com a integridade e confidencialidade das informações.

Cabe destacar a aproximação entre os léxicos: procedimento, fazenda e pessoa (que remete a usuários) demonstrando a identificação da preocupação com os riscos decorrentes dos procedimentos adotados pelos usuários nas atividades operacionais da companhia (realizadas nas fazendas).

Figura 20: Processos para a Gestão de Riscos em TI

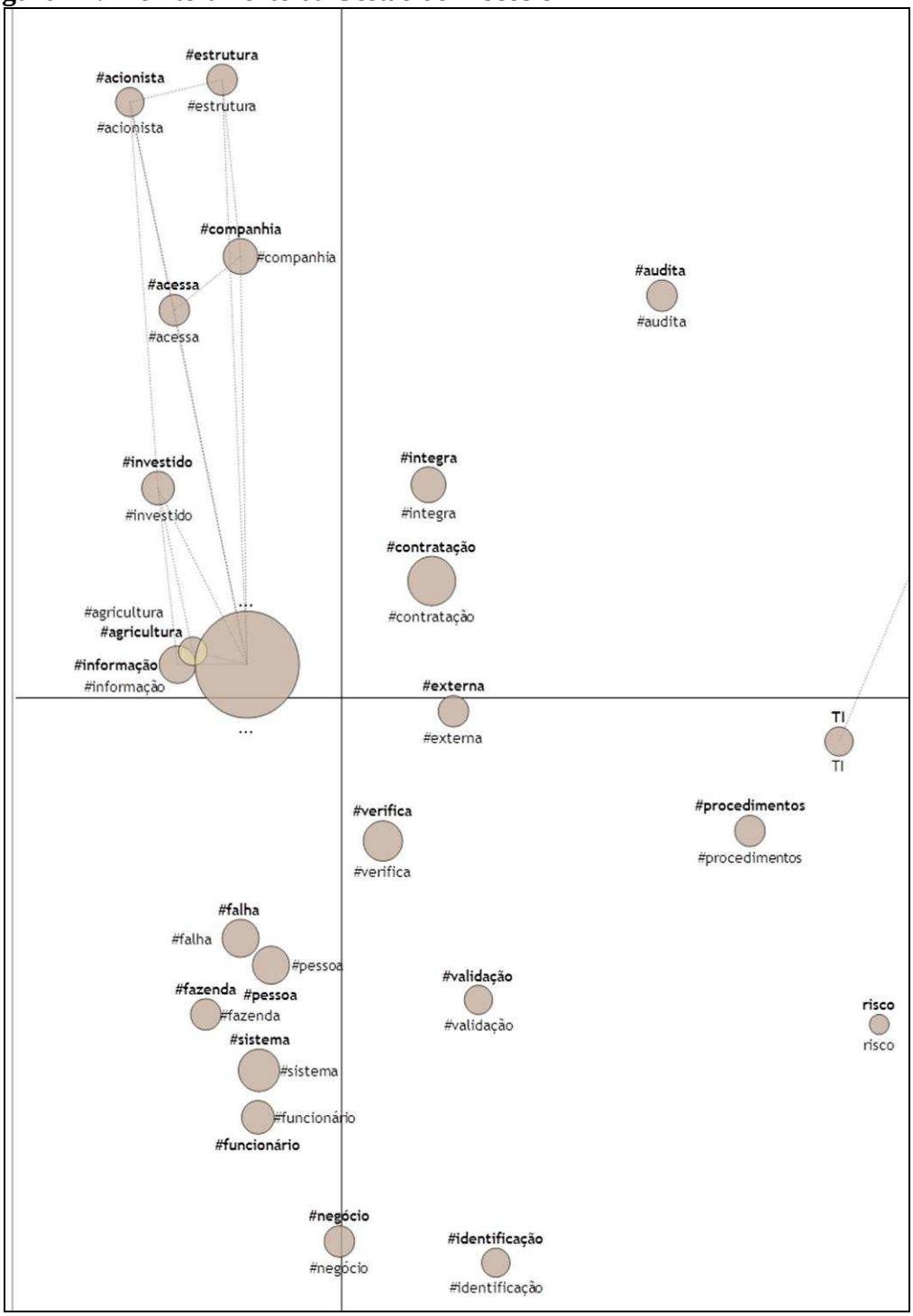


Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Outro aspecto a salientar na análise da Figura 20 é a existência dos léxicos: identificação (que remete a identificação dos riscos), pessoa (ilustra usuários) e gerentes. Este é um dos processos existentes na GRTI e contemplado no PO9.3 do COBIT, percebe-se que este foi o mais presente na análise dos níveis de maturidade do COBIT, segundo respostas do questionário e aparece em destaque agora na análise das falas dos entrevistados. Este fator demonstra uma forte preocupação dos entrevistados com o processo de identificação dos riscos de TI, e a participação os usuários neste processo.

Na análise léxica da categoria Monitoramento da Gestão de riscos em TI as variáveis foram identificadas mediante análise de conteúdo, sendo possível a obtenção do mapa fatorial apresentado na Figura 21.

Figura 21: Monitoramento da Gestão de Riscos em TI



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na análise da Figura 21 destaca-se a relação com forte significância das variáveis acionista, estrutura, companhia, acessa e informação. Mediante esta relação é identificado que a estrutura para monitoramento de riscos de TI esta mais centrada no controle de acesso das informações, fator comprovado pela política de RH (relacionada a novos usuários), ou a fechamentos de acessos de controles externos.

A aprovação e controle destes monitoramentos pouco contempla o monitoramento de planos e reporte de desvios a alta direção (neste caso representado nos léxicos pelos acionistas). Neste sentido identificou-se a falta de integração entre a gestão de riscos de TI (gestada no ambiente de TI) e o Comitê de riscos.

No Quadro 25 é apresentada uma análise consolidada dos principais achados obtidos neste estudo sobre o tema gestão de riscos em TI. Cabe salientar que a primeira coluna do Quadro 25 corresponde as categorias relativas a gestão de riscos em TI, identificadas no *Framework* metodológico (Quadro 17).

Quadro 25: Principais achados da gestão de riscos em tecnologia da informação (TI)

GESTÃO DE RISCOS EM TI	PRINCIPAIS ACHADOS			
	Entrevistas		**Questionário**	**Análise dos documentos**
Planejamento estratégico de TI – Planejar e organizar	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	Segurança, investido (que remete a investimentos em TI), pessoa (usuários), procedimentos, ERP, estratégia, companhia e mercado	Não localizado	Não localizado
Requisitos de negócio (confidencialidade, Integridade, disponibilidade) primários para a gestão de riscos em TI	1) Ações como: Investimentos em ERP, Auditoria externa, e atuação da central NOC (núcleo de operações e controle) proporcionam a manutenção dos requisitos; 2) Foram identificadas vantagens decorrentes das ações para manutenção dos requisitos que atuam para redução de custos e tempo nos processos de negócio. 3) evidencia-se que a confiabilidade das informações pode ser obtida mediante melhoria nos processos de negócio, reduzindo assim os custos de manutenção das informações destes processos, por exemplo mediante redução das falhas ou erros; e 4) Identificou-se a preocupação da companhia em investimentos para controle de acesso e disponibilidade de informações, como por exemplo, investimentos em sistemas e links, para redução de seus riscos de TI.	Negócio (processos de negócio), confiabilidade, disponibilidade, custo, investido (investimento), informação, companhia e acesso	Não localizado	Não localizado
Investimentos e Recursos de TI – Adquirir e implementar	1) Foram identificados investimentos que visam proteger a empresa de eventuais riscos, principalmente em melhoria de sistemas e conectividade; 2) Os investimentos contemplam a participação dos usuários na etapa de validação; 3) Os investimentos em TI foram justificados pela necessidade de informações corretas e precisas em tempo adequado; 4) Os principais riscos relacionados aos investimentos foram relacionados a falhas e erros, 5) foi identificado à necessidade de avaliações sobre ampliação de investimentos em TI relacionados a procedimentos, processos de negócio, e controles internos.	Falha, negócio (que remete a processos de negócio) e identificação.	Não localizado	O investimento em sistema integrado foi identificado análise documental das demonstrações financeiras de 2011 da companhia, destacado como uma conquista naquele ano.

GESTÃO DE RISCOS EM TI	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Segurança nas informações - Uso de TI – Usuários	1) Identificou-se vantagens e desvantagens decorrentes do uso da TI. Destacando-se a facilidade de integração, e disponibilização de informações, rapidez nos fechamentos e agilidade nos controles internos, o custo com o volume de informações abastecidas nos sistemas,custo elevado com novas tecnologias, e em treinamentos. 2) Foram identificados riscos relacionados ao uso da TI como: vazamento de informações confidenciais, fraudes, invasão de externos aos sistemas provocando instabilidade. 3) Foram percebidas ações para prevenir os riscos dentre elas: controle de acessos externos aos sistemas, treinamento dos funcionários em relação ao uso da TI, restrição quanto ao uso do e-mail, controle de tamanhos e tipos de arquivos; e criação de controles e políticas de acesso e uso dos recursos de TI. 4) Foi identificada a participação dos usuários na adoção dos planos de segurança porém a participação dos usuários em nos processos de TI precisa ser mais efetiva, principalmente relacionada aos usuários das fazendas (unidades produtivas) para mitigar os riscos de TI e proporcionar o uso eficiente dos recursos	Pessoa (usuários), operação, dados, agricultura e integra (integração), Sistema, TI.	Não localizado	Não localizado
Processos de TI – Entrega e suporte	1) Foi identificada a participação dos usuários no processo de homologação das solicitações a TI, porém esta participação não se confirma na elaboração de processos e planos ou soluções para remediação de riscos.	Informação, fazenda (unidades produtivas) , acessa, sistema, companhia, procedimento, negócio, contratação e gerenciamento	Não localizado	Não localizado
Boas Práticas para Gestão Riscos em TI	1) 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, porém esta participação ainda precisa ser ampliada para haver uma disseminação de práticas que proporcionem redução efetiva de riscos; 2) Não foi identificado no caso de estudo uma estrutura de gerenciamento de riscos de TI integrada a estrutura corporativa de gerenciamento de riscos	Procedimento - Acessa - Funcionário - Contratação - TI - Sistema e Informação	Não localizado	Não localizado

GESTÃO DE RISCOS EM TI	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Processos de controle para a gestão dos riscos de TI (estabelecimento do contexto, identificação, avaliação, resposta, manutenção e monitoramento)	1) Identificou-se uma forte preocupação dos entrevistados com o processo de identificação dos riscos de TI, e a participação os usuários neste processo. 2) Identificou-se que a gestão de riscos de TI é realizada pela própria TI, sem conexão com a gestão de riscos da organização, sendo a avaliação dos riscos realizada de forma desestruturada; 3) Identificou-se que os riscos-chaves de TI são identificados, mas a identificação através de procedimentos padronizados ainda não ocorre. Adicionalmente houve posicionamentos quanto a não existência de prática regular de avaliações de probabilidade e o impacto dos riscos, tampouco análise quanto à efetividade das ações de mitigação.	Procedimento, fazenda, identificação (que remete a identificação dos riscos), pessoa (ilustra usuários) e gerentes	1) O alinhamento da gestão de riscos de TI (P09-1) ao negócio foi identificado como 1-Inicial, como justificativa identificou-se que a gestão de riscos de TI é realizada pela própria TI, sem conexão com a gestão de riscos da organização. 2) o estabelecimento do contexto de riscos (PO9.2) foi classificado como 2- Repetitivo A identificação deste processo em estágio não evoluído prejudica o processo de mitigação dos riscos de TI já que o objetivo das avaliações e critérios de riscos não é estabelecido de forma ampla; 3) A Identificação dos eventos (PO9.3), a Avaliação do Risco (PO9.4), e A Resposta ao Risco (PO9.5) foram selecionada pela maioria como nível de maturidade 3-Definido	Não localizado
Monitoramento da gestão de TI	1) Houve um desconhecimento por parte dos entrevistados da existência de processos para a manutenção e monitoramento dos planos de TI, 2) A aprovação e controle de monitoramentos pouco contempla o monitoramento de planos e reporte de desvios a alta direção. Neste sentido identificou-se a falta de integração entre a gestão de riscos de TI (gestada no ambiente de TI) e a atuação Comitê de riscos. 3) Adicionalmente foi identificada a participação dos usuários nos processos de TI e no gerenciamento do risco de TI, porém esta carece de um maior envolvimento dos usuários no gerenciamento e na efetiva participação no monitoramento dos controles gerando assim maior consciência ao risco	Acionista, estrutura, companhia, acessa e informação	A manutenção e monitoramento do Plano de Ação de Risco permearam entre os níveis 0-Inexistente e 2-Repetitivo. Neste sentido caberia um envolvimento maior de todos os gestores neste processo, bem como uma formalização deste.	Não localizado

Fonte: Elaborado pela autora (2012)

Nesta seção foi analisada a gestão dos riscos de TI no caso de estudo. Destas análises cabe destacar que a companhia adota ações para o gerenciamento destes riscos,como planos de segurança e investimentos em estrutura. Apesar disto, estas ações foram vistas como isoladas, dentro do próprio ambiente de TI.

Adicionalmente foi identificada a participação dos usuários nos processos de TI e no gerenciamento do risco de TI, 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). Na próxima seção a análise da gestão dos riscos corporativos foi realizada.

4.4. GESTÃO DOS RISCOS CORPORATIVOS

Esta seção aborda análises quanto à gestão dos riscos corporativos contemplando: a avaliação estratégica do risco, a perda de recursos, identificação de eventos, inter-relação entre os tipos de riscos, princípios para a gestão de riscos corporativos, estrutura para a gestão dos riscos, os processos para a gestão de riscos e a conscientização e resposta ao risco.

O primeiro aspecto a ser descrito é a avaliação estratégica do risco. Neste sentido a organização realiza a avaliação dos seus riscos de duas formas. Mediante atuação no comitê de riscos (riscos estratégicos e financeiros), e mediante avaliação nas diferentes áreas (riscos operacionais). Não foi identificada uma avaliação estratégica integrada de todos os tipos de riscos corporativos. Esta análise pode ser evidenciada nas palavras dos entrevistados.

> *[...] Cada área faz a sua parte, por exemplo, a área financeira trata os riscos através do comitê de riscos, preocupando-se com todas as questões financeiras.[...] O comitê de riscos está mais pros vieses financeiros, do que para os outros itens de riscos, eles são tratados dentro das suas áreas, não existe uma estratégia integrada. [...]* ***Membro do Comitê de Riscos.***
>
> *[...] Existe o comitê de riscos que se reúne semanalmente, tenho informação que anualmente a empresa tem planejamento estratégico, onde há reuniões e análises que contemplam todas as ameaças, as oportunidades e os pontos relacionados ao mercado... [...]* ***Coordenador de Sistemas.***

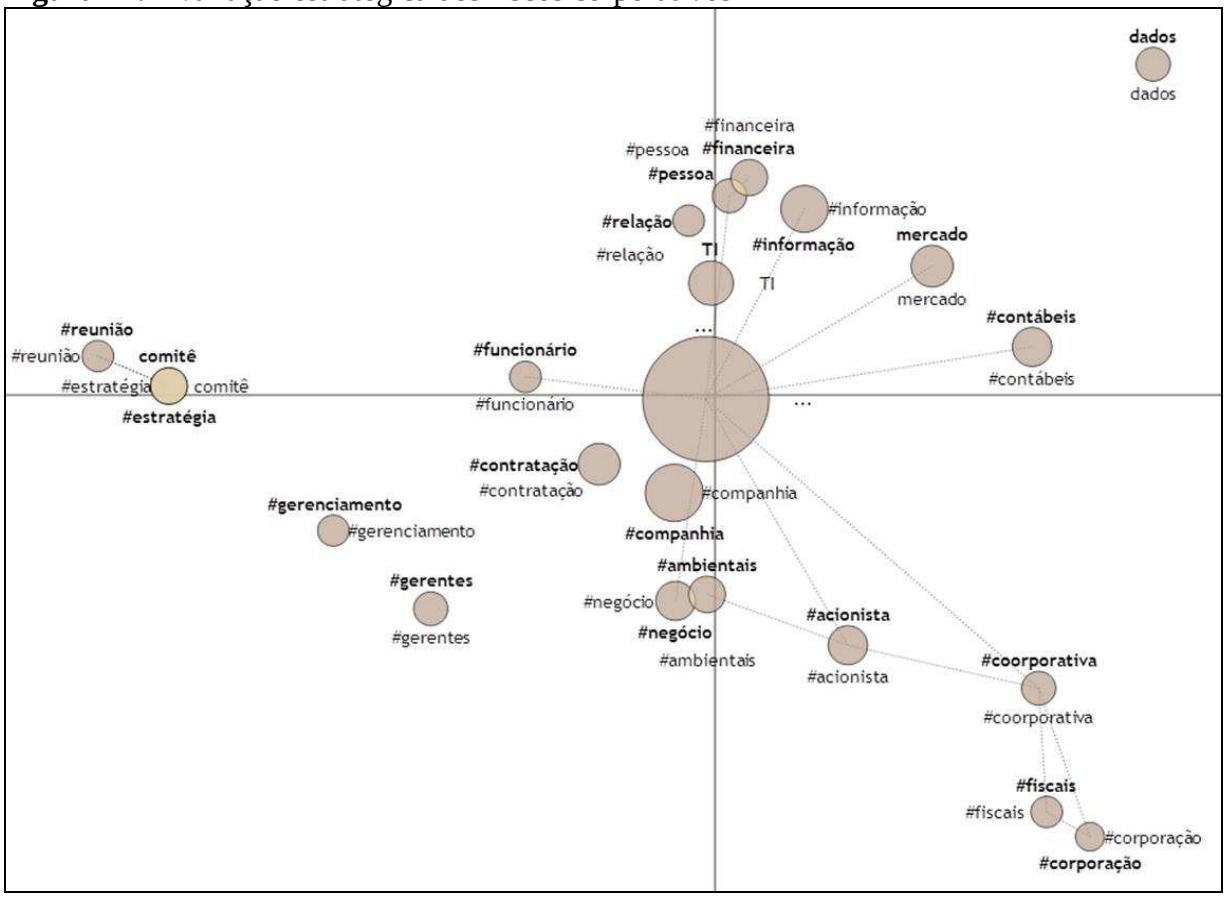
> *[...] Eu sei que a empresa se preocupa muito em proteger principalmente o aspecto financeiro e caixa. Como trabalhamos muito com exportação, somos afetados pela variação de dólares e outras moedas, neste sentido são realizadas algumas proteções... [...]* ***Gerente Corporativo de TI.***

Os trechos anteriores, extraídos da transcrição da entrevista com os Gestores, reiteram as afirmações realizadas anteriormente.

Para Frigo e Anderson (2011), a avaliação estratégica do risco pode complementar e alavancar a execução de processos em uma organização, ocasionando a melhoria da governança. Os entrevistados afirmaram concordar com esta percepção encontrada na literatura, afirmando que esta avaliação permite melhorar a governança, bem como as relações com o mercado, proporcionando melhores negócios e por consequência a melhores resultados.

A Figura 22 identifica as variáveis mais frequentes na análise léxica da categoria avaliação estratégica dos riscos corporativos.

Figura 22: Avaliação estratégica dos riscos corporativos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na Figura 22 é identificada a aproximação entre os léxicos: TI, financeira (que remete a informações financeiras), informação, mercado e contábeis. Tais aspectos estão relacionados à avaliação dos riscos corporativos para divulgação de informações contábeis financeiras ao mercado.

Outro aspecto de destaque é a relação de significância entre as variáveis: reunião, comitê e estratégia, bem como o afastamento destas do eixo principal do mapa e das demais variáveis. Desta relação se evidencia que a avaliação estratégica dos riscos ocorre no caso de estudo, mas não da forma integrada, existindo espaços para melhorias neste aspecto.

A perda de recursos, pode ser evitada mediante gerenciamento eficiente dos riscos permitindo que a organização minimizar seus impactos negativos que ocasionam a perda de recursos (custos ou prejuízos associados). Os entrevistados afirmaram concordar que o gerenciamento eficiente destes riscos possibilita evitar a perda de recursos, esta afirmação pode ser percebida na fala do gerente corporativo de TI e do Membro do Comitê de riscos conforme trecho seguinte extraído da transcrição das entrevistas.

> *[...] O gerenciamento pode minimizar os custos. Hoje não se tem conhecimento na organização de grandes confirmações de riscos e impactos negativos, o risco é probabilidade que a empresa tem, neste sentido nas nossas atividades não temos confirmação de que algum tipo de risco a empresa não tomou devidas precauções, não tomou cuidado e aconteceu, ele se efetivou com prejuízos graves associados. [...]* ***Gerente corporativo de TI.***
>
> *[...] Eu acho que, com certeza quanto melhor a gente construir formas de controles de riscos, melhor vamos conseguir evitá-los e minimizá-los. Por exemplo, já tivemos alguns problemas em algumas fazendas de abrir uma área para plantar que não poderia ter aberto, porque deveria ser uma reserva ou alguma coisa assim, então se tivesse um controle, um treinamento melhor dos funcionários das fazendas, esses tipos de riscos poderiam ser evitados, faltou de certa forma um controle que poderia ser mais eficaz. [...]* ***Membro do comitê de Riscos.***

Na percepção do Gerente Corporativo de TI não houve conhecimento de grandes eventos que pudessem causar um impacto negativo eminente com prejuízos graves associados. Já o membro do Comitê de riscos cita um exemplo de problemas ligados ao desflorestamento que gerou um impacto negativo. Apesar discordarem neste aspecto de existirem eventos, ambos citaram em suas arguições que o controle e gerenciamento destes riscos podem evitar perdas, corroborando com a percepção dos autores (IBGC (2007); COSO (2007); ISO 31000 (2009); AVEN (2011); GERIGK E CORBARI (2011)) sobre a gestão de riscos ser capaz de evitar perdas, acidentes e catástrofes associadas.

A Figura 23 identifica as variáveis mais frequentes na análise léxica da categoria perda de recursos (custos ou prejuízos associados) dos riscos corporativos.

Figura 23: Perda de recursos (custos ou prejuízos associados) a riscos corporativos

Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na Figura 23 é possível observar a aproximação entre as variáveis: negócio, investido (que remete a investimentos em TI), conselheiros, proteção e oportunidade. Desta aproximação pode ser identificado que existem oportunidades de melhorias na proteção do negócio, como por exemplo os investimentos em tecnologias para gerenciamento e por consequência redução de impactos negativos decorrentes de riscos estratégicos, financeiros e operacionais hoje não gerenciados, como por exemplo os riscos sociais.

A identificação de riscos pela companhia foi evidenciada na análise documento mediante os fatores de riscos listados em seu canal de relação com o investidor. A organização procura alertar aos seus investidores o impacto que tais fatores podem gerar nos negócios da companhia. Dividindo estes fatores em: a) Relacionados ao Setor Agrícola e Negócios da empresa; b) Relacionados ao Brasil; e c) Relacionados às ações da Companhia.

As informações detalhadas sobre estes riscos corporativos são identificadas no Quadro26.

Quadro 26: Fatores de Riscos Relevantes identificados na SLC.

Riscos Relacionados ao Setor Agrícola e aos Negócios da SLC Agrícola	Riscos Relacionados ao Brasil	Riscos Relacionados às Ações da Companhia
• Variações climáticas poderão impactar negativamente a produção e seus resultados. • A dependência do comércio internacional, a flutuação dos preços dos produtos agrícolas e flutuações no valor do real em relação ao dólar poderão prejudicar o desempenho financeiro da Companhia e os seus resultados operacionais. • Pragas ou doenças poderão prejudicar as colheitas e afetar os seus resultados e a sua imagem. • A produção é vendida para poucos clientes, com forte poder de negociação. • A SLC Agrícola pode enfrentar dificuldades na implementação de projetos de investimento, o que poderá afetar o seu crescimento. • A deficiência de logística de transporte, armazenamento e de processamento no Brasil constitui fator importante para expansão imobiliária agrícola futura, e a Companhia não pode garantir que conseguirá obter logística de transporte, armazenamento e de processamento eficiente para que sua produção chegue até os principais mercados de modo eficaz em termos de custo, ou em absoluto. • **A política de controle de riscos da SLC Agrícola pode não ser suficiente para cobrir eventuais riscos.** • A agricultura é uma atividade sazonal, o que pode ter um efeito adverso sobre as receitas da Companhia e os seus resultados. • A SLC Agrícola está sujeita a ampla regulamentação ambiental. • A Companhia está sujeita à ocorrência de incêndios e outros sinistros que poderão afetar as suas propriedades, a sua produção e os resultados da SLC Agrícola.	• O Governo Federal exerce influência significativa sobre a economia brasileira. Essa influência, bem como a conjuntura econômica e a política brasileira, poderá vir a causar um efeito adverso relevante nas atividades da SLC Agrícola, nos seus resultados operacionais e no preço de mercado das suas ações ordinárias. • A inflação e certas medidas tomadas pelo Governo Federal para combatê-la, incluindo aumentos nas taxas de juros, poderão contribuir para a incerteza econômica no Brasil, e podem gerar um efeito adverso relevante sobre a condição financeira da Companhia, seus resultados operacionais e o preço de mercado de suas ações. • A volatilidade do real em relação ao dólar pode ter um efeito adverso relevante sobre a SLC Agrícola e sobre o preço de mercado de suas ações. • Oscilações das taxas de juros poderão provocar efeito prejudicial no negócio da Companhia e nos preços de mercado das suas ações. • Acontecimentos e a percepção de riscos em outros países, especialmente em países de economia emergente, podem prejudicar o preço de mercado dos valores mobiliários brasileiros, incluindo as ações da SLC Agrícola.	• Um mercado ativo e líquido para as ações da SLC Agrícola pode não se desenvolver, limitando a possibilidade de venda daquelas ações pelo investidor. • A venda de número significativo de ações da Companhia pode afetar de maneira adversa o preço dessas ações ordinárias e a emissão de novas ações diluirá todos os demais acionistas. • A SLC Agrícola pode optar por não pagar dividendos aos seus acionistas. • A Companhia pode vir a obter capital adicional no futuro por meio da emissão de ações, o que poderá resultar numa diluição da participação de investidores na Companhia. • A SLC Agrícola possui controladores, que são uma família, cujos interesses poderão diferir daqueles de outros acionistas. • O Estatuto Social da Companhia contém disposições que podem dissuadir a aquisição da SLC Agrícola e dificultar ou atrasar operações que poderiam ser do interesse dos investidores.

Fonte: Adaptado de SLC (2012d)

Destaca-se no Quadro 26 a firmação de que política de controle de riscos adotada pode não ser suficiente para cobrir eventuais riscos, divergindo da afirmação de Gerigk e Corbari (2011) que citam a gestão de riscos como capaz de identificar os eventos que possam ter consequências operacionais, financeiras e estratégicas adversas e, então encontrar salvaguardas para prevenir ou minimizar o perigo causado por tais eventos. Demais fatores relacionados aos riscos corporativos são analisados com base nas entrevistas e questionários.

Contatou-se mediante as entrevistas que a identificação das fontes de riscos, áreas de impacto, eventos, causas e consequências potenciais, são realizadas pela organização, porém de forma desintegrada. Neste sentido, a identificação dos riscos operacionais ocorre dentro dos departamentos que podem gerar tais riscos, os gestores das próprias áreas avaliam com a diretoria ou presidência ações para minimizar tais impactos.

Os riscos estratégicos e financeiros são tratados mediante avaliações do comitê de riscos que traça planos para minimizar os impactos decorrentes destes tipos de riscos. Cabe destacar que segundo o COSO (2007) toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização.

No caso de estudo a percepção sobre os tipos de risco que impactam o negócio pode ser evidenciada na fala do Membro do Comitê de riscos.

> *[...] Nossa produtividade, é muito ariscada, tem riscos por todos os lados, não temos muito controle do custo nem controle de preços, tem esse impacto de legislação que é muito dinâmico, a produção em sí, se chove ou se não chove também influencia, porque é uma fábrica a céu aberto, nós tivemos que estruturar todo o negócio, por exemplo, as fazendas são localizadas em estados diferentes no Brasil, se em uma tem uma seca, em outra tem produtividade recorde. Isso acaba compensando um pouco os riscos inerentes ao próprio negócio, então eu diria que a nossa empresa tem uma participação muito grande com o risco, com o gerenciamento dos riscos. Todas as atividades são meio que montadas para reduzir os riscos que são inerentes ao negócio agrícola. [...]* ***Membro do comitê de Riscos.***

Alinhado a percepção do gestor citada no trecho da entrevista transcrita está a seguinte fonte de risco evidenciada no canal do investidor: (i) Variações climáticas poderão impactar negativamente a produção da SLC Agrícola e os seus resultados (SLC, 2012d).

Adicionalmente, salienta-se que esta não é a única fonte de risco identificada, no caso de estudo outras fontes podem ser percebidas na Tabela 2. Cabe destacar, que além de selecionar a importância, os participantes explicavam o motivo desta escolha, a fim de que as análises realizadas contemplassem características qualitativas dos dados coletados, estas respostas foram evidenciadas no Apêndice E.

Tabela 2: Importância dos tipos de riscos no caso de estudo

TIPO DE RISCOS		Gerente de Sistemas					Coordenador de TI					Membro do Comitê de Riscos				
		1 - Extrema	2 - Muito forte	3- Forte	4- Moderada	5 -Igual	1 - Extrema	2 - Muito forte	3- Forte	4- Moderada	5 -Igual	1 - Extrema	2 - Muito forte	3- Forte	4- Moderada	5 -Igual
Estratégico	Risco Econômico	x					x					x				
	Risco Político	x						x						x		
	Risco Ambiental	x					x						x			
	Riscos de Marca, Imagem ou Reputação	x						x					x			
	Riscos Sociais			x					x						x	
	Tecnológicos		x					x						x		
Financeiro	Mercado		x				x					x				
	Crédito		x				x						x			
	Liquidez		x					x					x			
Operacional	Pessoal		x				x						x			
	Processos		x					x					x			
	Tecnologia		x				x						x			
	Compliance	x					x						x			

Fonte: Elaborado pela autora com base nas respostas do questionário

No que concerne aos riscos estratégicos percebe-se na Tabela 2 o risco social como sendo o risco percebido como de menor importância na análise dos entrevistados, já o risco econômico foi citado como um risco de extrema importância, e o risco ambiental foi considerado com extremo para dois dos entrevistados, abaixo são evidenciadas as percepções dos respondentes conforme trechos extraídos dos questionários respondidos (Apêndice E).

> **Risco Econômico** *[...] Esta empresa produz commodities , ou seja, quem define os preços é o mercado por isso o controle dos custos é fundamental para viabilizar o negócio. Também é importante ressaltar que trata-se de uma empresa com capital aberto, onde a entrega do que foi prometido e geração de lucros é fundamental para a sua continuidade. [...]* ***Gerente de Sistemas;*** *[...] A SLC depende de disponibilidade de capital para financiar sua estratégia de crescimento [...]* ***Coordenador de TI;*** *[...] Oscilações de preços (no nosso caso, de commodities e de câmbio) podem causar literalmente a "quebra da empresa", se mal administrados [...]* ***Membro do Comitê de riscos***
>
> **Risco Ambiental** *[...] Existe um forte trabalho de conscientização, gestão e controle dos colaboradores e processos através de sistema especializado no assunto para cumprimento de normas legais e aplicação de melhores práticas no que se refere às questões ambientais. [...]* ***Gerente de Sistemas;*** *[...] A legislação ambiental é muito dura no Brasil e todo ônus é do produtor. [...]* ***Coordenador de TI;*** *[...]Nossa atividade se desenvolve no próprio meio-ambiente, portanto é muito visada e há significativo risco de questões ambientais (lembrar do novo código florestal, em votação no momento) [...]* ***Membro do Comitê de riscos***

A análise documental corroborou com a percepção dos entrevistados quanto ao risco econômico, no documento canal com o investidor foi salientando tais informações. Nesta mesma análise o risco político foi identificado como relevante, porém este não teve sua importância identificada como extrema pelos entrevistados. Isto pode ser comprovado mediante trecho do documento citado.

> **Risco Econômico** *[...] A dependência do comércio internacional, a flutuação dos preços dos produtos agrícolas e flutuações no valor do real em relação ao dólar poderão prejudicar o desempenho financeiro da Companhia e os seus resultados operacionais. [...]* ***SLC (2012d)***
>
> **Risco Político** *[...] O Governo Federal exerce influência significativa sobre a economia brasileira. Essa influência, bem como a conjuntura econômica e a política brasileira, poderá vir a causar um efeito adverso relevante nas atividades da SLC Agrícola, nos seus resultados operacionais e no preço de mercado das suas ações ordinárias. [...]* ***SLC (2012d)***

No que concerne aos riscos financeiros o risco de mercado pode ser percebido como extremo. Este aspecto também é evidenciado mediante análise documental do código de conduta da empresa SLC (2012b) que salienta: "A Gestão de Risco de Mercado, leva em conta um conjunto de conceitos consistentes com as melhores práticas internacionais e coerentes com os padrões definidos por órgãos reguladores do Brasil e do exterior."

Os entrevistados destacaram no questionário a possibilidade de perdas com o preço das mercadorias (commodities), logo devido à empresa não decidir sobre os preços de seus produtos, o risco de mercado passa a ser um risco inerente ao negócio da companhia, tal informação é percebida nos trechos extraídos dos questionários respondidos (Apêndice E).

> **Risco de Mercado** *[...] Conheço pouco deste assunto, mas sei que na área financeira da empresa existe um grupo especializado em gerenciar os riscos financeiros aos qual a empresa está exposta. [...]* ***Gerente de Sistemas;*** *[...] Toda receita é gerada baseado nos preços de commodities, ou seja, nós não definimos o valor dos nossos produtos [...]* ***Coordenador de TI;*** *[...]Sim. Enxergo esse item muito similar aos "riscos econômicos". [...]* ***Membro do Comitê de riscos***

O risco de crédito e liquidez foi percebido como importância entre muito forte, para a maioria dos entrevistados. Esta percepção foi confirmada analise documental , que nas fontes de riscos identificadas pela empresa que se concentram no impacto sobre os negócios da inflação, taxas de juros, preço de mercado de ações, e variações cambiais.

Nos riscos operacionais, o risco de *Compliance* foi selecionado por dois entrevistados como extremo. Tal risco também foi percebido na análise documental, mediante canal de relações da companhia: **"**A SLC Agrícola está sujeita a ampla regulamentação ambiental." [...] SLC (2012d). Os trechos extraídos dos questionários respondidos (Apêndice E), que colaboram com esta análise são abaixo listados.

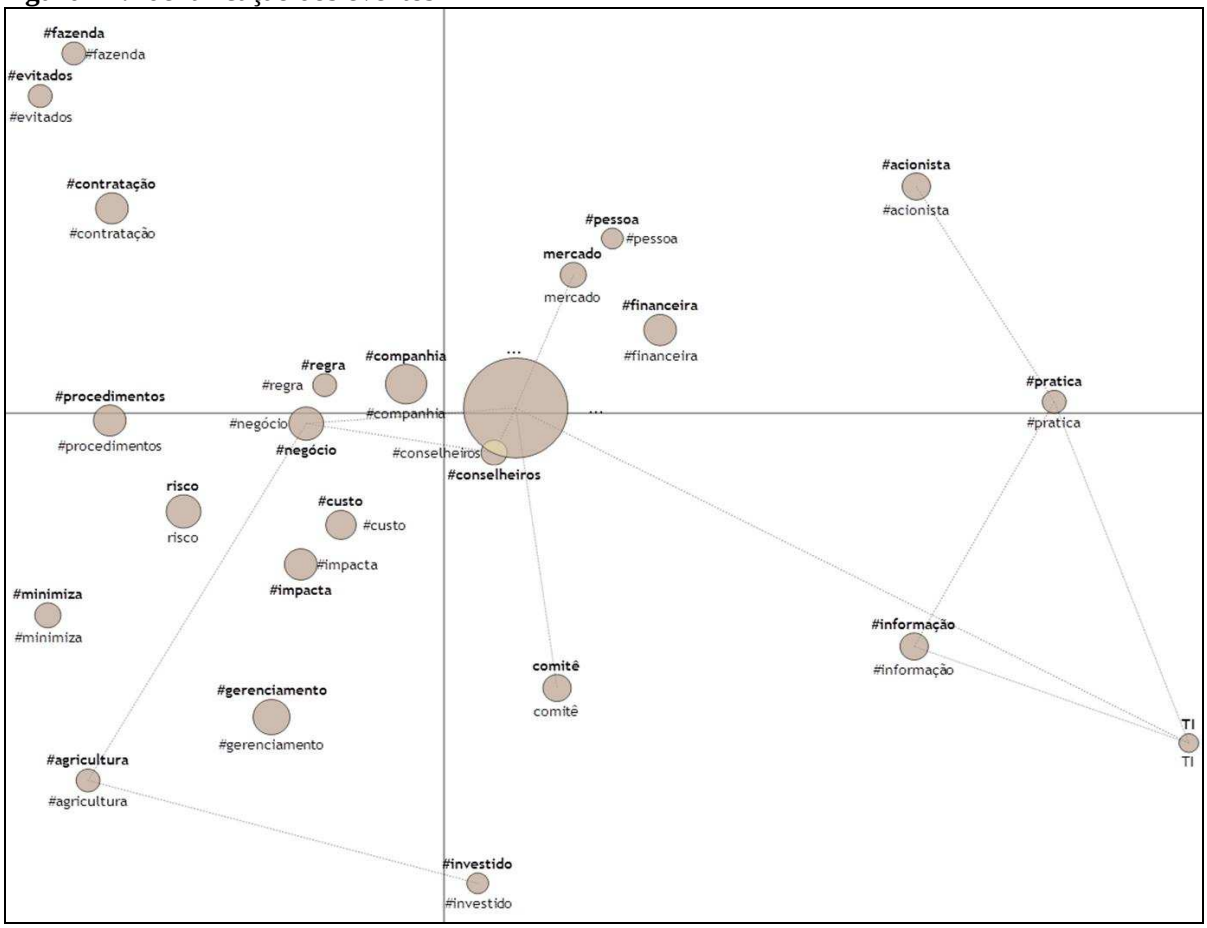
> **Risco de Compliance** *[...] Existem investimentos, conscientização dos colaboradores e gestão sobre as ações para mitigar riscos de não cumprimento de legislações, regulamentações externas ou normas internas observando todas os cenários nos quais a empresa está envolvida, tais como: ambiental, fiscal, societário, etc. [...]* ***Gerente de Sistemas;*** *[...]O que me ocorre nesse item é mais a questão de cumprimento da legislação trabalhistas (PPD´s), pois é difícil achar contingente disponível nessa categoria, principalmente nas fazendas.. [...]* ***Membro do Comitê de riscos***

Os Riscos de pessoal, processos e tecnologia tiveram a percepção dos entrevistados concentrada em sua maioria como muito forte, porém estes não foram percebidos como fontes de riscos relevantes na análise documental, abaixo são evidenciadas as percepções dos respondentes conforme trechos extraídos dos questionários respondidos (Apêndice E).

> **Risco Pessoal** *[...] Existem ações constantes e mensuradas para eliminar acidentes de trabalhos ou não cumprimento de acordos de trabalho que venham trazer danos às pessoas e a empresa.. [...]* ***Gerente de Sistemas;*** *[...] Se a empresa não cumpre rigorosamente a legislação trabalhista, corre risco de ter multas e seus créditos negados. [...]* ***Coordenador de TI;*** *[...] Existe o risco, mas não o considero extremo.. [...]* ***Membro do Comitê de riscos***
>
> **Risco Processos** *[...] Existe um controle de qualidade atuante junto à produção que garante a qualidade do produto que é expedido para o mercado, com isso garantindo que a qualidade do produto contratado seja entregue. [...]* ***Gerente de Sistemas;*** *[...] Qualquer erro no planejamento agrícola, plantio, fertilização ou colheita, podem impactar significativamente nos resultados. Ainda existem os fatores climáticos com variável de perda, caso os processos não sejam rigorosamente monitorados. [...]* ***Coordenador de TI;*** *[...] Má execução de atividades na lavoura (e até o desrespeito às regras de segurança) podem trazer riscos operacionais e de pessoal, reduzindo a eficiência e consequentemente, o lucro. [...]* ***Membro do Comitê de riscos***
>
> **Risco de Tecnologia** *[...] Existe um importante direcionamento dos investimentos para aquisições, manutenção e gestão dos ativos para manter equipamentos e sistemas devidamente preparados para suportar a operação da empresa.. [...]* ***Gerente de Sistemas;*** *[...] Hoje tudo depende de sistema e informações. Um navio que não embarque a carga negociada com o cliente pode gerar multas significativas [...]* ***Coordenador de TI;*** *[...] Esses mais relacionados à TI, na minha visão (sistema fora do ar, sem internet – isso acontece muito nas fazendas)produtos [...]. [...]* ***Membro do Comitê de riscos***

Nas análises anteriormente realizadas é possível perceber que a gestão dos riscos corporativos está melhor estruturada para identificação de riscos estratégicos e financeiros, do que quanto à identificação de riscos operacionais. Na Figura 24 são evidenciadas as variáveis mais frequentes na análise léxica da categoria identificação dos eventos relacionada aos corporativos.

Figura 24: Identificação dos eventos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

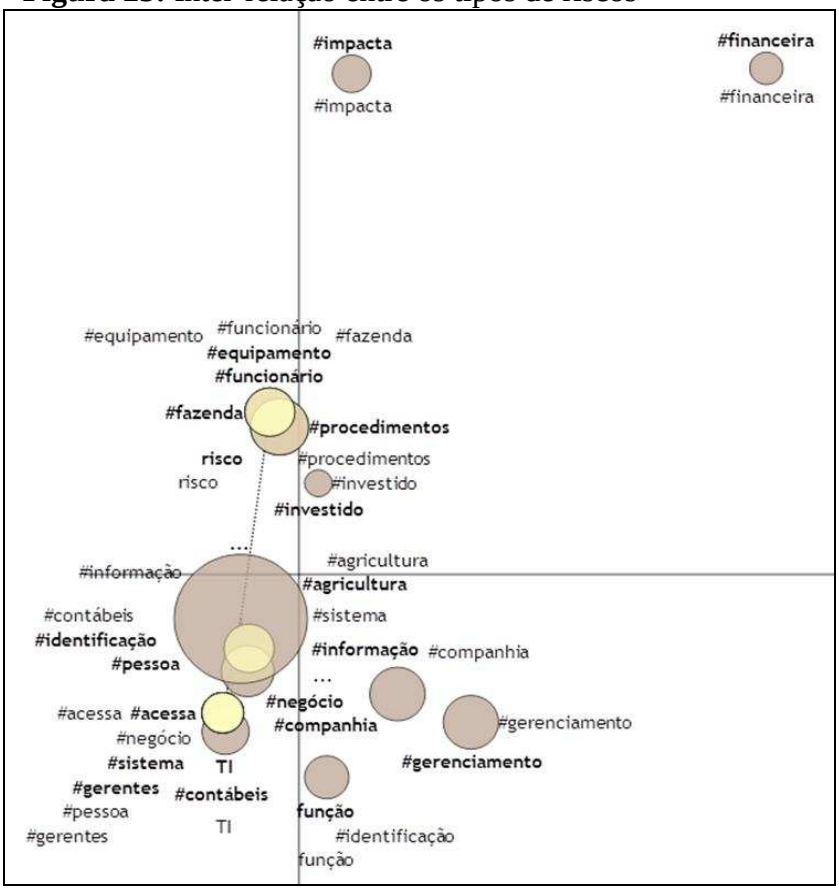
A partir da visualização do mapa fatorial anteriormente representado, evidenciam-se variáveis que permitem análises entre os léxicos relacionados às respostas de cada entrevistado. Percebe-se, por exemplo, a aproximação entre os léxicos, negócio (que remete a processos de negócio), regra, procedimento, custo e risco. Isso demonstra que existem procedimentos para identificação de riscos, porém a realização destes foi identificada como não sendo inter-relacionada entre os diversos tipos de riscos existentes. Esta afirmação se confirma pela visualização do léxico comitê (responsável pela avaliação e riscos corporativos e estratégicos) da variável fazenda (que remete a processos operacionais).

A falta de inter-relação entre a gestão dos diversos tipos de riscos se opõem às recomendações de Coimbra (2011) e Coso (2007), para este último um evento pode desencadear o outro, ou ainda vários eventos podem ocorrer concomitantemente. Logo, a gestão integrada destes tipos de riscos pode proporcionar uma gestão de riscos corporativos mais eficazes. Esta afirmação pode ser percebida na fala do coordenador de sistemas e do Membro do Comitê de Riscos, conforme trechos da entrevista transcrita:

> *[...]. Toda essa sincronização, para fazer realmente uma boa gestão de riscos e uma boa sincronização para que um risco não seja maximizado pelo outro. Isso pode acontecer, a existência de dependência de um risco específico sobre um segundo risco ou o impacto do primeiro pode se tornar muito maior, isso pode ocorrer, no momento que não existe uma área bem sincronizada na questão de tratamento de investigação de riscos, seja de fraude, de negócios, de perda de qualidade de informação, seja o que for. Hoje aqui na SLC Agrícola este processo precisaria ter melhor sincronia.. [...]* ***Coordenador de Sistemas.***
>
> *[...] Nossa atuação foca muito mais nos riscos financeiros, de legislação, de clima e riscos de alguma operação ocorrer de forma equivocada.. [...]* ***Membro do Comitê de Riscos.***

A análise léxica da categoria inter-relação entre os tipos de riscos proporcionou identificar os léxicos mais frequente na fala dos entrevistados.

Figura 25: Inter-relação entre os tipos de riscos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Na Figura 25 percebe-se a relação de significância entre as variáveis: procedimentos, negócio (remete a processos de negócio). Sendo que a variável procedimento esta muito próxima ao léxico risco e funcionário (usuários). Esta relação pode demonstrar a necessidade de procedimentos relacionados à identificação da inter-relação entre os diferentes tipos de riscos, mediante participação dos usuários. É válido destacar que mesmo havendo tipos de riscos diferenciados, cabe às organizações que realizem uma gestão integrada destes riscos, conforme recomendação do COSO (2007) um evento pode desencadear o outro, ou ainda vários eventos podem ocorrer concomitantemente.

A ISO 31000 (2009) estabelece princípios para a gestão de riscos que vislumbram uma gestão de riscos eficaz às empresas em todos os níveis. Os entrevistados foram questionados quanto ao atendimento de tais princípios pela gestão de riscos estabelecida na organização. Neste sentido tais respostas foram analisadas e tabuladas de forma resumida no Quadro 27. Cabe salientar que o Gerente Corporativo de TI tratou os princípios de forma conjunta na sua resposta salientando não ter conhecimento específico para analisar de forma isolada cada aspecto.

Quadro 27: Princípios para a Gestão de Riscos Corporativos.

Princípio	É atendido	Principais pontos observados nas entrevistas
Cria e protege valor	Sim	As ações realizadas para a gestão dos riscos que são controlados protegem o valor da companhia
Participa de todos os processos organizacionais	Não	Há possibilidade de ser mais abrangente atuando em todos os níveis da organização.
Participa da tomada de decisão	Sim	Em muitas questões chaves são realizadas análises dos riscos antes da decisão, isto também ocorre no dia a dia dos setores
Aborda explicitamente a incerteza	Sim	Analisa-se antes de avanços afim de evitar problemas. Porém há espaço para avaliações mais aprofundadas
Atua de forma Sistemática, estruturada e oportuna	Sim	Está estruturada principalmente em relação aos aspectos financeiros
Baseia-se nas melhores informações possíveis	Sim	Há uma busca pelas melhores informações/assessorias para a tomada de decisões.
Adéqua-se a realidade da organização	Sim	Está adequada as suas atividades
Considera fatores humanos e culturais	Sim	Há uma preocupação com os fatores humanos principalmente
Atua de forma transparente e inclusiva	Não	Um aspecto limitador deste princípio é alguns problemas de comunicação voltados aos processos da companhia
Atua de forma dinâmica e interativa, capaz de reagir a mudanças	Não	Há possibilidade de melhorias neste aspecto
Facilita a melhoria contínua da organização.	Sim	Há um aperfeiçoamento na de gestão de riscos. Porém é destacada a necessidade de uma melhoria mais rápida e

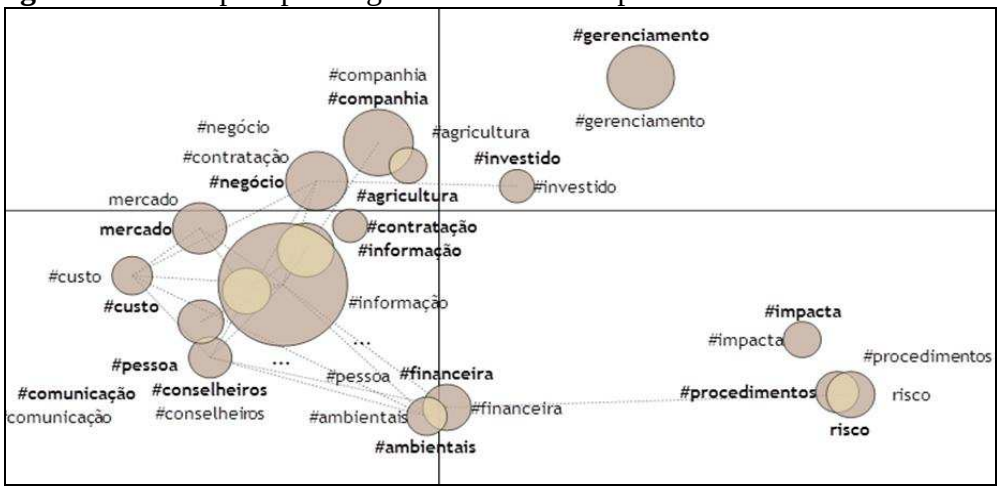
		dinâmica.

Fonte: Elaborado pela autora com base nas entrevistas

Destacam-se no Quadro 27 os princípios: (i) participação de todos os processos organizacionais; (ii) atuação de forma transparente e inclusiva; e (iii) atuação de forma dinâmica e interativa, elencados pelos entrevistados como não atendidos pela gestão de riscos da organização. O não atendimento de tais aspectos diverge da orientação da ISO 31000 (2009), que salienta que o sucesso da gestão de riscos depende da eficácia e da estrutura da gestão que fornece os fundamentos e os arranjos que irão incorporá-la mediante toda organização, em todos os níveis.

Neste sentido a atuação integrada, transparente e dinâmica auxiliaria no sucesso da companhia na percepção de seus riscos corporativos. Corroborando com esta percepção está a análise Léxica do mapa fatorial apresentado na Figura 26, evidencia como léxico mais citado pelos entrevistados está o gerenciamento, seguido do léxico companhia, e negócio. Esta ligação demonstra a necessidade da corporação de um gerenciamento de riscos corporativos integrado em todos os níveis organizacionais mediante o monitoramento destes riscos nos processos de negócio.

Figura 26: Princípios para a gestão de riscos corporativos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

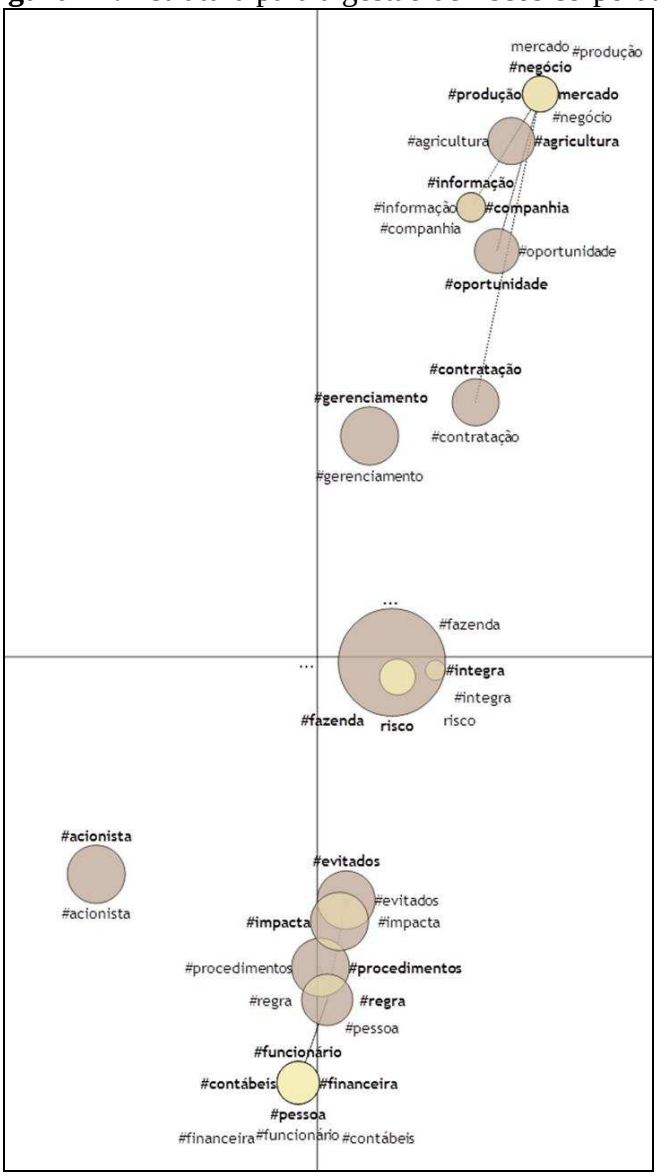
Além da adoção dos princípios, a estrutura para a gestão dos riscos é ponto de destaque na literatura pertinente. No caso de estudo não há propriamente reconhecida pelos entrevistados uma estruturada formal para gerenciar os riscos corporativos.

Os riscos estratégicos e financeiros são de forma mais abrangente tratados em reuniões semanais no comitê de riscos, já os riscos operacionais são trados dentro dos setores, onde cada um preocupa-se com os riscos gerados nos seus ambientes. A melhoria deste processo é obtida pela auditoria independente que além de auditar as informações contábeis, são responsáveis pela auditoria em processos dos setores.

A norma ISO 31000 (2009) prevê que a estrutura proposta auxilie na gestão de riscos e é importante que cada organização busque adaptar os componentes da estrutura às suas necessidades. Neste sentido, a estrutura presente na corporação, apesar de informal quando relaciona aos riscos operacionais, se adapta as necessidades do negócio. Mesmo assim cabe destacar a não identificação de componentes desta estrutura que vislumbrem um processo de melhoria continua na avaliação dos riscos corporativos.

Na Figura 27, são evidenciados como léxicos mais frequentes na análise da categoria estrutura para a gestão de riscos corporativos, destacando-se: gerenciamento, acionista, impacta, evitado, procedimentos. No mapa fatorial posteriormente apresentado percebem-se ao centro as variáveis integra e risco, distantes dos demais léxicos. Isto demonstra a falta de integração relacionada a identificação dos tipos de riscos, bem como a estrutura para os processos capazes de realizar seu gerenciamento.

Figura 27: Estrutura para a gestão de riscos corporativos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

A contribuição dos usuários na estrutura de gestão dos riscos de forma mais efetiva afim de uma conscientização ao risco é ponto a ser salientado. Isto pode ser observado na fala do Membro do Comitê de Risco conforme trecho da entrevista transcrita.

> *[...].Poderiam ser criadas mais regras, mais protocolos, evitando riscos, para não termos ações isoladas baseadas na opinião de cada um. Isso ocorre até na área financeira, nos lançamentos contábeis, quando trocamos uma pessoa, ocorre um lançamento diferente, isso é um item de menor impacto e erros nos processos. Acredito que isto estando bem definido, acaba reduzindo essa possibilidade de erros, estando os usuários desta forma preparados. [...]* ***Membro do Comitê de Riscos.***

Neste aspecto é salientada a participação do usuário mediante a criação de procedimentos para que estes estejam bem definidos, evitando assim o erro operacional de processos. Segundo o COSO (2007) este tipo de erro é oriundo de modificações de processos sem alteração adequada nos protocolos administrativos, ineficiência, insatisfação do cliente e diminuição da fidelidade dos processos.

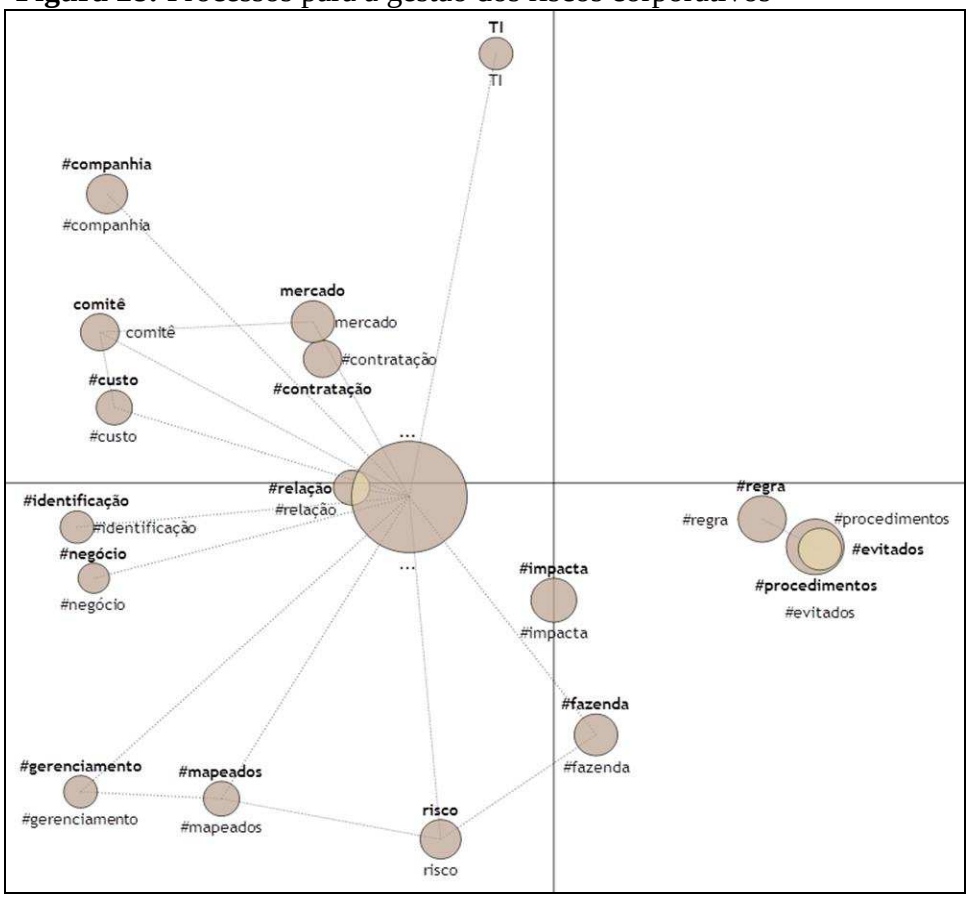
Quanto aos processos para a gestão de riscos citados na norma ISO 31000 (2009), os entrevistados atuantes na área de TI demonstraram não entender especificamente de cada processo. O Membro do comitê de riscos relacionou cada processo no âmbito da gestão, tais observações foram relacionadas abaixo:

> *[...] 1)* ***Comunicação e consulta às partes interessadas*** *Alguns processos, algumas áreas fazem isso bem, por exemplo, uma área que é crucial para nós é a segurança (cuida da segurança dos funcionários) nas fazendas, todas as semanas é realizada uma conversa com os operários sobre segurança (neste caso as partes interessadas são os funcionários). É uma conversa sobre como evitar esse tipo de coisa, de criar padrões, isto traz melhorias, nessa área eu acho que está bem, apesar de ainda acontecer, mas eu acho que a gente conseguiu evitar muito acidente com isso. Em algumas outras áreas acredito que falta conversa com os interessados, isso está faltando, faz parte da organização, que todo mundo tenha essa prática, falta às áreas se conversarem, por exemplo, a minha área com a área da contabilidade, a contabilidade com a área financeira, falta um pouco de diálogo com os interessados.2)* ***Estabelecimento do contexto:*** *Como eu não estou muito no dia a dia das outras áreas, até não saberia dizer como é esta interação da nossa empresa, por exemplo, com os fornecedores, ou com clientes, prestadores de serviços, mas acredito que estas relações são levadas em consideração. 3)* ***Avaliação dos Riscos:*** *Eu acho que de cada área vai fazer a sua parte, vai mapear quais são seus riscos, e uma vez que esses riscos forem identificados, já que podem trazer grandes prejuízos, vai se criar algum protocolo ou manual em que as pessoas vão ser treinadas para aquilo, então acontece dentro de cada área, e cada área cria as suas normas, para evitar o risco. 4)* ***Tratamento dos Riscos:*** *Como falei no item anterior, as áreas identificam e elas também tratam seus riscos.5)* ***Monitoramento e análise crítica dos Riscos:*** *Eu diria que é feito de forma desintegrada, ele é tratado dentro de cada área e cada área se preocupa com aquilo e fica por ali, talvez num dos momentos do diretor presidente, ou o diretor da área vai validar alguma coisa, não é uma coisa que acontece integrada. [...]* ***Membro do Comitê de Riscos.***

No trecho listado da entrevista transcrita é possível verificar que existem possibilidades de melhorias nos processos da gestão de riscos corporativos relacionadas à comunicação entre as áreas (departamentos), bem como com as partes interessadas do negócio. Um fator que corrobora com esta percepção é a falta de divulgação aos investidores (através de seu canal) dos riscos operacionais.

Novamente existe a confirmação de que as ações de avaliação, tratamento e monitoramento dos riscos foram realizadas de forma desintegrada, os riscos operacionais pelas áreas (departamentos) e os riscos estratégicos e financeiros mediante comitê de riscos. Na análise léxica demonstrada na Figura 28 pode ser visualizada a forte relação de significância entre as variáveis: gerenciamento, mapeados, risco, fazenda, que remete ao gerenciamento dos riscos operacionais. Isto demonstra que no processo de gestão de riscos corporativos o gerenciamento de riscos operacionais ocorre de forma isolada aos riscos estratégicos e financeiros (relacionado aos léxicos: negócio, comitê, e mercado).

Figura 28: Processos para a gestão dos riscos corporativos



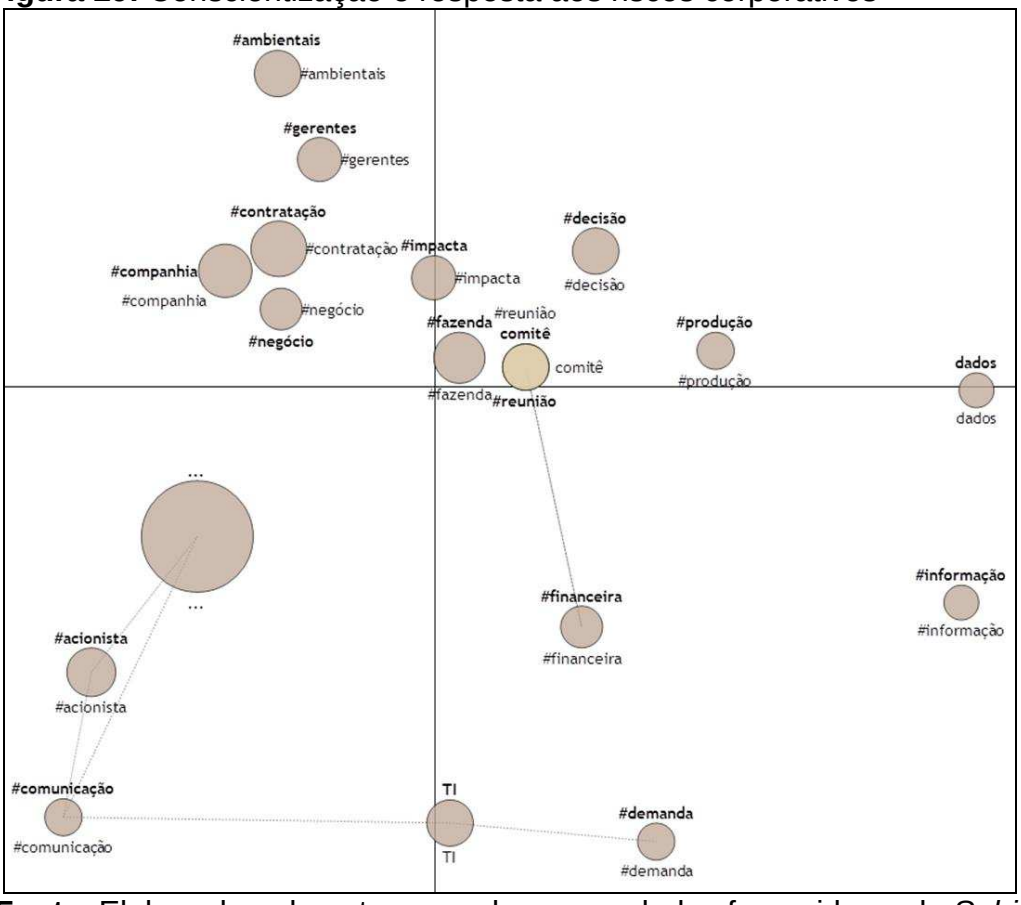
Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

A etapa de conscientização e resposta ao risco é estabelecida com a finalidade de alcance de uma resposta dentro da estrutura capaz de identificar riscos que podem ser aceitados ou minimizados. Neste sentido, buscou-se identificar se a gestão de riscos corporativos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações.

Identificou-se que as decisões tomadas pelos gestores não contemplam de forma consciente a resposta os riscos corporativos, uma vez que a comunicação de tais riscos não é realizada de forma eficiente. Contudo, a gestão dos riscos corporativos apesar de não ser de forma ampla e integrada realizada, proporciona o conhecimento e resposta aos tipos de riscos financeiros e estratégicos, mediante análises decorrentes do comitê de riscos, por exemplo: a política cambial adotada.

Esta reflexão pode ser confirmada mediante análise do mapa fatorial apresentado na Figura 29, pela aproximação com significância das variáveis: comitê e financeira (que remete a riscos financeiros). Outro ponto a ser salientado é a relação entre os léxicos: acionista e comunicação, que comprova a falta de comunicação com os acionistas relacionada a conscientização e resposta dos riscos corporativos.

Figura 29: Conscientização e resposta aos riscos corporativos



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

No Quadro 28 é realizada uma análise consolidada entre os principais achados desta seção. Cabe salientar que a primeira coluna do Quadro 28 corresponde as categorias relativas a gestão de riscos corporativos, identificadas anteriormente no *Framework* metodológico (Quadro 17).

Quadro 28: Principais achados da gestão de riscos corporativos

GESTÃO DE RISCOS CORPORATIVOS	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Avaliação estratégica do risco – Aproveitar oportunidades	A avaliação estratégica do risco ocorre mediante atuação no comitê de riscos (riscos estratégicos e financeiros), e mediante avaliação nas diferentes áreas (riscos operacionais). Não foi identificada uma avaliação estratégica integrada de todos os tipos de riscos corporativos. Esta avaliação permite melhorar a governança, bem como as relações com o mercado, proporcionando melhores negócios e por consequência a melhores resultados. Identificou-se que a avaliação estratégica dos riscos ocorre no caso de estudo, mas não da forma integrada, existindo espaços para melhorias neste aspecto.	TI, financeira (que remete a informações financeiras), informação, mercado e contábeis, reunião, comitê e estratégia	Não localizado	Não localizado
Perda de Recursos (custos ou prejuízos associados) – Danos – Consequências negativas	O controle e gerenciamento eficiente dos riscos corporativos pode evitar perdas (prejuízos graves associados), foi identificado a perda de recursos em função do desflorestamento (relacionado ao não gerenciamento do risco ambiental). Existem oportunidades de melhorias na proteção do negócio, como por exemplo os investimentos em tecnologias para gerenciamento e por consequência redução de impactos negativos decorrentes de riscos estratégicos, financeiros e operacionais hoje não gerenciados.	Negócio, investido (que remete a investimentos em TI), conselheiros, proteção e oportunidade.	Não localizado	Não localizado
Identificação dos eventos e categorização dos riscos (estratégicos, financeiros e operacionais)	A identificação das fontes de riscos, áreas de impacto, eventos, causas e consequências potenciais, são realizadas pela organização, porém de forma desintegrada. Neste sentido, a identificação dos riscos operacionais ocorre dentro dos departamentos que podem gerar tais riscos, os gestores das próprias áreas avaliam com a diretoria ou presidência ações para minimizar tais impactos. Os riscos estratégicos e financeiros são tratados mediante avaliações do comitê de riscos que traça planos para minimizar os impactos decorrentes destes tipos de riscos.	Negócio (que remete a processos de negócio), regra, procedimento, custo, risco, fazenda e comitê	No que concerne aos riscos estratégicos percebe-se na Tabela 2 o risco social como sendo o risco percebido como de menor importância na análise dos entrevistados, já o risco econômico foi citado como um risco de extrema importância, e o risco ambiental foi considerado com extremo para dois dos entrevistados. Nos riscos financeiros o risco de mercado pode ser percebido como extremo. Nos riscos operacionais, o risco de Compliance foi selecionado por dois entrevistados como extremo, no que tange aos riscos operacionais.	A identificação de riscos pela companhia foi evidenciada na análise documento mediante os fatores de riscos listados em seu canal de relação com o investidor, sendo eles: 1) Relacionados ao Setor Agrícola e Negócios da empresa; 2) Relacionados ao Brasil; e 3) Relacionados às ações da Companhia.

GESTÃO DE RISCOS CORPORATIVOS	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Inter-relação entre os tipos de riscos	Não foi identificada análises de inter-relação entre a gestão dos diversos tipos de riscos. Foi identificada a necessidade de estabelecimento de procedimentos relacionados à identificação de inter-relação entre os diferentes tipos de riscos mediante participação dos usuários, conforme recomenda a literatura.	Procedimentos, negócio (remete a processos de negócio), risco e funcionário (usuários).	Não localizado	Não localizado
Princípios para a gestão de riscos corporativos	A Participa de todos os processos organizacionais, a atuação de forma transparente e inclusiva, e a atuação de forma dinâmica e interativa, foram identificados como principios não atendidos pelas atividades da organização. Destaca-se como fator limitador deste atendimento problemas de comunicação interna. Foi identificada a necessidade da corporação de um gerenciamento de riscos corporativos integrado em todos os níveis organizacionais mediante o monitoramento destes riscos nos processos de negócio.	Gerenciamento, companhia, negócio (que remete a processos de negócio),	Não localizado	Não localizado
Estrutura para gerenciamento dos riscos (concepção, implementação, monitoramento e melhoria contínua) - mandado e comprometimento	No caso de estudo não há propriamente reconhecida pelos entrevistados uma estrutura formal para gerenciar dos riscos. Identificou-se a atuação do comitê para gerenciamento dos riscos financeiro, , já os riscos operacionais são trados dentro dos setores, onde cada um preocupa-se com os riscos gerados nos seus ambientes. A melhoria deste processo é obtida pela auditoria independente que além de auditar as informações contábeis, são responsáveis pela auditoria em processos dos setores.	Gerenciamento, acionista, impacta, evitado, procedimentos, integra e risco	Não localizado	Não localizado

Fonte: Elaborado pela autora (2012)

Cabe destacar que apesar da tecnologia ser um aspecto de relevante importância no planejamento agrícola e processos da organização, bem como o investimento em novas tecnologias estar presente no código de conduta relacionado ao compromisso com a sustentabilidade (SLC, 2012b), não houve destaque desta fonte de riscos nas entrevistas no que concerne aos riscos corporativos. Este fator pode estar relacionado à atuação da TI de forma não integrada e conectada a gestão de riscos corporativos da corporação.

Na próxima seção foram realizadas análises sobre a relação entre a gestão de riscos da tecnologia da informação (TI) e a Gestão dos Riscos Corporativos.

4.5. GESTÃO DE RISCOS DE TI *versus* GESTÃO DOS RISCOS CORPORATIVOS

Esta seção apresenta análises voltadas à relação entre a gestão dos riscos de TI e a gestão dos riscos corporativos. Para tanto, os pontos abordados contemplam: a atuação de TI *versus* perspectivas de negócio; governança corporativa *versus* a gestão de riscos de TI e riscos corporativos; a criação de mecanismos de controle *versus* a redução de riscos de TI e riscos corporativos; A atuação dos usuários *versus* a segurança nos processos de negócio; A atuação do comitê de riscos *versus* a prevenção dos riscos corporativos e de TI; e a aproximação entre os riscos corporativos e riscos de TI.

A atuação da TI frente aos negócios é percebida pelos entrevistados mediante o auxilio que TI para melhorias nos processos organizacionais. Outro aspecto é a busca de formas de integrar as informações para melhor atendimento das necessidades informacionais. Esta avaliação pode ser confirmada no trecho da entrevista com o Coordenador de sistemas.

> *[...] Estamos preocupados em levantar informações que mostrem para o gestor, para as áreas e para as fazendas, as discrepâncias que podem estar acontecendo, o arsenal de ferramentas que eles têm nas mãos e que podem utilizar. Ajudamos a prevenir os riscos de negócio, trabalhando focados na cultura, mostrando que há possibilidades de consultas, relatórios, e também formas de apoiá-los a buscar eficiência, para alcançar melhores resultados nos negócios e consequentemente evitar talvez até algumas falhas.. [...]* ***Coordenador de Sistemas.***

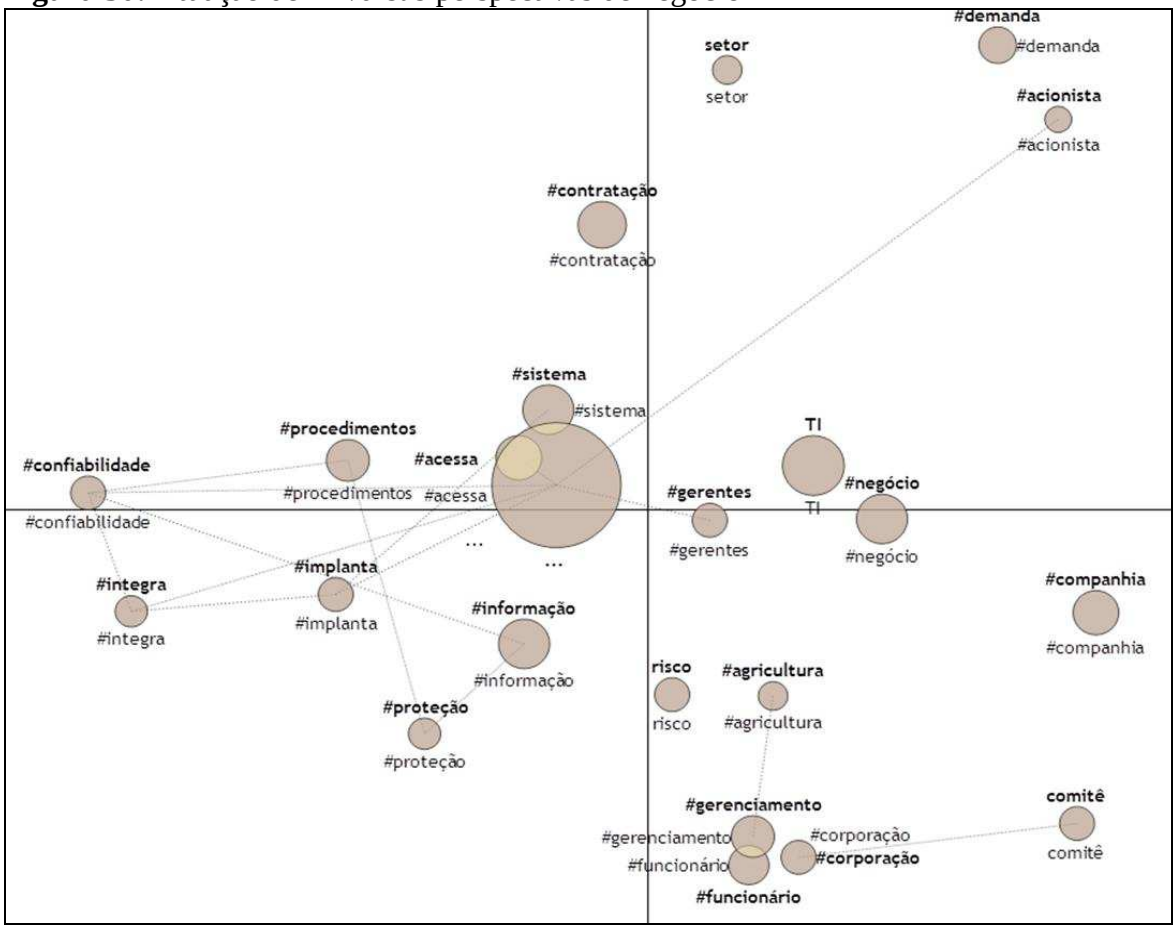
Para o Gerente corporativo de TI a relação da atuação de TI quanto às perspectivas de negócio ocorre de forma a complementar os controles internos utilizados pelas demais áreas, atuando de forma a facilitar e direcionar estes controles. Esta percepção esta alinhada a visão do Membro do Comitê de riscos conforme pode ser observado nos seguintes trechos das entrevistas transcritas

> *[...] Somos hoje uma prestadora de serviços, somos demandados pelos demais setores, porém seguimos o direcionamento das áreas de negócios. Se existe uma preocupação pra complementar determinados controles para os negócios a TI procura fazer com que o setor de sistema programe isso, ou seja, nós somos facilitadores nada mais que isso, nós só somos direcionadores nesse aspecto. [...]* ***Gerente Corporativo de TI.***
>
> *[...] Vejo que as áreas (como sempre ocorre nas empresas) passam a demanda para a TI, e a TI monta alguns relatórios, ajuda a tomar algumas decisões. Ela recebe a demanda de uma área que mapeou o que necessita no que pode ser melhorado. A TI ajuda a elaborar alguns relatórios para alimentar aquela área, e aquela área vai usar aquilo para atuar no seu negócio. [...]* ***Membro do Comitê de Riscos.***

Os aspectos analisados anteriormente com base nas entrevistas corroboram com a visão de Tarouco e Graeml (2011) “o alinhamento estratégico dos negócios e da TI deve, portanto, ser utilizado como ferramenta de gestão, focando as atividades que a gerência deve executar para atingir coesão entre os esforços desenvolvidos pela área de TI e pelas áreas funcionais e de negócio.”

Na análise léxica da relação entre TI e negócios podem ser visualizados como léxicos mais frequentes na Figura 30 as palavras mais citadas nas respostas dos gestores. Dentre elas destaca-se a aproximação entre os léxicos TI e negócio, próximos ao eixo central do mapa, esta visualização confirma os aspectos descritos anteriormente, a atuação de TI ocorre de forma a melhorar as perspectivas de negócio.

Figura 30: Atuação de TI *versus* perspectivas de negócio



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

Outro aspecto a destacar é a variável confiabilidade (requisito de negócio) ligada com significância aos léxicos: informação, procedimento, integra e proteção. Esta relação de grande significância evidencia que a atuação de TI frente às perspectivas do negócio visa manter a confiabilidade das informações, logo a manutenção deste requisito ocorre mediante uma atuação voltada à proteção das informações, ou seja, aliada a práticas de redução de riscos.

Aliado a esta percepção buscou-se identificar a crescente necessidade de informações e de controles (relacionadas aos riscos) com os princípios e preceitos da governança corporativa, tema inerente a gestão de riscos de TI e riscos corporativos. Neste aspecto, na análise documental do Código de conduta da companhia afirma os seguintes compromissos (SLC 2012b):

- Administrar a empresa de forma integra e transparente, incentivando o bom relacionamento junto às partes interessadas que envolvem o negócio (acionistas, clientes, fornecedores, funcionários, governo e sociedade);

- Disponibilizar e publicar informações, dados e relatórios de forma eficaz e transparente aos devidos públicos interessados;
- A empresa tem por prática a realização de auditorias internas e externas;
- A empresa possui Comitê de Sustentabilidade para definição de políticas e estratégias sustentáveis e Grupos de Melhorias ligadas a questões de qualidade.

Nos compromissos supracitados a relação com os riscos de TI se dá pelos compromissos informacionais (informações e dados), e com a qualidade. Já os riscos corporativos estão relacionados ao compromisso com as partes interessadas. Ambos os aspectos podem ser melhorados com a prática de auditorias em processos e relatórios (auditoria externa e interna).

Na percepção dos entrevistados é percebida a atuação da companhia quanto as práticas de governança com a redução dos riscos, de forma superficial. O coordenador de sistemas destaca a necessidade de maior clareza e interação destas práticas com os departamentos, o Gerente Corporativo de TI confirma esta percepção, observando que de forma informal esta relação se dá mediante a ética instituída no ambiente organizacional. O Membro do Comitê de Riscos salienta que o processo de governança gera uma troca entre a empresa, o mercado acionário e os investidores, capaz de gerar aprendizados possíveis de evitar riscos.

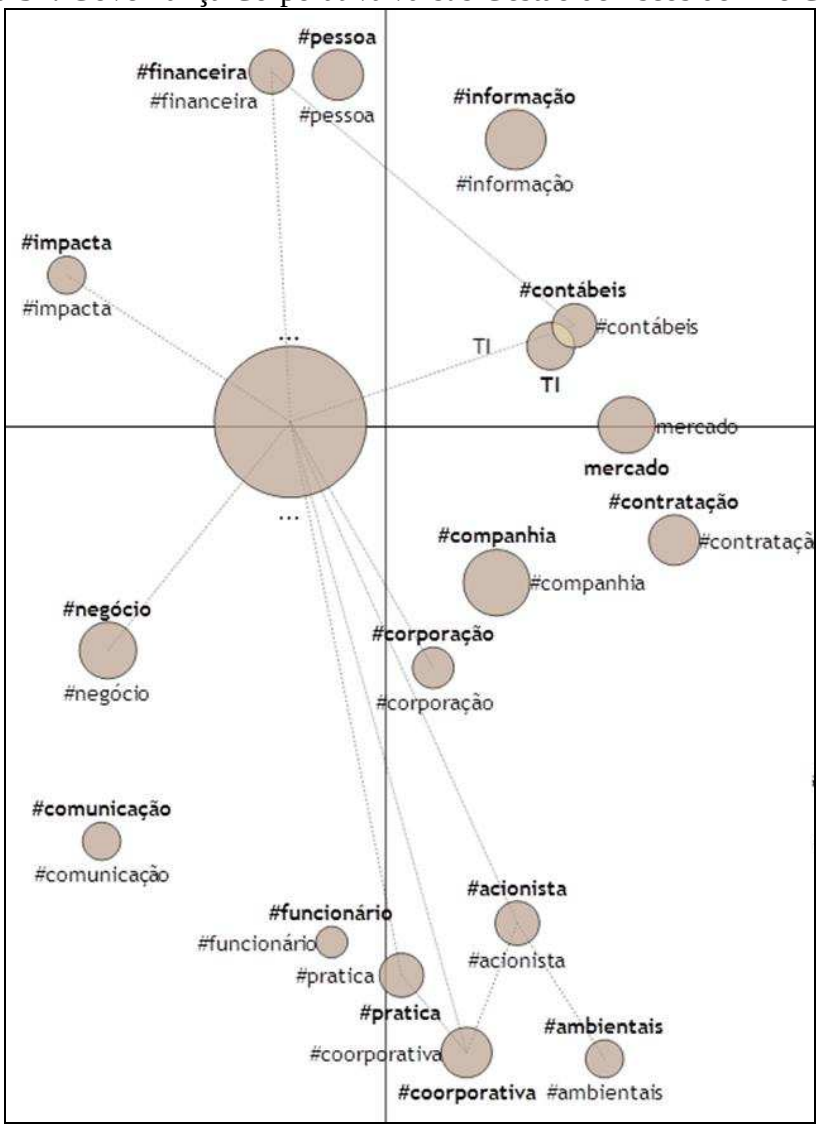
> *[...] Acho que diretamente as práticas de governança contribuem para minimizar riscos, apesar de não se ter muita clareza sobre estas práticas aqui na empresa. Na TI a gente foca muito mais nas nossas experiências, na parte de mercado, ou por imposição dos negócios. Não existe aquela preocupação interna dentro da SLC que nos dá alguns direcionadores para evitar riscos, algumas verificações ou controles que nós deveríamos ter. Acredito que há espaço para se fazer um avanço, uma sincronização maior, até mesmo um alinhamento maior dentro do grupo da SL, referente a esse assunto, porque hoje a meu ver isso não está assim tão conectado e difundido.. [...]* ***Coordenador de Sistemas.***
> *[...] A De maneira formal não vejo muita orientação não, muito informal, a maioria pelos princípios da organização, pela ética e outros, mas não tem uma coisa formalmente constituída. Por exemplo, não vejo a área de TI fazer parte ou se esta conectada formalmente em reuniões periódicas que tratem deste aspecto, isso não acontece, eu não vejo. Talvez fosse uma forma de contribuir de forma efetiva para melhorar esta gestão. Nossa participação esta muito ligada nos princípios que existem na cultura da corporação. [...]* ***Gerente Corporativo de TI.***
> *[...] Neste caso eu diria que a área faz o seu papel, porque o acionista traz muita coisa para dentro da empresa também, a gente tem contato com vários acionistas, ou investidores, uma visão mais amplas, porque tem investidores que não são acionistas, e trazem muitas coisas de práticas que a gente pode estar colocando e traz para dentro da empresa, já adotamos algumas coisas que são alertadas por investidores, então é uma troca de informações que vem também dos acionistas. No*

> *final acaba tudo passando para a TI, por que todos os dados que a gente contabiliza, e passa para o mercado, vem dos nossos programas, então à medida que da algum problema de TI, que da algum problema de parametrização, algum problema de tabela ou de software vai impactar lá na frente nas nossas transferências para os acionistas, então eu acho que embora não apareça de forma clara, é a TI que esta segurando todos os nossos dados, então eu acho que diria que faz parte, a governança vem também da TI, e é ela que formula os dados para nós, dados diretamente ligados. [...]* ***Membro do Comitê de riscos.***

Os aspectos anteriormente citados, extraídos da análise documental e análise das entrevistas, são reiterados com a visualização da Figura 31, que se refere ao cruzamento dos léxicos mais frequentes encontrados nas entrevistas, quando observada a menção a governança corporativa relacionada à gestão de riscos de TI e gestão de riscos corporativos.

O distanciamento do léxico comunicação do eixo central do mapa, não se relacionando de forma significativa com as demais variáveis confirma a necessidade de maior clareza da atuação da governança corporativa. Já o léxico TI se localizou próximo ao eixo central ligado com significância as variáveis: contábeis e financeira (informações contábeis financeiras), isso confirma a importância da atuação de TI na produção de informações que atendam ao negócio de forma a satisfazer a necessidade das partes interessadas. Sob este prisma destacam-se outras variáveis que se relacionaram com significância ao ponto central do mapa: impacta, negócio, corporação, acionista.

Figura 31: Governança Corporativa *versus* Gestão de riscos de TI e Corporativos



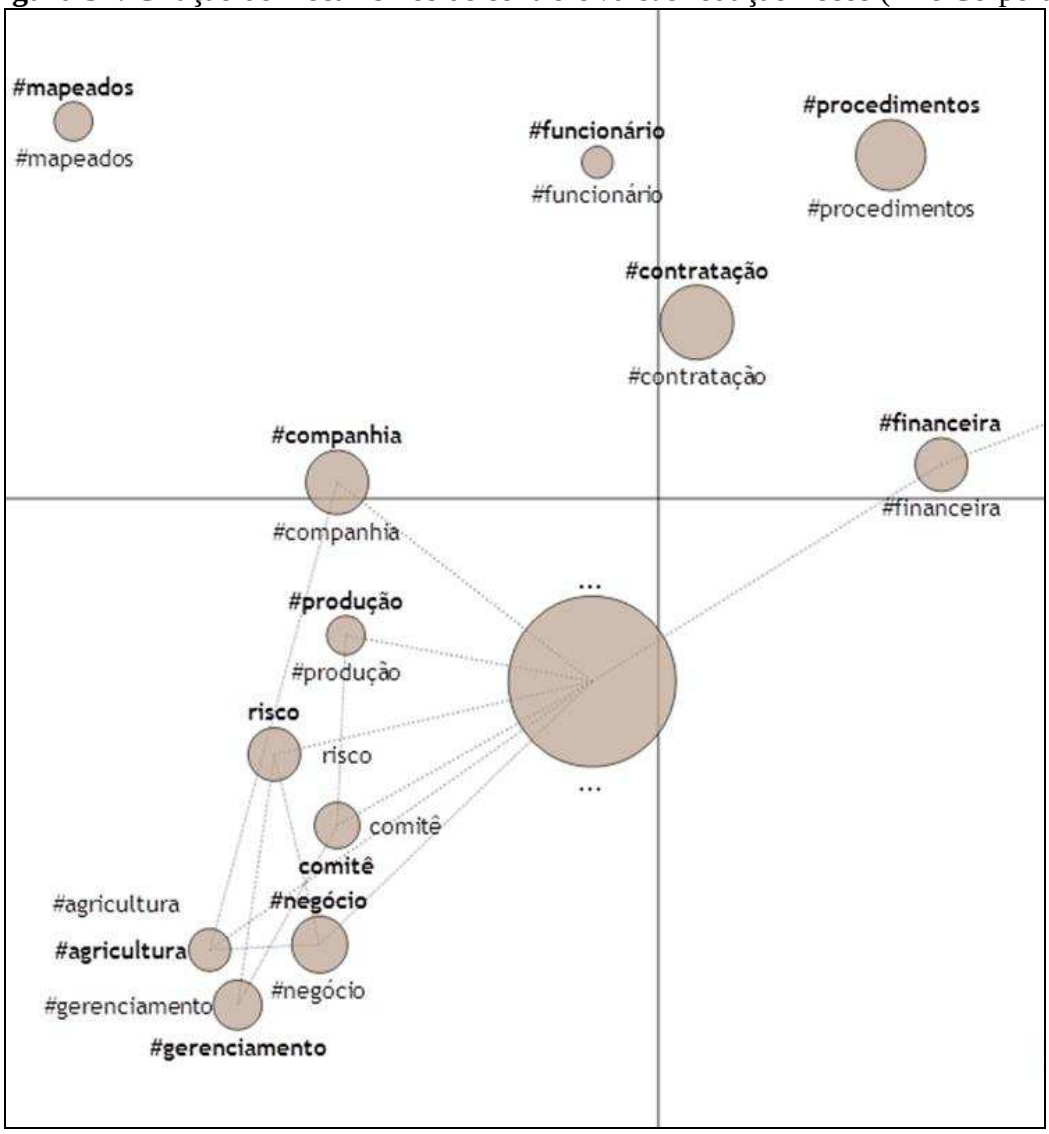
Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

A criação de mecanismos de controle esta associada à governança corporativa, refletindo na forma em que os processos e a gestão são conduzidos, afim de proteger a empresa de riscos indesejados (IBGC, 2009; JUNIOR, JUNQUEIRA e BERTUCCI, 2010). Os entrevistados salientaram que a adoção de controles internos possibilita a redução de riscos de TI e Corporativos, este último principalmente vinculado aos tipos operacionais. Nãs entrevistas, foram destacadas melhorias nestes controles em termos de sistema e ferramentas, ocasionando a melhoria da eficiência nos processos, evitando risco, principalmente com fraudes e perdas de informações.

A existência de regras e protocolos foi considerada importante para evitar qualquer tipo de riscos, conforme entrevistas realizadas. Esta afirmação, foi confirmada na análise documental, no relatório das demonstrações financeiras de 2011 foi constatada o aprimoramento dos controles internos mediante a implementação do sistema operacional (ERP) que integrou as informações das fazendas com a matriz (SLC, 2012b).

Percebe-se na análise léxica a variável procedimento próxima de funcionários (usuários) e dados representando a vinculação das regras e protocolos sobre os procedimentos para a geração de dados confiáveis, conforme mapa fatorial ilustrado na Figura 32. Para Spears e Barki (2010) a atuação dos usuários pode garantir a segurança nos processos de negócio, protegendo as informações financeiras e o relacionamento com as partes interessadas.

Figura 32: Criação de mecanismos de controle *versus* redução riscos (TI e Corporativos)



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

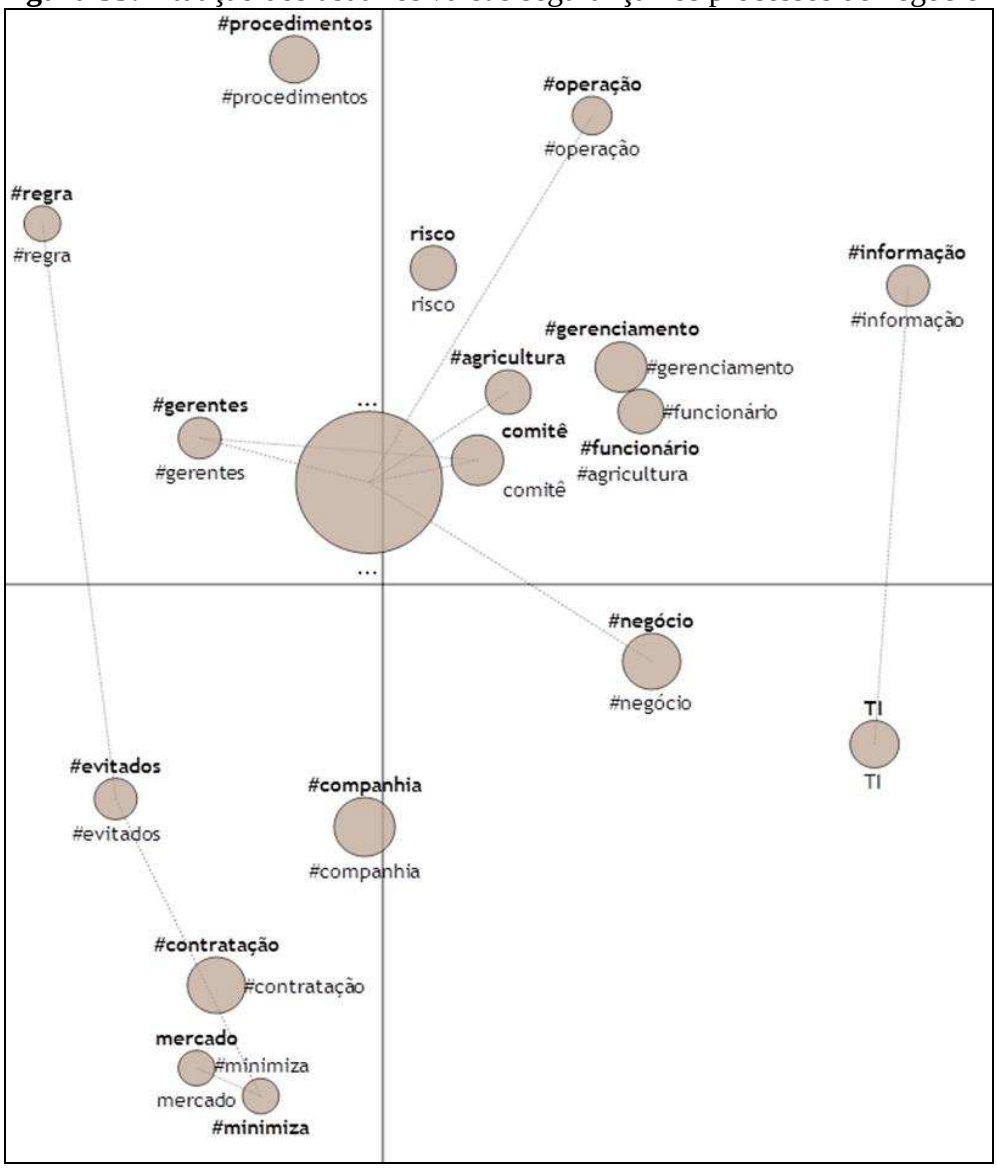
No mapa fatorial (Figura 32), percebe-se a variável risco relacionada com significância aos léxicos negócio, agricultura, gerenciamento e companhia. Esta relação corrobora ao entendimento sobre os controles internos protegerem as informações financeiras. Neste sentido os entrevistados destacaram que estes controles protegem as informações, porém existem alguns problemas relacionados principalmente a erros na produção destes informes. A atuação da auditoria externa quanto à identificação dos pontos a serem consertados proporciona a melhoria destes controles.

Este fator é evidenciado nas demonstrações financeiras da companhia, no âmbito da responsabilidade de administração sobre elas destacada no parecer da auditoria independente, cabendo aos controles internos a responsabilidade por permitir a elaboração de tais demonstrações, evitando distorções ocasionadas por fraudes e erros, conforme pode ser observado no trecho seguinte, extraído do relatório.

> *[...] A administração da Companhia é responsável pela elaboração e adequada apresentação das demonstrações financeiras individuais de acordo com as práticas contábeis adotadas no Brasil e das demonstrações financeiras consolidadas de acordo com as normas internacionais de relatório financeiro (IFRS), emitidas pelo International Accounting Standards Board – IASB, e de acordo com as práticas contábeis adotadas no Brasil, assim como pelos controles internos que ela determinou como necessários para permitir a elaboração dessas demonstrações financeiras livres de distorção relevante, independentemente se causada por fraude ou erro. [...]* ***SLC, 2012c.***

Quanto à atuação dos usuários *versus* segurança nos processos de negócio, buscou-se evidenciar variáveis que permitem análises entre os léxicos relacionados às respostas de cada entrevistado, quanto a esta categoria. Os léxicos mais frequentes podem ser observados na Figura 33.

Figura 33: Atuação dos usuários *versus* segurança nos processos de negócio



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

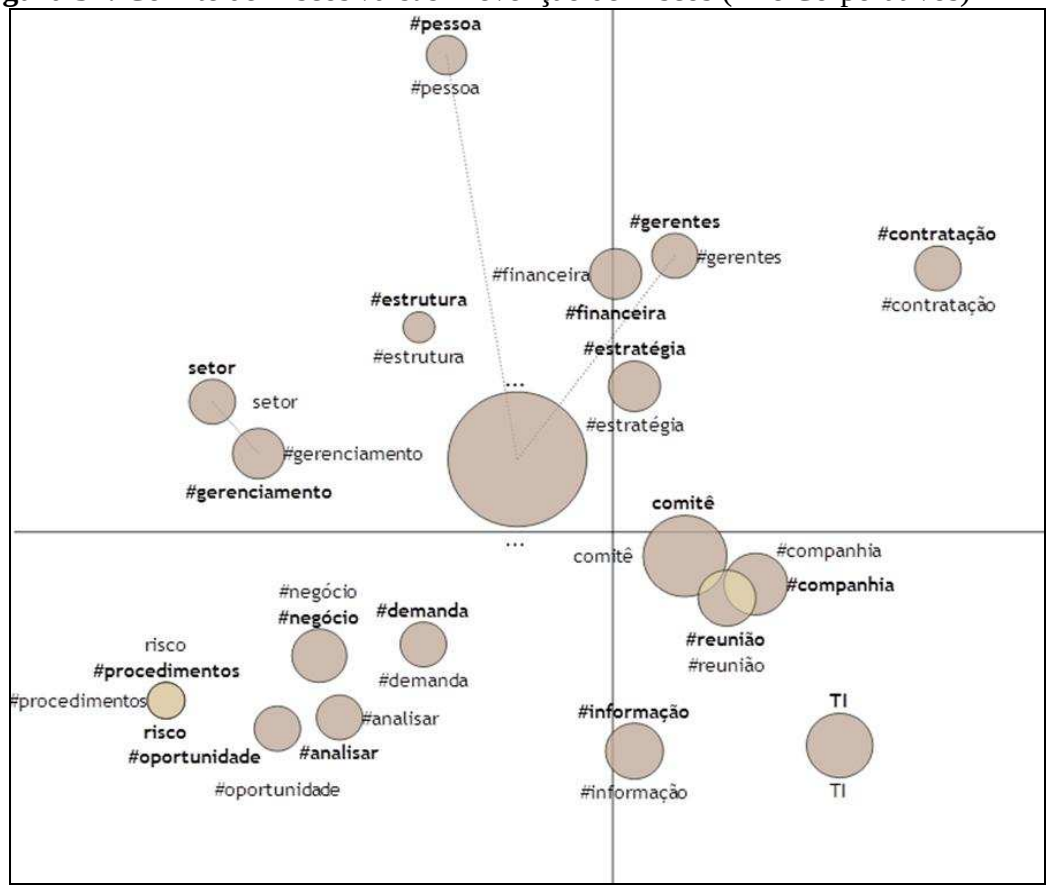
Percebe-se, por exemplo, a aproximação com significância entre os léxicos, Informações e TI, outro aspecto a destacar é esta mesma relação entre as variáveis: regra, evitado, contratação, minimiza e mercado.

Isso demonstra que a TI responde pelas necessidades de informações dos usuários, no processo de segurança da informação. Já o estabelecimento de processos de negócio precisa da contratação de regras e procedimentos mais eficientes, que alinhados as práticas de GC e as expectativas do negócio objetivem uma boa relação com o mercado, garantida pela segurança obtida na minimização de riscos decorrentes da atuação do usuário, como por exemplo os riscos corporativos operacionais de pessoal e processos.

Esta afirmação encontrada na análise léxica das entrevistas, é justificada pela participação dos usuários na gestão de riscos de segurança dos sistemas de informações mediante o alinhamento dos controles de segurança com os objetivos do negócio, conforme salientam na literatura Spears e Barki (2010). Cabe salientar que a participação do usuário no desenvolvimento das estratégias voltadas para a segurança da informação, ainda necessita ser ampliada principalmente mediante investimentos em treinamentos adequados, conforme pode ser observado nas entrevistas realizadas.

Outro aspecto de destaque na relação entre a gestão dos riscos corporativos e a gestão dos riscos de TI é a atuação do Comitê de Riscos. A criação de comitês para tratar de assuntos de interesse do conselho de administração é ponto recomendado nas práticas de governança corporativa (IBGC , 2007). Na análise das entrevistas identificou-se a atuação do comitê para a gestão de riscos, instaurado na companhia há quatro anos, cuja atuação concentra-se no encontro de ações focadas para a redução de impactos negativos e o aproveitamento dos impactos positivos, no que concerne aos riscos estratégicos e financeiros. Cabe destacar as reuniões semanais deste comitê.

Figura 34: Comitê de Riscos *versus* Prevenção de Riscos (TI e Corporativos)



Fonte: Elaborado pela autora com base nos dados fornecidos pelo *Sphinx*

A atuação do comitê não contempla os riscos corporativos operacionais (pessoal, processos, tecnologia, e *compliance*), não foi identificada a atuação deste comitê relacionada aos riscos de TI. A análise do mapa fatorial representado na Figura 34, colabora com esta percepção já que os léxicos: TI, informações, procedimentos mostraram-se distantes do eixo central.

Cabe salientar que apesar da composição do comitê ser formada pelos principais gestores da corporação, a participação dos gestores de TI não foi Identificada. Isto demonstra que na atuação deste comitê os aspectos relacionados a riscos de TI não foram de forma ampla considerada. As decisões necessárias quanto os riscos de TI concentram-se de forma mais efetiva na gestão do próprio departamento de TI, com o respaldo da diretoria administrativa ou presidência da companhia quando necessário.

As entrevistas contemplaram uma questão que buscava perceber a opinião dos entrevistados quanto a existência de uma aproximação entre riscos de TI e riscos corporativos. Quanto à forma desta relação ocorrer, as respostas que foram obtidas são analisadas a seguir.

O coordenador de Sistemas destacou a existência desta relação entre a gestão dos riscos corporativos e riscos de TI, devido ao uso da tecnologia. Porém a aproximação entre estas gestões (riscos de ti e corporativos) devem ser mais eficientes, sendo isto obtido mediante atuação de TI mais presente no comitê de riscos, bem como mediante a melhoria da cultura relacionada ao uso da tecnologia e possíveis riscos associados.

> *[...] A primeira forma seria fazer parte do comitê, este comitê está mais voltado às questões dos negócios, que não são da área de tecnologia. Na minha visão, a primeira forma de atuar nesta relação seria reformar nossos gestores em tecnologia, um trabalho de aculturamento destes profissionais em relação aos riscos possíveis, como funciona esse mundo, quais são as possibilidades, como é que as fraudes ocorrem, falar em riscos de descontinuidade do negócio ou o que pode ocorrer se o nosso Data Center parar. Se todos apoiassem e estivessem alerta para possíveis problemas, talvez se essas questões fossem fortalecidas um pouquinho mais com os gestores, realmente desenvolvendo este conhecimento. [...]* ***Coordenador de Sistemas.***

As dificuldades quanto a cultura dos gestores relacionada à gestão de riscos de TI, também pode ser percebida na fala do Membro do comitê de riscos, que mostrou desconhecer boa parte da atuação de TI relacionada a este aspecto. Adicionalmente este destacou que problemas relacionados à tecnologia podem comprometer as relações com o mercado acionário (representado pela CVM), demonstrando assim que um risco gerado no ambiente de TI pode gerar ou potencializar o efeito sob um risco corporativo, como por exemplo o risco de marca, imagem ou reputação.

> *[...] Eu não sei qual controle de acesso, também não sei exatamente quais são as ações, que eu tenho que ter caso um hacker entre para controlar o servidor, não sei exatamente o que é que eles fazem, para fazer isso. Enxergo, por exemplo, vou pegar um exemplo bem provável que faz o funcional site ou a nossa conexão com as fazendas, a gente pode não conseguir fechar o resultado em tempo, quer dizer, a gente tem uma comunicação hoje com as fazendas, a TI talvez tenha te falado que a gente coloca internet nas fazendas, só que não tem internet nas regiões lá, então a gente pega o ponto mais próximo e vai colocando, multiplicando assim, até chegar à fazenda, em seguida a gente fica fazendo quedas lá, e apesar da gente consegui telefone, eu sei que essa questão de telefone também esta com a TI, celulares, então isso às vezes dá problema mesmo, e tem coisas que são estruturais do país, e que faltam e a gente acaba tendo que fazer e que acabam impactando diretamente, é algo como eu não consigo acessar a internet aqui num dia que eu tenho que subir um arquivo para a CVM, eu vejo isso de varias formas. [...]* ***Membro do Comitê de Riscos.***

O Gerente corporativo de TI percebe a relação entre a gestão dos riscos de TI com os riscos corporativos, afirmando a inter-relação entre estes, assim como o Membro do comitê de riscos. Conforme trecho extraído da entrevista.

> *[...] Eu acredito que sim. Com certeza, tem riscos que são puramente de TI, mas há também riscos que são inter-relacionados. Hoje como falei, o principal risco que vejo é vazamento de informações, em termos de TI, a empresa por sua vez, se existe algum aspecto de concorrência, ou até de má fé , algum aspecto relacionado à atitude de algum funcionário que não está satisfeito com alguma prática, que possa fazer alguma denuncia, se a empresa não proteger as informações, pode acarretar em outros riscos que afetem o negócio, eu vejo que esses riscos são bastante conectados. Em minha opinião, o risco de TI, é um risco a mais nos riscos corporativos, caso os riscos de TI não sejam gerenciados ou não sejam monitorados, eles podem avançar para outros riscos de negócio.. [...]* ***Gerente Corporativo de TI.***

Da analise do texto extraído da entrevista percebe-se que o Gerente corporativo de TI considera os riscos de TI como sendo um tipo de riscos a mais nos riscos corporativos.

No Quadro 29 é realizada uma análise consolidada entre os principais achados desta seção. Cabe salientar que a primeira coluna do Quadro 29 corresponde as categorias relativas a gestão de riscos de TI versus gestão de riscos corporativos, identificadas anteriormente no *Framework* metodológico (Quadro 17).

Quadro 29: Principais achados Gestão de riscos de TI versus Gestão riscos corporativos

GESTÃO RISCOS DE TI versus GESTÃO RISCOS CORPORATIVOS	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Atuação de TI *versus* perspectiva de negócio	A TI atua de forma a auxiliar em melhorias nos processos organizacionais, com informações integradas para melhor atendimento das necessidades informacionais do negócio. Esta atuação contempla os controles internos utilizados pelas demais áreas, atuando de forma a facilitar e direcionar estes. A atuação de TI ocorre de forma a melhorar as perspectivas de negócio, frente às perspectivas do negócio visa manter a confiabilidade das informações, logo a manutenção deste requisito ocorre mediante uma atuação voltada à proteção das informações, ou seja, aliada a práticas de redução de riscos.	TI, negócio, confiabilidade, informação, procedimento, integra e proteção.	Não localizado	Não localizado
Governança corporativa *versus* gestão de riscos em TI e Riscos corporativos	Na percepção dos entrevistados é percebida a atuação da companhia quanto as práticas de governança com a redução dos riscos, de forma superficial. Identificou-se a necessidade de maior clareza e interação das práticas de GC com as atividades dos departamentos, o processo de governança gera uma troca entre a empresa, mesmo sendo esta interação realizada de forma informal mediante a ética no ambiente organizacional. Foi identicado queo processo de governança corporativa gera uma troca entre a empresa, o mercado acionário e os investidores, capaz de gerar aprendizados possíveis de evitar riscos.	Comunicação, TI, contábeis, financeira, impacta, negócio, corporação, acionista.	Não localizado	Identificou-se compromissos organizacionais relativos a GC. Estes compromisos se relacionam com os riscos de TI pelos compromissos informacionais (informações e dados), e com a qualidade das informações. Já os riscos corporativos estão relacionados ao compromisso com as partes interessadas. A melhoria destes aspectos ocorre com a prática de auditorias em processos e relatórios (auditoria externa e interna).
Criação de mecanismos de controle *versus* redução de riscos em TI e Riscos corporativos e Estabelecimento de controles internos	Adoção de controles internos possibilita a redução de riscos de TI e Corporativos, este último principalmente vinculado aos tipos operacionais. A existência de regras e protocolos foi considerada importante para evitar qualquer tipo de riscos. Os controles internos foram identificados como capazes de proteger as informações, porém existem alguns problemas relacionados principalmente a erros na produção destes informes, a atuação da auditoria na identificação dos pontos a serem consertados proporciona a melhoria deste risco.	Procedimentos, funcionários (usuários), dados, negócio, agricultura, gerenciamento e companhia.	Não localizado	Na análise documental constatou-se no relatório das demonstrações financeiras de 2011 o aprimoramento dos controles internos mediante a implementação do sistema operacional (ERP) que integrou as informações das fazendas com a matriz (SLC, 2012b). Foi evidenciado nas demonstrações financeiras da companhia a responsabilização dos controles internos por permitir a elaboração das demonstrações, evitando distorções ocasionadas por fraudes e erros,

GESTÃO RISCOS DE TI versus GESTÃO RISCOS CORPORATIVOS	PRINCIPAIS ACHADOS			
	Entrevistas		Questionário	Análise dos documentos
Atuação dos usuários *versus* segurança nos processos de negócio	A TI responde pelas necessidades de informações dos usuários, no processo de segurança da informação. Já o estabelecimento de processos de negócio precisa da contratação de regras e procedimentos mais eficientes, que alinhados as práticas de GC e as expectativas do negócio objetivem uma boa relação com o mercado.	Informações, TI, regra, evitado, contratação, minimiza e mercado.	Não localizado	Não localizado
Atuação Comitê de riscos *versus* prevenção de riscos de TI e Corporativos	A atuação do comitê para a gestão de riscos, instaurado na companhia há quatro anos, cuja atuação concentra-se no encontro de ações focadas para a redução de impactos negativos e o aproveitamento dos impactos positivos, no que concerne aos riscos estratégicos e financeiros. Esta atuação não contempla os riscos corporativos operacionais (pessoal, processos, tecnologia, e compliance), não foi identificada a atuação deste comitê relacionada aos riscos de TI.	TI, informações, procedimentos.	Não localizado	Não localizado
Aproximação entre riscos corporativos e riscos de TI	A existência desta relação entre a gestão dos riscos corporativos e riscos de TI, devido ao uso da tecnologia. As gestões (riscos de ti e corporativos) devem ser mais eficientes, sendo isto obtido mediante atuação de TI mais presente no comitê de riscos, bem como mediante a melhoria da cultura relacionada ao uso da tecnologia e possíveis riscos. Problemas relacionados à tecnologia podem comprometer as relações com o mercado acionário, demonstrando assim que um risco gerado no ambiente de TI pode gerar ou potencializar o efeito sob um risco corporativo. Os riscos de TI puderam ser identificados com um tipo de riscos a mais nos riscos corporativos.	Não localizado	Não localizado	Não localizado

Fonte: Elaborado pela autora (2012)

Na próxima seção foram realizadas análises consolidadas sobre os principais aspectos localizados na etapa de análise dos dados, com vistas a responder os objetivos específicos desta pesquisa.

5. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Esta seção busca relatar de forma consolidada os principais achados encontrados na análise de dados, de forma a atender aos objetivos deste estudo.

No que concerne ao primeiro objetivo específico, que buscava identificar os requisitos de negócio relacionados à gestão dos riscos da tecnologia da informação (TI) e a gestão dos riscos corporativos. Pode ser evidenciado na literatura que requistos de negócio como confidencialidade, integridade e disponibilidade podem ser mantidos, mediante uma gestão integrada entre riscos corporativos e riscos de TI.

Esta verificação pôde ser aprofundada no caso de estudo através da análise das vantagens, desvantagens e ações decorrentes da TI frente aos processos de negócio. Dentre elas destaca-se:

- Vantagens: i) facilidade na integração de informações independente da localização geográfica; ii) disponibilização de informações para os controles dos negócios operacionais e análises estratégicas; iii) uniformidade de informações; iv) Agiliza controles internos.
- Desvantagens: i) cultura das pessoas relacionada a mudanças tecnológicas; ii) Complexidade de uso de alguns recursos tecnológicos; iii) O custo com treinamentos necessários para utilização dos recursos; iv) custo elevado para implantação e manutenção de novas tecnologias.

Ao comparar as vantagens e desvantagens do uso da tecnologia pode ser percebido que decorrentes destas, riscos corporativos podem sem impulsionados como por exemplo riscos operacionais relacionados a processos ou pessoal. Identificou-se adicionalmente que o requisito confiabilidade das informações pode ser otimizado mediante melhorias nos processos de negócio, reduzindo assim os custos de manutenção das informações destes processos, mediante redução das falhas ou erros.

Além disto, ações como: investimentos em ERP, auditorias (externas e internas), e atuação da central NOC (núcleo de operações e controle) buscam proporcionar a manutenção dos requisitos de negócio. Estas ações foram percebidas como indicadas para a redução de custos e tempo nos processos de negócio, bem como para a manutenção da disponibilidade e integridade das informações.

O segundo objetivo buscou analisar a relação entre os modelos de gestão de riscos de tecnologia da informação (TI) e de gestão de riscos corporativos. Identificou-se na literatura modelos para a gestão de riscos, dentre eles o COBIT (desenvolvido pela ISACA) que através de seu processo de número nove (PO9) estabelece o processo para a avaliação e gerenciamento dos riscos de TI. Já no que concerne aos riscos corporativos a ISO 31000 (2009) foi evidenciada como um modelo que estabelece princípios e as diretrizes genéricas para a gestão dos riscos.

Da comparação destes dois modelos realizada na seção 2.3 (Gestão de riscos de TI versus Gestão de riscos corporativos) percebeu-se que os dois modelos possuem uma estrutura próxima, apesar de a Norma ISO 31000 (2009) estabelecer princípios para a gestão de riscos corporativos, e o processo de comunicação e consulta as partes interessadas, tais aspectos não foram abrangidos na estrutura para a gestão de riscos de TI proposta pelo COBIT. Identificou-se que o COBIT apresenta-se como um modelo mais focado na gestão e monitoramento dos riscos de TI, já a ISO 31000 busca operacionalizar de forma genérica desde os princípios a serem estabelecidos até a realização do monitoramento de toda a estrutura para gestão de riscos. Neste âmbito, concluí-se que as normas não são excludentes, elas acabam de certa forma se complementando não sendo percebidos motivos para elas não serem utilizadas em conjunto pelas corporações.

No caso de estudo a utilização dos modelos COBIT e ISO 31000 não ocorrem de forma plena, ou integrada. Pode ser identificado que os esforços existentes para gerenciamento dos riscos de TI e riscos de corporativos, se concentram principalmente nas etapas de identificação, avaliação e resposta a eventuais riscos. Processos como a manutenção e monitoramentos dos planos para remediação dos riscos puderam ser evidenciados como pouco elaborados, conforme analisado nas seções 4.3 e 4.4.

Tal aspecto ocorre possivelmente pela falta de comunicação existente entre as áreas em se tratando de gestão de riscos de TI e riscos corporativos. Além do não atendimento de princípios para gestão de riscos como: a participação da gestão de riscos nos processos organizacionais, a atuação de forma transparente e inclusiva e de forma dinâmica e interativa (capaz de reagir às mudanças).

Por fim o último objetivo específico contemplou analisar as práticas da gestão de riscos de TI e da gestão riscos corporativos, em relação aos processos organizacionais.

No que concerne à gestão de riscos em TI , percebeu-se nas análises que estas contemplam procedimentos com participação dos usuários, havendo uma preocupação com controles sobre acesso, sistemas e a qualidade das informações. Mesmo assim, esta participação precisa ser ampliada para haver uma disseminação de práticas que proporcionem redução efetiva de riscos.

Quanto aos riscos corporativos foi identificada uma gestão focada nos riscos do tipo estratégico e financeiros, mediante atuação do comitê de riscos. Já em se tratando dos riscos do tipo operacional, a gestão fica a cargo de cada setor, mediante os controles internos instaurados por eles, não sendo identificada neste sentido uma atuação inter-relacionada entre os diversos tipos de riscos corporativos, esta percepção foi relatada de forma aprofundada na seção 4.5 (gestão de riscos em TI *versus* gestão dos riscos corporativos).

Aspectos como a melhoria nas regras e protocolos relacionados aos processos de negócio foram identificados como importante para evitar qualquer tipo de riscos. Neste contexto, salientam-se os controles internos como capazes de proteger as informações, principalmente em problemas relacionados a erros na produção de informações. Para tanto a atuação da auditoria na identificação dos pontos a serem consertados auxilia na melhoria destes aspectos.

Adicionalmente identificou-se no estudo do caso riscos relacionados ao ambiente de TI e riscos corporativos, sendo eles: **Riscos de TI**: vazamento de informações confidenciais (por exemplo, preços e margens de lucro); fraudes relacionadas a sistemas; a invasão de externos aos sistemas provocando instabilidade (acessos indevidos). **Riscos Corporativos** – risco econômico (dependência do comercio internacional), risco político, risco de mercado (*preços de commodities*), risco de *compliance,* risco de pessoal, processos e tecnologia. Sendo que os três últimos citados não foram percebidos como fontes de riscos relevantes na análise documental.

Apesar de a tecnologia ser um aspecto de relevante importância no planejamento agrícola e processos da organização, bem como o investimento em novas tecnologias estar presente no código de conduta relacionado ao compromisso com a sustentabilidade (SLC, 2012b), não houve destaque desta fonte de riscos nas entrevistas no que concerne aos riscos corporativos. Este fator pode estar relacionado à atuação da TI de forma não integrada e conectada a gestão de riscos corporativos da corporação.

A gestão dos riscos no atual ambiente de negócios pode ser fator transformador de pontos negativos em oportunidades, pois esta gestão remete a redução de perdas com eventos inesperados, propiciando neste sentido o aumento da competitividade. Gerenciar os riscos significa instalar técnicas administrativas a fim de reduzir a probabilidade de ocorrência de eventos negativos sem, no entanto, incorrer em altos custos e nem paralisar as atividades (GERIGK e CORBARI, 2011).

Os dados analisados indicaram a atuação de TI no caso de estudo focado em encontrar melhorias nos processos organizacionais, contemplando os controles internos utilizados pelas demais áreas, atuando de forma a facilitar e direcionar estes. Cabe destacar que segundo o ITGI (2007) requisitos de negócio como a confiabilidade das informações são melhorados mediante uma atuação voltada à proteção das informações, ou seja, aliada a práticas de redução de riscos.

Os resultados decorrentes desta pesquisa indicaram que no caso investigado não existe um processo formal de gerenciamento de riscos de TI, apesar de existirem iniciativas pontuais. Já em se tratando dos riscos corporativos a atuação do comitê de riscos foi identificada, porém a estrutura instaurada não contempla a gestão do risco do tipo operacional. É importante destacar que tanto a ISO 31000 (2009) quanto o COBIT (ITGI, 2007) destacam a importância de uma estrutura para a gestão dos riscos que atue de forma a identificar os potenciais eventos causadores de impactos nas atividades das companhias.

Salienta-se neste sentido a gravidade que representa a ausência de mecanismos para o gerenciamento de riscos inter-relacionados, já que um risco pode vir a desencadear ou potencializar outros tipos de riscos conforme observa a ISO 31000 (2009). Da mesma forma, evidenciou-se uma atuação da gestão de riscos em TI não relacionada à gestão dos riscos corporativos, no que tange ao caso de estudo. Fatores como cultura organizacional, problemas com comunicação, atuação dos usuários frente às inovações tecnológicas, falta de treinamentos, e não estabelecimento e disseminação de princípios para a estrutura de gerenciamento dos riscos justificam esta falta de relação.

Além disto, cabe destacar a participação do usuário na estrutura para o gerenciamento de riscos. Neste sentido, identificou-se a participação significativa dos usuários na adoção dos planos de segurança. Porém, em processos de TI esta precisa ser mais efetiva, principalmente relacionada aos usuários das fazendas (unidades produtivas), gerando assim uma maior conscientização aos riscos e melhoria na segurança das informações, conforme recomendam BULGURCU, CAVUSOGLU E BENBASAT (2010) e SPEARS e BARKI (2010).

Em se tratando da relação existente entre a gestão de riscos de TI e a gestão dos riscos corporativos, os achados indicaram que esta é possível mediante a construção de uma estrutura para o gerenciamento que atue de forma inter-relacionada aos diversos tipos de riscos.

Aspectos foram identificados como pontos a serem contemplados nesta estrutura organizacional transferível para outros cenários, dentre eles:

a) atuação abrangente do comitê de riscos (em se tratando de riscos de TI bem como nos riscos corporativos do tipo operacional);

b) disseminação de práticas de governança corporativa para melhoria da cultura organizacional e comunicação;

c) atuação de auditorias internas e externas para melhorias nos controles internos e na estrutura de gerenciamento dos riscos;

d) monitoramento e controle sobre planos de ação para remediação de riscos.

Desta forma, as evidências indicaram oportunidades de melhorias da relação entre a gestão dos riscos de TI e riscos corporativos, bem como para manutenção de requisitos de negócio como a integridade, disponibilidade e confidencialidade das informações.

5.1. RECOMENDAÇÕES PARA ESTUDOS FUTUROS

Recomenda-se para estudos futuros análises voltados a avaliação inter-relacionada dos diferentes tipos de riscos. Dentre eles:

a) A realização de pesquisa que busque avalie os diferentes tipos de riscos corporativos neste trabalho identificados, mediante análises par a par, de acordo com a simulação contemplada neste estudo que utilizou o uso método *analytic hierarchy process* – AHP (Saaty, 1991), ver Apêndice F;

b) Realização de pesquisas similares em empresas de outros setores ou portes econômicos, ou em empresa do mesmo setor no futuro;

c) Realização de estudos que busquem identificar a gestão dos riscos de tecnologia da informação (TI) em processos de produção dependentes de grandes inovações tecnológicas, em empresas onde a tecnologia seja um importante direcionador de custos.

Por último, acredita que as contribuições desta dissertação reforçam a necessidade de uma estrutura para gestão de riscos, alinhada ao negócio, com vistas a redução de custos decorrentes de eventos não identificados. Neste sentido ao gerenciar de forma eficiente estes aspectos as companhias economizam recursos, e podem destinar estes a avanços tecnológicos, ou em outras ferramentas relacionada a melhoraria do seu desempenho.

REFERÊNCIAS

ALBERTIN, A. L.; ALBERTIN, R. M. de M. Dimensões do uso de tecnologia da informação: um instrumento de diagnóstico e análise. **RAP - Revista de Administração Pública.** Rio de Janeiro, v.46, n.1, p.125-51, jan./fev. 2012

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.

AS/NZS 4360:1999. Administración de Riesgos Estándar Australiano. Disponível em: < http://www.netconsul.com/riesgos/ar.pdf>. Acesso em: 09 mar. 2012

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO 31000**: Gestão de Riscos – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ISO/IEC 27002**. Tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

AVEN, T. On the new ISO guide on risk management terminology. **Reliability Engineering and System Safety**. n.96, p.719–726, 2011.

BANCO CENTRAL DO BRASIL - BCB. Resolução nº 2804 de 21 de dezembro de 2000, Dispõe sobre controles do risco de liquidez. Disponível em: < http://www.cnb.org.br/CNBV/resolucoes/res2804-2000.htm> Acesso em 03 mar. 2012.

BRITO, Osias. Controladoria: de risco-retorno em instituições financeiras. São Paulo: Saraiva, 2003. 225p.

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 > . 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.

CARMONA, E.; PEREIRA, A. C.; SANTOS, M. R.. A Lei Sarbanes-Oxley e a percepção dos gestores sobre as competências do auditor interno. **Revista Gestão e Regionalidade**. São Caetano do Sul, v.26, n.76, p.63-74, 2010.

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

COIMBRA, F. C. Estrutura de governança corporativa e gestão de riscos: um estudo de caso no setor financeiro. Tese (Doutorado em Administração). USP - Universidade de São Paulo, São Paulo, 2011.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. Gerenciamento de Riscos Corporativos. Estrutura Integrada: Sumário Executivo e Estrutura e Gerenciamento de Riscos na Empresa. 2007. Disponível em: < http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em 10 mar. 2012.

COMISSÃO DE VALORES MOBILIÁRIOS - CVM. Recomendações da CVM sobre governança corporativa (2002). Disponível em < http://www.cvm.gov.br/port/public/publ/cartilha/cartilha.doc >. Acesso em 15 jan. 2011.

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES. Relação de Cursos Recomendados e Reconhecidos. Disponível em: http://conteudoweb.capes.gov.br/conteudoweb/ProjetoRelacaoCursosServlet?acao=pesquisarIes&codigoArea=60200006&descricaoArea=CI%CANCIAS+SOCIAIS+APLICADAS+&descricaoAreaConhecimento=ADMINISTRA%C7%C3O&descricaoAreaAvaliacao=ADMINISTRA%C7%C3O%2C+CI%CANCIAS+CONT%C1BEIS+E+TURISMO. Acesso em: 19 mar. 2012.

CUNHA, P. R.; SILVA, J. O. da ; FERNANDES, F. C. Risco Empresariais Divulgados nas Ofertas Públicas de Ações no Brasil. **RBGN- Revista Brasileira de gestão de negócios. São Paulo**, v. 13, n.41, p. 454-471. Out./dez. 2011.

DANTAS, J.A.; RODRIGUES, F.F.; MARCELINO, G.F.; LUSTOSA, P.R.B. Custo-benefício do controle: proposta de um método para avaliação com base no COSO. **Revista Contabilidade Gestão e Governança.** Brasília**,** v.13, n.2, p.3-19. 2010.

EISENHARDT, Kathlenn M.; GRAEBNER, Melissa E. Theory building from cases: opportunities and challenges. **Academy of Management Journal**, v. 50, n.1, p.25–32. 2007.

FENKER, E.A. Risco ambiental e gestão de custos ambientais: um estudo de sua relação em empresas atuantes no Brasil. Dissertação (mestrado em Ciências Contábeis). UNISINOS-Universidade do vale do Rio dos Sinos,São Leopoldo, 2009.

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.

FRIGO, M. L.; ANDERSON, R. J. Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. **The Journal of Corporate Accounting & Finance.** p.81– 88. Mar./abr. 2011.

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, Antonio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2009.

GUIMARÃES, I.C.; PARISI, C.; PEREIRA, A.C.; WEFFORT, E. F. J..A importância da controladoria na gestão de riscos das empresas não financeiras: um estudo da percepção de gestores de riscos e *controllers.* **RBGN- Revista Brasileira de gestão de negócios. São Paulo**, v. 11, n.32, p. 260-275. Jul./set. 2009.

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Código das melhores práticas de governança corporativa. 2009. Disponível em: < http:// www.ibgc.org.br >. Acesso em 17 jan. 2011.

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de Orientação para Gerenciamento de Riscos Corporativos. 2007. Disponível em: < http://www.ictsglobal.com/new/arquivos/IBGC-orientacaogerriscoscorporativos.pdf>. Acesso em 17 jan. 2012.

INFORMATION SECURITY GOVERNANCE – ITGI. Cobit 4.1: objetivos de controle, diretrizes de gerenciamento, modelos de maturidade. 2007. Disponível em: < http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-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.

JO, H.; HARJOTO, M.A. The causal effect of corporate governance on corporate social responsibility. **Journal of Business Ethics**, p.53-72, 2012.

JUNIOR, R. R. da S.; JUNQUEIRA, L. R.; BERTUCCI, L. A. A Relação entre a adoção de praticas da governança corporativa e a alavancagem financeira das empresas Brasileiras do setor energético no ano de 2008. **GES - Revista Gestão e Sociedade.** Belo Horizonte, v.3, n. 6, p.315-334. Jul./dez. 2009.

KNORST, A. M.; VANTI, A.A.; ANDRADE, R.A.E.; JOHANN, S. L. Aligning information security whith de image of the organization and priorization based on fuzzy logic for the industrial automation sector. **Journal of Information Systems and Technology Management. São Paulo**, v.8, n.3, p. 555-580. Set./dez. 2011,

LOURENSI, A.; ZANOTTO, V. C. da S.; FERNANDES, L.; FERNANDES, F. C. RISK ASSESSMENT nas empresas do estado do Rio Grande do Sul e Santa Catarina: uma visão dos auditores independentes. *In:* 5º CONTECSI - International Conference on Information Systems and Technology Management. **Anais.** p. 601-615. São Paulo, 2008..

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.

LUCIANO, E. M.; TESTA, M. G. Controls of information technology management for business processes outsourcing based on COBIT. **Journal of Information Systems and Technology Management.** São Paulo, v. 8, n.1, p. 237-262. 2011.

MARINHO DA SILVA, B. A. ; MORAES, G. H. S. M. de. Influência dos direcionadores do uso da TI na Governança de TI. **RBGN- Revista Brasileira de gestão de negócios. São Paulo**, v. 13, n.38, p. 41-60. Jan/mar, 2011.

MARSHALL, C. L. Medindo e gerenciando riscos operacionais em instituições financeiras. Rio de Janeiro: Qualitymark, 2002.

RAFEQ, A. Using COBIT for Assessing IT Process Maturity: A Case Study. **COBIT Focus**. v.4, n.1. out, 2010.

RODRIGUES, L. C.; MACCARI, E. A.; SIMÕES. O desenho da gestão da tecnologia da informação nas 100 maiores empresas na visão dos executivos em TI. **Journal of Information Systems and Technology Management.** v.6, n.3. p.483-506. 2009.

ROSSONI, L.; SILVA, C. L. M. da. Organizational Institutionalism and Corporate Governance. **RAC - Revista de administração contemporânea - Edição especial.** Curitiba, p.173-198. 2010.

SAATY, T.L. Método de análise hierárquica. Tradução e revisão técnica Wainer da Silva e Silva. São Paulo: McGraw-Hill, Makron,1991. 368p.

SANTANA, A.; VERAS, M. Gerenciamento de riscos de TI e suas práticas nas organizações Brasileiras: um estudo de casos múltiplos. *In:* 8º CONTECSI - International Conference on Information Systems and Technology Management. **Anais.** São Paulo, p.570-598. 2011.

SÊMOLA, Marcos. Gestão da segurança da informação : uma visão executiva. Rio de Janeiro : Campus, 2003. 156 p.

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

SILVA NETTO, A. da.; SILVEIRA, M. A. P.. Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas empresas. **Journal of Information Systems and Technology Management.** v.4, n.3. p. 375-397. 2007.

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

SILVEIRA, J. C. ; DUCA, A. F.; MARIO, P. C. Um estudo dos impactos nos disclosure das empresas brasileiras que negociam suas ações na nyse, quanto às exigências trazidas pela lei sarbanes-oxley. *In*: X Congresso USP de Controladoria e Contabilidade. **Anais**. 2010.

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.

SCHNEIDER LOGEMANN & CIA – SLC. Apresentação para o Investidor. Disponível em:< http://www.mzweb.com.br/SLCAgricola2009/web/conteudo_pt.asp?tipo=29143&refbread=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 > Acesso em 12 abr. 2012b.

_____.Demonstrações Financeiras 2011.Disponível em: < 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.

TAROUCO, H.H.; GRAEML, A.R. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. **R.Adm - Revista de Administração**. São Paulo, v.46, n.1, p.07-18, Jan./mar. 2011.

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 framework 2010. **Academy of Information and Management Sciences Journal.** v.13, n.1. 2010

VANTI, A. A. ; ORTEGA, A. C. ; BLANCO, R. R. Avaliação de modelo de governança de TI com o uso de FAHP. *In*: 8th CONTECSI- International Conference on Information Systems and Technology Management. **Anais.** São Paulo, 2011.

WEBB, P.; POLLARD, C.; RIDLEY, G.. Attempting to Define IT Governance: Wisdom or Folly?. *In* Proceedings of the 39th Hawaii International Conference on System Sciences. **Anais**. 2006.

WEILL, P.; ROSS, J. W. Governança de TI: Como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores. São Paulo: M. Books, 2006.

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

ZONATTO, V. C. da S.; BEUREN, I. M. Categorias de riscos evidenciadas nos relatórios da administração de empresas brasileiras com ADRS. **RBGN- Revista Brasileira de gestão de negócios. São Paulo**, v.12, n.35, p. 260-275. Abr/jun, 2010.

APÊNDICE A - PROTOCOLO ESTUDO DE CASO

UNIVERSIDADE DO VALE DO RIO DOS SINOS

Programa de Pós-Graduação em Ciências Contábeis

Nível de Mestrado

Prezado (a) Sr (a):

Sou aluna do Programa de Pós-Graduação em Ciências Contábeis da UNISINOS – Universidade do Vale do Rio dos Sinos e estou desenvolvendo um estudo que tem por objetivo analisar a relação entre a Gestão de riscos de TI e o Gerenciamento de Riscos Corporativos.

A realização deste estudo reveste-se de importância pela carência de trabalhos específicos sobre a relação entre Gestão de Riscos de TI e a Gestão de Riscos Corporativos. Assim, venho solicitar a indispensável colaboração de V.S.ª no sentido de conceder respostas para a entrevista proposta, bem como autorização para realização do estudo de caso, sendo estes necessários para o desenvolvimento da pesquisa.

Informo que os resultados desta pesquisa serão disponibilizados à V.Sª e que os dados fornecidos serão tratados de forma comparativa e informativa, caso haja a necessidade de sigilo da razão social da empresa, nos comprometemos em respeitar e aplicar os cuidados necessários para a manutenção e zelo da política de imagem da empresa.

Sua contribuição e colaboração serão de fundamental importância para o estudo proposto, cujas informações encontram-se abaixo descritas no protocolo do estudo de caso.

Atenciosamente

Rosane Machado

Mestranda PPG Unisinos

PROTOCOLO DE ESTUDO DE CASO

1. VISÃO GERAL DO PROJETO DE ESTUDO DE CASO

a) TÍTULO:

ANÁLISE DA RELAÇÃO DA GESTÃO DOS RISCOS DA TECNOLOGIA DA INFORMAÇÃO (TI) E A GESTÃO DOS RISCOS CORPORATIVOS

b) OBJETIVO DO ESTUDO:

O objetivo geral proposto é de analisar a relação entre a gestão de riscos de TI e o gerenciamento dos riscos corporativos.

c) RESUMO:

Ao fim de garantir que as informações sejam seguras é preciso encontrar maneiras de minimizar os riscos inerentes ao negócio e ao ambiente de TI. Uma das formas de buscar a redução desta vulnerabilidade é mediante a gestão destes diferentes riscos. Para a ISO 31000 (2009), a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação, considerando a incerteza, a natureza desta incerteza, e como ela pode ser tratada. Este estudo comprova sua importância ao contribuir com a ampliação da pesquisa em torno dos temas riscos de TI, e riscos corporativos tornando-se relevante para o meio acadêmico e profissional, já que visa verificar a teoria encontrada neste âmbito e a aplicação prática dos conceitos mediante verificação no caso de estudo.

2. Tópicos principais abordados na revisão da literatura

a) Gestão de riscos em TI (GTI)

- Governança Corporativa e Surgimento da GTI
- *Control Objectives for Information and Related Technology* - COBIT
- P09 – COBIT – Modelo de avaliação dos Riscos de TI

b) Gestão de Riscos Corporativos

- A ISO 31000 (2009) estrutura genérica para avaliação dos riscos;
- Princípios para a Gestão de Riscos;
- Estrutura da Gestão de Riscos;
- Processos para a Gestão de Riscos;

3. Procedimentos de Campo

a) Aspectos Metodológicos:

Como estratégica metodológica foi utilizada a do estudo de caso. O estudo de caso segundo Yin (2010), ressalta o exame contextual detalhado de um número limitado de eventos ou condições e seus relacionamentos, sendo geralmente o objeto deste tipo de investigação uma entidade, pessoa ou um

grupo de pessoas.

b) Fontes de Evidências e Instrumentos de coleta de dados:

Para o bom andamento da pesquisa será necessário efetuar alguns procedimentos, tais como entrevista aplicada aos responsáveis pela área de riscos e tecnologia da informação, bem como análises de documentos internos e externos da organização.

c) Executor da Pesquisa:

Aluno/Pesquisador: Rosane Machado

Supervisão: professor Dr. Adolfo Alberto Vanti

Instituição: Unisinos – Universidade do Vale do Rio dos Sinos

Curso: Mestrado Acadêmico em Ciências Contábeis

Ênfase: Controladoria e Finanças

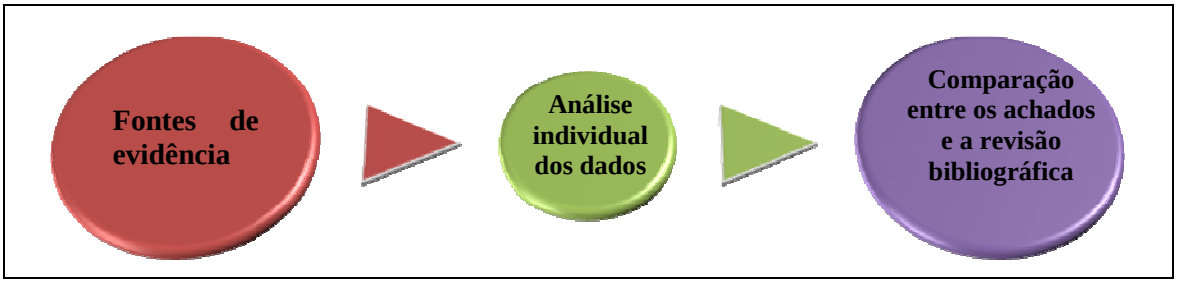
Linha de Pesquisa: Controle de Gestão

Contato: 51-9517-2514

Email: machado.rosane@gmail.com

4. Análise do caso de estudo

A análise dos dados se dará da seguinte forma:



1. Agrupar as análises das fontes de evidencias;
2. Agrupar as informações do caso apresentado seguindo a ordem dos tópicos do estudo;
3. Comparar o caso apresentado com a revisão bibliográfica;
4. Inserir os dados coletados no software *Sphinx* para análise léxica dos dados coletados;
5. Agrupar as informações obtidas com a revisão bibliográfica seguindo a ordem dos tópicos de estudo
6. Confeccionar o relatório de análise dos dados.

APÊNDICE B - ROTEIRO DA ENTREVISTA

ROTEIRO DA ENTREVISTA

BLOCO I – CARACTERIZAÇÃO DO RESPONDENTE

Nome do respondente:
Cargo (ocupação):
Tempo na Função e na empresa:
Formação acadêmica:
Idade:
Principais Responsabilidades:

BLOCO II – GESTÃO DOS RISCOS DE TI

CATEGORIA	QUESTÃO
1	Na sua percepção, como o modo que TI é gerenciado na organização permite o desenvolvimento do planejamento estratégico, planejamento de TI, e gestão de riscos? Este gerenciamento ocorre de forma crítica e realista? SIMONSON, JOHNSON e EKSTEDT (2010).
2	De que forma a confidencialidade, integridade e disponibilidade das informações atuam dentro da organização em relação aos riscos? Na sua percepção, como estes requisitos de negócio atendem as necessidades de informações da empresa? ITGI (2007).
3	Os investimentos realizados em TI são suficientes para permitir que as informações sejam corretas, precisas e estejam disponíveis no tempo adequado? Como isso é validado pelos usuários? De que forma estes investimentos podem proteger a empresa de riscos? COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).
3	Como a estrutura de TI presente na organização possibilita a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas)? De que maneira esta estrutura interage com a prevenção dos riscos? ITGI (2007).
4	Quais as vantagens ou desvantagens que a Tecnologia da Informação – TI oferece decorrentes de seu uso? Qual a sua percepção da relação desta utilização com os riscos? ALBERTIN e ALBERTIN (2012).
4	Como a empresa implanta planos de segurança para reduzir os riscos relacionados à segurança das informações? Qual o envolvimento funcional dos usuários? De que maneira eles participam da gestão de riscos e segurança? BULGURCU, CAVUSOGLU E BENBASAT (2010); SPEARS E BARKI (2010)
5	De que maneira os processos de TI possibilitam que a entrega e suporte dos serviços de TI atendam as necessidades dos usuários? Como a prestação de serviços de TI atua para minimizar os riscos? ITGI (2007).
6	Como a recomendação e comunicação de planos de ação de remediação dos riscos consideram a participação dos usuários para a gestão de riscos e segurança? Como esta gestão se integra aos processos gerenciais? SPEARS E BARKI (2010); ITGI (2007).

7	Como a estrutura para gestão de riscos de TI é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? BULGURCU, CAVUSOGLU E BENBASAT (2010).
8	Que tipos de esforços são realizados pela corporação para manutenção e monitoramento de planos de ação para os riscos? Como estes esforços contemplam o desenvolvimento e a performance de controles? ITGI (2007); SPEARS E BARKI (2010)

BLOCO III – GERENCIAMENTO DOS RISCOS CORPORATIVOS

CATEGORIA	QUESTÃO
1	Como a organização realiza a avaliação estratégica de seus riscos? Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança ? FRIGO E ANDERSON (2011).
2	De que forma o gerenciamento dos riscos corporativos possibilitam evitar, reduzir, compartilhar ou aceitar os riscos? Na sua percepção este gerenciamento estabelecer respostas a estes, reduzindo surpresas, custos ou prejuízos associados? IBGC (2007); COSO (2007); ISO 31000 (2009); Aven (2011); GERIGK E CORBARI (2011).
3	A organização procura identificar os eventos que possam ter consequências operacionais, financeiras ou estratégicas adversas? Caso afirmativo, como são prevenidos ou minimizados tais eventos? COSO (2007); IBGC (2007); GERIGK e CORBARI (2011).
4	Como a gestão de riscos corporativos possibilitam uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos? Como isto ocorre? COSO (2007); IBGC (2007)
5	Você considera que os seguintes princípios são atendidos pela empresa, quanto à gestão de riscos. Explique como isso ocorre. ISO 31000(2009) 1) Cria e protege valor; 2) Participa de todos os processos organizacionais; 3) Participa da tomada de decisão; 4) Aborda explicitamente a incerteza; 5) Atua de forma Sistemática, estruturada e oportuna; 6) Baseia-se nas melhores informações possíveis; 7) Se adéqua a realidade da organização; 8) Considera fatores humanos e culturais; 9) Atua de forma transparente e inclusiva; 10) Atua de forma dinâmica e interativa, capaz de reagir a mudanças; 11) Facilita a melhoria contínua da organização.
6	Como a estrutura para gestão de riscos corporativos é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? BULGURCU, CAVUSOGLU E BENBASAT (2010).
6	A gestão dos riscos realizada na organização fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro? AVEN (2011).
7	Como os seguintes processos são considerados em relação aos processos de negócio organizacionais? ISO 31000(2009) 1) Comunicação e consulta às partes interessadas (internas e externas)

	2) Estabelecimento do contexto (parâmetros internos e externos que precisam ser levados em consideração) 3) Avaliação dos Riscos (identificação, análise e avaliação dos riscos) 4) Tratamento dos Riscos 5) Monitoramento e análise crítica dos Riscos
8	Como a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações? Estas decisões consideram a incerteza, a natureza desta incerteza, e como ela pode ser tratada? ISO 31000 (2009)

BLOCO IV – RELAÇÃO ENTRE GESTÃO DOS RISCOS DE TI E GERENCIAMENTO DOS RISCOS CORPORATIVOS

1) Como a TI atua para prevenir riscos inerentes ao negócio? Esta atuação pode ser considerada satisfatória dentro de uma perspectiva de negócio? ITGI (2007)
2) De que maneira os usuários participam do gerenciamento de riscos de segurança nos processos de negócios? Como a sua participação é percebida e qual é o impacto da participação na segurança do negócio? SPEARS E BARKI (2010).
3) Como a práticas de governança corporativa orientam o dia a dia do trabalho da organização? De que forma elas contribuem para a gestão de riscos em TI e gestão dos riscos corporativos? (IBGC 2009).
4) De que forma a adoção de mecanismos de controle possibilita redução dos riscos corporativos e riscos de TI? JUNIOR, JUNQUEIRA e BERTUCCI (2010).
5) Como os controles internos protegem as informações financeiras ? Esta proteção é capaz de produzir informações contábeis financeiras confiáveis? SPEARS E BARKI (2010).
6) De que maneira a atuação do comitê para a gestão de riscos ocorre? Como sua atuação contempla a prevenção de riscos de TI e risco corporativos? (IBGC 2009).
7) Em sua opinião existe uma aproximação entre os riscos de TI e riscos corporativos? Como isso seria possível?

APÊNDICE C - QUESTIONÁRIO

QUESTIONÁRIO

Escolha o nível de maturidade para os processos listados, utilize a linha vazia para explicar ações que que são tomadas pela corporação neste processo.

Para responder o questionário, considere a seguinte tabela do grau de maturidade do processo .

Grau de maturidade	Descrição (COBIT, 2007 p.68)
0 – Inexistente	Quando não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.
1 – Inicial	Os riscos de TI são considerados de forma inicial. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes. Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.
2 – Repetitivo, mas intuitivo	Quando Existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.
3 – Definido	Quando Uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos–chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela gestão de riscos estão definidas nas descrições de cargo.
4 – Gerenciado	Quando A avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os cenários de riscos relacionados a TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, e o comitê executivo e a Diretoria de TI estabeleceram os níveis de risco que a organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.
5 – Otimizado	Quando O gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A Direção de TI avalia continuamente as estratégias de mitigação de risco.

Processos COBIT		**Nível de maturidade**					
		0 - Inexistente	**1 - Inicial**	**2 – Repetitivo**	**3 - Definido**	**4 - Gerenciado**	**5- Otimizado**
PO9 - Avalia e gerencia os riscos (ITGI, 2007 p.66)							
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).							
Explique:							
PO9.2 Estabelecimento do Contexto de Risco 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 são avaliados.							
Explique:							
PO9.3 Identificação de Eventos 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 jurídicos, 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.							

Explique:							
PO9.4 Avaliação de Risco 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.							
Explique:							
PO9.5 Resposta ao Risco 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.							
Explique:							
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco 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 e 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.							
Explique:							

Você alteraria os critérios de avaliação utilizados? Por quê?

Qual a importância dos tipos de risco abaixo relacionados nas atividades organização? Para responder esta questão leve em consideração a seguinte tabela do grau de importância dos Riscos

Grau de importância	**Descrição**
Igual	Igualmente importante ou preferido
Moderado	Levemente mais importante ou preferido
Forte	Medianamente mais importante ou preferido
Muito Forte	Fortemente mais importante ou preferido
Extrema	Extremamente mais importante ou preferido

	Extrema	**Muito forte**	**Forte**	**Moderada**	**Igual**
Riscos Econômicos Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.					
Qual o significado de sua resposta:					
Riscos Políticos Eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.					
Qual o significado de sua resposta:					
Riscos Ambiental Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.					
Qual o significado de sua resposta:					
Riscos de Marca, Imagem ou Reputação					

É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e,conseqüentemente, a consecução de transações com estes clientes.					
Qual o significado de sua resposta:					
Riscos Sociais São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.					
Qual o significado de sua resposta:					
Riscos Tecnológicos (estratégicos) São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.					
Qual o significado de sua resposta:					
Riscos de Mercado A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).					
Qual o significado de sua resposta:					
Riscos de Crédito É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação					
Qual o significado de sua resposta:					
Riscos de Liquidez Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.					
Qual o significado de sua resposta:					
Riscos de Pessoal Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.					
Qual o significado de sua resposta:					
Riscos de Processos Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.					
Qual o significado de sua resposta:					
Risco de Tecnologia (operacional) Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).					
Qual o significado de sua resposta:					
Riscos de compliance Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.					

Você alteraria os critérios de avaliação utilizados? Por quê?

APÊNDICE D – ENTREVISTAS TRANSCRITAS

ENTREVISTA – COORDENADOR DE SISTEMAS

BLOCO I – CARACTERIZAÇÃO DO RESPONDENTE

Cargo (ocupação): Coordenador de sistemas da SLC Agrícola.
Tempo na Função e na empresa: No grupo SLC já estou há 8 anos, aqui na SLC Agrícola estou há 4 anos nesta mesma função. Antes da SLC trabalhei em outras empresas de grande porte com a mesma atuação. Nesse cargo estou há vinte e três anos, contando todas essas empresas. Comecei muito cedo na coordenação de sistemas, sempre mais focado na área de negócios de sistemas.
Formação acadêmica: Sou formado em administração de empresas com ênfase em análise de sistemas, e tenho especialização em gestão empresarial.
Idade: 46 anos
Principais Responsabilidades: Sou responsável pela implementação e manutenção dos sistemas de todas as fazendas e unidades do grupo, vinculados a mim estão todos os analistas de negócios, responsáveis pela parte funcional, técnica de sistemas e processos da empresa, e também a equipe de analistas de sistemas desenvolvedores. Nosso pessoal dá suporte e manutenção aos sistemas o qual só nós podemos fazer alguma manutenção, vinculados a nós há também empresas terceirizadas, grande parte não é desenvolvida dentro de casa, é feito externamente, através de chamadas, de exportação de dados, de trabalho de desenvolvimento externo, especificação interna. É um alto volume de desenvolvimento externo, consequente de homologação e testes internos.

BLOCO II – GESTÃO DOS RISCOS DE TI

CATEGORIA	QUESTÃO
1	**SIMONSON, JOHNSON e EKSTEDT (2010).** **Na sua percepção, como o modo que TI é gerenciado na organização permite o desenvolvimento do planejamento estratégico, planejamento de TI, e gestão de riscos?** Eu vejo assim, aqui nós somos afetados por toda essa questão de dispersão geográfica, as fazendas hoje estão em locais bastante distantes dos centros urbanos, a tendência é ficarem cada vez mais distantes. Hoje pela característica de sistemas que são implementados aqui, por serem sistemas centralizados (todo o *Data Center* e as sistematizações estão localizadas na matriz), por exemplo, hoje para se abrir uma fazenda nova ou criar uma nova unidade dentro da empresa, sem dúvida alguma há a questão da tecnologia presente e da informação. Comunicação e telecomunicações também são fundamentais. Então vejo como necessário ter essa convergência entre o planejamento estratégico de TI e a questão dos riscos, pelo menos, levar em conta a questão de como incrementar isso, sistematicamente falando, ter um ERP centralizado para que as coisas funcionem de forma conectada é necessário que tudo esteja bem sincronizado e alicerçado, ou seja, muito bem unido para poder funcionar corretamente e evitar riscos. Eu vejo que o planejamento estratégico em parte está voltado a TI, mas não todo, hoje eu entendo que aqui no grupo esta vinculação ainda é pouca, nós precisávamos ter um pouco mais de conhecimento e informação sobre o que a empresa quer saber praticamente, até para podermos suportar de forma mais eficiente o nosso trabalho, principalmente apoiando e ajudando no planejamento estratégico e também na hora de migrar do planejamento estratégico para o planejamento tático da empresa, neste ponto acredito que ainda pecamos um pouco como TI, é necessário uma boa comunicação da estratégica para chegar à parte tática. Neste quesito creio que nós pecamos um pouco, acho que temos bastante no que melhorar dentro da empresa. Quanto à gestão de riscos, nós precisamos dizer exatamente o que queremos investigar e o que vai ser considerado. A SLC Agrícola por ser uma empresa grande e de capital aberto, onde informações importantes e privilegiadas não podem cair

	no mercado, já que é uma empresa que vende *commodities*, apesar disso não se pode fazer grandes investimentos em seguranças, em redundâncias, em controles, claro que a gente tem um grande cuidado, temos regras de políticas acessos, nós temos controles de liberação de acesso, trabalhamos nisso no nosso dia a dia. Temos auditoria externa que funciona para isso, verificar processo evitando riscos de TI, apesar disso, nós não somos uma empresa de tecnologia, que tem milhões de controles, e assinaturas de última geração, não fazemos isso, mas com certeza trabalhar a segurança não é um ponto que deixamos passar no dia a dia, implementando as melhores práticas de controle ou de acesso a informação. **Este gerenciamento ocorre de forma crítica e realista?** Acredito que sim, que ocorre de forma realista, devido a avaliações que contemplam a tecnologia no momento de algumas escolhas, apesar da TI ser uma área totalmente meio ela não é uma área fim. Com certeza no momento que a direção da empresa estrategicamente pensa em aumento de área, em aumento do negócio, a TI não é o impeditivo pra ir adiante ou deixar de ir, mas sem dúvida alguma, hoje ela é um ponto importante a ser considerado, não é o fundamento, mas é importante pelas características de sua função. Hoje por exemplo, não é possível transmitir uma nota fiscal eletrônica sem estar conectado com o SEFAZ, e com a Secretaria da Fazenda do Estado. Hoje em dia, não há como abrir mão da tecnologia, da telecomunicação e dos sistemas pra poder tocar o negócio no dia a dia.
2	**ITGI (2007).** **De que forma a confidencialidade, integridade e disponibilidade das informações atuam dentro da organização em relação aos riscos?** Para a SLC, manter a informação de forma confiável é bastante forte e muito importante para o negócio, visto que nós temos que divulgar resultados, e os resultados tem prazos pra serem divulgados, somos auditados justamente por empresas que são dependentes da SLC, isso quer dizer que, são empresas contratadas pelos acionistas, não pela empresa e isto gera uma confiabilidade bastante grande. A SLC Agrícola investiu muito nos últimos anos exatamente em colocar ERP integrado para todos os seus sistemas, que até então eram todos feitos em casa, e também tem a exigência do mercado em relação a este ERP, para que se possa garantir a integridade e a qualidade da informação, evitando ao máximo re-digitações ou de re-informação de dados ao longo do processo ate chegar no efetivo processo de apuração contábil. Então hoje toda a informação já faz parte da origem, quer dizer toda a operação vai ser contabilizada a partir da compra, a pessoa da área fiscal já digita baseada nas informações do pedido, fechando com a ordem de compra, que já tem toda uma definição de apuração contábil, em termos de contas e em termos de demonstração de resultado, assim como toda a parte de saídas da empresa tudo é configurado primeiramente no sistema, então com isso há a garantia de que os erros serão mínimos. Erros podem acontecer ao longo do processo, mas que sejam mitigados ao longo do mesmo, e com isso garantir que a informação chegue lá fora apurada e contingente com a realidade do que aconteceu, sendo apropriada de forma correta contabilmente, em termos de custo, e de valores, e em última estância com foco na informação confidencial mesmo, extraída para tomada de decisão da empresa. Eu acho que ainda não atendem completamente as necessidades, assim nós implantamos o ERP em toda a SLC Agrícola ano passado, em maio, estamos fechando o primeiro ano de uso da ERP totalmente integrado na empresa. Antes eram sistemas desintegrados, feitos em casa, eles tinham planilhas pra cá, planilhas pra lá. Apenas houve a integração de fato nesse último ano que a gente começou a utilizar o novo sistema, com isso e com toda a implantação de ERP e melhorias, mudamos muito o processo da empresa. Nesse último ano trabalhamos pesado para realizar a estabilização de tudo isso, não só o sistema, mas também o processo. Nós começamos a trabalhar em viagens e informações para apoio e decisão, mas neste sentido temos um campo muito vasto, muito bom ainda pra SLC Agrícola, hoje as informações geradas são informações importantes, mas ainda são muitas para o nível operacional. Algumas coisas no nível tático e estratégico da empresa, assim como as tomadas de decisões ainda não são devidamente

	incrementados em ferramentas de BI, em termos de sistema, esse é o próximo passo, acho que não se tem como implementar um BI num sistema de apoio pra tomar decisões se não tiver uma boa base de dados, que seja solida, confiável, e de boa sustentação para gerar os demais dados em cima disso ou gerar as informações a partir deles. Por este motivo, hoje, com certeza ainda é pequena essa questão de trabalho, e a nossa expectativa para este segundo ano é começar a trabalhar mais fortemente nessas informações e na geração delas. **Na sua percepção, como estes requisitos de negócio atendem as necessidades de informações da empresa?** Entendo que atendem muito bem, o grupo SLC Agrícola tem um diferencial por ser uma empresa de capital aberto, hoje quando um acionista vê o seu dinheiro sendo investido na empresa, a primeira coisa que pensa é em como essa empresa é controlada, quando se fala que tem sistemas que são feitos em casa, e que tem suas peculiaridade de uso doméstico, normalmente isso gera uma certa insegurança, tanto que as auditorias externas, quando são auditadas por uma empresa tem sistemas feitos em casa, comparados com os sistemas de mercado, geralmente a quantidade de informações que eles buscam no sistema feito em casa, é muito maior, faz parte do jogo, isso até existir a confiança necessária, que aquilo que se tem feito em casa é um sistema confiável, não que o ERP sistema integrado de mercado não tenha falhas, ele pode ter falhas mas geralmente ele gera uma confiança muito maior, para a auditoria, até por que eles podem utilizar as práticas que utilizaram em outras empresas, sabem exatamente onde fazer todos as conferencias no sistema, o máximo que vai mudar naquela aquisição é uma configuração ou uma característica que foi implementada um pouquinho diferente, mas em termos de estrutura, de bancos de dados, acesso, ou em termos de controles, é uma empresa muito igual. Então quando auditoria chega aqui é muito mais fácil pra eles,e também para o acionista. As necessidades de informações da empresa se modificaram quando a SLC Agrícola abriu o capital, e começou a fazer seus informes, verificar se isso foi informado etc, as informações passaram a ser mais precisas e controlados em função da divulgação para o mercado. Informamos que implementamos o sistema em todas as unidades da empresa, exatamente para termos disponibilidade para o acionista, para que por exemplo, a pessoa que está lá na Ásia, na Europa, ou na América do Norte, possa obter as informações se decidir investir na empresa.
3	**COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).** **Os investimentos realizados em TI são suficientes para permitir que as informações sejam corretas, precisas e estejam disponíveis no tempo adequado?** Eu acredito que sim, que hoje está adequado, não é o melhor volume, com certeza tem oportunidades de haver mais investimentos, mas por exemplo, esse investimento feito todo em ERP, para montagem de toda a estrutura, não só a estrutura de sistemas de acesso à informação, como toda a parte de integração das fazendas de telecomunicação, dados, impostos, o uso é bastante grande, nesse aspecto houve início de investimento adequado dentro da empresa. **Como isso é validado pelos usuários?** Para toda e qualquer demanda que chega pra área de TI (quando eu falo em TI eu falo de infraestrutura também, não só sistemas) existe uma formalização dessa demanda, esses registros são feitos pelo usuário, ele abre um chamado, solicitando os serviços de acordo com sua necessidade, a partir disso nossas áreas técnicas atuam para verificar se há um investimento necessário , que deve ser validado pelo gestor daquela área, autorizado ou não o investimento, quando a solicitação é resolvida é informado aos usuários e tem um momento que ele pode se pronunciar, dizendo se funcionou ou não funcionou, ou seja, se pronunciar formalmente sobre isso, realizando sua avaliação. **De que forma estes investimentos podem proteger a empresa de riscos?** Hoje, muitos investimentos continuam sendo feitos em sistemas, e melhorias de sistemas, então com certeza ele protege cada vez mais a SLC Agrícola de varias questões, por exemplo, protege para não atrasar a entrega aos supermercados, a partir do momento que eu tenho os dados integrados, há muito mais agilidade de se fazer os fechamentos, realizar as apurações e identificar falhas que por ventura acontecem, isso protege o negócio. Antes disso tem todo

	um controle que deve ser feito, antigamente não se tinha isso, é uma questão de controle mesmo, de validação, de reposição de estoque, validação de recebimento e de pagamentos. Sendo assim, tudo isso hoje está muito sincronizado, toda a informação que é passada para uma fazenda que está a seis mil quilômetros daqui da central, instantaneamente está sendo testado pelo nosso pessoal e podem ser realizadas as verificações necessárias, isso não elimina, mas, mitiga sensivelmente toda e quaisquer problemas operacionais, seja de considerar informações indevidas, sendo até para mitigar erros, ou a questão de fraude. Esses investimentos conseguem melhorar o controle, consegue ser mais repetitivo no acompanhamento da operação, por exemplo no sistema integrado.
3	**ITGI (2007)** **Como a estrutura de TI presente na organização possibilita a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas)?** A TI está dividida em infraestrutura e sistemas. são 8 pessoas na minha equipe, ligados diretamente a mim, 6 analistas de negócios, e 2 de sistemas a qual é o meu foco. Hoje acontece assim, com certeza os ativos são de muitas empresas, e com o amadurecimento desses ativos dentro da empresa a gente trabalhou bastante em termos de recriação de avaliador, bons alertas, e identificação de pontos críticos e para que toda a nossa base instalada esteja em bancos de dados, sejam sistemas, sejam ativos que são utilizados para telecomunicação ou segurança. Neste sentido, hoje a equipe está trabalhando e buscando melhorias, buscando melhores práticas e controle pra tudo e também para os processos. Hoje em dia, muitos de nossa equipe já trabalham com geração de alertas, pra se definir onde é que são os pontos críticos e onde pode haver falhas, podem trazer consequências para os negócios. Temos uma equipe monitorando 24 por 7 esses alertas e questões, e ai sim proativamente disparam ações pras equipes que vão dar o devido suporte, e isso não só infra como sistemas, então por exemplo, se tem hoje um processo crítico nos negócios da empresa, como a geração da nota fiscal eletrônica, se não sair a nota fiscal eletrônica, não pode sair nenhum produto da fazenda, e vai parar a fazenda e a expedição vai parar. Em cima disso, sempre que há qualquer oscilação de *links* que é a seleção do próprio serviço de geração da nota fiscal eletrônica tem um alerta no sistema, a manutenção de NOC de alertas, se deu algum problema já é disparado um primeiro alerta , aí se faz a codificação necessária, ou se verifica se é um problema específico daquela região, se não há problemas naquela ligação, ou na estrutura da região, a ligação já vai chamar a equipe que de suporte sistêmico e de infraestrutura pra poder ir adiante. A equipe esta dimensionada pra suportar isso, mas graças a essas questões corporativas que são colocadas ao longo do processo, elas vão nos ajudando a fazer o monitoramento e trabalhar em cima da restrição, da regra, e quando da à exceção, o pessoal é acionado e faz esse devido combate pra não ter problema. **De que maneira esta estrutura interage com a prevenção dos riscos?** A inteiração da área para a questão de risco é proativa, trabalha com base em histórico, a partir de um risco já ocorrido, e por isso existem alertas que são disparados, e a equipe então entra em ação, hoje nós estamos trabalhando de duas formas aqui na SLC Agrícola, ou seja, temos duas frentes já preparadas para trabalhar em termos de sistemas e gestão de riscos, focamos muito a questão de acesso mesmo, e informação, justamente para que ninguém tenha acesso ao que não devia. Sendo que estamos trabalhando de duas formas, focando nos acessos externos e internos também. Porque assim como mostram as estatísticas, normalmente as grandes fraudes não vêm dos *hackers* como se fala hoje em dia, vem pelo acesso interno mesmo, que alguém abriu e passou a informação pra fora. Este trabalho esta ficando muito forte na SLC, queremos implantar esse ano ainda um termo para definir claramente quais são os acessos que uma pessoa pode ter baseada na sua função, isso deve estar dentro do sistema, exatamente assim, por exemplo, um auxiliar do almoxarifado... Quais são os acessos que precisa ter? Que tipo de informação precisa pra desempenhar sua atividade? Focando em não ter acesso em excesso ou nem pouco acesso, mas sim o suficiente para

	desempenhar sua função dentro da empresa, e tornar isso padrão, porque a tendência são as fazendas da SLC Agrícola trabalharem quase como unidade de negócios independentes, e a partir do momento em que você começa a manter um padrão começa a complicar bastante, por exemplo, um auxiliar de almoxarifado, numa fazenda pequena tem acesso somente para o almoxarifado, como a gente diz, em outra fazenda pode ser até um faturista, pois auxiliar de almoxarifado também é faturista, ai as coisas começam a dar problema. Neste ponto você começa a ter eventualmente aquelas questões que as auditorias externas descobrem, de governança como é que fica a segregação na função, e de acesso. Trabalhamos exatamente para definir claramente esses perfis, ou seja, a partir do acesso da função e em cima disso, implementar na empresa essa metodologia, porque atualmente não é assim, hoje é conforme o gestor vai pedindo e entendendo o que é importante, e por isso vai liberando acesso. A solicitação esta a cargo do gestor, a concessão não, a concessão está dentro da área de TI, que libera a validação. Na prática funciona assim, o gestor da pessoa faz aquele acesso para ela e passa pelo analista de negócios pra definir quais perfis ele considera importantes para aquele acesso, e passa também pelo dono da informação, por exemplo, um funcionário pode pedir acesso até para visualizar um razão da empresa, um balancete, e quanto a sequencia da informação, então nesse caso, sempre terá que passar por alguém da contabilidade, no nosso caso passa por um gerente contábil. E daí quando vai dar o "ok", pode liberar acesso pra essa pessoa, porque daí o contador vai fazer o acesso, ou vai dizer não, que não tem que dar acesso para esse cara, pois, ele é auxiliar de almoxarifado, ou seja, ele não precisa ter esse tipo de acesso, então sempre tem esse crivo. Vamos dizer assim, do líder que nós chamamos aqui na empresa, líder do processo, realmente ele pode ter aquele aceso ou não, mesmo assim se vê que tem falhas no sistema, por isso esta sendo criada essa matriz de responsabilidade, para dar esses acessos, sendo homologados com as áreas, a partir daí fica muito claro como deve funcionar, se a pessoa vai ser contadora, é fácil saber quais vão ser os acessos dela, ou se pessoa vai ser um auxiliar de almoxarifado, quais são os acessos dele, esse é um *viés,* essa é a primeira parte, já a segunda parte, é realmente a informação de como analisar o negócio, identificando o ponto de fragilidade em termos de informação e em termos de um acesso privilegiado, até um *bug* que o sistema ofereça. Por exemplo, o sistema também pode dar uns *bugs*, porque em um acesso de consulta, o usuário conseguiria fazer um *update* de informações, houve um usuário nosso que identificou esse problema uma vez, só que nem nós conseguimos reproduzir, o cliente conseguiu fazer uma coisa bastante diferente, e foi difícil de conseguir reproduzir, então se trabalhou com o próprio usuário entendendo como é que se fazia, foi feito o passo a passo com ele até conseguirmos identificar onde que ocorriam os *bugs* na tela de consulta, ele conseguia alterar uma informação do sistema, então são fragilidades do dia a dia que está se defendendo, trabalhando e corrigindo.
4	**ALBERTIN e ALBERTIN, (2012).** **Quais as vantagens ou desvantagens que a Tecnologia da Informação – TI oferece decorrentes de seu uso?** Uma vantagem do uso da informação na SLC Agrícola hoje é a facilidade na integração de tudo isso, da dispersão geográfica, da continuidade de informações, e de sua disponibilização, tanto para os controles dos negócios operacionais do dia a dia, quanto para as formações de fechamento, e outras informações que são necessárias. Outra vantagem é que de alguma forma se consegue apurar mais rapidamente os resultados da empresa. No nosso caso, em função da agricultura, por exemplo, a gente tem acesso rápido a muitos dados que são gerenciados, bem como em termos de clima, de solo, de pragas da lavoura, são muitas informações. A tecnologia da informação agiliza estes controles e possibilita realizar os cruzamentos para tomar as melhores decisões. Tudo isso de forma centralizada e unificada dentro dos sistemas. As uniformidades das informações, dos controles, das unidades e de medidas dentro da empresa, são um ponto bastante importante. A padronização também é um ponto bem importante, fruto da utilização da tecnologia. O lado negativo que percebo, é realmente a mudança de cultura, isso no momento que implementam ERP, ou de uma nova tecnologia, para nós foi

	necessário uma mudança de cultura muito grande, e também a quantidade de informações e de inteirações nos sistemas cresceram drasticamente, antes as pessoas não precisavam informar todos esses dados, consequentemente não tinham todas as informações que precisavam no sistema e também muito do que era feito, era em função do que elas já trabalharam e já conheciam de longa data naquela forma, era mais simples permanecer com os controles manuais. Quando houve a implantação do sistema integrado, a cultura das pessoas foi sim uma dificuldade bastante grande, para entender essa nova realidade que trazia um monte de telas, um monte de campos validados e isso pesou bastante, então virou um ponto negativo, um pouco da complexidade, vamos dizer assim, a complexidade no uso do sistema, visto que é uma empresa de agricultura, das pessoas que estão envolvidas dentro das fazendas, não são todas que tem uma boa formação, muitas vezes é difícil conseguir buscar uma mão de obra qualificada no interior do país. A necessidade de treinamento, em função disto, é a capacitação e investimento em pessoas. **Qual a sua percepção da relação desta utilização com os riscos?** Para mim quando estamos falando em risco, estamos falando em dados pra poder suportar os negócios, evitando erros ou fraudes e coisas do tipo, eu acredito que hoje em dia, a tecnologia da informação é fundamental para se ter maior agilidade na identificação das questões que aconteceram dentro dos negócios, mantendo assim formas de controle e acompanhamento. Com o uso da TI é possível um cruzamento entre os dados utilizados. Possibilita integrar de um modo muito mais fácil às informações. Acredito que o uso da tecnologia vem a apoiar, vamos dizer assim, há mitigação dos riscos, mas, com certeza não resolve cem por cento, porque muitos riscos estão voltados aos processos, do objetivo, da intenção que as pessoas têm em fazer as coisas, por exemplo, temos um caso de um funcionário que conseguiu descobrir que era possível alterar dados em uma tela de consulta, nesse caso, não usou isso para fraudar, mas poderia ter usado, ele conseguiu burlar o sistema, então com certeza tem a TI, como todos os sistemas e processos. A telecomunicação, que através de seu uso não resolve tudo, mas dá uma boa sustentação para mais rapidamente conseguir identificar as questões, trabalhar em cima dela, e demonstrar para as pessoas que acompanham a empresa que existe controle, acompanhamento, fechamento, e apuração coerente dos resultados. De alguma forma há um controle sim, e que esse controle que rapidamente pode ser a ferido, não precisa esperar fechar um mês, um trimestre, ou esperar fechar um exercício pra poder identificar que tinham falhas, que tinham rupturas no processo.
4	**BULGURCU, CAVUSOGLU E BENBASAT (2010); SPEARS E BARKI (2010)** **Como a empresa implanta planos de segurança para reduzir os riscos relacionados à segurança das informações?** Hoje basicamente são sistemas que realmente detém todo esse controle de acesso, porém, só controle de acesso não é suficiente, para a metodologia de acesso, há necessidade de uma matriz de responsabilidades, para que seja possível definir claramente quais são os grupos de acesso, isso em termos de sistemas. Em todo o nosso sistema tem algumas características que a própria auditoria nos cobra todos os anos, por exemplo, a troca das senhas de acesso tem certa complexidade, e no momento que a pessoa errar alguma letra, vai espirar a senha, e não vai mais conseguir entrar no sistema, pra conseguir entrar novamente, terá que ligar para um número e se identificar, informando número de identidade, CPF, e data de nascimento, isso tudo para se ter certeza que é mesmo aquela pessoa que esta solicitando o acesso, desta forma é possível garantir que se tenha controle em termos de acesso indevido de informações. Outro plano de segurança para as informações é que nós usamos um terminal, que tem todo um controle de acesso em cima dele também, e serve para evitar que os nossos negócios estejam suscetíveis a acessos externos não autorizados ou, por exemplo, quando realmente temos a invasão por acesso a alguma porta que a gente não tinha fechado, ou coisa do tipo, hoje existe uma equipe dentro da área de infraestrutura que tem este compromisso de realizar essa verificação das portas e controles de acesso dentro dessa rede. **Qual o envolvimento funcional dos usuários?** Hoje o envolvimento deles é praticamente

	nulo. Toda a política de segurança, se tratando de acesso, de aplicativos tecnológicos da empresa, de sistemas ou em termos de infraestrutura, a participação do usuário para os planos é nula. Nós persistirmos em toda a política de acesso fechando com os usuários e quais acessos eles terão para desempenhar corretamente sua função dentro da empresa. **De que maneira eles participam da gestão de riscos e segurança?** Eles assinam uma política quando entram na empresa, que se refere a varias questões, como no uso do e-mail (tipo de informação que podem ser enviadas), no uso de má fé nos sistemas, e no uso de informações que utilizam no seu dia a dia, enfatizando o cuidado que eles devem ter no uso das informações. Há uma serie de questões que esta política prevê, e todos os colaboradores da SLC precisam assinar, estando assim cientes no uso das ferramentas de trabalho do dia a dia. Esta é a forma na qual vejo os usuários participando da gestão dos riscos relacionados à informação, se comprometendo e estando cientes desta política.
5	**ITGI (2007).** **De que maneira os processos de TI possibilitam que a entrega e suporte dos serviços de TI atendam as necessidades dos usuários?** Toda e qualquer demandam para TI é realizada com base em um minucioso trabalho, é realizado um levantamento dos requisitos para aquele atendimento que no final é homologado pelos usuários. A demanda chega para nossa área com uma boa especificação daquilo que esta sendo solicitado e com todo o detalhamento funcional pra realmente entender que o que foi feito, então os analistas de negócio interagem com os usuários para verificar a solicitação e para que não haja dúvida quanto ao serviço de qualidade prestado por TI. Hoje na SLC não é qualquer um que faz solicitação pra TI, por exemplo, imagine que lá na fazenda um contador identificou uma quantidade de melhorias no relatório, este abre uma solicitação de serviço, essa solicitação de serviço não cai diretamente na TI, cai para o usuário chave, o usuário chave é alguém da área, que a conhece muito bem, e que também conhece muito bem o sistema, e essa pessoa faz uma pré-análise identificando se realmente a questão faz sentido, se eventualmente já não existe uma forma de atender aquela solicitação sem uma modificação e se realmente não tem como fazer, aí sim vai para a área de TI, para o analista de negócios. Ele então faz todo o detalhamento funcional que posteriormente é homologado pelo usuário, tanto o usuário chave quanto o solicitante (quem fez aquela demanda) só a partir daí, que vai para a área técnica, que realiza o desenvolvimento, este pode ser interno ou externo, dependendo do que o sistema está trabalhando vai tudo para o desenvolvimento, e depois para o teste e homologação com o usuário, e finalmente é realizada a entrega, somente após ser testado. Acredito que com esta interação entre usuário solicitante, usuário chave e analista de negócios de TI a entrega dos serviços prestados por TI ganha muita qualidade. **Como a prestação de serviços de TI atua para minimizar os riscos?** Hoje nós temos alguns processos nos sistemas, que são para mitigar estes riscos, ou pra evitar problemas, alguns até automatizamos, por exemplo, todos e qualquer funcionário, que é demitido da empresa, neste momento, já é emitida uma mensagem dos recursos humanos (sistema da folha de pagamento), para que nossa equipe possa bloquear as permissões, e isso ocorre de forma automática. Este é um exemplo de atuação que visa prevenir os riscos de má intenção dos usuários. Sabemos que apesar dos controles automatizados, pode haver falhas, mas nós visamos o processo para redução destes riscos. Por exemplo, com acessos, reenviar a lista de usuários ativos e verificar se estes acessos são realmente coerentes, validando alguns acessos e prevenindo acessos indevidos.
6	**SPEARS E BARKI (2010); ITGI (2007).** **Como a recomendação e comunicação de planos de ação de remediação dos riscos consideram a participação dos usuários para a gestão de riscos e segurança?** Nossos planos de ação consideram a parte de revogação e de controles de acesso, este foi um ponto muito trabalhado com o pessoal dos Recursos Humanos. Outro ponto é considerar a participação não só do usuário para estes planos, mas do gestor do usuário. Explicitamente, não consigo enxergar a participação direta do usuário nos planos de segurança.

	Como esta gestão se integra aos processos gerenciais? De certa forma existe uma integração e preocupação da gestão da empresa nessa questão, quanto à qualidade das informações, logo com sua segurança. Porém não vejo aqui grandes inovações neste sentido, mas existe a preocupação com o que é fundamental. Já trabalhei em corporações em que a preocupação com os riscos de TI é muito maior que na SLC. Neste sentido, apesar de ser uma empresa de capital aberto, eu não demasiada preocupação quanto a acesso, ou acesso indevido, principalmente por parte dos gestores de negócios. A SLC claro que tem suas preocupações com relação a isso, mas não chega a ser com toda essa veemência que se vê em muitas organizações. Isso é um fator que me assustou um pouco quando eu cheguei aqui na SLC, pelo seguinte, hoje ela é uma grande empresa do mercado de *commodities*, não vejo muita concorrência, ou uma preocupação excessiva com a concorrência, existe muitas vezes até uma parceria com os concorrentes, é muito comum existir uma troca de experiências entre eles, como por exemplo, abrir seus números simplesmente para entenderem as suas dificuldades e se ajudarem, e compartilhar ideias. Hoje a SLC Agrícola tem o nome bem conhecido no mercado agrícola pelos seus processos e sua produtividade, então ela é muito requisitada, ela não retêm suas informações, e ela abre mesmo, a única parte na qual têm um pouco mais de preocupação é na de controle de acesso de informações de interesse direto de acionistas, informações privilegiadas, por exemplo, quanto ao valor de ações, de queda ou alta. Problemas em termos de divulgação de informações antes do que deviam ser comunicadas, e coisa do tipo, enfim só neste aspecto que eu vejo um cuidado excessivo, mas outras informações eu não vejo assim, o que é uma grande preocupação do concorrente. Nós em TI temos muito mais preocupação com isso do que os gestores, responsáveis pelos processos gerenciais da empresa.
7	**BULGURCU, CAVUSOGLU E BENBASAT (2010).** **Como a estrutura para gestão de riscos de TI é organizada na corporação?** Na verdade não tem uma estrutura formal para a gestão de riscos, por exemplo, como se pode perceber que há em um banco. Não existe formalmente, e informalmente hoje ela esta distribuída, um pouco na TI com participação das áreas de negócios. Existem algumas solicitações das áreas de negócios, muitas vezes na parte contábil e fiscal, que vislumbram minimizar alguns riscos, então estas áreas interagem com TI para implementar controles e reduzir estes pontos. Mas não vejo maior controle de gestão de riscos de TI, a gente não tem uma preocupação integrada com isso, e muito menos não se tem um único organismo dentro da empresa focado para esta questão. Talvez até possa existir o intuito de fazer esse gerenciamento, mas eu não vejo esse sentimento ou de forma abrangente na empresa esse controle. **Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco?** Acredito que de trabalhando de forma proativa, buscando a prevenção de erro ou melhoria de processos. Hoje a cultura é um problema, a consciência de que uma simples ação incorreta pode desencadear uma série de problemas. Trabalhar neste sentido ajudaria.
8	**ITGI (2007); SPEARS E BARKI (2010)** **Que tipos de esforços são realizados pela corporação para manutenção e monitoramento de planos de ação para os riscos?** Na parte de sistemas, hoje se trabalha muito com a equipe que nos dá suporte, os usuários chaves. Outro ponto é a criação das chamadas trancas no sistema, que por um lado realmente evitam falhas e eventualmente informações equivocadas, consequentemente evitam risco para os negócios e também que algo de errado ocorra. **Como estes esforços contemplam o desenvolvimento e a performance de controles?** Estes esforços possibilitam que os usuários tenham o devido controle dos processos. No dia a dia, nosso trabalho também se preocupa em buscar formas de evitar o erro e a falha, melhorando o desenvolvimento do sistema, utilizando-se de problemas já ocorridos para evitar falhas futuras.

BLOCO III – GERENCIAMENTO DOS RISCOS CORPORATIVOS

CATEGORIA	QUESTÃO
1	**FRIGO E ANDERSON (2011)** **Como a organização realiza a avaliação estratégica de seus riscos?** Existe o comitê de riscos que se reúne semanalmente, tenho informação que anualmente a empresa tem planejamento estratégico, onde há reuniões e análises que contemplam todas as ameaças, as oportunidades e os pontos relacionados ao mercado. Baseado nessas informações eles fazem avaliações estratégicas, e consequentemente um plano tático para mitigar essas questões. Neste momento toda a empresa é envolvida, inclusive a TI, nosso gerente participa também do planejamento estratégico da empresa e lá ele coloca todas as questões técnicas de TI que precisam ser consideradas na definição do plano estratégico, e depois no desenrolar do plano tático. **Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança ?** Eu acho que sim, com certeza.
2	**IBGC (2007); COSO (2007); ISO 31000 (2009); Aven (2011); GERIGK E CORBARI (2011).** **De que forma o gerenciamento dos riscos corporativos possibilitam evitar, reduzir, compartilhar ou aceitar os riscos?** Acredito que se antecipando das questões, porque toda a questão de risco na verdade é uma antecipação ao que pode acontecer, de fazer várias leituras da situação, tentando identificar as questões de risco, e transformá-las em oportunidades de melhorias. No momento que se faz avaliações semanais, consequentemente depois do plano estratégico, que é muito focado nestas questões, se consegue antecipar e deixar claro pra todos os envolvidos quais são as questões nas quais é preciso ter maior enfoque, o que precisa ser observados, o que precisa ser acompanhado, ser medido, e por fim mitigadas de acordo com a possibilidade que se tem. De acordo com o interesse da empresa, muitas vezes é a questão de mitigar riscos (que eventualmente até elimina o risco) envolve investimento, é uma questão de necessidade, tanto como as análises do que vamos fazer ou não vamos fazer. Isso permite chegar num controle, por exemplo, até hoje a SLC Agrícola não tem um site de contingências, por uma definição de negócios seria muito caro fazer isso. Sendo assim, hoje nós temos um grande servidor, mas não um grande *site*, a empresa faz escolhas no sentido de priorizar, focar e investir naquilo que entende como mais necessário. **Na sua percepção este gerenciamento estabelece respostas a estes, reduzindo surpresas, custos ou prejuízos associados?** Acredito que sim, o gerenciamento apropriado consegue evitar custos. Caso consigamos nos antecipar ao que pode acontecer, podemos atuar de forma preventiva, evitando surpresas.
3	**COSO (2007); IBGC (2007); GERIGK e CORBARI, (2011).** **A organização procura identificar os eventos que possam ter consequências <u>operacionais, financeiras ou estratégicas</u> adversas? Caso afirmativo, como são prevenidos ou minimizados tais eventos?** Não tenho muito conhecimento sobre todas estas questões, mas acredito que a própria formação do comitê de riscos busca minimizar riscos, principalmente os financeiros.
4	**COSO (2007); IBGC (2007) Como a gestão de riscos corporativos possibilitam uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos? Como isto ocorre?** Como eu falei antes, hoje eu não vejo toda essa sincronização de tudo isso, eu acho que temos muito ainda para crescer neste aspecto, atuando para minimizar riscos nos negócios, quer dizer, as áreas da empresa, em suas diversas funções, e diversas responsabilidades. Toda essa sincronização, para fazer realmente uma boa gestão de riscos e uma boa sincronização para que um risco não seja maximizado pelo outro. Isso pode acontecer, a existência de dependência de um risco específico sobre um segundo risco ou o impacto do primeiro pode se tornar muito maior, isso pode ocorrer, no momento que não existe uma área bem sincronizada na questão de

	tratamento de investigação de riscos, seja de fraude, de negócios, de perda de qualidade de informação, seja o que for. Hoje aqui na SLC Agrícola este processo precisaria ter melhor sincronia.
5	**ISO 31000(2009) Você considera que os seguintes princípios são atendidos pela empresa, quanto à gestão de riscos. Explique como isso ocorre.** **1) Cria e protege valor.** Acredito que sim, porque um dos valores da empresa é sua própria ação. No momento que a gente não cuida da nossa informação, e que a deixa disponível no mercado de forma equivocada, com certeza a gente perde com isso, então certamente esta gestão cria valor. **2) Participa de todos os processos organizacionais:** Ainda não, isto ainda faz parte de uma caminhada que a gente tem que evoluir na SLC Agrícola. **3) Participa da tomada de decisão:** Em parte sim , acho que hoje quando o nosso setor, ou seja, quando nós mesmos do TI temos que tomar alguma decisão, consideramos com certeza a questão dos riscos. Esta análise faz parte do nosso dia a dia, porém considero que neste ponto temos um caminho ainda para percorrer, mas com certeza é um dos pontos que consideramos. **4) Aborda explicitamente a incerteza:** Sim, acho que aborda a incerteza sim, o negócios agrícola trabalha muito com a incerteza no momento, muitas variáveis que não se tem controle, variáveis como a produção realizada a céu aberto, produto, entregas, a própria oscilação do mercado de *comodities*, onde você não define preços, o mercado define os preços, ou seja , então você tem que se adequar, onde é que esta o ganho em custo, não em melhor valor de venda, não tem como fazer diferente. Neste sentido acho que sim, aborda as incertezas, mas existem boas oportunidades pra fazer melhorias nisso, melhoria de capacidade, de ir mais ao fundo em algumas questões, de conseguir ter uma abrangência um pouco maior dos riscos. **5) Atua de forma Sistemática, estruturada e oportuna:** Acho que sim, existe essa reunião em comitê semanal, e um setor dentro da própria empresa voltado à estratégias. Há também trabalhos de gestão de riscos que acontecem no dia a dia dos departamentos. De certa forma existe uma sistematização, mas, desestruturada, talvez aí haja espaços para oportunidades de melhorias, sem dúvidas. **6) Baseia-se nas melhores informações possíveis;** Na SLC há uma preocupação em informações com qualidade. O pessoal na parte de negócios investiu no ano passado, e ainda está investindo no plano estratégico, fizeram uma pesquisa muito profunda de mercado, um trabalho bastante apurado, completo e sério sobre o assunto, para definir o rumo da empresa. Neste sentido, eu acho que sim, que a gestão baseia-se em boas informações. Na questão da gestão de riscos ainda temos caminho para percorrer. **7) Se adéqua a realidade da organização**; Sim, eu acho que sim. Porém poderia ser um processo mais integrado para refletir melhor a realidade dos processos da empresa. 8) **Considera fatores humanos e culturais:** Acredito que contempla, mas como disse, de forma estruturada ainda não existe uma gestão de riscos**.** 9) **Atua de forma transparente e inclusiva;** Mais ou menos, eu acho que hoje a questão da comunicação, de fazer com que a comunicação funcione e que as informações relevantes permeiem todos os níveis da empresa, é um desafio não só para a gestão de riscos mas, para toda a SLC Agrícola . **10) Atua de forma dinâmica e interativa, capaz de reagir a mudanças**: Eu acho que não, tem muitas oportunidades de melhorias na forma de atuação. Nessa questão de ser dinâmico, não é possível ter uma visão dinâmica por não estar dentro do comitê, eu, de fora não vejo essa dinamicidade toda. Para as questões dos riscos de negócios, tem muitas oportunidades mesmo de melhorias. **11) Facilita a melhoria contínua da organização:** Não totalmente, no momento que não se tem uma comunicação, uma dinamicidade e rapidez em passar as informações em todos os níveis, acaba ficando um pouco prejudicado quanto a essa questão de melhoria contínua, ainda mais no que diz respeito a gerenciamento de riscos.

6	**BULGURCU, CAVUSOGLU E BENBASAT (2010).** **Como a estrutura para gestão de riscos corporativos é organizada na corporação?** Sei da existência do comitê de riscos que se reúne nas segundas, mas não vejo uma estrutura organizada que contemple qualquer tipo de ameaça. Mais uma iniciativa individual das áreas. **Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco?** Acredito que pelas suas ações, pela disseminação de uma cultura de prevenção de um maior cuidado com os processos de cada setor.
6	**AVEN (2011)** **A gestão dos riscos realizada na organização fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro?** Parcialmente, eu acho que ela ajuda, existem muitas melhorias para manter as áreas devidamente integradas, como um time para toda avaliação possível de riscos, de catástrofes, existe sim, mas não tem toda essa organização, digo de novo, uma caminhada bastante grande neste sentido precisa ser realizada dentro da corporação.
7	**ISO 31000(2009)** **Como os seguintes processos são considerados em relação aos processos de negócio organizacionais? 1) Comunicação e consulta às partes interessadas (internas e externas) 2) Estabelecimento do contexto (parâmetros internos e externos que precisam ser levados e consideração) 3) Avaliação dos Riscos (identificação, análise e avaliação dos riscos) 4) Tratamento dos Riscos 5) Monitoramento e análise crítica dos Riscos.** Não tenho conhecimento destas etapas dentro dos processos de negócio, apenas da realidade do ambiente de TI. Neste sentido prefiro não opinar.
8	**ISO 31000 (2009)** **Como a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações? Estas decisões consideram a incerteza, a natureza desta incerteza, e como ela pode ser tratada?** Não existe isso hoje, não vejo no dia a dia dos nossos gestores, tomarem decisões baseados na formação do risco claro, existe o risco de negócio. Mas não vejo preocupação efetiva com grandes incrementos para os negócios, se isso fosse levado em consideração agregaria muito mais qualidade, segurança e controle, informações muito mais precisas.

BLOCO IV – RELAÇÃO ENTRE GESTÃO DOS RISCOS DE TI E GERENCIAMENTO DOS RISCOS CORPORATIVOS

ITGI (2007)

1) Como a TI atua para prevenir riscos inerentes ao negócio? Hoje a TI atua de forma proativa, uma demonstração disso é a implantação de um sistema confiável (ERP integrado). Trabalhamos nas estruturas de rede, telecomunicação e servidores que garantam o mínimo de segurança de acesso para a continuidade dos negócios, isso nos possibilitou chegar até aqui, estamos em um momento de estabilização, e já partindo para a sabedoria nos sistemas. A TI atua hoje focando não só no sistema, como foi antes, mas também para apoiar as melhorias que irão auxiliar os negócios. O pessoal de TI está mais próximo das áreas, e já trabalha também focado nos seus processos, nas atividades realizadas dentro das áreas, identificando não só melhorias no trabalho do dia a dia, como também buscando formas de melhor integrar as informação e de melhor atender as necessidades dos negócios, preocupando-se com formas de melhorar o processo para alcance de metas que precisam ser atingidas. Estamos preocupados em levantar informações que mostrem para o gestor, para as áreas e para as fazendas, as discrepâncias que podem estar acontecendo, o arsenal de ferramentas que eles têm nas mãos e que podem utilizar. Ajudamos a prevenir os riscos de negócio, trabalhando focados na cultura, mostrando que há possibilidades de consultas, relatórios, e também formas de apoiá-los a buscar eficiência, para alcançar melhores resultados nos negócios e consequentemente evitar talvez até algumas falhas.

Esta atuação pode ser considerada satisfatória dentro de uma perspectiva de negócio? Eu acho

que tem muito para evoluirmos ainda, por exemplo, neste primeiro ano que trabalhamos com a implantação geral do ERP, a minha equipe trabalhou muito em apagar incêndio, acho que não só a equipe te TI, mas também as demais equipes, os usuários, em implantar sistema e resolver os probleminhas. Neste sentido o desafio que eu propus pra e equipe foi o de nós deixarmos de ser bombeiros, quer dizer, apagarmos menos incêndios numa árvore, e passarmos a ser mais guarda florestal, ou seja, sermos proativos, identificando as possibilidades e dificuldades e começar a trabalhar nesse aspecto, esse é o nosso desafio daqui pra frente, então acho que hoje nós estamos ainda muito a quem do que a gente pode oferecer, para a empresa.

SPEARS E BARKI (2010)

2) **De que maneira os usuários participam do gerenciamento de riscos de segurança nos processos de negócios? Como a sua participação é percebida e qual é o impacto da participação na segurança do negócio?** Os usuários hoje participam nos informando de falhas que acontecem nos sistemas, e solicitando melhorias. É com base na experiência adquirida nestes atendimentos que criamos controles, para evitar futuras falhas.

IBGC (2009).

3) **Como as práticas de governança corporativa orientam o dia a dia do trabalho da organização?** Minha percepção hoje sobre a governança coorporativa na empresa é que ela ainda é superficial. Superficial é um termo muito pesado talvez, essa prática da governança não é visivelmente clara em todas as áreas, agente sabe que existe , mas não há muita participação das áreas neste aspecto. Não existe uma boa comunicação disso, por exemplo, de quais são as melhores práticas adotadas pela empresa, quem é o responsável pela governança coorporativa da SLC Agrícola. Isso é uma grande pergunta. Qual é a área que pensa nisso e que audita isso? É importante para termos a certeza que existe alguém verificando as situações que estão acontecendo e prejudicando esta governança. Na minha percepção, isso hoje na SLC tem muito que se desenvolver, tem sim boas práticas dentro das áreas, como a ética por exemplo. Mas, hoje as boas práticas não estão bem sincronizadas, porém tem oportunidade de sincronizar tudo isso melhorando a governança coorporativa. Para mim estas questões de governança não existem por si só, e sim pra levantar os negócios, não pelo controle, é o controle com fim claro, em prol do negócio, hoje não se tem essa clareza.

De que forma elas contribuem para a gestão de riscos em TI e gestão dos riscos corporativos? Bom, acho que diretamente as práticas de governança contribuem para minimizar riscos, apesar de não se ter muita clareza sobre estas práticas aqui na empresa. Na TI a gente foca muito mais nas nossas experiências, na parte de mercado, ou por imposição dos negócios. Não existe aquela preocupação interna dentro da SLC que nos dá alguns direcionadores para evitar riscos, algumas verificações ou controles que nós deveríamos ter. Acredito que há espaço para se fazer um avanço, uma sincronização maior, até mesmo um alinhamento maior dentro do grupo da SL, referente a esse assunto, porque hoje a meu ver isso não está assim tão conectado e difundido.

JUNIOR, JUNQUEIRA e BERTUCCI, (2010)

4) **De que forma a adoção de mecanismos de controle possibilita redução dos riscos corporativos e riscos de TI?** Os controles que temos hoje são basicamente operacionais no sistema que implantamos, e em cima das estruturas de TI, que são utilizadas hoje dentro do grupo SLC, e especialmente na SLC Agrícola. Já houve uma melhoria significativa nestes controles internos, em termos de sistemas, ferramentas, e dispositivos, melhorando o controle existente sobre as operações e processos exatamente para evitar riscos, fraudes e perdas dentro da empresa.

SPEARS E BARKI (2010)

5) **Como os controles internos protegem as informações financeiras? Esta proteção é capaz de produzir informações contábeis financeiras confiáveis?**Sem dúvidas eles protegem, toda a integração que é realizada é fundamental para que exista este controle. Seja controle de acesso, de processos ou de procedimentos, isso nos dá mais tranquilidade. Sabemos que as informações são confiáveis, pois o sistema nos permite isso, temos controle de quem esta acessando aquelas informações, quem as gera e as determina. Estas coisas refletem em maior qualidade da informação

contábil que está sendo usada, divulgada e utilizada dentro da corporação.

IBGC (2009)

6) **De que maneira a atuação do comitê para a gestão de riscos ocorre?** Eu vejo a atuação do comitê de riscos muito mais voltada para atuação financeira, do que atuando para TI. Sei que o comitê se reúne todas as segundas feiras em uma reunião semanal, mas praticamente não existem ações naquele comitê que chegam à nossa área com o intuito de mitigar riscos ou informando riscos eminentes para que possamos trabalhar em cima deles, nesse tempo que estou aqui na SLC, nenhuma vez eu vi alguma ação do comitê neste sentido.

   Como sua atuação contempla a prevenção de riscos de TI e risco corporativos? No meu ponto de vista, as ações que a gente vê dentro da TI são muito mais voltadas ás melhores práticas de mercado, do que pela imposição ou solicitação do comitê de riscos da empresa. Vejo pouca interferência do comitê de riscos nas questões de TI, eventualmente ele pode sugerir a adoção de alguma política, como por exemplo, a proibição do MSN para que TI controle, mas não que isso chegue a ser uma prevenção ou preocupação intensa com os riscos de TI. Quanto a riscos corporativos não tenho conhecimento.

7) **Em sua opinião existe uma aproximação entre os riscos de TI e riscos corporativos? Como isso seria possível?** Eu acho que sim, em boa parte sim, não digo que é cem por cento por dois vieses, um viés da questão da informação por ser uma empresa de capital aberto, pois informações privilegiadas podem ser disponibilizadas indevidamente, ou estas informações podem ser convenientes para o mercado, para as pessoas que usam essa informação, um controle de dentro para fora, e internamente também. A questão de acesso de informações ou manipulações de dados que podem facilitar a questão de fraude, questão de desvios, qualquer coisa do tipo que possa estar acontecendo.

   Como isso seria possível? A primeira forma seria fazer parte do comitê, este comitê está mais voltado às questões dos negócios, que não são da área de tecnologia. Na minha visão, a primeira forma de atuar nesta relação seria reformar nossos gestores em tecnologia, um trabalho de aculturamento destes profissionais em relação aos riscos possíveis, como funciona esse mundo, quais são as possibilidades, como é que as fraudes ocorrem, falar em riscos de descontinuidade do negócio ou o que pode ocorrer se o nosso Data Center parar. Se todos apoiassem e estivessem alerta para possíveis problemas, talvez essas questões sendo fortalecidas um pouquinho mais com os gestores, realmente desenvolvendo este conhecimento, pra que possamos nos ajudar eventualmente, ou até mesmo estar gerando algumas questões pra TI realmente trabalhar em cima delas, é uma aproximação neste aspecto.

ENTREVISTA – GERENTE CORPORATIVO DE TI

BLOCO I – CARACTERIZAÇÃO DO RESPONDENTE

Cargo (ocupação): Gerente Corporativo do Grupo SLC Responsável pela TI das empresas SLC Agrícola, SLC Eventos, Ferramentas Gerais, SLC Comercial e Hotel Ouro Verde.
Tempo na Função e na empresa: Treze anos de função, cinco anos na empresa e vinte e quatro anos na área de TI.
Formação acadêmica: Graduação em administração de empresa com ênfase em análise de sistemas / Pós Graduação em análise de sistemas, gestão da produção e governança.
Idade: 46 anos
Principais Responsabilidades: Gerenciar toda a estrutura (sistemas e infraestrutura) de TI da corporação. A parte de infraestrutura contempla servidores, segurança, telecomunicações, serviços ao usuário, e na parte de sistemas aplicativos de gestão e *softwares* de negócios. são aproximadamente 60 pessoas diretamente ligadas à estrutura de TI da SLC.

BLOCO II – GESTÃO DOS RISCOS DE TI

CATEGORIA	QUESTÃO
1	**SIMONSON, JOHNSON e EKSTEDT (2010).** **Na sua percepção, como o modo que TI é gerenciado na organização permite o desenvolvimento do planejamento estratégico, planejamento de TI, e gestão de riscos?** Bom à TI tem participação no comitê executivo aqui da SLC Agrícola (formado por diretores e alguns gerentes que tem reporte direto ao presidente), a TI participa do planejamento estratégico, conhecendo o direcionamento que a empresa está dando para os seus negócios, a TI é envolvida em todas essas questões. Procuramos estar preparados em termo de infraestrutura e sistemas pra acompanhar a necessidade da empresa. Na parte de riscos não há uma estrutura constituída, um setor de gerenciamento de riscos de TI, porém há grande preocupação, principalmente na questão do uso de informações pelos usuários, para isso controles de perfil de usuários são criados, nenhum perfil é autorizado pelo usuário, apenas pelo gestor da área demandante. O acesso externo às informações também é fato preocupante, tratado com base em mecanismos de controle de acessos. **Este gerenciamento ocorre de forma crítica e realista?** O gerenciamento de TI hoje ocorre de forma crítica e busca contemplar as necessidades dos usuários sem por em risco as informações. Alguns pontos ainda podem ser melhorados. Um exemplo de implantação de melhoria é a implantação de um software único de gestão, que gera mais confiança, principalmente para os investidores, em um passado não muito distante operávamos com vários tipos de sistemas não integrados.
2	**ITGI (2007).** **De que forma a confidencialidade, integridade e disponibilidade das informações atuam dentro da organização em relação aos riscos?** A confiabilidade tem relação com a gestão de mudança. Todas às modificações solicitadas são pré-aprovadas pelos usuários em um ambiente de teste, que funciona como um ambiente de homologação. No ambiente de produção nada pode ser modificado sem a avaliação do usuário final da área demandante. Em relação à **disponibilidade**, existe uma central de operações chamada NOC (núcleo de operações e controle) onde são monitorados todos os *links* e acessos. Qualquer tentativa de acesso a site indevido, ou até mesmo de inclusão no nosso *site* o *fail* protege as informações de forma a manter disponibilidade, ou seja, nós temos um compromisso de manter a disponibilidade das informações. A **confidencialidade** das informações também é obtida através da gestão das mudanças que são realizadas no sistema. Um exemplo de gestão da mudança é quando, por exemplo, o usuário precisa calcular o custo de um produto, e o programa para isto está validado, rodando normalmente, caso alguém peça uma alteração em cima daquele programa, seja mudar

	uma formula no cálculo, ou incluir uma rotina nova, a alteração precisa necessariamente ser validado antes de entrar pra produção pelo usuário que solicitou, pra ver se o analista de TI que codificou essa rotina fez a alteração corretamente, de acordo com o que foi solicitado. Neste sentido existe uma participação efetiva do usuário neste processo. A **Integridade** é usada como, por exemplo, em uma rotina de backup, pra proteção caso tenha alguma falha física em algum componente, aí é possível restaurá-lo. Não tive conhecimento de casos nesses cinco anos que eu estou aqui, de perda de integridade, sumiço de informação, ela pode estar errada, mas sempre tem um motivo, uma causa, alguém que entrou com algum dado errado ou um programa que calculou alguma coisa errada, sempre tem uma causa, não é assim, " os dados são modificados e não se sabe quem fez". Há controle sobre estas alterações o que garante maior confidencialidade. **Na sua percepção, como estes requisitos de negócio atendem as necessidades de informações da empresa?** Existe uma grande preocupação com a informação ,em ela estar correta, disponível e saber se é integra. Neste sentido que a atuação de TI opera e consegue atender as necessidades de informações da empresa.
3	**COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).** **Os investimentos realizados em TI são suficientes para permitir que as informações sejam corretas, precisas e estejam disponíveis no tempo adequado? Como isso é validado pelos usuários? são** suficientes especialmente na SLC Agrícola investimentos na questão da disponibilidade, a companhia optou por ter sistemas online, então hoje todas as fazendas tem um *link* principal de rádio terrestre, um *link* de dados e um *link* de contingências por satélite, isto comprova o grande volume de investimento nesta questão. Estes investimentos geram maior conectividade entre as redes para tornar disponíveis os sistemas para os usuários, inclusive àqueles que trabalham nas fazendas. O **usuário** é quem origina a necessidade, e faz uma avaliação no final. Mas os investimentos são aprovados pelo comitê executivo, a TI leva a necessidade ou parte deles. Por exemplo, se é necessário adquirir uma fazenda nova, o comitê nos passa as coordenadas geográficas, a TI vai lá e faz uma visita, vê a viabilidade técnica e já faz o projeto, existem projetos feitos em fazendas bastante distantes, então, por exemplo, as operadoras de Telecom, a OI, a Embratel, não entregam no ponto dentro da fazenda, elas entregam numa cidade próxima, às vezes nem tão próximas, nós temos que fazer repetição via rádio, pra chegar com o sinal de dados dentro da rede da fazenda isso tudo é investimento que a gente está fazendo. Neste sentido eu considero que os investimentos são suficientes para proteger a empresa de eventuais riscos. **De que forma estes investimentos podem proteger a empresa de riscos?** Olha, vou te dar um exemplo, em algumas dessas torres retransmissoras o investimento é feito em casinhas de painel solar, com banco de baterias, estas são coisas que a empresa está executando, se preparando pra minimizar o risco de naquele local haver alguma indisponibilidade, nosso compromisso é 99%, sempre há algum evento, já tivemos situações de raios com queima de equipamentos e tal, mas nós estamos preparados e investindo pra minimizar esses tipos de riscos.
3	**ITGI (2007).** **Como a estrutura de TI presente na organização possibilita a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas)?** Aqui na SLC existe uma área chamada de gestão de ativos, essa área basicamente é responsável por isso, depois de realizado todo o processo de aprovação de um investimento esta área faz o registro desse ativo, e faz o encaminhamento pra equipe técnica que vai fazer a instalação, é esta área que encaminha toda a parte burocrática dos documentos, para o setor de patrimônio. No grupo são aproximadamente sessenta pessoas ligadas à estrutura de TI, na SLC Agrícola, a estrutura de TI está dividida em pessoas voltadas ao sistema, e a infraestrutura. Hoje há um supervisor aqui na Agrícola para sistemas, Já a infraestrutura está divida em quatro equipes: banco de dados (data Center), Servidores e rede, telecomunicação (links, rádio e

	voz) e *service desk* e suporte. **De que maneira esta estrutura interage com a prevenção dos riscos?** Buscando minimizar os riscos gerados no ambiente de TI, como por exemplo: o vazamento de informações, acessos indevidos. Um risco grande que vejo, é nós não termos um site backup, o nosso site esta no nosso *Data Center* nós temos no backup, mas se ocorrer um desastre naquele site, vamos falar de por exemplo um desastre natural, alguma coisa assim, não estamos preparados. Muitas empresas hoje já se ocupam em ter em um local distante as informações duplicadas, nós não temos isso hoje. É mais do que um backup operando, o backup nós temos, mais quanto tempo nós levaríamos pra colocar em dia, colocar no ar esse, no caso se ocorresse um desastre natural, ou um acidente. Este é um problema estrutural que afeta a prevenção dos riscos.
4	**ALBERTIN e ALBERTIN, (2012).** **Quais as vantagens ou desvantagens que a Tecnologia da Informação – TI oferece decorrentes de seu uso?** A principal **vantagem** é a integração, a informação em tempo real, um exemplo disso é a emissão da nota fiscal eletrônica. A TI possibilita acesso à conectividade de bancos, clientes, fornecedores e outras áreas internas dentro da fazenda, ou seja, é um sistema bastante integrado, obviamente que isso tem um custo, o custo da conectividade e o custo das *interfaces* do sistema, uma área faz uma coisa, a outra área tem que complementar uma informação, fica um processo mais horizontal não tanto verticalizado. Uma **desvantagem,** é o custo elevado, hoje precisamos estar conectados o tempo inteiro, nosso custo com *links* é alto, outra desvantagem que vejo (pode não ser bem uma desvantagem) é que a tecnologia acaba travando um pouco o processo, não deixa em alguns momentos o usuário realizar operações manualmente, claro com o intuito de evitar erros , ela obriga que os processos sejam seguidos. **Qual a sua percepção da relação desta utilização com os riscos?** Na minha visão, o maior risco é o vazamento de informações confidencias, hoje em dia, é muito difícil controlar tudo isso, um funcionário pode pegar e exportar dados pra uma planilha e levar em um pen drive, sabendo assim da área de produção, qual são os insumos que estão sendo plantados ou nossos preços e margens, neste sentido acredito que o maior risco atualmente é o controle de vazamento de informações, que está amplamente vinculada às atitudes das pessoas e usuários. Uma medida preventiva aqui na empresa é a aposta no treinamento de seus colaboradores. O acesso externo das informações é mais fácil de ser protegido, é mais tranqüilo, porém há uma preocupação maior em controlar os acessos internos, (relatórios, pen drives). Um dos controles que se tem para se proteger destas situações é em relação a envio de e-mails em tamanho de arquivos e cheque de conteúdos. Em relação à pen drive, e materiais impressos controles ainda precisam ser trabalhados.
4	**BULGURCU, CAVUSOGLU E BENBASAT (2010); SPEARS E BARKI (2010)** **Como a empresa implanta planos de segurança para reduzir os riscos relacionados à segurança das informações?** Existem políticas para a segurança das informações. Por exemplo, no momento da contratação o funcionário assina uma política, um termo de compromisso o qual relata que as informações são da empresa e não são dele. Pode haver investigação a qualquer momento das informações usadas na caixa de e-mail, já que o e-mail é estritamente profissional e que os sites acessados precisam ser de conteúdo relacionado com o trabalho, isso tudo está contemplado na política, e fica na ficha de RH do funcionário. Existe também monitoramento em cima dos *proxi*s. No momento, estamos testando outros aspectos de segurança (projeto piloto) que são: a instalação de câmeras de segurança na fazenda, inspecionando caminhões, armazéns e depósitos de peças, visando a proteção da estrutura. Estas são algumas ações para tentar proteger a segurança da informação. **Qual o envolvimento funcional dos usuários?** As ações não contemplam a participação do usuário para sua criação, a política de segurança de acessos, por exemplo, não teve participação do usuário, teve participação da TI com o RH e o comitê executivo

	(composto pelos diretores e o presidente). Na parte dos planos de segurança, voltada à segurança física, por exemplo, as câmeras de segurança instaladas nas fazendas que contemplaram o envolvimento dos gestores que contribuíram com algumas idéias, visando identificar o que precisa ser monitorado, qual a localização, qual a freqüência de armazenamento e quem vai monitorar o processo. **De que maneira eles participam da gestão de riscos e segurança?** Na gestão dos riscos de TI e segurança eles não têm participação, neste ponto os controles são responsabilidade da TI. Eles não têm noção do assunto, portanto, não participam. A gente tenta fazer o trabalho de aculturamento, salientando a importância de não compartilhar senhas, mas isso é um processo difícil, ligado à própria cultura pessoal do funcionário. Os planos de segurança contemplam proibições, como por exemplo, de acesso a internet, neste caso as regras são impostas pela TI com base nas diretrizes solicitadas pela diretoria executiva, protegendo então os acessos e por conseqüência as informações. Mas os usuários não têm muita noção, não participam da elaboração destas regras.
5	**ITGI (2007)** **De que maneira os processos de TI possibilitam que a entrega e suporte dos serviços de TI atendam as necessidades dos usuários?** Trabalhamos com base em uma metodologia de gestão de demandas, que ocorre em formato eletrônico, ou seja, sistematizado. As demandas são recebidas e priorizadas, na seqüência o líder de processo, o gestor da área ou usuário chave (aquele que domina aquela rotina no sistema) executa o processo, esta é uma forma de haver certeza que o que está sendo feito é exatamente o que a empresa esta demandando, não apenas aquilo que a TI acha que tem que fazer. **Como a prestação de serviços de TI atua para minimizar os riscos?** Buscando atuar de acordo com boas práticas, como pessoas capacitadas e treinadas. Nossa equipe é focada em dar segurança, são cinco profissionais que pensam na segurança, pensam no acesso, e na política o dia todo no setor de NOC (núcleo de operações de controle).
6	**SPEARS E BARKI (2010); ITGI (2007).** **Como a recomendação e comunicação de planos de ação de remediação dos riscos consideram a participação dos usuários para a gestão de riscos e segurança?** Um exemplo de participação dos usuários é a confecção dos perfis de usuários que são validados por seus gestores. Por exemplo, caso alguém tenha acesso a um sistema, aplicativo ou a alguma fazenda indevidamente, temos um risco identificado. Para evitar esta situação, temos um processo de aprovação de pesquisa, além disso, a gente tem o controle compensatório, que é normalmente, a circulação desses perfis pelos gestores para que estes sejam revalidados, então é uma forma de envolver os usuários, identificando o acesso ao sistema por pessoa e por usuário, a fim de confirmar se cada um tem mesmo o acesso que precisam ter daí o gestor da área revalida, que é para quem nós pedimos a suspensão, cancelamento, ou para incluir mais alguém. Esta é uma forma de envolvê-los no controle dos acessos. **Como esta gestão se integra aos processos gerenciais?** Hoje eu vejo assim, as áreas são totalmente dependentes da TI, quase não tem nenhum processo que eles não dependam, o sistema está todo integrado e totalmente informatizado, por isso, é difícil não ver a TI vinculada, neste sentido. A TI tem metas de cumprir, por exemplo, fechamento das informações mensais junto com a área contábil, fornecer fluxo de caixa, dados de pagamentos e recebimentos de bancos através de TI. Para a própria produção agrícola, hoje não se faz mais planejamento agrícola em planilhas, ou em papel, é tudo informatizado. Neste sentido vejo que a TI está presente nos processos gerenciais.
7	**BULGURCU, CAVUSOGLU E BENBASAT (2010).** **Como a estrutura para gestão de riscos de TI é organizada na corporação?** Não realizamos efetivamente gestão de riscos, a gente faz gestão de segurança, neste aspecto temos pessoas dedicadas para isso, e estes processos minimizam os riscos relacionados principalmente a acessos indevidos.

	Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? Este aspecto é como um trabalho de formiguinha, às vezes parece que o usuário esta contra a TI, pois eles são as pessoas que dizem não, que não pode isso, não pode aquilo, então o pessoal de TI precisa explicar porque estamos querendo bloquear aquele acesso, porque é necessária uma assinatura a mais, um controle a mais. Eu não vejo uma formula mágica para resolver isso e conscientizar o pessoal rapidamente. Graças a Deus, não tivemos nenhum incidente de vazamento de informações, ou de prejuízo relativo a isto, talvez se houvesse um susto, um fato, a ficha iria cair mais rápido, como não houve é formiguinha mesmo, e no dia á dia, alertando e cumprindo os processos.
8	**ITGI (2007); SPEARS E BARKI (2010)** **Que tipos de esforços são realizados pela corporação para manutenção e monitoramento de planos de ação para os riscos?** A auditoria externa nos processo de TI é um fato que visa à manutenção e implantação destes planos. O fato de existir um alinhamento entre auditoria externa de TI e auditoria externa financeira, proporciona validação dos processos realizados. A auditoria externa de TI identifica quais os controles ou processos de TI que devem ser focados e acompanhados para minimizar, e também controlar os riscos destes processos. **Como estes esforços contemplam o desenvolvimento e a performance de controles?** Na minha percepção eles contribuem com a melhoria dos controles, já que a auditoria verifica se os processos estão bem controlados na TI, se isso ocorrer o risco no aspecto financeiro pode ser menor, conforme o que eles encontrarem na nossa área, eles podem minimizar ou aumentar os controles na área financeira, eu vejo que assim que ocorre a integração.

BLOCO III – GERENCIAMENTO DOS RISCOS CORPORATIVOS

CATEGORIA	QUESTÃO
1	**FRIGO E ANDERSON (2011).** **Como a organização realiza a avaliação estratégica de seus riscos?** Quanto à parte de gestão de riscos corporativos, não sou especialista e tenho pouco conhecimento realmente, eu sei que a empresa se preocupa muito em proteger principalmente o aspecto financeiro e caixa. Como trabalhamos muito com exportação, somos afetados pela variação de dólares e outras moedas, neste sentido são realizadas algumas proteções, mas eu não conheço exatamente quais são esses trabalhos que são realizados. **Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança?** Acredito que sim, hoje vejo a organização como uma empresa muito cuidadosa em aspectos legais e fiscais, os gestores são cobrados para que os riscos trabalhistas sejam evitados, os riscos em termos de meio ambiente já que este é um aspecto relacionado ao próprio negócio. Neste aspecto existem grupos de trabalhos, nesse sentido é uma empresa muito idônea, muito preocupada com o meio ambiente, embora o que exatamente e como cada um desses riscos é trabalhado eu não tenho domínio, mas acredito que estes controles e ações das áreas para mitigar os riscos melhoram a governança da corporação.
2	**IBGC (2007); COSO (2007); ISO 31000 (2009); Aven (2011); GERIGK E CORBARI (2011).** **De que forma o gerenciamento dos riscos corporativos possibilitam evitar, reduzir, compartilhar ou aceitar os riscos?** Na medida em que a empresa pratica ações que podem reduzir o impacto destes riscos é possível minimizar o custo que poderia estar associado a este fato. **Na sua percepção este gerenciamento estabelecer respostas a estes, reduzindo surpresas, custos ou prejuízos associados?** Eu acredito que este gerenciamento pode minimizar os custos. Hoje não se tem conhecimento na organização de grandes confirmações de riscos e impactos negativos, o risco é probabilidade que a empresa tem,

	neste sentido nas nossas atividades não temos confirmação de que para algum tipo de risco a empresa não tomou devidas precauções, não tomou cuidado e aconteceu, ele se efetivou com prejuízos graves associados.
3	**COSO (2007); IBGC (2007); GERIGK e CORBARI, (2011).** **A organização procura identificar os eventos que possam ter consequências operacionais, financeiras ou estratégicas adversas? Caso afirmativo, como são prevenidos ou minimizados tais eventos?** Acredito que sim, principalmente o financeiro voltado à proteção do caixa da empresa. Um dos riscos que eu sei que a empresa trata de cuidar é o risco no aspecto de seqüência no conhecimento, como a empresa esta crescendo e tem áreas novas sendo abertas, há uma constante preocupação em não perder o conhecimento, reservar os funcionários que avançam com o sucesso da empresa. Existem também ações voltadas a aspectos ambientais.
4	**COSO (2007); IBGC (2007)** **Como a gestão de riscos corporativos possibilitam uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos? Como isto ocorre?** Prefere não opinar em função de não ter conhecimento específico sobre a gestão de riscos corporativos.
5	**Você considera que os seguintes princípios são atendidos pela empresa, quanto à gestão de riscos. Explique como isso ocorre. ISO 31000(2009)** **1) Cria e protege valor;** **2) Participa de todos os processos organizacionais;** **3) Participa da tomada de decisão;** **4) Aborda explicitamente a incerteza;** **5) Atua de forma Sistemática, estruturada e oportuna;** **6) Baseia-se nas melhores informações possíveis;** **7) Se adéqua a realidade da organização;** **8) Considera fatores humanos e culturais;** **9) Atua de forma transparente e inclusiva;** **10) Atua de forma dinâmica e interativa, capaz de reagir a mudanças;** **11) Facilita a melhoria contínua da organização.** A gestão de riscos existe na organização, principalmente em função de ser uma companhia que opera na bolsa de valores, só o fato de existir um setor que se preocupe com estas questões já demonstra a preocupação da empresa neste sentido. Acredito que a empresa contemple na gestão dos riscos corporativos estes pontos, mas não tenho conhecimento do aprofundamento de cada um destes.
6	**BULGURCU, CAVUSOGLU E BENBASAT (2010).** **Como a estrutura para gestão de riscos corporativos é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco?** Existe a atuação do comitê de riscos, que se encontra toda segunda-feira, mas não sei exatamente as ações que são tomadas. A TI se preocupa com os riscos do seu ambiente, acredito que os demais setores também tenham esta preocupação.
6	**AVEN (2011).** **A gestão dos riscos realizada na organização fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro?** Não temos conhecimento de nenhum evento grave em função disso, acredito que a gestão de riscos esta sendo bem sucedida, e que possibilita explorar oportunidades e evitar perdas.
7	**ISO 31000(2009)** **Como os seguintes processos são considerados em relação aos processos de negócio organizacionais?** **1) Comunicação e consulta às partes interessadas (internas e externas)**

	2) Estabelecimento do contexto (parâmetros internos e externos que precisam ser levados em consideração) **3) Avaliação dos Riscos (identificação, análise e avaliação dos riscos)** **4) Tratamento dos Riscos** **5) Monitoramento e análise crítica dos Riscos** A Gestão de Riscos de TI é realizada pela Gestão de TI, e contempla a avaliação dos riscos gerados naquele ambiente. Os riscos corporativos são tratados nas áreas, através do comitê de riscos e da área de RI.
8	**ISO 31000 (2009)** **Como a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações? Estas decisões consideram a incerteza, a natureza desta incerteza, e como ela pode ser tratada?** Os riscos inerentes a sistemas, a TI e a comunicação, isto é conhecido e as ações são priorizadas por TI. Os riscos inerentes á empresa chegam ao nosso conhecimento mais em função das necessidades dos demais setores, em formato de demanda, oportunidades de negócio em que a TI consegue auxiliar.

BLOCO IV – RELAÇÃO ENTRE GESTÃO DOS RISCOS DE TI E GERENCIAMENTO DOS RISCOS CORPORATIVOS

ITGI (2007) **1) Como a TI atua para prevenir riscos inerentes ao negócio?** A participação de TI é acessória. Somos área de serviços e uma área de suporte, às vezes podemos estar atuando em uma demanda para prevenir riscos e nem sabemos, faz parte do processo da área e agente acaba ajudando na implementação. Somos hoje uma prestadora de serviços, somos demandados pelos demais setores, porém seguimos o direcionamento das áreas de negócios. Se existe uma preocupação pra complementar determinados controles para os negócios a TI procura fazer com que o setor de sistema programe isso, ou seja, nós somos facilitadores nada mais que isso, nós só somos direcionadores nesse aspecto. **Esta atuação pode ser considerada satisfatória dentro de uma perspectiva de negócio?** Creio que sim. Somos área de serviço, área de suporte, às vezes podemos estar atendendo uma demanda pra minimizar os riscos, pra ter um controle a mais, e em alguns casos nem temos conhecimento do resultado daquela implantação e dos ganhos, faz parte do processo da área que estamos atendendo e nós a incrementamos, eu imagino que hoje, a gente facilita principalmente para a questão de risco legal e fiscal, o fato de ter tudo registrado em sistema eletrônico e documentado, facilita muito o controle. Não existe uma relação formal aqui, eu acho que a uma relação informal.
SPEARS E BARKI (2010). 2) **De que maneira os usuários participam do gerenciamento de riscos de segurança nos processos de negócios? Como a sua participação é percebida e qual é o impacto da participação na segurança do negócio?** Como eu falei, os usuários têm alçadas para poder operar o sistema, não é qualquer um que pode acessar tudo. Por exemplo, se alguém da área de engenharia agrícola pedir acesso ao sistema de produção ou de ordem de compra, por exemplo, não basta o gerente de aquele cidadão conceder esta alçada para ele, o gerente de compras também tem que dar um aceite nisto. Eles não têm participação efetiva para atuar no gerenciamento de riscos, por isso existem bloqueios, permissões para proteger as informações e acessos. A TI ajuda implementando processos neste sentido, processos que as áreas de negócios se responsabilizam por quem pode fazer o que, dentro do seu sistema.
IBGC (2009) **3) Como a práticas de governança corporativa orientam o dia a dia do trabalho da organização? De que forma elas contribuem para a gestão de riscos em TI e gestão dos riscos corporativos?** De maneira formal não vejo muita orientação não, muito informal, a maioria pelos princípios da organização, pela ética e outros, mas não tem uma coisa formalmente constituída. Por exemplo, não vejo a área de TI fazer parte ou se esta conectada formalmente em reuniões periódicas que tratem deste aspecto, isso não acontece, eu não vejo. Talvez fosse uma forma de contribuir de forma

efetiva para melhorar esta gestão. Nossa participação esta muito ligada nos princípios que existem na cultura da corporação.

JUNIOR, JUNQUEIRA e BERTUCCI, (2010).

4) **De que forma a adoção de mecanismos de controle possibilita redução dos riscos corporativos e riscos de TI?** Nós temos nossos controles internos de TI, acredito que as áreas também tenham, então a área comercial tem os seus, a área de produção, financeira e tal. Como é que a TI interage com eles, quando somos demandados, quando, por exemplo, colocamos uma trava no sistema de compras pra não deixar criar ordem de compra ou necessidade de aprovações, ou mesmo alçadas nas aprovações no sistema de compras, me coloca dois aprovadores no sistema de aprovações para bancos, então neste momento agente interage com TI paras áreas e controles.

SPEARS E BARKI (2010).

5) Como os controles internos protegem as informações financeiras? Esta proteção é capaz de produzir informações contábeis financeiras confiáveis? Acredito que estes controles são capazes de proteger as informações financeiras e contábeis. Isso ocorre nos processo de cada setor, assim como nos processos contábeis, que assim como já mencionei, em função das permissões que são concedidas para os setores. Isso permite que as informações possam ser mais confiáveis.

IBGC (2009)

6) **De que maneira a atuação do comitê para a gestão de riscos ocorre?** Eu sei que o Comitê se encontra todas as segundas feiras, mas não tenho muito conhecimento sobre o que é tratado. Sei que há uma grande preocupação nestas reuniões com aspectos inerentes ao cambio, pois como somos exportadores este fator é um risco para o negócio e há uma grande preocupação da companhia com isto.

Como sua atuação contempla a prevenção de riscos de TI e risco corporativos? Não tenho informações sobre a contemplação destes riscos, os riscos que temos identificado são nas operações, nas demandas e nos processos realizados por TI, e é pouca a atuação deste comitê com a atuação de TI.

7) **Em sua opinião existe uma aproximação entre os riscos de TI e riscos corporativos? Como isso seria possível?** Eu acredito que sim. Com certeza, tem riscos que são puramente de Ti, mas há também riscos que são inter-relacionados. Hoje como falei, o principal risco que vejo é vazamento de informações, em termos de TI, a empresa por sua vez, se existe algum aspecto de concorrência, ou até de má fé , algum aspecto relacionado à atitude de algum funcionário que não está satisfeito com alguma prática, que possa fazer alguma denuncia, se a empresa não proteger as informações, pode acarretar em outros riscos que afetem o negócio, eu vejo que esses riscos são bastante conectados. Em minha opinião, o risco de TI, é um risco a mais nos riscos corporativos, caso os riscos de TI não sejam gerenciados ou não sejam monitorados, eles podem avançar para outros riscos de negócio.

ENTREVISTA TRANSCRITA – MEMBRO DO COMITE DE RISCOS

BLOCO I – CARACTERIZAÇÃO DO RESPONDENTE

Cargo (ocupação): Gerente de relações com o investidor (membro do comitê de riscos)
Tempo na Função e na empresa: 6 anos de empresa, na área de RI 3 anos, no comitê de riscos 3 anos..
Formação acadêmica: Bacharel em Administração de empresas e Direito
Idade: 30 anos
Principais Responsabilidades: Produzir documentos, informações trimestrais e anuais para os investidores e atualização esporádicas para a CVM. Contato todo com o mercado financeiro (fornecedores). Sou gerente de RI e abaixo de mim tem uma analista, e um auxiliar, essa é a área de RI está ligada a área administrativa financeira. Sou responsável pela parte de relacionamento com os investidores, então além de me envolver com elaboração das informações trimestrais e anuais, eu tenho uma série de informações com os investidores que já tenham ações da empresa, ou fundos de investimentos, gestores de fundos que são daqui, ou de fora, a gente acaba tendo mais contato com o investidor internacional, de interesse na área agrícola, ele é muito forte fora do Brasil.

BLOCO II – GESTÃO DOS RISCOS DE TI

CATEGORIA	QUESTÃO
1	**SIMONSON, JOHNSON e EKSTEDT (2010).** **Na sua percepção, como o modo que TI é gerenciado na organização permite o desenvolvimento do planejamento estratégico, planejamento de TI, e gestão de riscos?** É aquela coisa, é que a TI é uma área de apoio, então tudo que eles conseguem fazer funcionar a gente usa para produzir tudo, então eu vejo uma forma daquilo que a gente falou antes, se não tivesse tudo funcionando rápido ou não tivesse acesso aos arquivos funcionando, servidor funcionando e a internet com uma velocidade mínima para eu trabalhar, eu não vou conseguir fazer muita coisa, então creio que é uma área de apoio, uma área barbada, que tem que estar operando, para a empresa funcionar. **Este gerenciamento ocorre de forma crítica e realista?** Sim, eu acho que tem, critica tem bastante,
2	**ITGI (2007).** **De que forma a confidencialidade, integridade e disponibilidade das informações atuam dentro da organização em relação aos riscos? Na sua percepção, como estes requisitos de negócio atendem as necessidades de informações da empresa?** Eu vejo que nesse aspecto há novamente uma critica que é quase diária, como por exemplo, às vezes como recentemente aconteceu na quinta feira à tarde, uma queda da rede, aí ninguém mais consegue acessar os arquivos e param de trabalhar, ficam olhando um para a cara do outro, então a gente acaba sentindo o impacto que isso tem o nosso trabalho. É aquela coisa, quando esta funcionando ninguém fala nada, quando cai à luz, todo mundo fica desesperado,.
3	**COHAN (2005); LUCHT, HOPPEN e MAÇADA (2007).** **Os investimentos realizados em TI são suficientes para permitir que as informações sejam corretas, precisas e estejam disponíveis no tempo adequado?** Pelo que eu vejo, acredito que a gente poderia melhorar um pouco ainda o investimento, por exemplo, em uma internet mais rápida, em computadores melhores e não computadores antigos que não estão mais funcionando direito. A nossa própria internet usada na fazenda, ela ainda precisa de uma conexão mais moderna, então a gente poderia ter investido um pouco mais, para melhorar a comunicação. **Como isso é validado pelos usuários?** Bom é que o usuário acaba sentindo se algo não esta funcionando bem, então ele vai ver aquilo vai ver o acesso e como é que está, vai ver a planilha e o software que foi solicitado, pra entender porque o serviço não está atendendo, então vai acabar fazendo uma validação para o próprio uso.

	De que forma estes investimentos podem proteger a empresa de riscos? Eu acho que qualquer investimento que for feito na TI que permita que as informações sejam corretas, em tempo correto, e rapidamente, vai evitar possivelmente algum risco de, por exemplo, a nossa RI tem que achar um jeito de divulgar, se eu não divulgar no prazo eu tenho uma multa, perco a credibilidade no mercado caso eu não consiga entregar a tempo a informação, então certamente isso reduz os riscos.
3	**ITGI (2007).** **Como a estrutura de TI presente na organização possibilita a melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas)? De que maneira esta estrutura interage com a prevenção dos riscos?** A essa perguntas prefiro não responder, porque teria que ser muito mais genérico, porque eu não estou no dia a dia.
4	**ALBERTIN e ALBERTIN, (2012).** **Quais as vantagens ou desvantagens que a Tecnologia da Informação – TI oferece decorrentes de seu uso?** Bom, em primeiro lugar, a questão da rapidez, eu acho que quando eles conseguem nos possibilitar uma conexão de internet estável e rápida, ela traz uma serie de benefícios para nós, uma serie constante de arquivos da rede. Meu computador esta funcionando adequadamente, porém, às vezes você chega de manha aqui e não consegue abrir nem os e-mails, não consegue acessar os arquivos, ou demora muito para abrir um arquivo, então é um processamento que não é normal, nem no software, nem nos programas, e aí ele traz prejuízos, então ele tem que primar para o bom funcionamento de tudo que é disponibilizado. **Qual a sua percepção da relação desta utilização com os riscos?** Acredito que os riscos estão mapeados nas áreas, e sendo assim sempre tem certo envolvimento da TI em alguns desenvolvimentos para ajudar a prover uma solução para quilo, se é preciso criar algum controle interno, um controle de semanal, ou se eu preciso de algum assunto x a TI pode ajudar a criar isso, talvez haja interação assim das áreas com a TI.
4	**BULGURCU, CAVUSOGLU E BENBASAT (2010); SPEARS E BARKI (2010)** **Como a empresa implanta planos de segurança para reduzir os riscos relacionados à segurança das informações? Qual o envolvimento funcional dos usuários? De que maneira eles participam da gestão de riscos e segurança?** Bom, essa pergunta ai prefiro não responder, porque eu não estou no dia a dia da área de TI.
5	**ITGI (2007).** **De que maneira os processos de TI possibilitam que a entrega e suporte dos serviços de TI atendam as necessidades dos usuários?** É, eu acho que nessa questão da gente ficar sem essa rede, ou sem internet é raro, eu não diria que é alguma coisa problemática aqui na matriz. Eu vejo mais isso nas fazendas, os caras sem acesso a internet, então eu acho que às vezes até mesmo pela localização a gente tem problemas, não sei quando disso é "culpa" da TI, e quanto é problema de serviço lá na região mesmo, mas eu vejo que é um meio de ficarem sem contato com a matriz, e isso obviamente atrasa muito o trabalho. **Como a prestação de serviços de TI atua para minimizar os riscos?** Sim, mas tem sim um processo participativo, que de certa forma é natural, muitos por estarem na lavoura e fazer um processo, uma aplicação ou um plantio, vai mapear os problemas dos riscos, riscos acarretam em futuros problemas pra gente, desta forma os usuários vão trazer algumas soluções baseados nos riscos. Até mesmo a própria questão de a gente estar trabalhando com uma agricultura em escalas complexas, já nos mantém testando coisas novas, como máquinas novas. Hoje em dia, para o que faz a colheitadeira, por exemplo, a gente testa as maquinas pra eles, e às vezes eles vão fazer um mutirão e nós vamos estar fazendo testes pra eles, então a gente esta com produtos novos que a gente está testando, inaugurando, e os nosso usuários trazem os problemas que enfrentam.
6	**SPEARS E BARKI (2010); ITGI (2007).** **Como a recomendação e comunicação de planos de ação de remediação dos riscos**

	consideram a participação dos usuários para a gestão de riscos e segurança? Creio que a gente começa mapeando os riscos, e acaba criando em função do risco financeiro, uma espécie de controle, e esses controles acabaram mudando um pouco as tarefas, de cada área. **Como esta gestão se integra aos processos gerenciais?** A partir disso é que as coisas vão ter que ser realizadas agora, de cada forma, isso alterou as tarefas e os processos das áreas, então se era feito de uma forma mais solta, mais discricionária, agora ela tem uma regra para ser realizada, por causa do risco, que não pode ser deixado na mão do usuário, porque ele pode cometer o erro que vai trazer um prejuízo financeiro.
7	**Como a estrutura para gestão de riscos de TI é organizada na corporação? Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco? BULGURCU, CAVUSOGLU E BENBASAT (2010).** Vou responder esta questão de forma mais genérica, sei que tem a parte de sistemas e a parte de infraestrutura.
8	**ITGI (2007); SPEARS E BARKI (2010)** **Que tipos de esforços são realizados pela corporação para manutenção e monitoramento de planos de ação para os riscos? Como estes esforços contemplam o desenvolvimento e a *performance* de controles?** Eu acho que como a gente foi ficando maior e mais complexo, dessa forma eu volto para aquela questão do protocolo e dos manuais, acho que essa é a melhor forma mesmo de controle, então, eu vi acontecer muita coisa neste sentido, a partir de agora vai ter um processo, a partir de agora vai ser assim, antes era o "Zezinho" quem fazia e brigavam com ele, agora o "Zezinho" foi embora, e então foi criada uma regra, eu mesmo na área de RI criei uma, a gente tem hoje para cada um dos processos uma "receita de bolo", informando como as atividades são realizadas, como é que são trocadas com as pessoas recentemente, e aí essa pessoa que saiu descreve o que fazia, e como fazia. Sendo assim a pessoa nova já sabe como é que é, e desse jeito não deixando margem para erros dos novatos por não saberem o que fazer ou como fazer. Exatamente por isso são criadas muitas regras e muitos protocolos internos

BLOCO III – GERENCIAMENTO DOS RISCOS CORPORATIVOS

CATEGORIA	QUESTÃO
1	**FRIGO E ANDERSON (2011).** **Como a organização realiza a avaliação estratégica de seus riscos? Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança?** Bom, eu diria que cada área faz a sua parte, por exemplo, a área financeira trata os riscos através do comitê de riscos, preocupando-se com todas as questões financeiras. Outro exemplo é o nosso gerente de RH, que é gerente de RH e sustentabilidade, ele tem uma pessoa, um coordenador, que é responsável pela parte de coordenação ambiental, que pensa as questões ambientais (esta preocupação é bastante forte para nossa empresa). Existem muitas áreas espalhadas pelo país, como a gente está mexendo com o ambiente no dia a dia, a gente tem uma legislação ambiental muito forte, e também um controle muito forte da parte do RH. Verificando as condições de trabalho das pessoas, neste sentido a área de RH mapeia e atende todos esses riscos, controlando eles na própria área. Existem reuniões periódicas de todos os gerentes da matriz, onde este assunto é comentado. Por exemplo, agora a gente está com problemas nos PPD (pessoas portadoras de deficiências), não estamos conseguindo atender a cota de 5%, não conseguimos achar gente e agora o ministério do trabalho está nos autuando por isso, porém não achamos pessoal com estas características. Estas questões, estes riscos são problema do RH, que discute a nível de diretoria, porque, enfim as ações para reduzir estes riscos vêm do RH, seja realizando campanhas nas fazendas, junto aos setores ou verificando o que pode ser feito. O comitê de riscos está mais pros vieses financeiros, do que para os outros itens de riscos, eles são tratados dentro das suas áreas, não existe uma estratégia integrada**.**

	Esta avaliação permite alavancar a execução de processos ocasionando a melhoria da governança ? Acredito que sim, acho que a partir do momento que conseguirmos mapear melhor isso, tratar melhor esses assuntos, fica mais fácil até transmitir isso pra todo o mercado, e principalmente o mercado interessado na empresa. Por exemplo, nessa parte ambiental, a gente basicamente atende o que a legislação pede, ambientalmente e socialmente, por exemplo, quando compramos uma área de 100 hectares a gente tem que ter uma reserva legal 20% que não pode usar para plantar, temos que deixar a reserva legal. Então a isso tudo a gente está atendendo, há muito fazendeiros que não atendem, ou seja, que não está cumprindo a lei, a gente basicamente cumpre a lei, mas eu acho que quanto mais a gente conseguir mapear e ter dados sobre isso, mais fácil fica, até para que isso se apresente de uma forma transparente para todo o mercado interessado. Acredito que este mapeamento dos riscos está melhorando, ainda não é ideal, podemos ter um mapeamento melhor disso, estamos crescendo bastante e temos que melhorar os controles disso.
2	**IBGC (2007); COSO (2007); ISO 31000 (2009); Aven (2011); GERIGK E CORBARI (2011). De que forma o gerenciamento dos riscos corporativos possibilitam evitar, reduzir, compartilhar ou aceitar os riscos?** Eu acho que, com certeza quanto melhor a gente construir formas de controles de riscos, melhor vão conseguir evitá-los e minimizá-los. Por exemplo, já tivemos alguns problemas em algumas fazendas de abrir uma área para plantar que não poderia ter aberto, porque deveria ser uma reserva ou alguma coisa assim, então se tivesse um controle, um treinamento melhor dos funcionários das fazendas, esses tipos de riscos poderiam ser evitados, faltou de certa forma um controle que poderia ser mais eficaz. **Na sua percepção este gerenciamento estabelece respostas a estes, reduzindo surpresas, custos ou prejuízos associados?** Sim, com certeza, acho que principalmente se tratando nesse aspecto ambiental, focando mais, porque acho que é o que mais custa, e agora o congresso esta para colocar um novo código florestal, que estabelece novas regras, isso nos impacta completamente, o controle neste aspecto precisa ser muito rigoroso, para evitar problemas com isso. Existe também a questão do clima, não é um problema ambiental, é um problema de vulnerabilidade ao negócio, se chove, se não chove, isso pode trazer mais ou menos produtividade, em vez de colher 55 sacas de soja, posso colher 45, por exemplo, me refiro mais diretamente na questão de legislação ambiental, o que o código ambiental exige da empresa e o que a empresa tem que cumprir de procedimentos nesta área.
3	**COSO (2007); IBGC (2007); GERIGK e CORBARI, (2011).** **A organização procura identificar os eventos que possam ter consequências <u>operacionais, financeiras ou estratégicas</u> adversas?** Sim, cada vez mais estamos melhorando, estamos procurando padronizar a nossa atividade, nós crescemos de 7 para 14 fazendas em 5 anos, saímos de 117 mil hectares, para 250 mil hectares plantados em fazendas diferentes, a gente teve que contratar muita gente nova, gerentes, agrônomos, operadores de máquinas , então temos procurado, cada vez mais padronizar as nossas utilidades, porque dentro do processo de colheita e de plantio muitas coisas podem acontecer de forma errada, muito pode ser feito de forma errada. Vou te dar um exemplo, quando a gente aplica as defensivas na lavoura, com uma máquina pulverizadora, ela vai aplicando o defensivo, que é liquido, se ele é aplicado até duas horas antes de chover perde o efeito, ou seja, se é aplicado e chove o produto escorre se não houver uma padronização disso um cuidado para evitar que a chuva lave o produto, incorremos em custos. Se existe uma padronização dos processos, isso vai garantir, não só a produtividade mais toda a gestão de custo e o aumento de eficiência. A empresa busca identificar todas estas questões relacionadas ao risco, dentro das áreas dos processos. **Caso afirmativo, como são prevenidos ou minimizados tais eventos**? Eu acho que assim, talvez separando por áreas, as questões de mercado, de preços e de *comodities*, estão bem trabalhadas pelo comitê de riscos, é um processo bem eficaz de mapeamento,

	controle, e diluição de riscos. Na verdade a nossa produtividade, é muito ariscada, tem riscos por todos os lados, não temos muito controle do custo nem controle de preços, tem esse impacto de legislação que é muito dinâmico, a produção em sí, se chove ou se não chove também influencia, porque é uma fabrica a céu aberto, então nós tivemos que estruturar todo o negócio, por exemplo, as fazendas são localizadas em estados diferentes no Brasil, então se em uma tem uma seca, em outra tem produtividade recorde. Isso acaba compensando um pouco os riscos inerentes ao próprio negócio, então eu diria que a nossa empresa tem uma participação muito grande com o risco, com o gerenciamento dos riscos. Todas as atividades são meio que montadas assim, para reduzir os riscos que são inerentes ao negócio agrícola, o nosso desafio hoje é mais no sentido de padronizar os processos e deixar tudo bem definido, tem que ter protocolos e procedimentos para tudo.
4	**COSO (2007); IBGC (2007)** **Como a gestão de riscos corporativos possibilitam uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos? Como isto ocorre?** Eu não sei se é uma resposta integrada, por exemplo, nossa atuação foca muito mais nos riscos financeiros, de legislação, de clima e riscos de alguma operação ocorrer de forma equivocada. Cada um destes aspectos de forma isolada. Digamos que o risco financeiro não vai impactar no risco climático, eu não vejo esta percepção de preocupação integrada. Por exemplo, se uma colheita pegar fogo, temos seguro para isso, procedimentos para apagar o fogo, uma brigada de incêndio em cada uma das fazendas. Já aconteceu de morte de funcionário no silo, às vezes acontece do funcionário cair, por falta de uso de equipamento como o cinto. Nós tentamos reduzir isso com treinamentos e toda a semana tem discussão sobre a segurança nas fazendas, então eu acho que são riscos em separados, que são tratados de forma separada.
5	**ISO 31000(2009)** **Você considera que os seguintes princípios são atendidos pela empresa, quanto à gestão de riscos. Explique como isso ocorre.** **1) Cria e protege valor;** Sim, eu acho que a partir do momento que nós realizamos uma gestão de riscos financeiros, de legislação ou risco climático,assim, eu estou protegendo o valor do negócio, se eu não gerencio bem isso, eu posso quebrar a empresa, devido a imagens negativas, enfim, vai faltar dinheiro, isso é essencial, por que faz parte do negócio. Outro risco que mapeamos é o nível de endividamento da empresa, hoje temos um endividamento baixo. Todos esses controles conservam o negócio o preservam. **2) Participa de todos os processos organizacionais;** Ainda não, eu acredito que a gestão de riscos aqui poderia ser mais abrangente, esta focada em alguns fatores chaves, e a gente tem procurado permeá-la em todos os níveis da organização, porém, acho que ainda não contempla todos os processos. **3) Participa da tomada de decisão;** Sim, tem várias questões em gestão de risco, fazemos uma análise para poder tomar a decisão de vender ou não soja, o risco impacta nessa decisão. Na hora de comprar ou não uma fazenda, há preocupação com problema de documentação naquela área, uma área que tem uma região mais sensível ambientalmente, por exemplo, que é perto de um parque, de uma área indígena, nestes casos temos que desistir de comprar para não termos problemas, isso tudo impacta muitas vezes por essas razões e pelo mapeamento dos riscos. **4) Aborda explicitamente a incerteza;** Eu diria que sim, sempre que você tem uma fumaça no ar que possa gerar um problema a gente sempre acaba não avançando por que vai dar problema. **5) Atua de forma Sistemática, estruturada e oportuna;** Acredito que sim, é um processo que está bem organizado assim, bem feito, a gente conhece o nosso negócio, sabe onde é que estão os riscos, e procura sempre investigar o máximo cada ação antes de praticar, para não ocorrer riscos maiores. **6) Baseia-se nas melhores informações possíveis**; Sim, em todo o processo da gestão de risco financeiros, nas compras de fazendas, nas compras ambiental, procuramos buscar as

	melhores assessorias para tomar as decisões. **7) Se adéqua a realidade da organização;** Sim, com certeza, ele esta adequado as atividades. **8) Considera fatores humanos e culturais**; Creio que sim, eu acho que sempre considerou, agora, pensando mais nesta questão de expansão da empresa, e o que a gente precisa de gente para tocar uma nova fazenda, quais são os limitadores, como é que é o perfil das pessoas que a gente esta contratando, eu acho está sim. **9) Atua de forma transparente e inclusiva**; A transparência ainda é um problema para nós, principalmente na questão de riscos. Como é uma atividade que tem muitas questões polemica, você se preserva em alguns aspectos. A primeira vez que você fala para o mercado, por exemplo, que esta abrindo uma área bruta, uma área nativa, e sabendo que tem muitas pessoas, muitos ambientalistas que acham que não temos que abrir nenhuma área a mais, que as áreas nativas têm que ser deixadas para os nativos, isso complica. Mesmo porque se você não abrir, vai faltar comida um pouco mais ali na frente, é uma atividade que neste aspecto, a gente não gosta de falar muito sobre. Também falo de transparência dentro da empresa, eu acho que a gente enfrenta problemas de comunicação aqui, às vezes as coisas que estão acontecendo não são comunicadas em tempo, e de forma assertiva para todos, impacta também neste aspecto, mas estamos buscando melhorar nisto. **10) Atua de forma dinâmica e interativa, capaz de reagir a mudanças;** Eu acho que a gente poderia mudar mais rápido, tem alguns processos e alguns procedimentos que ainda demoram muito para serem alterados, esse é um ponto que ainda poderia melhorar muito. **11) Facilita a melhoria contínua da organização.** Sim, sim eu acho que justamente, a gente vem melhorando, vem aperfeiçoando, mas talvez esse processo poderia ser mais rápido.
6	**BULGURCU, CAVUSOGLU E BENBASAT (2010).** **Como a estrutura para gestão de riscos corporativos é organizada na corporação?** Eu diria que tem alguns riscos que são endereçados pelas áreas, se é uma coisa mais abrangente, que tem um impacto maior, é discutida com a diretoria. **Como os usuários poderiam contribuir de forma mais efetiva para uma maior conscientização ao risco?** Poderiam ser criadas mais regras, mais protocolos, evitando riscos, para não termos ações isoladas baseadas na opinião de cada um. Isso ocorre até na área financeira, nos lançamentos contábeis, quando trocamos uma pessoa, ocorre um lançamento diferente, isso é um item de menor impacto e erros nos processos. Acredito que isto estando bem definido, acaba reduzindo essa possibilidade de erros, estando os usuários desta forma preparados.
6	**AVEN (2011).** **A gestão dos riscos realizada na organização fornece ferramentas adequadas para equilibrar os conflitos inerentes em explorar as oportunidades de um lado, e evitar perdas, acidentes e catástrofes, por outro?** Sim, normalmente sim, já foi feito muita coisa, mais ainda não dá pra considerar que está de todo adequada, faltam alguns processos, a padronização precisa melhorar. Nós poderíamos evitar ainda muita coisa que acontece se tivéssemos um controle melhor, uma padronização melhor dos processos.
7	**Como os seguintes processos são considerados em relação aos processos de negócio organizacionais? ISO 31000(2009)** **1) Comunicação e consulta às partes interessadas (internas e externas)** Alguns processos, algumas áreas fazem isso bem, por exemplo, uma área que é crucial para nós é a segurança (cuida da segurança dos funcionários) nas fazendas, todas as semanas é realizada uma conversa com os operários sobre segurança (neste caso as partes interessadas são os funcionários). É uma conversa sobre como evitar esse tipo de coisa, de criar padrões, isto traz melhorias, nessa área eu acho que está bem, apesar de ainda acontecer, mas eu acho que a gente conseguiu evitar muito acidente com isso. Em algumas outras áreas acredito que falta conversa com os interessados, isso está faltando,

	faz parte da organização, que todo mundo tenha essa prática, falta às áreas se conversarem, por exemplo, a minha área com a área da contabilidade, a contabilidade com a área financeira, falta um pouco de diálogo com os interessados. **2) Estabelecimento do contexto (parâmetros internos e externos que precisam ser levados em consideração):** Na minha percepção sim, como eu não estou muito no dia a dia das outras áreas, até não saberia te dizer assim como é que é a interação da nossa empresa, por exemplo, com os fornecedores, ou com clientes, prestadores de serviços, mas acredito que estas relações são levadas em consideração. **3) Avaliação dos Riscos (identificação, análise e avaliação dos riscos)** Eu acho que de cada área vai fazer a sua parte, vai mapear quais são seus riscos, e uma vez que esses riscos forem identificados, já que podem trazer grandes prejuízos, vai se criar algum protocolo ou manual em que as pessoas vão ser treinadas para aquilo, então acontece dentro de cada área, e cada área cria as suas normas, para evitar o risco. **4) Tratamento dos Riscos:** Como falei no item anterior, as áreas identificam e elas também tratam seus riscos. **5) Monitoramento e análise crítica dos Riscos:** Sim, eu diria que é feito de forma desintegrada, ele é tratado dentro de cada área e cada área se preocupa com aquilo e fica por ali, talvez num dos momentos do diretor presidente, ou o diretor da área vai validar alguma coisa, não é uma coisa que acontece integrada.
8	**ISO 31000 (2009)** **Como a gestão de riscos auxilia aos tomadores de decisão a fazerem escolhas conscientes e priorizar ações?** Eu acho que estabelece as regras, por exemplo, pegando a questão do gestor, a gente tem limites que respeita, temos uma reunião, uma agenda no comitê de riscos, começa com os aspectos do mercado, depois vem para o câmbio, depois os custos, e no final a gente toma as decisões. Criamos um protocolo, uma forma de fazer isso, que marcou todos os elementos que a gente trabalha, temos uma instrução e um manual para seguir, então isso ajuda muito, a gente a,seguir o processo. **Estas decisões consideram a incerteza, a natureza desta incerteza, e como ela pode ser tratada?** Sim, elas consideram os tipos de impactos que podem acontecer. O quanto é volátil, por exemplo, nas empresas e o quanto a gente pode ir avançando para cada semana, cada mês, e nas nossas travas que a gente faz com o *Hedge* cambial.

BLOCO IV – RELAÇÃO ENTRE GESTÃO DOS RISCOS DE TI E GERENCIAMENTO DOS RISCOS CORPORATIVOS

ITGI (2007) **1) Como a TI atua para prevenir riscos inerentes ao negócio?** Bom, das interações que eu observei, eu vejo que as áreas (como sempre ocorre nas empresas) passam a demanda para a TI, e a TI monta alguns relatórios, ajuda a tomar algumas decisões. Ela recebe a demanda de uma área que mapeou o que necessita no que pode ser melhorado. A TI ajuda a elaborar alguns relatórios para alimentar aquela área, e aquela área vai usar aquilo para atuar no seu negócio. **Esta atuação pode ser considerada satisfatória dentro de uma perspectiva de negócio?** O que eu sinto na nossa TI, aqui, é que realmente demoram muito, então é que as coisas chegam até eles, e eles conseguem fazer bem, há uma expressiva demora, eles são muito demorados. Claro que se tivesse mais gente, não posso afirmar, mas é essa a minha percepção. Sim, eles conseguem fazer o que é pedido, mas num prazo demorado.
SPEARS E BARKI (2010). **2) De que maneira os usuários participam do gerenciamento de riscos de segurança nos processos de negócios?** Eu vejo que é uma coisa que acontece no dia a dia, quando tu pedes uma parametrização x, ou um relatório x, eles montam com relação nos software, e aí eles não vêm exatamente como tu querias, ele não esta perfeito, é aí que entram as reuniões com a TI, em que você diz “olha não é bem como eu estava pensando, acho que da para melhorar aqui e ali vai ficar bom” como o usuário da ponta mesmo falou para a chefia, e procurou a TI para ir melhorando.

3) Como a sua participação é percebida e qual é o impacto da participação na segurança do negócio? É, eu acho que tem alguns usuários, por exemplo, que são mais ativos, que conseguem propor mais teorias, outros que simplesmente acabam impondo mais teorias, problemas e que acarretam em mais trabalhos, ou seja, tem que ficar mais tempo trabalhando por causa daquilo, e não fazem muita coisa assim, depende muito de quem é o usuário, acho que há alguns que conseguem propor formas de gerenciar melhor.

IBGC (2009)

4) Como a práticas de governança corporativa orientam o dia a dia do trabalho da organização? A governança é um termo bem amplo, eu diria que talvez a minha área e o ambiente que mais acaba tendo contato e preocupação com essa governança porque a gente tem que fazer a comunicação com todo o mercado, por exemplo, uns conselhos de administração que tem membros independentes não são só os funcionários da companhia controladora têm também dois exemplos fora da companhia, que estão envolvidos no conselho. Já se tem uma prática de governança, porque o conselho é entendido como um representante de todos os acionistas na empresa tem conselheiros que não são partes interessadas diretamente com o negócio, são membros externos, e estão lá para fazer uma crítica em ambos os acionistas. As nossas ações são só subordinadas, quer dizer que tem direito a votos preferenciais, além disso, toda a nossa divulgação é realizada de forma trimestral. A cada três meses alguém reporta para o mercado, o que está acontecendo e eu faço em inglês e português, fora isso a gente está sujeito a todo um documento que é chamado de formulário de referencias, que é um calhamaço de informações sobre a empresa, que a gente atualiza todos os anos, e escreve sobre planos, sobre como é que esta o nosso rendimento da empresa e de custos, então é um livro de transparência bastante elevado que a gente tem para o mercado. Isso é exigido, porque as informações são solicitadas, para um novo mercado lá na bovina, que é o nível mais alto de governança, então no mercado, para todo o pessoal já exige essas coisas. Ele diz "olha tu quer se alistar no mercado tu vai ter que fazer todas essas coisas, esse percentual de coisas independentes, formal na área, as informações em duas línguas", então eu diria que a governança está assim hoje, a gente esta atendendo o que pende no mercado. Eu diria que sobre os riscos em si a única coisa que a gente reporta mais e essa questão do *hedge* a gente indica quanto é que a gente esta travado, com toda a disposição que a gente tem, como a gente esta evoluindo ao longo dos meses, esses riscos financeiros de marketing são os únicos que a gente trata com os acionistas, os outros são mais operacionais, mas não é o que a gente esteja informando ao mercado hoje.

De que forma elas contribuem para a gestão de riscos em TI e gestão dos riscos corporativos? Bom, os riscos corporativos, eu diria que agora, a gente teve um exemplo que foi a nossa assembléia de acionistas, e um acionista que tem 5% pediu a instalação de um modelo fiscal, então a gente vai e instala o que foi solicitado por um minoritário, então não deixa de ser uma inerência dos acionistas terem essa companhia, obedecendo as regras societárias, se eu não me engano a partir de 3% pode pedir a instalação, então de nota fiscal, eu acho que essa inteiração existe. Neste caso eu diria que a área faz o seu papel, porque o acionista traz muita coisa para dentro da empresa também, a gente tem contato com vários acionistas, ou investidores, uma visão mais amplas, porque tem investidores que não são acionistas, e trazem muitas coisas de práticas que a gente pode estar colocando e traz para dentro da empresa, já adotamos algumas coisas que são alertadas por investidores, então é uma troca de informações que vem também dos acionistas. No final acaba tudo passando para a TI, por que todos os dados que a gente contabiliza, e passa para o mercado, vem dos nossos programas, então à medida que da algum problema de TI, que da algum problema de parametrização, algum problema de tabela ou de software vai impactar lá na frente nas nossas transferências para os acionistas, então eu acho que embora não apareça de forma clara, é a TI que esta segurando todos os nossos dados, então eu acho que diria que faz parte, a governança vem também da TI, e é ela que formula os dados para nós, dados diretamente ligados.

JUNIOR, JUNQUEIRA e BERTUCCI, (2010).

5) De que forma a adoção de mecanismos de controle possibilita redução dos riscos corporativos e riscos de TI? Eu acredito que é fundamental, os mecanismos de controles que a gente lutou para criar, acabaram prevenido uma serie de riscos, então a gente cria os mecanismos, cria as regras e protocolo que lá na frente vão evitar muitos desconfortos. Bom eles ocorrem, a gente tem de

fato uma serie de regras, de acesso, de controle das pastas, e enfim, eu vejo o que esta ocorrendo na empresa, e tenho que ter certeza que isso evitou muitos problemas, também acho que é um processo bem importante pra gente proteger nosso dados, e essa questão de controle de acesso, que você mencionou aí, acho que é crucial para as nossas informações.

SPEARS E BARKI (2010).

6) Como os controles internos protegem as informações financeiras? Bom eu acho, que as informações financeiras, como os dados contábeis são algo que eu vejo como a contabilidade cada vez está exigindo mais alguns tipos de relatórios, e tornando as relações mais fáceis de acessar, cada vez mais estamos vendo o trabalho manual de digitação e passando por uma coisa já feita e automática, então acho que isso aí, falta fazer bastante coisa ainda, que eu vejo que ainda a contabilidade acaba trazendo estações, e que não funcionou na planilha que a TI montou, que é pra ocupar vários dados e colocar um extrato, e ai acabaram tendo que fazer a mão, e deu um erro, e acaba que a gente tem uma janela para divulgar, para as pessoas no mercado, e acaba que a gente tem um limite, uma data x lá, às vezes ficamos quase que não batendo com as datas porque tem muito trabalho.

7) Esta proteção é capaz de produzir informações contábeis financeiras confiáveis? Hoje, ainda não, eu creio que ainda tem problema. E o que acontece, é uma auditoria que checa muita coisa, mas ainda assim encontramos alguns probleminhas, coisas que depois que vimos, acabou faltando, foi algo que foi feito errado, e depois tentam arrumar, só que como sai gente, entra gente nova, às vezes conseguimos ensinar, mas não é possível ensinar tudo.

IBGC (2009)

8) De que maneira a atuação do comitê para a gestão de riscos ocorre? Esse comitê esta instaurado há uns 4 anos, e desde então estamos com esse processo mais organizado. Na verdade, a gente sempre teve essa volatilidade de preços e de câmbio, faz parte do negócio, só que antes o processo de decisão, do quanto a gente iria travar o processo em si envolve travas de preços, travas de câmbio e *Hedge*, tanto de queda de preços de *comodities* em dólar, uma venda em dólar, que eu estou travando uma vez, e ai não varia mais, esse é um processo menos organizado. É focada só em análises de risco financeiro, a auditoria fez todo um trabalho no nosso setor, analisaram toda a volatilidade nos preços e como é que isso impacta os nossos resultados, então eles propuseram assim, limites de *Hedge* por trimestres, que a gente poderia ter, por exemplo, a soja, eles acham que no primeiro trimestres a gente tem que travar no máximo 50% e no mínimo 20% da nossa soja, dai vai acarretando no ano essas bandas, e eles nos propuseram bandas, a gente tem que ficar dentro dessas bandas, mais dentro da banda nós precisamos tomar algumas decisões semanais, é então hoje tem um processo bem mais organizado pra gestão dos riscos. O comitê de riscos está na verdade entre o conselho e o diretor presidente, porque o comitê reporta também para o conselho da administração. O comitê de riscos, os membros, o diretor presidente, diretor de profissão, diretor financeiro, o diretor de vendas, o gerente de suprimentos, gerente de custos, gerente financeiro, e o gerente de RI.

9) Como sua atuação contempla a prevenção de riscos de TI e risco corporativos? De fato cada membro do comitê pode eventualmente, pedir alguma coisa para a TI, porque a parte financeira traz muitos dados para o comitê que a gente vai analisar, só que aí ele tem as suas alterações lá com a TI, porque eles pegam um dado que a TI ajuda a produzir, então eu acho que indiretamente ocorre assim, o comitê vai demandar as coisas da TI para produzir informações melhores, atualizadas e mais apuradas, esse tipo de coisa que acontece. Não vai para o comitê, e o comitê de gestão de riscos financeiros, então os outros riscos que não são financeiros, não vão para nenhum comitê, eles são tratados pela área de RH, e a área de RH se for um dos mais baixos vai trazer para o presidente, vai colocar na reunião de segunda feira de tarde, que tem todos os diretores, não é um comitê, é uma reunião de diretoria, não só financeiros.

10) Em sua opinião existe uma aproximação entre os riscos de TI e riscos corporativos? Como isso seria possível? Eu não sei qual controle de acesso, também não sei exatamente quais são as ações, que eu tenho que ter caso um hacker entre para controlar o servidor, não sei exatamente o que é que eles fazem, para fazer isso. Enxergo, por exemplo, vou pegar um exemplo bem provável que faz o funcional site ou a nossa conexão com as fazendas, a gente pode não conseguir fechar o

resultado em tempo, quer dizer, a gente tem uma comunicação hoje com as fazendas, a TI talvez tenha te falado que a gente coloca internet nas fazendas, só que não tem internet nas regiões lá, então a gente pega o ponto mais próximo e vai colocando, multiplicando assim, até chegar à fazenda, em seguida a gente fica fazendo quedas lá, e apesar da gente consegui telefone, eu sei que essa questão de telefone também esta com a TI, celulares, então isso às vezes dá problema mesmo, e tem coisas que são estruturais do país, e que faltam e a gente acaba tendo que fazer e que acabam impactando diretamente, é algo como eu não consigo acessar a internet aqui num dia que eu tenho que subir um arquivo para a CVM, eu vejo isso de varias formas.

APÊNDICE E – QUESTIONÁRIOS RESPONDIDOS

RESPONDENTE: GERENTE DE SISTEMAS

QUESTIONÁRIO

Escolha o nível de maturidade para os processos listados, utilize a linha vazia para explicar ações que que são tomadas pela corporação neste processo.

Processos COBIT		Nível de maturidade					
		0 - Inexistente	1 - Inicial	2 – Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
PO9 - Avalia e gerencia os riscos (COBIT, 2007 p.66)							
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).			**X**				
Explique: - (1 – inicial) No meu ponto de vista, os riscos de TI são avaliados de forma informal e quando solicitados em cada projeto sem haver maiores alinhamentos com a gestão de riscos da empresa.							
PO9.2 Estabelecimento do Contexto de Risco 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 são avaliados.				X			
Explique: - (2 – repetitivo) – Quando definida a necessidade de definição e acompanhamento dos riscos inerentes ao projeto e/ou ações de negócio, existe uma abordagem superficial para identificação dos riscos, ações de mitigação, acompanhamento da efetividade das ações e readequação das ações de acordo com a necessidade e mudanças de cenário.							
PO9.3 Identificação de Eventos 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 jurídicos, 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.				X			
Explique: - (2 – repetitivo) – No meu ponto de vista existe uma abordagem inicial e muitas vezes não muito aprofundada de avaliação de todos os riscos que envolvem as ações de projeto.							
PO9.4 Avaliação de Risco 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.				X			
Explique: - (2 – repetitivo) – Quando definida a necessidade de identificar os riscos, ainda não existe uma regularidade em avaliar a probabilidade e o impacto dos riscos, tampouco análise quanto à efetividade das ações de mitigação.							
PO9.5 Resposta ao Risco 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.		X					
Explique: (0 – Inexistente) – desconheço a existência de um processo de respostas a riscos nesta organização.							

PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco 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 e 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.		X					
Explique: (0 – Inexistente) – Sei da existência de um comitê de risco na organização, mas não conheço as suas ações.							

Você alteraria os critérios de avaliação utilizados? Por quê?
Sim. Entendo que seria importante incluir na avaliação do grau de maturidade das organizações uma forma de poder identificar e avaliar de forma clara os níveis operacionais, táticos e estratégicos da organização. A minha atuação nesta organização está muito voltada para questões táticas e operacionais, o que certamente distorceu de forma significativa o meu ponto de vista e respostas aos questionário.

Qual a importância dos tipos de risco abaixo relacionados nas atividades organização? Para responder esta questão leve em consideração a seguinte tabela do grau de importância dos Riscos

	Extrema	**Muito forte**	**Forte**	**Moderada**	**Igual**
Riscos Econômicos Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.	X				
Qual o significado de sua resposta: - Esta empresa produz commodities , ou seja, quem define os preços é o mercado por isso o controle dos custos é fundamental para viabilizar o negócio. Também é importante ressaltar que trata-se de uma empresa com capital aberto, onde a entrega do que foi prometido e geração de lucros é fundamental para a sua continuidade.					
Riscos Políticos Eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.	X				
Qual o significado de sua resposta: - Esta empresa atua 100% na agricultura a qual está sujeita à legislações ambientais, que são totalmente fomatadas pelos políticos e governos do pais.					
Riscos Ambiental Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.	X				
Qual o significado de sua resposta: - Existe um forte trabalho de conscientização, gestão e controle dos colaboradores e processos através de sistema especializado no assunto para cumprimento de normas legais e aplicação de melhores práticas no que se refere às questões ambientais.					
Riscos de Marca, Imagem ou Reputação É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e,conseqüentemente, a consecução de transações com estes clientes.	X				
Qual o significado de sua resposta: - Por ser uma empresa de capital aberto existe uma grande preocupação com o que é divulgado para o mercado visando com isso preservar a imagem da empresa.					
Riscos Sociais São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças			X		

na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.					
Qual o significado de sua resposta: - É possível observar ações da empresa visando observar as tendências de consumo do mercado de commodities, que em última instância é decorrente do comportamento das famílias, porque produz alimentos (milho e soja) e vestimentas (algodão).					
Riscos Tecnológicos (estratégicos) São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.		X			
Qual o significado de sua resposta: - Existe grandes investimento da empresa em tecnologia aplicada ao campo, desde equipamentos até sistemas para gestão, inclusive a empresa considera a gestão do conhecimento e tecnologia com um dos seus princípios que a diferencia das demais empresas que atuam no mesmo ramo.					
Riscos de Mercado A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).		X			
Qual o significado de sua resposta: - Conheço pouco deste assunto, mas sei que na área financeira da empresa existe um grupo especializado em gerenciar os riscos financeiros aos quais a empresa está exposta.					
Riscos de Crédito É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação		X			
Qual o significado de sua resposta: - Conheço pouco deste assunto, mas sei que na área financeira da empresa existe um grupo especializado em gerenciar os riscos financeiros aos quais a empresa está exposta.					
Riscos de Liquidez Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.		X			
Qual o significado de sua resposta: - Conheço pouco deste assunto, mas sei que na área financeira e contábil da empresa existe um grupo especializado em gerenciar os riscos de liquidez aos quais a empresa poderá ser exposta.					
Riscos de Pessoal Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.		X			
Qual o significado de sua resposta: - Existem ações constantes e mensuradas para eliminar acidentes de trabalhos ou não cumprimento de acordos de trabalho que venham trazer danos às pessoas e a empresa.					
Riscos de Processos Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.		X			
Qual o significado de sua resposta: - Existe um controle de qualidade atuante junto à produção que garante a qualidade do produto que é expedido para o mercado, com isso garantindo que a qualidade do produto contratado seja o entregue.					
Risco de Tecnologia (operacional) Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).		X			
Qual o significado de sua resposta: - Existe um importante direcionamento dos investimentos para aquisições, manutenção e gestão dos ativos para manter equipamentos e sistemas devidamente preparados para suportar a operação da empresa.					

Riscos de complience Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.	X				
Qual o significado de sua resposta: - Existem investimentos, conscientização dos colaboradores e gestão sobre as ações para mitigar riscos de não cumprimento de legislações, regulamentações externas ou normas internas observando todas os cenários nos quais a empresa está envolvida, tais como: ambiental, fiscal, societário, etc.					

Você alteraria os critérios de avaliação utilizados? Por quê?
Não. Acredito que estão adequados às questões que são elencadas.

RESPONDENTE: COORDENADOR DE TI

QUESTIONÁRIO

Escolha o nível de maturidade para os processos listados, utilize a linha vazia para explicar ações que são tomadas pela corporação neste processo.

Processos COBIT		**Nível de maturidade**					
		0 - Inexistente	**1 - Inicial**	**2 – Repetitivo**	**3 - Definido**	**4 - Gerenciado**	**5- Otimizado**
PO9 - Avalia e gerencia os riscos (COBIT, 2007 p.66)							
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).	**1**		X				
Explique: A Gestão de Riscos de TI é feita pela Gestão de TI, enquanto a gestão de riscos da organização é feita pela área de RI (relação com Investidores)							
PO9.2 Estabelecimento do Contexto de Risco 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 são avaliados.	**2**			X			
Explique:							
PO9.3 Identificação de Eventos 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 jurídicos, 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.	**3**				X		
Explique:							
PO9.4 Avaliação de Risco 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.	**3**			X			

Explique:							
PO9.5 Resposta ao Risco 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.	**3**				X		
Explique:							
PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco 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 e 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.	**2**		X				
Explique:							

Você alteraria os critérios de avaliação utilizados? Por quê?
Não.

Qual a importância dos tipos de risco abaixo relacionados nas atividades organização? Para responder esta questão leve em consideração a seguinte tabela do grau de importância dos Riscos

	Extrema	**Muito forte**	**Forte**	**Moderada**	**Igual**
Riscos Econômicos Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.	X				
Qual o significado de sua resposta: A SLC depende de disponibilidade de capital para financiar sua estratégia de crescimento					
Riscos Políticos Eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.		X			
Qual o significado de sua resposta: Restrições governamentais podem impedir a continuidade e expansão do negócio agrícola no Brasil					
Riscos Ambiental Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.	X				
Qual o significado de sua resposta: A legislação ambiental é muito dura no Brasil e todo ônus é do produtor					
Riscos de Marca, Imagem ou Reputação É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e,conseqüentemente, a consecução de transações com estes clientes.		X			
Qual o significado de sua resposta: Falta de qualidade nos produtos podem inviabilizar futuras exportações					
Riscos Sociais São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos			X		

humanos e paralisações da produção.					
Qual o significado de sua resposta: são poucos os profissionais qualificados que aceitam morar longe das metrópoles					
Riscos Tecnológicos (estratégicos) São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.		X			
Qual o significado de sua resposta: A Tecnologia da Informação e Comunicações é fundamental para o desenvolvimento do negócio da SLC					
Riscos de Mercado A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).	X				
Qual o significado de sua resposta: Toda receita é gerada baseado nos preços de commodities, ou seja, nós não definimos o valor dos nossos produtos					
Riscos de Crédito É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação	X				
Qual o significado de sua resposta: Sem crédito, a empresa para de crescer e perde valor no mercado					
Riscos de Liquidez Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.		X			
Qual o significado de sua resposta:					
Riscos de Pessoal Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.	X				
Qual o significado de sua resposta: Se a empresa não cumpre rigorosamente a legislação trabalhista, corre risco de ter multas e seus créditos negados.					
Riscos de Processos Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.		X			
Qual o significado de sua resposta: Qualquer erro no planejamento agrícola, plantio, fertilização ou colheita, podem impactar significativamente nos resultados. Ainda existem os fatores climáticos com variável de perda, caso os processos não sejam rigorosamente monitorados.					
Risco de Tecnologia (operacional) Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).	X				
Qual o significado de sua resposta: Hoje tudo depende de sistema e informações. Um navio que não embarque a carga negociada com o cliente pode gerar multas significativas.					
Riscos de complience Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de	X				

serviços.						

Você alteraria os critérios de avaliação utilizados? Por quê?
Não.

RESPONDENTE: MEMBRO DO COMITÊ DE RISCOS

QUESTIONÁRIO

Escolha o nível de maturidade para os processos listados, utilize a linha vazia para explicar ações que são tomadas pela corporação neste processo.

Processos COBIT	Nível de maturidade					
	0 - Inexistente	1 - Inicial	2 – Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado
PO9 - Avalia e gerencia os riscos (COBIT, 2007 p.66)						
PO9.1 Alinhamento da gestão de riscos de TI e de Negócios Estabelecer uma estrutura de gestão de riscos de TI alinhada com a estrutura de gestão de riscos da organização (corporação).		X				
Explique: Existe um certo alinhamento entre riscos de TI e riscos de negócio, mas não muito formalizado.						
PO9.2 Estabelecimento do Contexto de Risco 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 são avaliados.				X		
Explique: Em termos de risco de negócio, estão bem mapeados pela organização e há ações concretas. para mitigá-los.						
PO9.3 Identificação de Eventos 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 jurídicos, 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.				X		
Explique: Existe uma boa identificação de eventos que possam ameaçar o bom funcionamento do negócio e a natureza e abrangência do impacto são bem mapeadas.						
PO9.4 Avaliação de Risco 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.				X		
Explique: Principalmente os riscos financeiros são mensurados em sua probabilidade e são delineados obedecendo a métodos quantitativos e qualitativos.						
PO9.5 Resposta ao Risco 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.				X		
Explique: Sim, entendo que existem respostas aos riscos e que há um processo para responder a eles.						

PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco 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 e 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.			X				
Explique: Existem atividades de controle (principalmente financeiro), no entanto não em todos os níveis da organização.							

Você alteraria os critérios de avaliação utilizados? Por quê?

Qual a importância dos tipos de risco abaixo relacionados nas atividades organização? Para responder esta questão leve em consideração a seguinte tabela do grau de importância dos Riscos

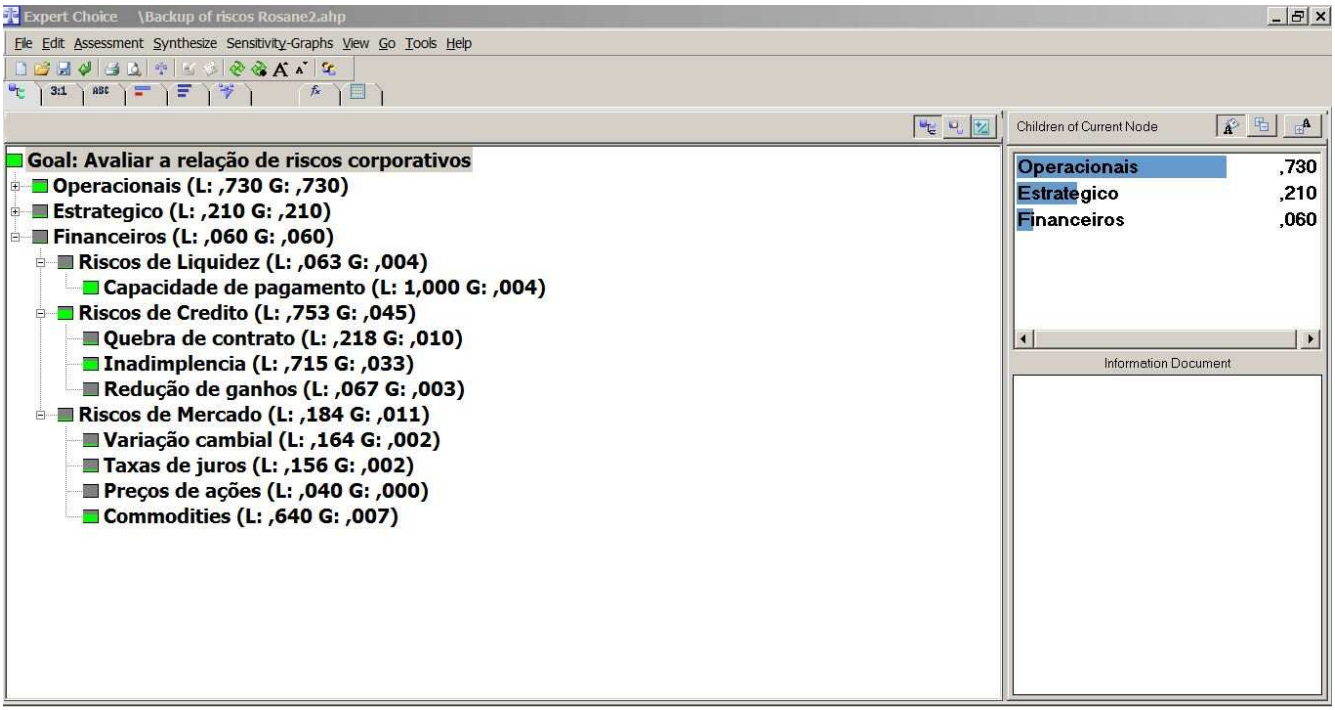
	Extrema	**Muito forte**	**Forte**	**Moderada**	**Igual**
Riscos Econômicos Os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.	X				
Qual o significado de sua resposta: Oscliações de preços (no nosso caso, de commodities e de câmbio) podem causar literalmente a "quebra da empresa", se mal administrados					
Riscos Políticos Eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.			X		
Qual o significado de sua resposta: Riscos regulatórios tem impacto relevante em todos os aspectos do negócios (em termos de alterações em linhas de financiamento – vitais para o negócio – isenções tributárias, leis trabalhistas, etc...)					
Riscos Ambiental Associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos.		X			
Qual o significado de sua resposta: Nossa atividade se desenvolve no próprio meio-ambiente, portanto é muito visada e há significativo risco de questões ambientais (lembrar do novo código florestal, em votação no momento)					
Riscos de Marca, Imagem ou Reputação É decorrente de veiculação de informações que afetam negativamente a imagem da instituição, pondo em risco a manutenção de clientes e,conseqüentemente, a consecução de transações com estes clientes.		X			
Qual o significado de sua resposta: Principalmente em relação a riscos ambientais e trabalhistas, há considerável risco (se não bem mapeados os riscos) de dano à imagem da empresa					
Riscos Sociais São alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.				X	
Qual o significado de sua resposta: Não vejo esse item como de grande risco para a empresa, pois não vemos grandes mudanças nos hábitos e costumes dos ambientes onde estamos inseridos. Se há mudanças, são muito lentas e de pouco impacto para o negócio.					
Riscos Tecnológicos (estratégicos) São novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.			X		

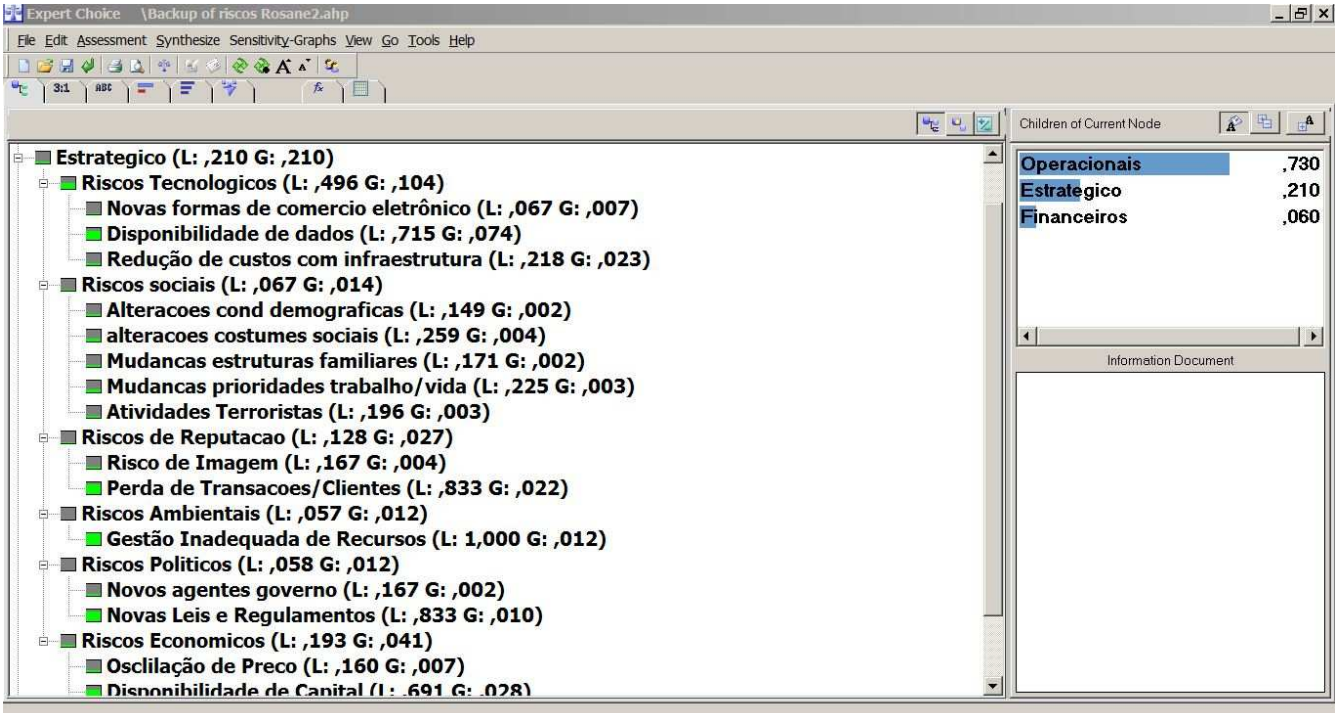
Qual o significado de sua resposta: Há uma série de novas tecnologias disponíveis no setor, mas nesse caso trazem mais benefícios do que prejuízos.					
Riscos de Mercado A possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, inclui os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).	X				
Qual o significado de sua resposta: Sim. Enxergo esse item muito similiar aos "riscos econômicos".					
Riscos de Crédito É definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas nas renegociações e aos custos de recuperação		X			
Qual o significado de sua resposta: A legislação que dá apoio ao sistema de financiamento de crédito agrícola está sempre sujeita a alterações e revisões, o que pode diminuir a disponibilidade de recursos para financiar a atividade.					
Riscos de Liquidez Define-se como risco de liquidez a ocorrência de desequilíbrios entre ativos negociáveis e passivos exigíveis - descasamentos entre pagamentos e recebimentos - que possam afetar a capacidade de pagamento da instituição, levando-se em consideração as diferentes moedas e prazos de liquidação de seus direitos e obrigações.		X			
Qual o significado de sua resposta: Pode haver momento em que queremos vender nossos produtos mas não se acha "comprador" pois o mercado está aguardando possíveis alterações nos preços.					
Riscos de Pessoal Acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.		X			
Qual o significado de sua resposta: Existe o risco, mas não o considero extremo.					
Riscos de Processos Modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.		X			
Qual o significado de sua resposta: Má execução de atividades na lavoura (e até o desrespeito às regras de segurança) podem trazer riscos operacionais e de pessoal, reduzindo a eficiência e consequentemente, o lucro.		**X**			
Risco de Tecnologia (operacional) Representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais).		X			
Qual o significado de sua resposta: Sim, esses mais relacionados à TI, na minha visão (sistema fora do ar, sem internet – isso acontece muito nas fazendas).					
Riscos de compliance Relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços. **Qual o significado de sua resposta**: O que me ocorre nesse item é mais a questão de cumprimento da legislação trabalhistas (PPD´s), pois é difícil achar contingente disponível nessa categoria,		X			

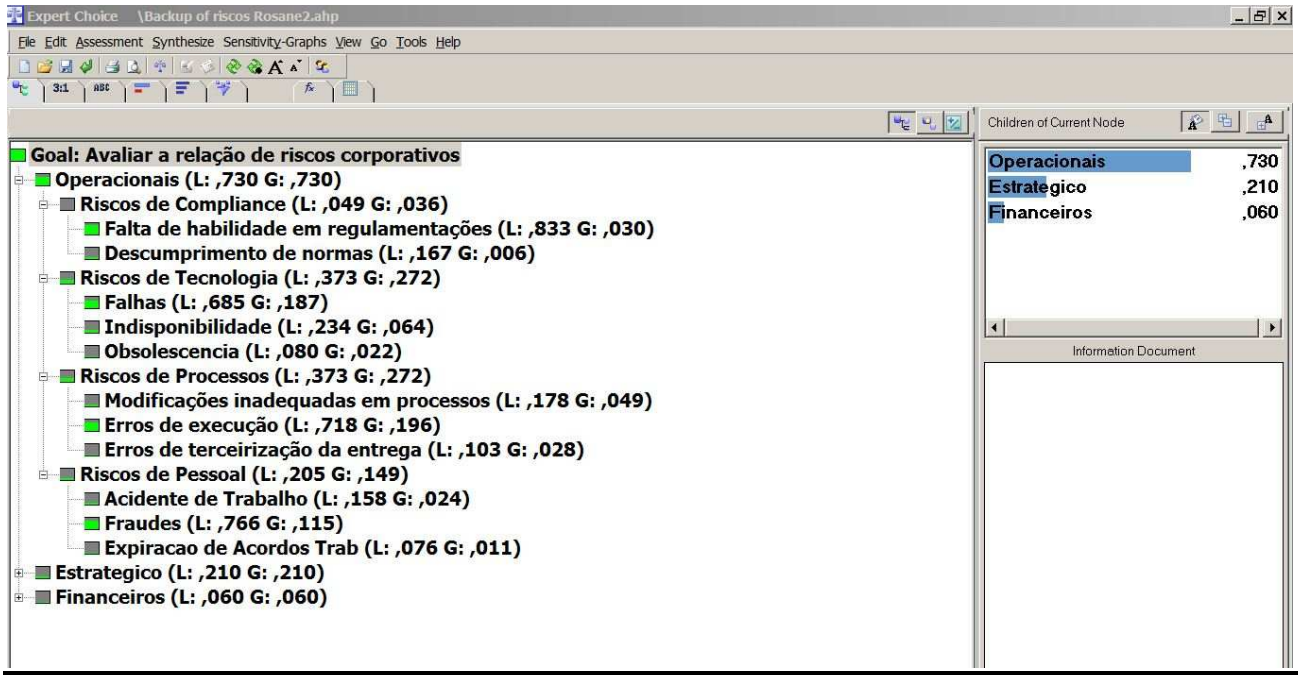
principalmente nas fazendas.					

Você alteraria os critérios de avaliação utilizados? Não. Por quê?

APÊNDICE F –AVALIAÇÃO PAR A PAR RISCOS CORPORATIVOS






Expert Choice \Backup of riscos Rosane2.ahp
File Edit Assessment Synthesize Sensitivity-Graphs View Go Tools Help
Goal: Avaliar a relação de riscos corporativos
Operacionais (L: ,730 G: ,730)
Riscos de Compliance (L: ,049 G: ,036)
Falta de habilidade em regulamentações (L: ,833 G: ,030)
Descumprimento de normas (L: ,167 G: ,006)
Riscos de Tecnologia (L: ,373 G: ,272)
Falhas (L: ,685 G: ,187)
Indisponibilidade (L: ,234 G: ,064)
Obsolescencia (L: ,080 G: ,022)
Riscos de Processos (L: ,373 G: ,272)
Modificações inadequadas em processos (L: ,178 G: ,049)
Erros de execução (L: ,718 G: ,196)
Erros de terceirização da entrega (L: ,103 G: ,028)
Riscos de Pessoal (L: ,205 G: ,149)
Acidente de Trabalho (L: ,158 G: ,024)
Fraudes (L: ,766 G: ,115)
Expiracao de Acordos Trab (L: ,076 G: ,011)
Estrategico (L: ,210 G: ,210)
Financeiros (L: ,060 G: ,060)
Children of Current Node
Operacionais ,730
Estrategico ,210
Financeiros ,060
Information Document