UnilaSalle Editora

DESENVOLVE: Revista de Gestão do Unilasalle (ISSN2316-5537)

http://revistas.unilasalle.edu.br/index.php/desenvolve

Canoas, v. 6, n. 2, 2017

http://dx.doi.org/10.18316/desenv.v6i2.3559

Análise relacional da gestão de risco da tecnologia da informação com a corporativa

Rosane Machado Maciel[1]

Alexandre André Feil[2]

Resumo: A gestão de riscos é um processo inalienável e imprescindível na *práxis* administrativa das corporações. Neste sentido, este estudo objetiva analisar a relação entre a gestão de riscos de TI e de riscos corporativos da empresa Agrícola. A pesquisa tipifica-se como qualitativa e estudo de caso. O procedimento técnico relaciona-se a entrevistas semiestruturadas, questionário fechado e documental secundária. A análise das informações coletadas ocorreu com auxílio do *software*Sphinx Léxica 5.1. Os resultados indicam que a gestão de risco na TI é realizada com ausência de estrutura formal, sem integração e efetiva participação dos colaboradores. Na gestão de riscos corporativos, os esforços são direcionados aos riscos estratégicos e financeiros e há ausência da observação dos princípios recomendados na gestão dos riscos. Conclui-se que há uma relação entre a gestão de riscos de TI e corporativos, mas considerada frágil na empresa Agrícola. Além disso, não existe um processo formal de gerenciamento de riscos de TI, apesar de existirem iniciativas pontuais.

Palavras-Chave: Riscos Corporativos; Governança Corporativa; Gestão Corporativa.

Relational analysis of the risk management of information technology with corporate

Abstract: Risk management is an inalienable and indispensable process in the administrative praxis of corporations. In this sense, this study aims to analyze the relationship between IT and corporate risk management of an agricultural company. This research is typified as qualitative and case study, the technical procedure is related to semi-structured interviews, closed questionnaire, and secondary documentary. The analysis of the information collected was carried out with the help of the Sphinx Léxica 5.1 software. The results indicate that IT risk management is carried out with no formal structure, without integration and effective employee participation. Incorporate risk management, efforts are directed at strategic and financial risks, and there is a lack of observance of the recommended principles in risk management. It is concluded that there is a relationship between IT risk management and corporate risk management, but considered fragile in the agricultural company. In addition, there is no formal IT risk management process, although there are occasional initiatives.

Keywords: Corporate Risks; Corporate Governance; Corporate Management.

1. Introdução

A utilização da internet pelas corporações provocou profundas alterações nos negócios. Esta tecnologia promove rapidez nas operações, com menor custo e tempo de resposta, e fomenta acesso imediato às informações (SMITH; KUMAR, 2004). O relacionamento entre a Tecnologia da Informação

[1] Mestre em Ciências Contábeis pela Universidade do Vale do Rio dos Sinos (UNISINOS). Graduada em Ciências Contábeis pela Universidade Feevale. Professora dos cursos de MBA na Universidade do Vale do Rio dos Sinos (UNISINOS). Endereço postal: Av. Unisinos, 950 - Cristo Rei, São Leopoldo - RS, 93022-750. Email: machado.rosane@gmail.com

[2] Doutor em Qualidade Ambiental pela Universidade Feevale. Mestre em Ambiente e Desenvolvimento pelo Centro Universitário UNIVATES. Especialização em Gestão de negócios pelo Centro Universitário UNIVATES. Graduado em Ciências Contábeis pela pelo Centro Universitário UNIVATES. Atua como docente do curso de Ciencias Contábeis da Univates, editor geral da Revista estudo & Debate e Coordenador Científico do Tecnovates.

(TI) e a internet nutriram inovações nos procedimentos adotados em relação aos processos dos negócios (LUCIANO; TESTA, 2011). Diante disto, as corporações careceram da gestão desta informação – efetiva forma de controle – ante o risco de continuidade das atividades (BARTHELEMY, 2003).

A gestão de TI tipifica a gestão e a utilização da tecnologia na corporação, promovendo mecanismos que permitem o desenvolvimento do planejamento estratégico e planejamento de TI (SIMONSON; JOHNSON; EKSTEDT, 2010). A gestão de TI é essencial na governança corporativa, pois pode incentivar iniciativas estratégicas no *site* corporativo, entretanto as formas de controle destas informações são escassas (HÉROUX; FORTIN, 2013). A governança de TI influencia no desempenho da organização mediante a criação de valor e a gestão do risco do negócio (XUE; LIANG; BOULTON, 2008).

A gestão de risco, por sua vez, é inalienável e imprescindível na administração das corporações (MÜLLER; DRAX, 2014). Sendo assim, as operações corporativas ocorrem contendo graus distintos de riscos, ou seja, de incertezas e ameaças endógenas e exógenas (KANNAN; THANGAVEL, 2008). Além disso, os riscos corporativos podem ser gerenciados e mitigados, mas não excluídos, pois esta exclusão pode prejudicar oportunidades potenciais e a geração de resultados econômicos futuros (GARVAN, 2007).

OCOBIT[3],a ISO 31000, a ISO 27002, o IBGC[4], o COSO[5], entre outros, encorajam um comportamento consistente da corporação, alinhando as diretrizes dos investimentos em TI com a missão, os valores, a cultura e a estratégia (WEILL; ROSS, 2005).

Neste contexto, este estudo objetiva analisar a relação entre a gestão de riscos de TI e de riscos corporativos da empresa Agrícola[6]. A importância desta análise contribui com a ampliação da literatura relacionada aos temas da gestão de riscos de TI e corporativos. Este estudo empírico torna-se relevante frente a estes temas, pois possibilita ajudar no entendimento da forma com que os riscos afetam o ambiente corporativo e a gestão dos riscos a que a corporação está exposta.

2. Referencial Teórico

2.1 Gestão de Riscos Corporativos

Os riscos compreendem os eventos que podem afetar de forma negativa o alcance dos objetivos das organizações na medida em que aumentam a probabilidade de sua ocorrência (BHARAT; KAPIL; SUBHASH, 2012). A mitigação do risco permite uma eficiente governança corporativa, entretanto esta mitigação na área de TI não é utilizada de forma plena e com êxito (ANTHONY JUNIOR; NOR;JOSOH, 2016).

[3] COBIT – Control Objectives for Information and Related Technologies Disponível em: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf

[4] 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.

[5] COSO - Committee of Sponsoring Organizations of the Tread Way Commission. Disponível em: http://www.coso.org

[6] O nome da empresa foi alterado para preservar sua identidade, em nada prejudicando os resultados do presente artigo.

O desafio, com que as organizações se deparam frente ao risco, é de encará-lo com pró-atividade, pois perdem mais tempo e recursos reagindo após os eventos, ao invés de mitigá-los antes de sua ocorrência (MÜLLER; DRAX, 2014). As ferramentas, técnicas, processos e formas metodológicas que podem ser utilizadas na mitigação dos riscos organizacionais centram-se na sua gestão (FADUN, 2013).

A gestão de riscos fornece as ferramentas adequadas para o equilíbrio entre a exploração das oportunidades e a mitigação das perdas, acidentes, entre outros (AVEN, 2011). Gerigk e Corbari (2011) salientam que se trata da identificação dos eventos que podem gerar consequências operacionais, financeiras e estratégicas adversas. Além disso, auxilia na redução de perdas de recursos, de reputação da corporação (Coso, 2007), nas tomadas de decisões conscientes a partir de incertezas e riscos (ISO 31000, 2015). Em suma, Kutsch e Hall (2009) destacam que a gestão de risco possui o propósito de mitigar os eventos negativos e/ou transformá-los em oportunidades, ou seja, em eventos positivos.

Segundo COSO (2007), a finalidade da gestão de riscos centra-se em: a) alinhar o impulso ao risco com a estratégia adotada; b) fortalecer as decisões em resposta aos riscos; c) reduzir as surpresas e prejuízos operacionais; d) identificar e administrar riscos múltiplos e entre empreendimentos; e) aproveitar oportunidades e f) otimizar o capital. A ISO 31000 (2015) estabelece os princípios básicos para uma eficaz gestão de risco: 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.

A implantação de um modelo de gestão de riscos deve ser realizada de forma a gerar benefícios para a corporação (IBGC, 2007). Como, por exemplo, a definição de regras claras da governança, da capacitação de capital intelectual, processos e sistemas, do uso de controles eficazes, das (não) conformidades relativas às obrigações legais, entre outros, um dos modelos utilizados é a ISO 31000(2015).

A Norma ISO 31000(2015) auxilia as organizações na análise e na avaliação dos riscos para terem escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação, levando em consideração a incerteza, a natureza desta incerteza e o seu tratamento (ISO 31000, 2015). Esta norma 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 genéricos 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 deve ser considerada ao longo da vida útil da organização, podendo ser aplicada a qualquer tipo de riscos, independentemente de sua natureza, ou consequência (ISO 31000, 2015).

2.2 Gestão de Riscos em TI

O aumento da utilização da TI pelas corporações contribuiu com a importância atribuída à segurança

das informações, entretanto ainda continuam suscetíveis de riscos (YUE et al., 2007). Yue et al. (2007) salientam que as corporações devem compreender os riscos de segurança desta informação antes de tomar decisões de mitigação e proteção. Os requisitos básicos à segurança da informação vinculam-se ao caráter de: i) confiabilidade: as informações devem ser protegidas conforme o grau de sigilo do conteúdo, limitando o acesso e o uso; ii) integridade: as informações devem ser íntegras, ou seja, sem adulteração; iii) disponibilidade: a informação gerada deve estar disponível no momento de sua demanda. (ITGI, 2009).

A gestão da TI é um processo de alinhamento da TI com as ações, desempenho, metas e as atribuições de responsabilidade, para atingir os objetivos mútuos (WEILL; ROSS, 2005). Esta gestão é parte integrante da governança corporativa que assegura a expansão das estratégias por meio da *práxis* da TI (ITGI, 2009) e visa a garantir a integração entre os negócios e TI (GRENBERGEN; HAES, 2005).

Os riscos de TI são difíceis de serem quantificados e, além disso, ocorrem por meio de causas diversas que necessitam de abordagens distintas de gerenciamento e mitigação (HUGHES, 2006). Além disso, os riscos de TI devem ser identificados, mensurados e gerenciados, considerando-se uma visão global de todas as áreas e os riscos da corporação, e esta abordagem de gerenciar e equilibrar o risco é denominada de gestão de riscos de TI (HUGHES, 2006).

Os modelos de gestão de risco de TI auxiliam na gestão eficiente de seus recursos, por exemplo, o COBIT[7](ITGI, 2009) e a ISO 27002. O COBIT centra-se nas ferramentas para alcançar um eficiente controle e gestão de TI. A implementação do COBIT pode proporcionar os seguintes benefícios (ITGI, 2009): a) melhor alinhamento com base no negócio; b) compreensão clara da estrutura operacional e funcional da TI; c) clareza na divisão das responsabilidades com base na orientação para processos; d) desburocratização por terceiros e órgãos reguladores; e) comunicação simples e clara para compreensão por parte dos *stakeholders* e f) abrange e cumpre os requisitos do COSO no âmbito da TI.

Para execução da avaliação e gerenciamento dos riscos de TI, objetivos de controle foram detalhados no P09 do COBIT, sendo eles: o alinhamento da gestão de riscos de TI e de Negócios; o estabelecimento do contexto de risco; a identificação de eventos; a avaliação de risco; a resposta ao risco e a manutenção e o monitoramento do plano de ação de Risco.

2.3 A gestão de Riscos em TI *versus* Gestão dos Riscos Corporativos

A TI como geradora de serviços e informações está continuamente envolvida nos processos corporativos. Destaca-se que sua forma de execução pode se diversificar, em função da complexidade, a partir do suporte à habilitação, até a contribuição na remodelação dos processos de negócio (WEILL; ROSS, 2005). Esta interação entre as perspectivas de negócios e os riscos relacionados a sistemas ou infraestrutura de TI vislumbra mutuamente a proteção da companhia dos riscos corporativos, principalmente aqueles dos tipos estratégico, tecnológico e operacional de tecnologia (SANTANA; VERAS, 2011).

[7] COBIT - Control Objectives for Information and Related Technologies Disponívelem: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf

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 (2015) e o COBIT, comparados no quadro 1.

Quadro 1: Comparação entre a ISO 31000 e o COBIT

ETAPA	ISO 31000 (Riscos Corporativos)	COBIT (Riscos de TI)
Princípios	Estabelece 11 princípios para a gestão de riscos eficaz em todos os níveis.	Não deixa claros os princípios para a gestão de riscos.
Estabelecimento do contexto	Estabelecimento do contexto em externo e interno e seus fatores. A norma apresenta os fatores.	A definição do contexto interno e externo e os critérios de avaliação.
Comunicação e Consulta	Trata a comunicação e a consulta às partes interessadas (internas e externas), em todas as fases da gestão de riscos.	Não trata especificamente deste ponto.
Identificação dos eventos	Identifica eventos, fontes de riscos, áreas de impacto, causas e consequências potenciais.	Identifica eventos e potencial impacto nos objetivos ou operações. Determina a natureza do impacto, registra e mantém um histórico dos riscos relevantes.
Análise do risco	Desenvolve a compreensão dos riscos para posterior avaliação e tratamento do risco.	Etapa de identificação dos riscos.
Avaliação do Risco	Auxilia a tomada de decisão com base nos resultados na análise de riscos, identificando seu tratamento e prioridades.	Avaliação regular da probabilidade e impacto dos riscos, com métodos quali-quantitativos, de forma individual, por categoria e por portfólio da organização.
Resposta ou Tratamento ao Risco	Nesta, é estabelecido o processo e as opções que modificarão os riscos. Após implementado o tratamento, são fornecidos novos controles ou modificados os existentes.	Desenvolve e mantém a resposta aos riscos, assegurando controles com adequada relação custo-benefício e mitigação contínua.
Manutenção e Monitoramento do Plano de Ação de Risco	Indica a análise crítica dos riscos, sendo estes vigiados regularmente, mediante ações pré-definidas no escopo da gestão de riscos.	Prioriza e planeja as atividades de controle global para implementar as respostas aos riscos, incluindo a identificação de custos, benefícios e responsabilidade pela execução.

Fonte: Adaptado pelo autor de ISO 31000(2015) e COBIT (ITGI,2009).

A análise das informações do quadro 1 demonstra que os dois modelos possuem uma estrutura similar, apesar de a Norma ISO 31000 (2015) estabelecer princípios para a gestão de riscos corporativos. O processo de comunicação e a consulta às partes interessadas não foram abrangidos na estrutura para a gestão de riscos de TI proposta pelo COBIT. Além disso, percebe-se que o COBIT é um modelo focado na gestão e no monitoramento dos riscos de TI, enquanto a ISO 31000 visa a 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, reforça-se que as normas não são excludentes, mas complementares.

A gestão da TI possui relação com os riscos operacionais da corporação (Prado; Souza, 2014), estes riscos estão sumarizados no quadro 2.

Quadro 2: Relação entre riscos corporativos e riscos de TI

Tipo de Evento	Riscos Corporativos	Riscos de TI
Fraudes internas	Omissão intencional de posições, roubo por empregados e negociadores entrantes em uma conta própria do empregado.	Segurança da informação, ISO 27001.
Fraudes externas	Roubo, falsificação, cheque sem fundo, dado decorrente de fraude de computador.	Ataques digitais (internos e externos).
Práticas empregatícias e segurança no ambiente de trabalho	Reclamações trabalhistas, questões de saúde laboral e regras de segurança, atividades de trabalho organizadas, reclamações por discriminação e obrigações gerais.	Teletrabalho, legislações específicas para centros de serviço.
Clientes, produtos e práticas de negócio	Brechas fiduciárias, uso indevido de informações confidenciais de cliente, atividades de negociação impróprias nas contas dos bancos, lavagem de dinheiro e venda de produtos não autorizados.	Manipulação indevida de dados, erro de processamento, ações intencionais.
Danos a ativos físicos	Terrorismo, vandalismo, terremotos, incêndios e enchentes.	Ataques digitais e falta de plano de contingência.
Interrupção dos negócios e falhas de sistemas	Falhas de hardware e de software, problemas de telecomunicações, interrupção no fornecimento de energia.	Gerenciamento da continuidade de serviços de TI.
Execução, entrega e gestão de processos	Erros na entrada de dados, falhas na gestão de colaterais, documentação legal incompleta, acesso não consentido a conta de clientes, desempenho indevido da contraparte não cliente, disputa de fabricantes.	Falta de automatização de processos, uso de fontes de informação inadequada.

Fonte: Prado e Souza (2014, p. 54).

Na análise do quadro 2, percebe-se que a relação entre os riscos Corporativos e de TI está mais ligada a aspectos operacionais das organizações. Os tipos de riscos operacionais mais comuns são de pessoal, de processos, de tecnologia e de *compliance,* todos estes geralmente acarretam na redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo, além da potencial geração de passivos contratuais, regulatórios e ambientais (IBGC, 2007).

3. Procedimentos Metodológicos

3.1 Classificação da Pesquisa

A tipificação desta pesquisa é qualitativa, pois é caracterizada pela descrição, considera a relação entre o mundo real e o sujeito, realizando análises não possíveis de serem quantificadas (GIL, 2009). O procedimento técnico adotado é o estudo de caso, que envolve a utilização de um ou mais casos em profundidade para criar construções teóricas, proposições ou teorias (EISENHARDT; GRAEBNER, 2007).

A coleta foi realizada com aplicação de entrevistas semiestruturadas, questionário fechado e documentos. A entrevista semiestruturada foi realizada com o uso de um roteiro pré-estabelecido para obtenção de informações dos entrevistados, já o questionário fechado contemplou uma série ordenada de perguntas objetivas e instruções, com vistas a esclarecer sua aplicação e facilitar o preenchimento.

Como fonte secundária, foi realizada uma pesquisa documental que buscou evidências que pudessem ser cruzadas com as respostas obtidas nas entrevistas e no questionário (GIL, 2009; SILVA; MENEZES, 2005). Os documentos utilizados na pesquisa foram aqueles disponibilizados no portal do investidor da empresa (relatórios trimestrais, demonstrações financeiras, comunicados e documentos entregues à Comissão de Valores Mobiliários - CVM). Dentre os documentos selecionados, destaca-se a apresentação para o Investidor, o Código de Ética e Conduta da Agrícola, as Demonstrações Financeiras de 2011 a 2014 e o guia dos Fatores de Risco.

3.2 Unidade de Análise

A empresa-objeto deste estudo foi a empresa Agrícola - ramo de *commodities* agrícola - fundada em 1977, que possui sede administrativa no Rio Grande do Sul e unidades produtivas em seis estados brasileiros. No ano safra 2014-15, possuía 370 mil hectares plantados principalmente com culturas de soja, milho e algodão. A receita líquida da companhia, em 2015, foi de R$ 1,8 bilhões de reais, e o quadro funcional era de aproximadamente 2.260 empregos fixos, podendo ser classificada como empresa de grande porte (BNDES, 2017).

Esta empresa possui no departamento de TI aproximadamente 60 funcionários, e sua gestão era realizada pelo gerente corporativo de TI que possuía a responsabilidades de gerenciar a estrutura de TI (sistemas e infraestrutura) da corporação. Além desse, também havia o Comitê de gestão de riscos, que era constituído pelo Presidente, um Conselheiro, três Diretores e quatro Gerentes. Diante deste cenário, são três os membros que participaram das entrevistas, em função de seu sólido conhecimento na área foco do estudo, a saber, o Gerente Corporativo de TI, o Coordenador de sistemas e o Diretor de Relações com o Investidor (Membro do Comitê de riscos).

Os critérios utilizados para escolha do caso de estudo foram: a) possuir setor de TI e comitês ou setores de gestão de riscos; b) interesse e disponibilidade na participação desta pesquisa e abertura e fornecimento das informações e c) situar-se no RS.

3.3 Coleta dos Dados

A coleta dos dados ocorreu por meio da pesquisa documental, das entrevistas e da aplicação de questionário fechado. A pesquisa documental ocorreu pela coleta de relatórios trimestrais, demonstrações financeiras e comunicados disponibilizados no *site* corporativo da Agrícola, acessando a aba Relações com Investidores. Os relatórios coletados da Agrícola compreendem: a) a apresentação para o investidor; b) Código de Ética e Conduta; c) Demonstrações Financeiras 2015 e d) Fatores de Risco.

A seleção dos participantes considerou a atuação relacionada à gestão de riscos da Unidade de Estudo. A utilização dos dados ocorreu mediante uma solicitação formal à diretoria da Agrícola por meio

de oficio e, após sua aprovação, iniciou-se este estudo. As entrevistas também foram autorizadas pelo entrevistado, por meio de declaração de ciência da gravação das entrevistas.

As entrevistas foram realizadas por meio de um agendamento prévio via correio eletrônico (*e-mail*), explicando os objetivos e roteiro (dividido em blocos). As entrevistas foram gravadas em arquivo digital e transcritas; após, os entrevistados receberam por *e-mail* suas respostas, que foram validadas, sendo possível desta maneira a correção de erros oriundos do processo de transcrição. As entrevistas ocorreram no período de janeiro a fevereiro de 2016. A caracterização dos entrevistados foi detalhada no quadro 3.

Quadro 3: Principais características dos participantes das entrevistas

	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 Empresas, 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 em 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 pelos autores.

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; em relação à faixa etária, este participante é o de menor idade, 30 anos.

O questionário foi dividido em duas partes. Na primeira, foi sinalizado um dos cinco níveis de maturidade (0 - Inexistente; 1 - inicial; 2 - repetitivo; 3 - definido; 4 - gerenciado e 5 – otimizado) com cada um dos seis processos do PO nº9 do COBIT, sendo eles: alinhamento da gestão de riscos de TI e de negócios; estabelecimento do contexto de risco; identificação de eventos; avaliação de risco; resposta ao risco e manutenção e monitoramento do plano de ação de risco (ITGI, 2009).

Na segunda parte do questionário, foi atribuído o grau de importância a cada um dos tipos de riscos corporativos nas atividades da organização, teve como base Saaty (1991) (Igual, Moderado, Forte, Muito Forte, Extrema), relacionando-se aos riscos: a) estratégicos: econômicos, políticos, ambientais, de marca, imagem ou reputação, sociais, tecnológicos; b) financeiro: de mercado, de crédito ou de liquidez e c) operacionais: de pessoal, de processos, de tecnologia e de *compliance*.

3.4 Tratamento, Análise dos Dados e Limitações do Método

As informações coletadas nas entrevistas foram tratadas a partir do *software Sphinx* Léxica 5.1. Por meio 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. As combinações da análise de conteúdo e da análise léxica permitiram que os dados das entrevistas fossem analisados de forma ampla e organizada (FREITAS, 2011). Após a conclusão da análise de conteúdo, procedeu-se à análise léxica das palavras mais frequentes na fala dos entrevistados.

As informações derivadas dos questionários foram tabuladas com o auxílio de planilhas eletrônicas, o que permitiu o agrupamento dos níveis de maturidade e graus de importância, escolhidos pelos respondentes; após, realizou-se sua análise. Para documental secundária, realizou-se a leitura, seleção e organização das informações subjetivas e objetivas dos documentos, buscando complementar os achados das entrevistas e questionários.

As limitações do método relacionam-se à utilização de entrevistas, em especial, ao agendamento dos entrevistados para atendimento dos pesquisadores, o que de certa forma pôde 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.

4. Resultados e Discussões

4.1 Resultados da Análise da Gestão de Riscos em TI

Os principais aspectos encontrados sobre a gestão de riscos em TI foram categorizados em cinco grupos, por meio da análise léxica (Quadro 4).

Quadro 4: Síntese da avaliação da gestão de riscos em TI

Categorias	Léxicos mais frequentes	Análise resumida (Categorias *versus* léxicos)
Planejamento estratégico de TI e Requisitos de negócio	Investimentos, usuários, procedimentos, ERP, estratégia, companhia, mercado, negócio, confiabilidade, disponibilidade, custo, investido, informação, companhia e acesso	Foram identificadas ações para sistema ERP, controle de acesso, sistemas e *links* e auditoria externa da TI. Essas podem proporcionar a manutenção dos requisitos, gerando redução tempo e custos com falhas e erros, melhorando assim a confiabilidade das informações. O envolvimento de todos os colaboradores de TI no planejamento estratégico ainda é fator a ser trabalhado na organização.
Infraestrutura e uso da TI, segurança das informações	Falha, negócio, identificação, pessoa, operação, dados, agricultura, fazenda, integração,sistema, informação, acessa, procedimento, contratação e gerenciamento	Constataram-se investimentos em ERP (melhorias), Sistemas, links, conectividade, que visam a proteger a empresa de riscos com vazamento de informações confidenciais, fraudes, invasão de externos aos sistemas, instabilidade. E planos de ações para mitigá-los, dentre eles: controle de acessos externos aos sistemas, restrição ao uso do e-mail, controle de arquivos, políticas de acesso, treinamentos. A participação dos usuários foi percebida na etapa de validação de investimentos e homologação de solicitações a TI, contudo não foi localizada na elaboração de processos e planos, ou soluções para remediação de riscos de TI.
Boas Práticas para Gestão de Riscos em TI	Procedimento, acessa, funcionário, contratação, sistema e informação	Os procedimentos de TI contemplam em alguns casos a participação dos usuários, relacionados principalmente 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 controle efetivo dos riscos.
Processos para controle de Risco	Procedimento, fazenda, identificação, pessoa (usuários) e gerentes	Não foi localizado processo organizado para controle dos riscos de TI, contudo percebeu-se forte preocupação com o processo de identificação dos eventos. Riscos-chave de TI são identificadas, mas sem procedimentos padronizados. Evidenciou-se falta de prática regular para avaliações de probabilidade e impacto dos riscos, bem como análise quanto à efetividade das ações de mitigação.
Monitoramento da gestão de TI	Acionista, estrutura, companhia, acessa e informação	A existência de processos para a manutenção e o monitoramento dos planos de TI não foi percebida. A aprovação, o controle e os monitoramentos de planos, bem como o reporte de desvios não são repassados à alta direção, o que resulta na falta de integração entre a gestão de riscos de TI (ambiente de TI) e a atuação no Comitê de riscos (ambiente corporativo). A participação dos usuários carece de um maior envolvimento na gestão e no monitoramento dos controles, gerando maior consciência ao risco.

Fonte: Elaborado pelos Autores.

A categoria planejamento estratégico da TI revela uma relação entre os léxicos, tais como segurança, investido, usuários, procedimentos, ERP, estratégia, companhia e mercado; e um distanciamento entre a estratégia e usuários. Este resultado sugere a necessidade de um envolvimento mais integrado de todos no entendimento das estratégias de negócio, de TI e participação dos usuários. Este distanciamento da

participação dos usuários pode comprometer a segurança das informações, corroborado por Spears e Barki (2010).

Nos requisitos de negócio, a confiabilidade está relacionada com o léxico negócio, indicando sua obtenção mediante melhoria nos processos de negócio; além desta, o léxico disponibilidade esteve de forma frequente na fala dos entrevistados. Os requisitos integridade, conformidade e confidencialidade não apresentam relação com os demais requisitos. Sendo assim, este resultado sugere uma fragilidade na questão da segurança da informação, pois, segundo Beal (2005), a confidencialidade e a integridade são essenciais no processo de proteção das informações.

Os investimentos em TI foram suficientes para os atuantes na área, já o membro do Comitê de riscos elencou necessidades em infraestrutura e comunicação (internet e conexões). A análise fatorial desta categoria apresenta aproximação entre os léxicos falha, negócio e identificação, sinalizando a necessidade de investimentos em processos de negócio para a identificação de falhas. A validação dos usuários nos recursos a serem investidos foi citada na formalização da necessidade e avaliação do investimento (depois de realizado). O investimento em sistema integrado foi percebido na análise documental das demonstrações financeiras de 2015 da companhia, destacando-se como uma conquista naquele ano. Sendo assim, a ausência de investimentos para redução de erros ou falhas pode acarretar problemas no próprio sistema operacional ou nos controles internos, conforme alertado por Cohan (2005) e Lucht, Hoppen e Maçada (2007).

Sobre o uso da TI (entrega e suporte), foram percebidas vantagens quanto à facilidade de integração e disponibilização de informações, rapidez nos fechamentos, agilidade nos controles internos e desvantagens em relação ao custo com treinamentos, volume de informações abastecidas nos sistemas e custo elevado com novas tecnologias. Percebem-se nas vantagens as oportunidades no aproveitamento dos benefícios oferecidos pelo uso da TI; neste sentido, a TI auxilia os negócios, enfatiza Albertin e Albertin (2012).

Constatou-se a participação dos usuários na adoção dos planos de segurança. Contudo, para haver uma disseminação de práticas que proporcionem melhorias nos processos para controle do risco (estabelecimento do contexto, identificação, avaliação, resposta, manutenção e monitoramento), esta necessita ser efetiva, principalmente, para usuários das fazendas (unidades produtivas), recomendado por Bulgurcu, Cavusoglu e Benbasat (2010). Esta reflexão também é defendida por Spears e Barki (2010), que recomendam a gestão em segurança da informação com ênfase nas pessoas.

A maturidade dos processos para a gestão de riscos de TI indica abordagem superficial (nível 0) ao contexto do risco. A maturidade da identificação dos eventos, a avaliação do Risco e a resposta ao risco é nível 3, indicando que os riscos que podem ser identificados, mas o uso de procedimentos padronizados não ocorre. Não foi localizada a existência de prática regular de avaliações de probabilidade e o impacto dos riscos, tampouco análise quanto à efetividade das ações de mitigação.

A manutenção e o monitoramento do plano de ação de risco geraram divergência de opiniões que permearam entre os níveis 0 e 2 de maturidade. Nesta etapa, os léxicos acionista, estrutura, companhia,

acesso e informação apresentaram maior aproximação. O Coordenador de Sistemas desconhece a existência de processos para a manutenção e monitoramento de riscos; já o Membro do Comitê de Riscos entende que as atividades de controle não são observadas em todos os níveis da organização.

O alinhamento da gestão de riscos de TI ao negócio foi identificado segundo respostas de todos os entrevistados como nível 1. A gestão de riscos em TI é realizada pela própria TI, de forma desestruturada e sem conexão com a gestão de riscos da organização, ou seja, não é integrada com a estrutura corporativa para gerenciamento de riscos. Sendo assim, esse fato pode dificultar a manutenção dos requisitos de negócio. Há a percepção de que a maturidade dos processos na gestão do risco é considerada repetitiva (nível 2,0), isso significa que não há treinamento ou comunicação formal de procedimentos padronizados, e a responsabilidade é de cada indivíduo; sendo assim, o ambiente é passível de erros e do uso ineficiente de recursos (ITGI, 2009).

A análise documental, quanto à gestão de riscos corporativos, revela fatores de riscos relevantes que foram agrupados em três aspectos. A) Riscos do setor Agrícola: Variações climáticas, dependência do comércio internacional; flutuação dos preços em relação ao dólar; pragas ou doenças prejudiciais às colheitas; concentração de clientes; deficiência de logística, armazenamento e de processamento no Brasil; atividade sazonal; ampla regulamentação ambiental. B) Riscos Relacionados ao Brasil: A conjuntura econômica e a política, inflação e suas medidas governamentais; a taxas de juros no preço do mercado de ações; acontecimentos e percepção de riscos em outros países, em especial, em países emergentes. C) Riscos Relacionados às ações da companhia: Um mercado ativo e líquido para as ações da Agrícola pode não se desenvolver; uma significativa negociação de ações pode afetar o valor das ações ordinárias; o não pagamento de dividendos; o fato de os interesses dos controladores da Agrícola serem diferentes dos demais acionistas; o estatuto social pode dificultar operações de interesse dos investidores.

Na avaliação dos níveis de importância (aplicação dos questionários) dos riscos estratégicos, o risco social apresentou menor importância, já os riscos econômicos e ambientais foram citados como de extrema importância, confirmando os achados para estes eventos na análise documental. O risco político teve destaque nos relatórios, mas não teve sua importância identificada como extrema pelos entrevistados. Nos riscos financeiros, os riscos de crédito e liquidez foram avaliados com importância muito forte, já o de mercado como extremo.

As análises quanto à gestão dos riscos de TI indicaram que a companhia adota ações para mitigação destes riscos, como planos de segurança, auditoria externa e investimentos em estrutura. Apesar disso, essas ações foram vistas como isoladas, dentro do próprio ambiente de TI, e sem efetiva participação dos usuários. Não foi percebida uma estrutura formal para controle e monitoramento dos riscos, sendo a estrutura existente organizada apenas para identificação dos eventos; sendo assim, estes resultados não condizem com as sugestões da ISO 31000 (2015) e da COBIT (ITGI, 2009). Salienta-se 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 (2015). Na próxima seção, a análise da gestão dos riscos corporativos será realizada.

4.2 Resultados da Análise da Gestão de Riscos Corporativos

Os fatores analisados sobre a gestão de riscos corporativos foram resumidos no quadro 5. A análise da categoria avaliação estratégica dos riscos revelou não ser integrada com todos os riscos corporativos, ocasionando uma fragilidade na segurança da informação. Portanto, Frigo e Anderson (2011) apontam que a avaliação estratégica do risco pode alavancar a melhoria da governança, bem como as relações com o mercado, evitando perdas (prejuízos graves associados), otimizando oportunidades e proporcionando melhores negócios e, por consequência, melhores resultados.

Quadro 5: Síntese da avaliação da gestão de riscos corporativos

Categorias	Léxicos mais frequentes	Análise resumida (Categorias *versus* léxicos)
Avaliação estratégica do risco	TI, financeira, informação, mercado e contábeis, reunião, comitê e estratégia.	A avaliação estratégica do risco ocorre mediante atuação no comitê de riscos (riscos estratégicos e financeiros) e avaliação nas diferentes áreas (riscos operacionais). Não foi constatada a avaliação estratégica integrada de todos os tipos de riscos corporativos.
Perda de Recurso e seus Danos	Negócio, investido, conselheiros, proteção e oportunidade.	Foi identificada a perda de recursos em função do desflorestamento (relacionado ao não gerenciamento do risco ambiental) e do risco de mercado, possíveis perdas com o preço das mercadorias (commodities).
Identificação dos eventos ecategorização dos riscos	Negócio, regra, procedimento, custo, risco, fazenda e comitê.	A identificação dos riscos operacionais é realizada dentro dos departamentos que podem gerar tais eventos; já os riscos estratégicos e financeiros são tratados mediante avaliações do comitê de riscos. Ambos traçam planos para minimizar os impactos decorrentes dos eventos.
Inter-relação entre os tipos de riscos	Procedimentos, negócio (remete a processos de negócio), risco e funcionário (usuários).	Não foram identificadas análises de inter-relação entre a gestão dos diversos tipos de riscos. O estabelecimento destes procedimentos mediante a participação dos usuários auxiliaria na mitigação dos eventos.
Princípios para a gestão de riscos corporativos	Gerenciamento, companhia, negócio (que remete a processos de negócio).	A Participação de todos os processos organizacionais e a atuação de forma transparente e inclusiva, dinâmica e interativa foram detectadas como princípios não atendidos pela organização. Destacam-se como fator limitador deste atendimento problemas de comunicação interna.
Estrutura para gerenciamento dos riscos (concepção, implementação, monitoramento e melhoria contínua) mandado e comprometimento	Gerenciamento, acionista, impacta, evitado, procedimentos, íntegra e risco	No caso de estudo não foi reconhecida uma estrutura formal para gerenciar riscos, contudo a gestão de alguns tipos de eventos ocorre de forma desintegrada, cuja melhoria é obtida pela auditoria independente, responsável pela melhoria dos processos organizacionais.

Fonte: Elaborado pelos Autores.

Na categoria identificação dos eventos, a relação léxica entre o negócio, regra, procedimento, custo e risco, quando comparada com os resultados das entrevistas, confirma a existência de procedimentos

para identificação de riscos, porém não inter-relacionada. Este resultado também é confirmado pelo distanciamento léxico entre o comitê de riscos e estratégias e a fazenda. A falta de inter-relação entre a gestão dos diversos tipos de riscos se opõe 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.

Os princípios não atendidos pela gestão de riscos corporativos, revelados pelas entrevistas, relacionam-se a: (i) participação de todos os processos organizacionais; (ii) atuação de forma transparente e inclusiva e (iii) atuação de forma dinâmica e interativa. 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.

A estrutura para o gerenciamento dos riscos corporativos está melhor organizada para identificação de riscos estratégicos e financeiros, do que para os riscos operacionais, sendo os dois primeiros tratados de forma mais abrangente, em reuniões semanais no comitê de riscos. Já os operacionais são tratados dentro dos setores, nos quais cada um se preocupa com os riscos gerados no seu ambiente. A melhoria deste processo é obtida pela auditoria independente que audita as informações contábeis e alguns processos dos setores.

Destaca-se a não identificação de componentes que vislumbrem um processo de melhoria contínua na avaliação dos riscos corporativos, principalmente no que diz respeito a aspectos operacionais. Para estes tipos, ações formais de avaliação, tratamento e monitoramento não foram identificados, a melhoria desta estrutura permitiria consciência e resposta ao risco, principalmente do tipo operacional, reduzindo impactos negativos. Neste sentido, comparando-se com a ISO 31000 (2009), percebe-se que cada organização pode adaptar os componentes da estrutura às suas necessidades, apesar de informalmente.

A análise dos riscos operacionais, em especial, com pessoal, processos e tecnologia, revela-se como muito forte, enquanto o risco de *compliance* foi selecionado como extremo, corroborando a preocupação dos entrevistados quanto à regulamentação ambiental.

Na avaliação da gestão de riscos corporativos, foi percebida uma estrutura desintegrada entre os diferentes tipos de riscos. A atuação do comitê de riscos está direcionada aos tipos estratégicos e financeiros, que possuem melhor estrutura de gerenciamento do que os do tipo operacionais. Problemas como comunicação interna, ampla participação, falta de ações formais de gerenciamento dos riscos resultam na falta de atendimento a alguns princípios recomendados para a gestão de riscos corporativos.

4.3 Resultados da Análise da Relação da Gestão de Riscos da TI e Corporativos

Os principais resultados da relação entre os riscos em TI e corporativos foram agrupados em categorias (Quadro 6). A atuação da TI frente aos negócios ocorre mediante melhorias nos processos

organizacionais, principalmente nas integrações das informações. As definições das perspectivas de negócio são complementares em relação aos controles das demais áreas para facilitar e direcionar estes controles. A relação entre a necessidade de informações e controles relativos ao risco com a governança corporativa, com base na análise documental (Código de conduta da companhia), ocorre pelos compromissos informacionais (informações e dados) e com a qualidade. Já os riscos corporativos estão relacionados ao compromisso com as partes interessadas.

Quadro 6: Avaliação da Gestão de riscos de TI versus Gestão riscos corporativos

Categorias	Léxicos mais frequentes	Análise resumida (Categorias *versus* léxicos)
Atuação de TI *versus* perspectiva de negócio	TI, negócio, confiabilidade, informação, procedimento, íntegra e proteção.	A TI atua de forma a auxiliar em melhorias nos processos organizacionais, com informações integradas para melhor atendimento das necessidades informacionais do negócio, contemplando os controles internos utilizados pelas demais áreas. Ocorre de forma a melhorar as perspectivas de negócio, objetivando manter a confiabilidade das informações, com atuação voltada à proteção das informações, ou seja, aliada a práticas de redução de riscos.
Governança corporativa – GC *versus* gestão de riscos em TI e Riscos corporativos	Comunicação, TI, contábeis, financeira, impacta, negócio, corporação, acionista.	A atuação da companhia, quanto às práticas de governança voltadas à redução dos riscos, foi citada pelos entrevistados como superficial. Identificou-se a necessidade de maior clareza e interação das práticas de GC com as atividades dos departamentos.
Criação de mecanismos de controle *versus* redução de riscos em TI e Riscos corporativos	Procedimentos, funcionários (usuários), dados, negócio, agricultura, gerenciamento e companhia.	Os controles internos foram identificados como capazes de proteger as informações, foram relatados problemas decorrentes a erros na produção destes informes (risco de pessoal). A atuação da auditoria na identificação dos pontos a serem consertados proporciona a melhoria deste risco.
Atuação dos usuários *versus* segurança nos processos de negócio	Informações, TI, regra, evitado, contratação, minimiza e mercado.	No caso de estudo, a TI responde pelas necessidades de informações dos usuários. Já o estabelecimento de processos de negócio precisa da contratação de regras e procedimentos mais eficientes que, alinhados às práticas de GC e às expectativas do negócio, objetivem melhor relação com o mercado.
Atuação Comitê de riscos *versus* prevenção de riscos de TI e Corporativos	TI, informações, procedimentos.	A atuação do comitê para a gestão de riscos, existente há quatro anos, concentra-se em ações focadas na redução de impactos negativos e no aproveitamento dos impactos positivos, no que concerne aos riscos estratégicos e financeiros. Não contempla os riscos operacionais (pessoal, processos, tecnologia e *compliance*). Não foi identificada a atuação deste comitê relacionada aos riscos de TI.
Aproximação entre riscos corporativos e riscos de TI	Não localizado	As gestões (riscos de TI e corporativos) podem ser mais eficientes com atuação presente da TI no comitê de riscos, melhorando o uso da tecnologia e possíveis riscos associados. 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.

Fonte: Elaborado pelos Autores.

Os entrevistados salientaram que a adoção de controles internos e a existência de regras e protocolos possibilitariam a redução de riscos de TI e Corporativos. Nas entrevistas, foram destacadas necessidades de melhorias nestes controles em termos de sistema e ferramentas. Observa-se uma percepção de que a criação de mecanismos de controle está associada à governança corporativa, refletindo na forma com que os processos e a gestão são conduzidos, a fim de proteger a empresa de riscos indesejados, concordando com Silva Junior, Junqueira e Bertucci (2009).

Quanto à atuação dos usuários *versus* segurança nos processos de negócio, constataram-se necessidades de melhorias na contratação de regras e procedimentos, alinhados às práticas de Governança Corporativa e às expectativas do negócio. Esta avaliação foi complementada pela visualização da aproximação léxica, Informações e TI, mesma relação percebida entre as variáveis: regra, evitado, contratação, minimiza e mercado. As melhorias apontadas são embasadas em Spears e Barki (2010), pois afirmam que a atuação dos usuários pode garantir a segurança nos processos de negócio, protegendo as informações financeiras e o relacionamento com as partes interessadas.

Cabe destacar que, apesar de a tecnologia ser um aspecto relevante no planejamento agrícola, nos processos da organização e no investimento em novas tecnologias, não foi mencionado nas entrevistas o que concerne aos riscos corporativos. Este fator pode estar relacionado à atuação da TI de forma não integrada e desconectada à gestão de riscos.

A relação da gestão de riscos da TI e corporativos ocorre mediante a atuação da TI frente às perspectivas de negócio. Diante disso, aspectos como a interação e a clareza nas práticas de governança corporativa, a melhoria dos controles internos, a atuação abrangente do comitê de riscos e a adoção de regras e procedimentos para estrutura de riscos possibilitariam melhor gestão dos eventos, oportunizando a mitigação de riscos.

A gestão dos riscos no atual ambiente de negócios pode ser fator transformador de pontos negativos em oportunidades, pois esta gestão remete à redução de perdas com eventos inesperados, propiciando 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; CORBARI, 2011).

5. Considerações Finais

O escopo central deste estudo analisou a relação entre os modelos de gestão de riscos de TI e de gestão de riscos corporativos. Os principais resultados quanto à gestão de riscos de TI revelam que a Agrícola adota ações de mitigação dos riscos com ausência de uma estrutura formal de controle e monitoramento; além disso, são isoladas e sem a efetiva participação dos colaboradores. A gestão de riscos corporativos carece de integração entre os distintos tipos de riscos, tendo maior direcionamento para os riscos estratégicos e financeiros, e há ausência da observação dos princípios recomendados na gestão dos riscos.

A relação entre a gestão dos riscos de TI e a gestão de riscos corporativos ocorre, na Agrícola, pela forma com que a TI se posiciona frente às perspectivas do negócio, pois os aspectos de integração e a clareza nas práxis da governança, os controles internos e a adoção estrutural da gestão de riscos oportunizam a mitigação dos riscos. Em se tratando da relação existente entre a gestão de riscos de TI e a gestão dos riscos corporativos, os resultados sugerem que esta é possível mediante a construção de uma estrutura para o gerenciamento que atue de forma inter-relacionada aos diversos tipos de riscos.

Em suma, há uma relação entre a gestão de riscos de TI e corporativos, mas considerada frágil, e essa pode ser fortalecida, pois a gestão de riscos deve ser realizada como uma espécie de "malha" que permeie todos os riscos, e sua integração é essencial para controle, monitoramento e mitigação dos riscos. As evidências indicaram oportunidades de melhorias da relação entre a gestão dos riscos de TI e os riscos corporativos, bem como para manutenção de requisitos de negócio como a integridade, a disponibilidade e a confidencialidade das informações.

As contribuições deste estudo reforçam a necessidade de uma estrutura para gestão de riscos, alinhada ao negócio, com vistas à redução de custos decorrentes de eventos não identificados. Neste sentido, ao gerenciar de forma eficiente estes aspectos, as organizações economizam recursos e podem destiná-los a avanços tecnológicos, ou a outras ferramentas relacionadas à melhoria do seu desempenho.

Referências

ALBERTIN, A. L.; ALBERTIN, R. M. Dimensões do uso de tecnologia da informação: um instrumento de diagnóstico e análise. **RAP - Revista de Administração Pública**, v. 46, n. 1, p. 125-151, 2012.

ANTHONY JUNIOR, B. A.; NOR, R. N. H.; JOSOH, Y. Y. The Development and Initial Results of a Component Model for Risk Mitigation in IT Governance. **Journal of Science, Technology and Innovation Policy**, v. 2, n. 2, p. 1-13, 2016.

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

BNDES - Banco Nacional do Desenvolvimento. **Carta Circular Nº 34.** Dispõe sobre: Normas Reguladoras do Produto BNDES.2017. Disponível em: <http://www.bndes.gov.br/wps/wcm/connect/site/fd1526d1-a56e-4e54-acb0-ac5a09736640/16Circ34_AOI.pdf>. Acesso em: 10 fev. 2017.

BARTHELEMY, J. The Hard and Soft Sides of IT Outsourcing Management. **European Management Journal**, v. 21, n. 5, p. 539–548, 2003.

BEAL, A. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações - São Paulo: Atlas, 2005.

BHARAT, S.; KAPIL, D. S.; SUBHASH, C. A. New Model for Software Risk Management. **Int. J. Computer Technology & Applications**,v. 3, n. 3, p. 953-956, 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, p. 523-548, 2010.

COIMBRA, F. C. um estudo de caso no setor financeiro. 2011. Tese (Doutorado em Administração). –

Programa de Pós-Graduação em Administração. Universidade de São Paulo (USP), São Paulo, 2011.

COSO - Committee of Sponsoring Organizations of the Tread Way Commission. **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. 2016.

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

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

FADUN, O. S. Risk management and risk management failure: lessons for business enterprises. **International Journal of Academic Research in Business and Social Sciences**, v. 3, n. 2, p. 225-239, 2013.

FREITAS, H. Análise de conteúdo: Faça Perguntas as Respostas obtidas com sua 'Pergunta'! **Revista de Administração Contemporânea**, v. 15, n. 4, p. 748-760, 2011.

FRIGO, M. L.; ANDERSON, R. J. Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. **The Journal of Corporate Accounting & Finance,** v. 22, n. 3, p. 81-88, 2011.

GARVAN, J. R. Risk management: the unifying framework for business scholarship. **Risk Management and Insurance Review***,* v. 10, n. 1, p. 1-12, 2007.

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**, v. 8, n. 1, p. 45-57, 2011.

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

GRENBERGER, W.; HAES, S. Measuring and improving information technology governance through the Balanced Scorecard. **Information Systems Control Journal**, v. 2, p. 199-211, 2005.

HÉROUX, S.; FORTIN, A. Exploring information technology governance and control of web site content: a comparative case study. **Journal of Management & Governance**, v. 17, n. 3, p. 673-721, 2013.

HUGHES, G. Five steps to IT risk management best practices. **Risk Management**, v. 53, n. 7, p. 1-34, 2006.

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. 2017.

ITGI - Information Security Governance. **Cobit 4.1:** objetivos de controle, diretrizes de gerenciamento, modelos de maturidade. 2009. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf>. Acesso em: 15 jan. 2017.

ISO 31000. **Gestão de Riscos** – Princípios e Diretrizes. Rio de Janeiro: ABNT, 2015.

KANNAN, N.; THANGAVEL, N. Risk management in the financial services industry. **Academic Open Internet Journal**, v. 22, n. 7, p. 1-20. 2008.

KUTSCH, E.; HALL, M. The rational choice of not applying project risk management in information technology projects. **Project Management Journal**, v. 40, n. 3, p. 72-81, 2009.

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**, v. 8, n. 1, p. 237-262, 2011.

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: ENANPAD – ENCONTRO NACIONAL DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, XXXI, 2007. Rio de Janeiro. **Anais eletrônicos...** Curitiba: Anpad**,** 2007.

MÜLLER, R.; DRAX, C. Necessity and Development of Risk Management. In: MÜLLER, R.; DRAX, C. **Aviation Risk and Safety Management**. Springer International Publishing, 2014. p. 21-37.

PRADO, E.; SOUZA, C. A. **Fundamentos de sistemas de informação**. Elsevier Brasil. 2014.

SAATY, T.L. **Método de análise hierárquica**. São Paulo: McGraw-Hill, Makron. 1991.

SANTANA, A.; VERAS, M. Gerenciamento de riscos de TI e suas práticas nas organizações Brasileiras: um estudo de casos múltiplos. In: CONTECSI - INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT. 8o., 2011. São Paulo. **Anais eletrônicos...** São Paulo: Contecsi, p. 570-598, 2011.

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

SILVA, E. L.; MNEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. ed. rev. atual. Florianópolis: UFSC. 2005.

SIMONSON, M.; JOHNSON, P.; EKSTEDT, M. The Effect of IT Maturity on IT Governance Performance. **Information Systems Management**, v. 27, p. 10-24, 2010.

SMITH, M. A.; KUMAR, R. A theory of application service provider (ASP) use from a client perspective. **Information & Management**, v. 41, p. 977-1002, 2004.

SPEARS, J. L.; BARKI, H. User participation in information systems security risk management. **MIS Quarterly Executive**, v. 34, n. 3, p. 503-522, 2010.

TAROUCO, H.; GRAEML, A. Governança de Tecnologia da Informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias de TI. In: ENADI -ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, II, 2009. Recife. **Anais eletrônicos...** Curitiba: Anpad, 2009.

WEILL, P.; ROSS, J.A matrix approach to designing IT governance. **Sloan Management Review**, v. 46, n. 2, p. 26-34, 2005.

XUE, Y.; LIANG, H.; BOULTON, W. R. Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context. **MIS Quarterly**, v. 32, n. 1, p. 67–96, 2008.

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

YUE, W. T. Network externalities, layered protection and IT security risk management. **Decision Support Systems**, v. 44, n. 1, p. 1-16, 2007.