XX SEMEAD
Seminários em Administração
novembro de 2017
ISSN 2177-3866

ANÁLISE DO RELACIONAMENTO EXISTENTE ENTRE A GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO, O GERENCIAMENTO DO RISCO CORPORATIVO E AS FUNÇÕES DE COMPLIANCE

FERNANDO ATZ
UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)
fernando.atz@hotmail.com

MELISSA GERHARD
mgerhard@unisinos.br

VIVIANE DA COSTA FREITAG
UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)
vivifreitag@gmail.com

ADOLFO ALBERTO VANTI
UNIVERSIDADE FEDERAL DE SANTA MARIA (UFSM)
adovanti1@gmail.com

ANGEL COBO
UNIVERSIDAD DE CANTABRIA
angel.cobo@unican.es

ANÁLISE DO RELACIONAMENTO EXISTENTE ENTRE A GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO, O GERENCIAMENTO DO RISCO CORPORATIVO E AS FUNÇÕES DE *COMPLIANCE*

Resumo

A governança de TI estimula comportamentos desejáveis com vistas ao atingimento de metas da organização. O gerenciamento do risco corporativo, por sua vez, objetiva projetar possíveis riscos aos quais as organizações estão suscetíveis, de forma a viabilizar que estas atinjam suas metas. Já as funções de *compliance* ocupam-se de garantir que as normas internas e externas das organizações sejam cumpridas. Alinhado à esses conceitos, o objetivo deste estudo é analisar o relacionamento existente entre a governança da tecnologia da informação, o gerenciamento do risco corporativo e as funções de *compliance*. Foram realizadas cinco entrevistas em uma empresa de grande porte do ramo metalúrgico situada no Rio Grande do Sul. As análises, realizadas por meio do Método Multicriterial de Apoio à Decisão *Analytic Hierarchy Process* (AHP), indicaram que o gerenciamento do risco corporativo é tido como o mais importante, indicando uma prioridade relativa de 73%. A governança de TI ocupou a segunda prioridade relativa, com 22% e por último as funções de *compliance*, com apenas 5% de prioridade relativa. Ainda, cada uma destas três abordagens foi analisada separadamente, com tabulações e análises adicionais que evidenciaram um alinhamento dos respondentes no que tange as prioridades que a empresa deve ter.

Palavras-chave: gerenciamento do risco corporativo; governança de TI; *compliance.*

Abstract

IT governance encourages desirable behaviors to achieve organizational goals. Corporate risk management, in turn, aims to project possible risks to which organizations are susceptible, in order to enable them to achieve their goals. Compliance functions are concerned to ensure that internal and external standards of organizations are fulfield. In line with these concepts, the objective of this study is to analyze the relationship between IT governance, corporate risk management and compliance functions. Five interviews were carried out at a large metallurgical company located in Rio Grande do Sul. Analyzes carried out using the AHP methodology indicated that corporate risk management is considered the most important, indicating a relative priority of 73%. IT governance ranked second, with 22% and lastly compliance, with only 5% relative priority. Furthermore, each of these three approaches was analyzed separately, with tabulations and additional analyzes that showed an alignment of the respondents regarding the priorities that the company should have.

Keywords: enterprise risk management; IT governance; compliance.

1 Introdução

Dentre os muitos ativos envolvidos na administração de uma empresa, a informação e as tecnologias coletadas, arquivadas e disseminadas podem ser considerados os ativos de maior insegurança para seus administradores. Uma das razões para isso é a rigidez parcial dos sistemas de TI, que podem não acompanhar as mudanças constantes e que são necessárias nos negócios organizacionais. A implantação da Governança de TI, como forma de sustentar as estratégicas da empresa, pode garantir melhores desempenhos e sucessos, representando um diferencial em relação a outras organizações. (WEILL; ROSS, 2006).

A atuação ativa da Governança de TI em uma organização estimula, em seus colaboradores, comportamentos adequados com valores, estratégias, normas e cultura organizacional. (WEILL; ROSS, 2006). Neste sentido, as organizações têm utilizado também o *compliance*. Este vem sendo utilizado com o objetivo de cumprir as tarefas estabelecidas e de estar em conformidade com a legislação e a regulamentação aplicável aos negócios, ao código de ética e as políticas da organização, cumprindo regulamentos impostos às atividades. Assim permitindo a agregação da segurança e dos controles na organização, a fim de se obter maior clareza nas tomadas de decisões e no aumento do valor do intangível das empresas. (SCHILDER, 2006).

Uma estrutura de *compliance* deve contemplar práticas relacionadas à governança corporativa e gestão de riscos. Ao ser adotada por uma organização, a estrutura de *compliance* deve integrar o gerenciamento nas operações, funcionários e dependências locais e internacionais, fomentadas efetivamente por uma cultura de integridade e responsabilidade. (NEWTON, 2002).

Adicionalmente à governança e ao *compliance*, empresas procuram formas de gerenciar seus riscos. Este visa possibilitar à organização que cumpra seus objetivos, projetando possíveis riscos aos quais as empresas estão sujeitas e os mensurando. (COSO, 2007). Aspectos como capital de terceiros, níveis de estoque e fluxo de caixa são utilizados nesta mensuração. (NOCCO; STULZ, 2006). Ainda, deve ser definido o grau de exposição da empresa a determinado risco, para que ela possa determinar qual o tratamento a ser dado a ele. A identificação e o gerenciamento dos riscos são realizados através de simulações de cenários, utilizando-se as principais variáveis dos negócios envolvidos. (IBGC, 2015).

Através da metodologia AHP (*Analytic Hierarchy Process*), que visa estabelecer prioridades e consistência lógicas, o objetivo deste artigo é analisar relacionamento existente entre a governança da tecnologia da informação, o gerenciamento do risco corporativo e as funções de *compliance*. Com a utilização de um instrumento de pesquisa, cinco colaboradores de uma empresa de grande porte do ramo metalúrgico, situada no Rio Grande do Sul, foram entrevistados.

Este estudo está estruturado em cinco capítulos, sendo esta, a introdução, a primeira, seguida pela revisão da literatura e da metodologia de pesquisa. O quarto capítulo apresenta a análise de resultados, seguido das conclusões do estudo e das referências utilizadas na sua elaboração.

2 Revisão de Literatura

Este capítulo apresenta o embasamento teórico do estudo, como forma de suporte à pesquisa empírica. Foram abordados os seguintes temas: governança corporativa e governança da tecnologia da informação, *compliance* e gerenciamento do risco corporativo.

2.1 Governança Corporativa e Governança da Tecnologia de Informação

Para Weill e Ross (2006), a governança corporativa tem muito a contribuir com a governança de TI. A adoção às práticas de governança corporativa pode ocorrer devido à pressão do mercado acionário, por causa de regras existentes em determinadas listagens e espontaneamente, entre outros possíveis motivos. (AGUILERA; CUERVO-CAZURRA, 2004).

Apesar de possuir um elevado número de empresas com controle familiar, é factível a existência de conflitos entre acionistas minoritários e controladores no mercado de ações. Nessa perspectiva, na tentativa de atenuar conflitos de interesse, o sistema de gestão vem sendo estimulado a implantar e valorizar a governança corporativa. Esta seria uma das formas de atenuar possíveis conflitos de interesse entre proprietários e gestores das organizações. (LEAL; SAITO, 2003). Todavia, tais ações podem acarretar em mais e maiores custos e não eliminar o problema do conflito de interesses existentes, apenas o reduzindo. (JENSEN; MECKLING, 1976)

A governança de TI é descrita como sendo "a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI". (WEILL; ROSS, 2006, p.8). Outro aspecto relacionado à governança de TI e reportado pelos autores trata-se do fato de o tomador de decisões ser determinado pela própria governança. Deste modo, um desalinhamento entre comportamentos desejáveis e a governança evidencia o surgimento de problemas, que podem ser desde operacionais até mesmo estratégicos.

Foram identificados cinco importantes fatores para realizar esta avaliação de desempenho da Governança de TI, sendo eles: o ambiente da empresa, os arranjos de governança, sua consciência, seu desempenho e o desempenho financeiro. Cada um destes fatores deve ser mensurado para a correta avaliação de desempenho da governança nas organizações. Estando definida a governança, seu desempenho "consistirá, portanto, na eficácia com que os arranjos de governança estimulam comportamentos desejáveis e, em última instância, em quão bem a firma atinge suas metas de desempenho desejadas". (WEILL; ROSS, 2006, p.121).

Quadro 1 - Avaliação do Desempenho de Governança de TI

Ambiente	**Arranjos de Governança**	**Consciência da Governança**	**Desempenho da Governança**	**Desempenho Financeiro**
Estratégias - Excelência operacional - Intimidade com o clientes - Liderança do produto	**Principais decisões e arquétipos de TI**	**Porcentagem de gerentes em posição de liderança que podem descrever a governança**	**Média de quatro medidas de desempenho ordenadas pela importância**	**Lucros** - Margem percentual - ROE - ROA

Tamanho - Número de unidades de negócios	**Mecanismos** - Conselhos - Service Level Agreements (SLAs) - Organização da TI - Cobrança reversa - Comitê de arquitetura	**Abordagem de comunicação** - Reuniões - Documentos - Portal	**Uso eficaz da TI para:** - Controle de custos - Crescimento - Utilização de ativos - Flexibilidade do negócio	**Utilização de Ativos** - ROA
Sinergia		**Exceções** - Percentual de projetos		**Crescimento** - Mudança percentual de Receita
Intensidade da TI - Dinheiro - Pessoas				**Dados mensurados utilizando-se:** -Mudança percentual média em três anos ajustada à indústria

Fonte: Weill; Ross (2006, p.122)

Os cinco fatores da avaliação de desempenho da governança de TI são apresentados no Quadro 1, assim como os mecanismos utilizados para a mensuração de cada um deles. Tal mensuração do desempenho possui, conforme Weill e Ross (2006) quatro objetivos: utilização da TI com relação custo/benefício boa; eficácia da TI para uso de ativos; TI utilizado de forma eficaz para o crescimento; e eficácia de TI para obtenção de flexibilidade nos negócios. As capacidades da tecnologia da informação são moldadas pela integração e padronização de dados, aplicações e infra-estrutura organizados de forma lógica. Padronizar proporciona eficiência e previsibilidade para as organizações. Ainda, sua atuação estimula a adequação a valores, normas, culturas e estratégias da empresa. (WEILL; ROSS, 2006). Ao encontro dessa visão, outra área existente trata de estar em linha, em conformidade, com regulações internas e externas. (MORAIS, 2005). Esta, conhecida como *compliance*, é abordada na seção seguinte.

2.2 *Compliance*

Compliance é o dever de cumprir, de estar em conformidade e fazer cumprir regulamentos internos e externos impostos às atividades da organização. A função de *compliance* é controlar os riscos reais e consequentes do legal funcionamento das instituições. (MORAIS, 2005). Assim, tem se tornado cada vez mais um fator diferencial para a competitividade das organizações, pois o mercado busca e valoriza a transparência e a ética nas interações econômicas e sociais. (SCHILDER, 2006).

A organização precisa conquistar o *compliance* como uma forma de fortalecer sua participação no mercado em que atua; por sua vez, a sociedade deve entender a ética como uma forma de ação conveniente e como uma condição de desenvolvimento da sociedade. (SCHILDER, 2006).

De acordo com o *Ethics Resource Center* (2007), algumas características pessoais do profissional de *compliance* são necessárias para o desempenho de suas funções, conforme o Quadro 2.

Quadro 2 - Características Pessoais do Profissional de *Compliance*

Integridade	Uma pessoa íntegra procura viver seguindo as suas convenções, convicções, ética e princípios, tendo maior legitimidade para falar com os colegas e colaboradores sobre temas de ética.
Reputação	O profissional de deve cuidar da sua própria reputação, não só agindo com honestidade, mas também parecendo honesto.
Caráter forte	A postura ética do profissional de *compliance* deve ser exemplar. Ser e viver um exemplo dentro da organização é essencial para se conquistar uma cultura organizacional na qual as normas e códigos internos e externos são levados a sério.
Autoridade	Tendo em vista a natureza da função, é importante que o profissional tenha autoridade para que as suas ações sejam respeitadas, seus treinamentos seguidos e que os colaboradores tenham receio de sofrer sanções por ele impostas, quando desrespeitarem a política da empresa.
Habilidades interpessoais	Para orientar os membros da organização é necessária a competência para liderar pessoas, capacidade de intervir em situações delicadas, comunicar e promover mudanças na organização.
Persistência	Mudança de cultura requer tempo e ações contínuas de conscientização por parte do profissional de *compliance*. O profissional de *compliance* tem que ter a paciência e a persistência para ultrapassar as barreiras e dificuldades associadas à implantação da mudança de cultura. As estratégias mais eficientes para garantir o comprometimento com o *compliance* são as que se baseiam em argumentos bem fundamentados.
Conhecimento atualizado de normas e requisitos de *compliance*	Os requisitos regulatórios estão em constante alteração e os sistemas de controles internos e gestão de riscos se desenvolvem cada vez mais para atender às exigências de órgãos reguladores. É necessário o profissional manter-se atualizado em relação aos requisitos legais.

Fonte: Adaptado de *Ethics Resource Center* (2007)

Para que a função de *compliance* seja eficaz, é essencial o comprometimento da direção e seus administradores fortalecendo, junto aos funcionários, o comprometimento de todos e definindo a responsabilidade e participação de cada um deles na organização. (SCHILDER, 2006).

É parte do escopo de trabalho da área de *compliance* prestar assessoria aos negócios da empresa no que diz respeito a questões regulatórias. O lançamento de uma nova linha de negócios ou um novo produto podem requerer uma análise da área de *compliance*, visto que a alteração de procedimentos ou novas regras podem afetar o negócio. A existência de um monitoramento por *compliance* pode prover à organização uma fonte oportuna de *feedback*, focado para a adesão de outros departamentos às devidas obrigações regulatórias. (KOW, 2006).

A relação da área de *compliance* com a alta direção da empresa deve ser estreita e os recursos para o desempenho de um trabalho efetivo devem ser disponibilizados. Também, para um desempenho eficiente de suas funções, a equipe de *compliance* deve ser suficientemente independente. Um dos maiores paradoxos do profissional de *compliance* é sua proximidade com o negócio, isso porque a proximidade é essencial para um bom desempenho das atividades, mas pode tornar-se um obstáculo quando tratam de questões significativas. (KOW, 2006).

Como forma de auxiliar às empresas no desenvolvimento da sua governança e das funções de *compliance*, elas precisam ter a capacidade de identificar e de gerenciar os riscos envolvidos nas suas atividades.

2.3 Gerenciamento do Risco Corporativo

Risco é a consequência da incerteza nos objetivos, qualquer empresa está cercada por riscos, que consistem na possibilidade de que os resultados sejam diferentes dos esperados, podendo envolver perdas ou novas oportunidades. O risco, quer por possíveis falhas, quer por erros, está intrínseco em todas as atividades e sua administração se reflete nos processos de tomada de decisão, inclusive quanto a informação envolvida no processo decisório da organização. Possíveis peculiaridades e desafios na avaliação do risco oferecem oportunidades para que as organizações analisem possíveis problemas em seus processos interno. (BROMILEY ET AL, 2015).

Nas organizações é essencial que o risco seja monitorado pelos gestores e diretores. O principal objetivo da governança corporativa é a criação de valor e a otimização dos riscos; deste modo, a governança de TI deve gerenciar e avaliar as atividades e os riscos de TI. (ISACA, 2012).

Os riscos são classificados em: risco de mercado, risco de crédito, risco de liquidez, risco operacional, risco legal e regulatório, risco de negócio, risco estratégico e risco de reputação. (HAHN, KUHN, 2012). O risco operacional consiste em uma ameaça para os objetivos organizacionais, pois são consequência da incerteza existente em relação à eventos tais como: a perda por processos internos inadequados ou falhas decorrentes no controle interno, representados pelas pessoas, ferramentas, procedimentos e/ou sistemas. (HAHN, KUHN, 2012). O Quadro 3 apresenta a categorização de eventos de risco operacional:

Quadro 3 - Categorização de eventos de Risco Operacional

Clientes, produtos e práticas de negócio	Manipulação de mercado, práticas anti concorrenciais, quebra de contrato.
Danos a ativos físicos	Desastres naturais, terrorismo, vandalismo.
Interrupção dos negócios e falha do sistema	Interrupção de operação, falha de software e hardware.
Execução de processos e gestão	Erro nos dados de entrada, erro de contabilidade, relatórios legais defeituosas, bens perdidos por negligência.
Fraude interna	Roubo de bens, sonegação fiscal, corrupção, fraude contábil.
Fraude externa	Roubo de informações confidenciais, ataques de hackers, falsificação de documentos.
Práticas de emprego e segurança	Segregação, assédio, práticas ilegais.

Fonte: Longo (2012)

O roubo de informações pode resultar em perda da vantagem competitiva, por isso os funcionários são responsáveis por diversos tipos de perdas por erros ocasionados por incompetências, más decisões ou a falta de cumprimento das regras. Devido a isso, e ao fato de o risco operacional ser parte de qualquer atividade, é muito difícil de ele ser totalmente mitigado (LONGO, 2012), deste modo, a gestão de riscos deve ser parte integrante dos processos de governança das empresas.

A utilização eficiente da gestão da informação, por parte das organizações, pode contribuir de maneira relevante na mitigação dos riscos operacionais, auxiliando a gestão do

conhecimento e a gestão de riscos operacionais, pois a informação e o conhecimento são fundamentais para o desempenho das organizações. (LONGO, 2012)

O efeito do gerenciamento de risco corporativo, tanto em nível 'macro' quanto 'micro', cria valor para as organizações. O gerenciamento de *trade-off* de risco-retorno auxilia as empresas no que tange o acesso aos mercados de capitais ou outras necessidades em termos de recursos para implantação de estratégias. "O reconhecimento de que não há formas econômicas de transferir riscos que sejam exclusivos das operações comerciais de uma empresa pode servir para enfatizar o valor potencial de reduzir a exposição da empresa a outros riscos 'não essenciais'". (NOCCO; STULZ, 2006, p.9).

COSO (2007, p. 4) define o gerenciamento de riscos como sendo:

> um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Um dos aspectos abordados pelos autores Nocco e Stulz (2006) é a determinação da quantidade ou nível ideal de risco que a empresa deve suportar. Os autores destacam que nível de estoques, fluxo de caixa e capital de terceiros são abordados para a mensuração do risco organizacional. A redução de risco pode impactar na redução de capital próprio oneroso necessário para a sustentabilidade dos riscos operacionais. Ainda, cabe à diretoria da empresa a análise entre a adoção de uma gestão de risco mais ativa ou maiores níveis de estoque e caixa.

Em se tratando de mensuração, os autores Beasley, Branson e Hancock (2010) enfatizam a importância de se distinguir indicadores de desempenho de indicadores de risco. Isso devido ao fato de os indicadores de desempenho das organizações possuírem como foco dados históricos de suas principais unidades operacionais. Tais medidas não permitem a identificação de 'alertas precoces', adequados para riscos em desenvolvimento.

Indicadores de desempenho são importantes para a gestão de um negócio bem sucedido, permitindo que as empresas identifiquem aspectos de baixo desempenho, questões que necessitam mais recursos e energia, entre outras informações necessárias aos administradores. Estes fazem uso tanto dos indicadores de desempenho quanto dos indicadores de risco, os quais fornecem informações sobre riscos emergentes (BEASLEY, BRANSON, HANCOCK, 2010).

COSO (2007) apresenta que os riscos corporativos possuem oito componentes, inter-relacionados, sendo estes: o ambiente interno, a fixação de objetivos, a identificação de eventos, a avaliação de riscos, a resposta ao risco, atividades de controle, informações e comunicações e o monitoramento. O gerenciamento de riscos corporativos pode ser considerado um processo multidirecional e interativo, e não um processo em série. Todos os componentes influenciam e são influenciados pelos outros.

Após se definir o grau de exposição da empresa a um determinado risco, determina-se qual o tratamento a ser dado a ele. Para a definição do grau de exposição, ao menos dois aspectos são considerados: a probabilidade de acontecimento do risco e o impacto do mesmo.

O impacto considerado 'intangível' também deve ser levado em consideração. O impacto financeiro pode ser mensurado através de metodologia denominada "planejamento sob incerteza". "Para viabilizar tal quantificação é necessário que a organização (i) tenha o seu negócio modelado em alguma ferramenta que possibilite simulações e (ii) seja capaz de gerar cenários das principais variáveis e consistentes entre si." A identificação e o gerenciamento dos riscos de forma integral fazem parte das recomendações, como por exemplo riscos múltiplos e comuns a áreas diferentes (IBGC, 2015, p.22)

Os eventos que permitem a sinalização de problemas podem ocorrer tanto nas operações internas da organização quanto podem ser riscos emergentes de eventos externos, como alterações macroeconômicas que influenciam o nível de atividade da organização. Indicadores de risco refletem a exposição ao risco de diversas áreas da organização, evidenciando riscos em desenvolvimento e potenciais oportunidades. A consequência seria a necessidade de realização de ações, também em diversas áreas da organização (BEASLEY, BRANSON, HANCOCK, 2010).

Após a apresentação da governança da tecnologia da informação, das funções de *compliance* e do gerenciamento do risco corporativo é possível analisar o relacionamento existente entre eles. Para isso, no próximo capítulo apresenta-se a metodologia da pesquisa adotada para esta análise.

3 Metodologia da Pesquisa

O objetivo deste artigo foi analisar o relacionamento existente entre a governança da tecnologia da informação, do gerenciamento do risco corporativo e das funções de *compliance*. Assim, para responder a este objetivo foi aplicado o método AHP, como forma de avaliação deste alinhamento.

3.1 O Método AHP

O AHP (*Analytic Hierarchy Process*) é uma ferramenta de tomada de decisões que pode auxiliar no ajuste de prioridades e torna a decisão racional e não subjetiva e intuitiva. Seu uso é recomendado quando há suficiente independência e capacidade de discriminação entre as alternativas de decisão. (SAATY, 1991).

O método AHP possui três princípios: construção de uma hierarquia, estabelecimento de prioridades e consistência lógica das prioridades. A sistemática de análise pelo AHP consiste em medições relativas, que comparam duas a duas a influência de critérios na decisão, comparando-as como mais ou menos influente (PARTOVI; WHITERS; BRADFORD, 2002).

3.2 Coleta de Dados

A coleta das informações, mediante instrumentos de coleta de dados, foi realizada presencialmente pelos pesquisadores com 5 colaboradores da empresa: uma gerente contábil, um *controller,* duas coordenadoras de controladoria e um analista de controladoria. O critério utilizado para a seleção dos respondentes baseou-se nos temas envolvidos: *compliance*, gerenciamento do risco e governança de TI.

O gerente contábil (Respondente 2) e o *controller* (Respondente 5) foram selecionados por possuírem uma visão macro da empresa e interagir com agentes internos e externos a ela, permitindo uma abordagem ampla dos temas abordados. As duas coordenadoras de controladoria (Respondentes 1 e 4) e o analista de controladoria (Respondente 3) possuem uma visão mais detalhada dos processos internos, o que permite analisarem os temas em uma relação mais particular da empresa.

A elaboração dos construtos referentes ao desempenho de governança de TI, funções de *compliance* e arquitetura de risco foram fundamentadas na literatura, conforme demonstrado na Quadro 4:

Quadro 4 - Constructos

Desempenho de Governança de TI	Funções de *Compliance*	Gerenciamento do Risco Corporativo
WEILL E ROSS (2006)	ETHICS RESOURCE CENTER (2007); KOW (2006); SCHILDER (2006)	BEASLEY; BRANSON; HANCOCK (2010); BROMILEY EET AL (2015), COSO (2007), ISACA (2012), LONGO (2012), NOCCO; STULZ (2006)
Ambiente	Os sistemas de controles internos e gestão de riscos se desenvolvem para atender às exigências de órgãos reguladores.	O processo de gestão busca fornecer uma maneira de determinar quais riscos são aceitáveis e como podem ser tratados internamente.
Arranjos de Governança	Normas externas e normas internas estão alinhadas.	O risco está intrínseco em todas as atividades e sua administração se reflete nos processos de tomada de decisão.
Consciência da Governança	O conselho de *compliance* é envolvido quando uma nova linha de negócios ou produto é lançado.	A diretoria da empresa analisa a adoção de uma gestão de risco mais ativa.
Desempenho da Governança	A assessoria em questões regulatórias relevantes sobre os negócios da empresa é uma responsabilidade fundamental da *compliance*.	A utilização eficiente da gestão da informação, por parte das organizações, pode contribuir de maneira relevante na mitigação dos riscos operacionais. Para tanto, a empresa realiza treinamentos e valoriza a comunicação.
Desempenho Financeiro	Existe o comprometimento da direção e seus administradores fortalecendo, junto aos funcionários, o comprometimento de todos, definindo a responsabilidade de cada um.	A gestão de riscos é parte integrante dos processos de governança da empresa
	A ética é vista como uma forma de ação.	O risco seja monitorado pelos gestores e diretores

	Existe o fortalecimento da cultura de controles internos, a cultura de fazer o correto.	Ações em diversas áreas da organização são realizadas no que tange o gerenciamento do risco corporativo.
		O gerenciamento de riscos corporativos pode ser considerado um processo multidirecional e interativo.

Fonte: Weill, Ross (2006); Ethics Resource Center (2007); Kow (2006); Schilder (2006); Beasley; Branson; Hancoch (2010); Bromiley et al (2015), Coso (2007), Isaca (2012), Longo (2012), Nocco; Stulz (2006).

Os respondentes, apoiados pelos pesquisadores, priorizaram construtos e dimensões da estrutura referencial, com base na metodologia proposta pelo AHP e construíram matrizes de preferências, segundo a escala de Saaty (1991). A escala é apresentada no Quadro 5.

Quadro 5 - Modelo de escala de importância de Saaty

Escala numérica	Escala Verbal	Explicação
1	Ambos elemento são de igual importância	Ambos elementos contribuem com a propriedade de igual forma
3	Moderada importância de um elemento sobre o outro	A experiência e a opinião favorecem um elemento sobre o outro
5	Forte importância de um elemento sobre o outro	Um elemento e fortemente favorecido
7	Importância muito forte de um elemento sobre o outro	Um elemento e muito fortemente favorecido sobre o outro
9	Extrema importância de um elemento sobre o outro	Um elemento e favorecido pelo menos com uma ordem de magnitude de diferença
2, 4, 6, 8	Valores intermediários entre as opiniões adjacentes	Usados como valores de consenso entre as opiniões

Fonte: Saaty (1991)

Os resultados obtidos com os julgamentos, através da comparação paritária são colocados numa matriz **A** quadrada **n x n**. Este procedimento se repete para todos os elementos do nível, com respeito a todos os elementos de um nível acima. A partir desta matriz, foram calculadas as prioridades relativas de cada uma delas. A prioridade relativa tem por objetivo identificar a ordem de importância de cada critério, para isto é calculada a média aritmética dos valores de cada linha da matriz normalizada obtida. (SAATY, 1991).

Após a coleta e sistematização dos dados, estão apresentados, no capítulo seguinte, os resultados pertinentes à pesquisa.

4 Análise dos Resultados

A empresa objeto do estudo possui aproximadamente 2.000 colaboradores e duas sedes manufatureiras no país. No segundo semestre de 2016 a empresa iniciou o processo de implantação de práticas de *compliance.* A governança de TI e o gerenciamento do risco corporativo, por sua vez, não possuem processos definidos ou responsáveis designados.

As análises foram realizadas em quatro etapas, sendo a primeira a identificação das prioridades relativas quando comparados: gerenciamento do risco corporativo, desempenho da governança de TI e funções de *compliance*. As outras três etapas foram compostas pelas análises de cada componente destes três fatores, conforme descrito na metodologia. Em cada uma das análises, apresenta-se primeiramente a matriz resultante do agrupamento das cinco entrevistas realizadas e na sequência as tabelas com as prioridades em termos percentuais.

A primeira matriz as prioridades relativas de cada um dos respondentes, que se consolida em uma matriz com as cinco entrevistas. Na matriz consolidada, observa-se que a prioridade 1 corresponde ao gerenciamento do risco corporativo, a prioridade 2 diz respeito ao desempenho da governança de TI e a prioridade 3 às funções de *compliance.*

As matrizes individuais evidenciam a existência de um alinhamento entre as respostas dos cinco entrevistados. Verifica-se que quatro dos cinco respondentes utilizaram pontuações altas, ratificando a importância dos três componentes para a empresa. A média normalizada, obtida a partir dos dados dos cinco respondentes, é apresentada o quadro 6 evidencia a priorização dos fatores decisórios para os entrevistados.

Quadro 6 - Prioridade relativa dos critérios analisados

Critério	Prioridade
Gerenciamento do Risco Corporativo	73%
Desempenho da Governança de TI	22%
Função de Compliance	5%

Fonte: Dados da pesquisa.

Na Tabela 1 é possível verificar que a prioridade relativa do gerenciamento do risco corporativo é de 73%. Tal indicador evidencia que, na média, os respondentes priorizam aspectos de gerenciamento de risco em um processo de tomada de decisões. Na sequência encontra-se o desempenho da Governança de TI. Esta, porém, com uma prioridade relativa de 22%, ou seja, um terço do indicador referente ao gerenciamento do risco corporativo. Por último encontram-se as funções de *compliance*, com prioridade relativa de 5%.

Considerando a realidade da empresa analisada, verificou-se que a mesma possui controles internos rígidos e auditorias internas e externas que os validam trimestralmente. Por sua vez, a governança de TI possui uma equipe de auditoria específica e especializada em processos que a envolvam, não sendo, portanto, a mesma equipe das demais auditorias realizadas na empresa. Assim, os resultados evidenciados na Tabela 2 são em virtude da empresa e dos funcionários possuírem forte cultura organizacional quanto ao desempenho da governança de TI e das funções de *compliance*, por isso possuem menores prioridades quando comparadas ao gerenciamento do risco corporativo.

Desdobrou-se então a análise de cada um dos elementos do gerenciamento do risco corporativo, da Governança de TI e *compliance* considerados. Primeiramente foram analisadas as questões envolvendo o gerenciamento do risco corporativo, cuja prioridade

relativa demonstrou-se significativamente maior em relação às demais. Para a sua análise foram levados em consideração oito elementos que podem ser observados na tabela 2.

O quadro 2 apresenta os resultados dos critérios abordados no gerenciamento do risco corporativo. Os respondentes 1, 3 e 5 tiveram suas respostas mais alinhadas entre si quando comparadas aos respondentes 2 e 4. Ainda, verifica-se a partir das pontuações utilizadas, que a visão de cada entrevistado, em relação ao gerenciamento do risco corporativo, é sensivelmente diferente.

Quadro 7 - Prioridade Relativa do Gerenciamento do Risco Corporativo

Critério	**Prioridade**
O gerenciamento de riscos corporativos pode ser considerado um processo multidirecional e interativo.	39,44%
O risco está intrínseco em todas as atividades e sua administração se reflete nos processos de tomada de decisão.	18,57%
A diretoria da empresa analisa a adoção de uma gestão de risco mais ativa.	12,35%
A utilização eficiente da gestão da informação, por parte das organizações, pode contribuir de maneira relevante na mitigação dos riscos operacionais. Para tanto, a empresa realiza treinamentos e valoriza a comunicação.	11,05%
A gestão de riscos é parte integrante dos processos de governança da empresa	8,69%
O risco seja monitorado pelos gestores e diretores	4,28%
Ações em diversas áreas da organização são realizadas no que tange o gerenciamento do risco corporativo.	3,79%
O processo de gestão busca fornecer uma maneira de determinar quais riscos são aceitáveis e como podem ser tratados internamente.	1,83%
Total	100%

Fonte: Dados da pesquisa.

Assim, analisando o quadro 7 constata-se que o critério “o gerenciamento de riscos corporativos pode ser considerado um processo multidirecional e interativo” encontra-se com o maior índice de prioridade relativa, de 39,44%. Tal índice indica que, em média, os respondentes concordam ser este o aspecto mais importante a ser considerado quanto ao gerenciamento do risco corporativo da empresa. Tal resultado está em linha com o posicionamento da empresa, que possui uma gestão de recursos descentralizada (humanos, financeiros, entre outros). Com um índice de 18,57% os respondentes elegeram o fato de o risco estar intrínseco em todas as atividades e a administração da empresa refletir nos processos de tomada de decisão. É possível verificar que ambos os processos envolvem uma visão mais gerencial, mas ampla do negócio. Isso porque tratam-se de questões estratégicas do negócio, que desenham e delineiam a forma de atuação das lideranças da empresa.

Por outro lado, aspectos como o monitoramento do processo do risco por gestores e diretores, ações em diversas áreas e o fato do processo de gestão fornecer uma maneira de determinar quais riscos são aceitáveis (e como podem estes ser tratados internamente) apresentaram uma prioridade relativa consideravelmente baixa. Os demais processos encontram-se com valores de prioridade entre 8,69% e 18,57%.

Tais resultados vêm de encontro às afirmações de COSO (2007) no que diz respeito aos riscos corporativos inter-relacionados com: o ambiente interno, a fixação de objetivos, a identificação de eventos, a avaliação de riscos, a resposta ao risco, as atividades de controle, informações e comunicações e o monitoramento também se fazem presentes nas prioridades dos respondentes. Essa priorização da visão macro da empresa é evidenciada também nas prioridades do desempenho da governança de TI, conforme quadro 8.

A partir da matriz de prioridades da governança de TI verifica-se que o posicionamento dos cinco respondentes é semelhante para cada um dos cinco critérios elencados. Tal alinhamento pode permitir à empresa um melhor aproveitamento da área de governança de TI a fim de se alcançar os seus objetivos.

Quadro 8 - Prioridade Relativa do desempenho da Governança de TI

Critério	**Prioridade**
Ambiente	55,00%
Arranjos de Governança	25,10%
Consciência da Governança	5,30%
Desempenho Financeiro	2,50%
Total	100%

Fonte: Dados da pesquisa.

A média normalizada da prioridade relativa do desempenho da governança de TI apresentou, primeiramente, o ambiente, com um índice de 55%. Dentre as priorizações obtidas, em segundo lugar, com uma prioridade muito inferior à anterior, encontram-se os arranjos de governança, com um índice de 25,1%. Em seguida, com um índice de 12,10%, a consciência da governança. As respostas evidenciam baixo grau de importância o desempenho financeiro com uma prioridade relativa de 2,50%, sendo este critério o de menor importância, para os respondentes, em relação ao assunto. Por fim, o desempenho da governança (não somente a governança de TI) ficou em quarto lugar nas prioridades dos respondentes, com um índice de 5,30%.

Tais resultados demonstram-se alinhados com os achados teóricos, uma vez que o ambiente relaciona-se diretamente com o comportamento daqueles pertencentes ao mesmo, conforme afirmam Weill e Ross (2006). Por fim, são apresentados os resultados das priorizações referentes às funções de *compliance*. Tal indicador, que na visão global apresentou priorização de 5% (Tabela 1), foi desdobrada em sete critérios, e os resultados obtidos são apresentados no quadro 4.

As matrizes apresentadas no quadro 9 evidenciam, em sua maioria, um alinhamento entre as respostas dos entrevistados. O respondente 4 (coordenadora de controladoria) apresenta respostas diferentes dos demais entrevistados, o que pode ser justificado por uma formação acadêmica diferente dos demais, por sua posição hierárquica na empresa ou simplesmente por possuir uma visão diferente dos demais entrevistados. É possível verificar que, com exceção do respondente 4, as altas pontuações indicam a importância que os respondentes dão ao tema.

Quadro 9 - Prioridade Relativa das funções de *Compliance*

Critério	**Prioridade**
Os sistemas de controles internos e gestão de riscos se desenvolvem para atender às exigências de órgãos reguladores.	38,50%
Normas externas e normas internas estão alinhadas.	24,00%
O conselho de *compliance* é envolvido quando uma nova linha de negócios ou produto é lançado.	15,20%
A assessoria em questões regulatórias relevantes sobre os negócios da empresa é uma responsabilidade fundamental da *compliance*.	11,40%
Existe o comprometimento da direção e seus administradores fortalecendo, junto aos funcionários, o comprometimento de todos, definindo a responsabilidade de cada um.	5,70%
A ética é vista como uma forma de ação.	3,30%
Existe o fortalecimento da cultura de controles internos, a cultura de fazer o correto.	1,90%
Total	100%

Fonte: Dados da pesquisa.

Assim como nos demais desdobramentos analisados, nas funções de *compliance*, as questões relativas à visão macro da empresa ficaram com percentuais superiores às demais questões. É possível verificar no quadro 9 que a conformidade com leis, normas e políticas internas ocupa o primeiro lugar dentre as prioridades, com um índice de 38,5%. A segunda priorização, com 24%, diz respeito ao alinhamento das normas externas com as normas internas.

Os critérios considerados de cunho operacional situam-se no centro no quadro 9, com índices de 15,2% e 11,4%, sendo eles o envolvimento do conselho de *compliance* no lançamento de produtos ou linha de negócios e a assessoria em questões regulatórias relevantes sobre os negócios da empresa.

Por fim, com prioridades relativamente baixas, de 5,7%, 3,3% e 1,9% encontram-se, respectivamente, o comprometimento da direção e dos administradores, a ética vista como forma de agir na organização e o fortalecimento da cultura de controles internos. Este último pode ser considerado um tanto quanto contraditório, uma vez que a maior prioridade relativa apresentada pelos respondentes justamente diz respeito à conformidade interna da empresa.

A seguir são apresentadas as considerações finais do estudo, respaldadas nas análises realizadas neste capítulo.

5 Considerações Finais

O estudo teve como objetivo analisar relacionamento existente entre a governança da tecnologia da informação, o gerenciamento do risco corporativo e as funções de *compliance*. Para isso foram realizadas entrevistas com cinco colaboradores de uma empresa de grande porte do ramo metalúrgico do Rio Grande do Sul, as quais foram analisadas pela metodologia AHP. Os resultados evidenciaram uma maior preocupação dos respondentes quanto ao gerenciamento do risco corporativo, com um índice de prioridade relativa de 73%. Em seguida, com um índice de prioridade de 22%, ficou a governança de TI. As funções de

compliance ficaram em último lugar, quanto a esta preocupação, com prioridade relativa de apenas 5%.

O desdobramento da matriz inicial (Tabelas 1 e 2) em outros 20 aspectos foi desenvolvido com o intuito de reforçar o relacionamento existente entre tais fatores e validar a matriz original. Os indicadores obtidos reforçam a ideia de que os colaboradores estão alinhados entre si e com a empresa quanto ao entendimento das prioridades dela. O primeiro desdobramento realizado, abordando o gerenciamento do risco corporativo evidenciou uma prioridade relativa de 39,44% para o critério que considera este como sendo um processo multidirecional e interativo. A empresa possui uma gestão de recursos (humanos, financeiros, entre outros) descentralizada, o que pode influenciar nas respostas obtidas. O segundo aspecto considerado com maior prioridade relativa foi o fato de o risco estar intrínseco em todas as atividades e a administração da empresa refletir nos processos de tomada de decisão, com um índice de 18,57%. É possível verificar que ambos tratam de questões estratégicas do negócio, que definem e delineiam a forma de atuação das lideranças da empresa.

Em relação à governança de TI, a média normalizada da prioridade relativa apresentou o ambiente, com um índice de 55%, seguido pelos arranjos de governança, com um índice de 25,1%. As respostas evidenciam baixo grau de importância para o desempenho financeiro com uma prioridade relativa de 2,50%, sendo este critério o de menor importância, para os respondentes, quanto ao assunto governança de TI.

Assim como nos demais desdobramentos analisados, nas funções de *compliance* (Tabelas 4 e 6), as questões com maiores percentuais foram aquelas relativas à visão macro da empresa. A conformidade com leis, normas e políticas internas ocupa o primeiro lugar dentre as prioridades, com um índice de 38,5%. A segunda priorização, com 24%, diz respeito ao alinhamento das normas externas com as normas internas.

A partir dos resultados obtidos é possível afirmar que a maior ênfase dos respondentes está no gerenciamento do risco corporativo. A preocupação com o desempenho da governança de TI e *compliance* não são tão latentes, quando comparadas com o gerenciamento do risco corporativo, em virtude da atual condição da empresa analisada. Esta possui um alto número de controles internos, focados no atendimento de legislações externas e atendimento à auditoria (externa e interna). Ainda, em termos de governança de TI, a empresa possui trimestralmente auditorias interna e externa que validam processos, controles internos e acessos concedidos.

Referências

AGUILERA, R.V.; CUERVO-CAZURRA, A. **Codes of good governance worldwide:** what is the trigger? Organization Studies, London, v. 25, n. 3, p. 417-446, 2004.

BEASLEY, M.S.; BRANSON, B.C.; HANCOCK, B.V. **Developing key risk indicators to strengthen enterprise risk management**, 2010. Disponível em: www.coso.org/.../COSOKRIPaperFull-FINALforWebPostingDec1. Acesso em: 22 nov 2016.

BROMILEY, P. et al. **Enterprise Risk Management: Review, Critique, and Research Directions**. Long Range Planning, v. 48, n. 1, p. 265-276, Jan. 2015.

COSO. **COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION.** Gerenciamento de Riscos Corporativos – Estrutura Integrada, 2007.

ETHICS RESOURCE CENTER. **Leading corporate integrity:** defining the role of the chief ethics & compliance officer (CECO). Washingtom: ERC, 2007.

HAHN, G. J; KUHN, H. Value-based performance and risk management in supply chains: A robust optimization approach. **International. Journal of Production Economics**, 2012.

IBGC. **Governança Corporativa. Instituto Brasileiro de Governança Corporativa**, 2015. Disponível em: http://www.ibgc.org.br. Acesso em: 25 nov 2016.

ISACA. COBIT 5: **Modelo Corporativo para Governança e Gestão de TI.** Rolling Meadows, IL (EUA): Information Systems Audit and Control Association, 2012.

JENSEN, M. C.; MECKLING, W. H. Theory of the firm: managerial behaviour, agency costs and ownership structure. **Journal of Financial Economics**, [S.l.], v. 3, n. 4, 1976.

KOW, W.T. Compliance function in financial institutions. **iFast Financial**, 2006

LEAL, R. P. C.; SAITO, R. Finanças corporativas no Brasil. **RAE Eletrônica**, São Paulo, v. 2, n. 2, 2003.

LONGO, E. **The knowledge management role in mitigating operational risk.** Synapsing, São Paulo, Brasil, p. 314-320, 2012.

MORAIS, E.J. **Controles internos e estrutura de decisão organizacional: o caso da Contadoria do Banco do Brasil.** Dissertação (Mestrado em Administração) – Universidade Federal do Paraná, Curitiba, 2005.

NEWTON, A. **The Handbook of Compliance** - making ethics work in financial services. The edition published by Mind into Matter. 2002.

NOCCO, B.W.; STULZ, R.M. Enterprise Risk Management: Theory and Practice. **Journal of Applied Corporate Finance**, 2006.

PARTOVI, F.; WHITERS, B.; BRADFORD, J. **How Tompkins rubber company used Analytic Hierarchy Process to enhance ISO-9000 related decision making, Production and Inventory Management Journal. Alexandria**, USA, v. 43, nºs 1 e 2, first/second quarters, 2002.

SAATY, T. **Método de análise hierárquica**. São Paulo: Makron, 1991.

SCHILDER, A. **Banks and the compliance challenge. Speech by the Professor Arnold Schilder, Chairmain of the BCBS Accounting Task Force and Executive Director of the Governing Board of the Netherlands Bank, at the Asian Banker Summit**, Bangkok, Mar 2006.

WEILL, P.; ROSS, J.W. Governança de TI, Tecnologia da Informação. Revisão Técnica: Tereza Cristina M. B. Carvalho. São Paulo: M. Books do Brasil Editora Ltda, 2006.