ENGEMA
Encontro Internacional sobre Gestão Empresarial e Meio Ambiente

Gestão de riscos de segurança da informação e governança de TI no setor público

JACKSON GOMES SOARES SOUZA
CEETEPS / IFSP
jackson.gomes@gmail.com

NEEMIAS DE MACEDO FERREIRA
CEETEPS
neemias.ferreira@gmail.com

LEONARDO YUKIO KUSSAMA
CEETEPS
2007leok@gmail.com

RENATA MARIA NOGUEIRA DE OLIVEIRA
CEETEPS
renata@gmail.com

CARLOS HIDEO ARIMA
CEETEPS
harima@arimaweb.com.br

Gestão de riscos de segurança da informação e governança de TI no setor público

Resumo – A informação é um recurso necessário para o desenvolvimento do ciclo de negócios das organizações, desde sua criação, até o momento em que é destruída. A Tecnologia da Informação (TI) desempenha um papel significativo neste processo, estando cada vez mais avançada e difundindo-se nas organizações, nos ambientes sociais, públicos e corporativos devendo, portanto, ser tratada como um ativo estratégico. A mensuração da performance é essencial para a governança de TI, e identificar os processos e controles críticos relacionados à mesma são fundamentais para que os executivos possam elevar esses processos ao nível de capacidade desejado. Devido à dificuldade encontrada por algumas organizações vinculadas ao setor público em avaliar os riscos inerentes às suas atividades, especialmente no que tange à segurança de seus ativos de informação e as possíveis vulnerabilidades da TI, este estudo apresenta uma revisão bibliográfica que fornece subsídios e proporciona uma visão concisa de como futuras pesquisas poderão verificar, por meio de indicadores, a forma pela qual a Gestão de Risco de Segurança da Informação pode ser apresentada na governança de TI do setor público.

Palavras-chave: Governança Corporativa, Governança de TI, Gestão de Riscos, Segurança da Informação.

Information security risk management and IT governance in the public sector

Abstract – Information is a necessary resource to develop organizations business cycle from its creation to the moment it is destroyed. Information Technology (IT) plays a significant role in this process by advancing and diffusing in organizations, social, public and corporate environments and should, therefore, be treated as a strategic asset. Measuring performance is essential for IT governance, while identifying critical processes and controls are essential for executives to reach the desired level of capacity. Considering the challenges experienced by some public institutions on evaluating the risks concerning their activities, especially regarding the security of their information assets and potential IT vulnerabilities, this issue presents a literature review that provides a concise view of how future research could measure, through indicators, how Information Security Risk Management can be presented on IT governance in the public sector.

Keywords: Corporate Governance, IT Governance, Risk Management, Information Security.

1. Introdução

A informação é um recurso necessário para o desenvolvimento do ciclo de negócios das organizações, desde sua criação, até o momento em que é destruída. A Tecnologia da Informação (TI) desempenha um papel significativo neste processo, estando cada vez mais avançada e difundindo-se nas organizações, nos ambientes sociais, públicos e corporativos devendo, portanto, ser tratada como um ativo estratégico. (ISACA, 2012).

A governança corporativa integra componentes de forma holística ao envolver princípios, processos, informação, serviços, infraestrutura, recursos humanos e *stakeholders* internos e externos responsáveis pela gestão destes componentes, proporcionando a estrutura pela qual os objetivos da organização são estabelecidos, assim como determinando e monitorando os meios para alcança-los (OECD, 2004).

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

Para o Instituto de Governança de TI – ITGI, a Governança de TI é um componente da governança corporativa, sendo de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que asseguram que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização, habilitando-a a obter todas as vantagens de sua informação, maximizando os benefícios, oportunidades e capacidade competitiva (ITGI, 2007).

Ainda segundo o ITGI, organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação ao utilizá-la para direcionar os valores das partes interessadas e gerenciar os riscos associados, tais como as crescentes demandas regulatórias e a dependência crítica de muitos processos de negócio da TI.

A mensuração da performance é essencial para a governança de TI, e identificar os processos e controles críticos relacionados à mesma são fundamentais para que os executivos possam elevar esses processos ao nível de capacidade desejado. A Figura 1 ilustra quatro áreas de foco que contribuem para que haja para que haja transparência dos custos, do valor e dos riscos de TI conforme o modelo de Objetivos de Controle para Informação e Tecnologias Relacionadas (COBIT) 4.1.

Figura 1 – Áreas de Foco na Governança de TI

Fonte: ITGI (2007), p.8

O processo de governança de TI envolve, deste modo, a gestão de riscos e esta, por sua vez, trata dos riscos relacionados à segurança da informação. A identificação e mensuração destes riscos é de grande interesse por parte dos gestores e demais envolvidos no processo de gestão de riscos de segurança da informação por proporcionar maior controle quanto às incertezas e o impacto destas no objetivo do negócio.

Portanto, este estudo se justifica pela dificuldade encontrada por algumas organizações em avaliar os riscos e oportunidades inerentes às suas atividades, especialmente no que tange à segurança de seus ativos de informação e a TI, buscando responder ao seguinte questionamento: Como a Gestão de Risco de Segurança da Informação pode ser apresentada na governança de TI do setor público?

2. Revisão bibliográfica

2.1 Governança corporativa

Governança é uma palavra que traz consigo a conotação de sabedoria e responsabilidade; de o que é apropriado. Pode ser definida como o sistema pelo qual as empresas são dirigidas e controladas (CADBURY, 1992) e tem como significado tanto a ação ou o método de governar, sendo este último o mais utilizado como referência pelas empresas.

Artero (2007) afirma que, dentre as possíveis definições para governança, as que demonstram particular relevância são as de controlar, direcionar e regular; a maneira como algo é administrado, gerenciamento e o sistema de regulação. Destaca ainda que a definição do termo corporação inclui um corpo de pessoas unidas, autorizados legalmente a agir como um único indivíduo, criados e regidos por certos direitos e deveres.

Para o Instituto Brasileiro de Governança Corporativa – IBGC, governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle (IBGC, 2015). As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.

O ITGI (2003) destaca que são os valores das partes interessadas que impulsionam o empreendimento, de modo que a definição da estratégia, o desempenho, os recursos e a gestão de riscos são núcleos de responsabilidade da governança corporativa, englobando assim as relações entre a administração da entidade e seu corpo diretivo, seus proprietários e demais partes interessadas, fornecendo a estrutura pela qual:

- Os objetivos globais da entidade são definidos.
- O método para se atingir esses objetivos é determinado.
- A maneira como o desempenho será mensurado.
- Os recursos serão utilizados de forma responsável.
- Os riscos serão adequadamente gerenciados.

A governança corporativa é um processo metódico de avaliação e é moldada para os sistemas de decisão (ALEXANDER, 2000; BRIS et al., 2008) e, apesar de não haver um modelo único, é possível identificar elementos em comum que delimitam as boas práticas de governança corporativa (OECD, 2004).

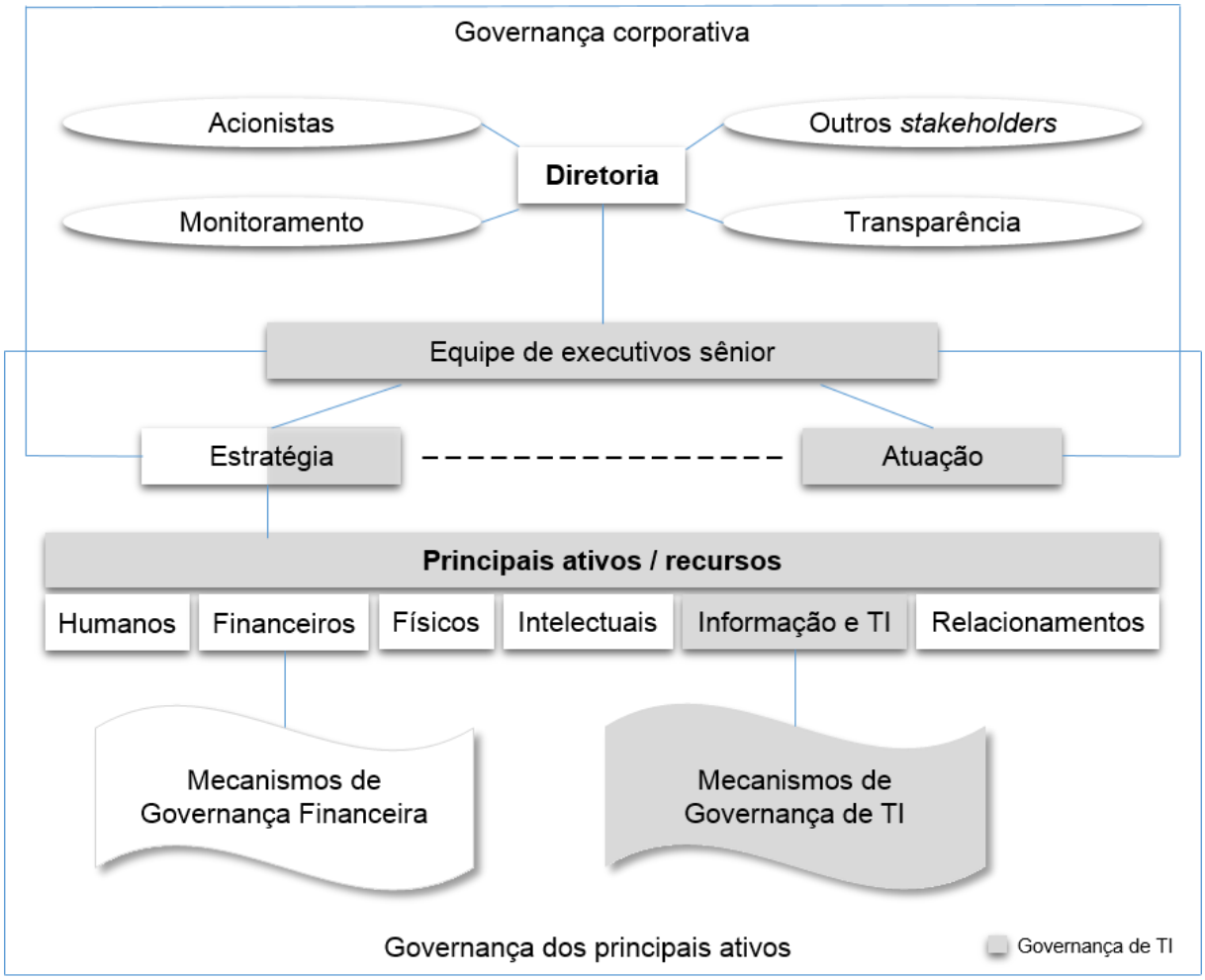
A governança pode ser aplicada a diversas áreas da empresa e a direção da organização geralmente possui como foco a eficiência, redução de custos e ampliação da a receita e

capacidades, os quais estão interligados com a informações e a Tecnologia da Informação (TI), sendo vital considerar a TI como um importante ativo (HARDY, 2006).

Segundo o IBGC (2015), a governança corporativa surgiu para superar o "conflito de agência" clássico. Nesta situação, o proprietário (acionista) delega a um agente especializado (administrador) o poder de decisão sobre a empresa (nos termos da lei), situação em que podem surgir divergências no entendimento de cada um dos grupos daquilo que consideram ser o melhor para a empresa e que as práticas de governança corporativa buscam superar. Este tipo de conflito é mais comum em sociedades como os Estados Unidos e Inglaterra, onde a propriedade das companhias é mais pulverizada.

De forma a integrar os principais ativos ou recursos de governança corporativa e governança de TI, Weill e Ross (2007) propõem um modelo, representado pela Figura 2, que contempla as relações da diretoria com a equipe de executivos sênior como agentes articuladores de estratégias, atuando para executá-las conforme a necessidade da diretoria.

Figura 2 – Governança Corporativa e dos Principais Ativos



Fonte: Weill e Ross (2004), p.5

Portanto, é possível concluir que a Governança Corporativa é primeiramente de responsabilidade da alta direção ao criar valor por meio de seus principais ativos, consistindo em aspectos de liderança e atuação estratégica, onde os mecanismos de governança criados pelos executivos integram a estrutura organizacional de forma independente ou interligada

buscando garantir que as diversas áreas, assim como a de TI, suporte e aprimore os objetivos da organização.

2.2 Governança de TI e o setor público

Cada vez mais a Tecnologia da Informação (TI) é vista como um importante ativo das empresas, sejam públicas ou privadas, agindo como uma força motriz que provê soluções cada vez mais complexas, de modo que sua governança é um fator crítico de sucesso (HARDY, 2006).

Como consequência, as organizações e seus executivos se esforçam para manter informações de alta qualidade que irão apoiar decisões corporativas de modo a agregar valor ao negócio a partir dos investimentos em TI, atingindo objetivos estratégicos pela utilização eficiente de TI (ISACA, 2012).

Visando aprimorar o foco neste sentido, integrantes do Comitê Técnico de Tecnologia da Informação desenvolveram um guia de governança para gerenciamento de processos e decisões relativas à informação e serviços de comunicação utilizados pelas organizações, de modo que estes processos pudessem ser controlados por especialistas de TI: a norma ISO/IEC 38500/2008.

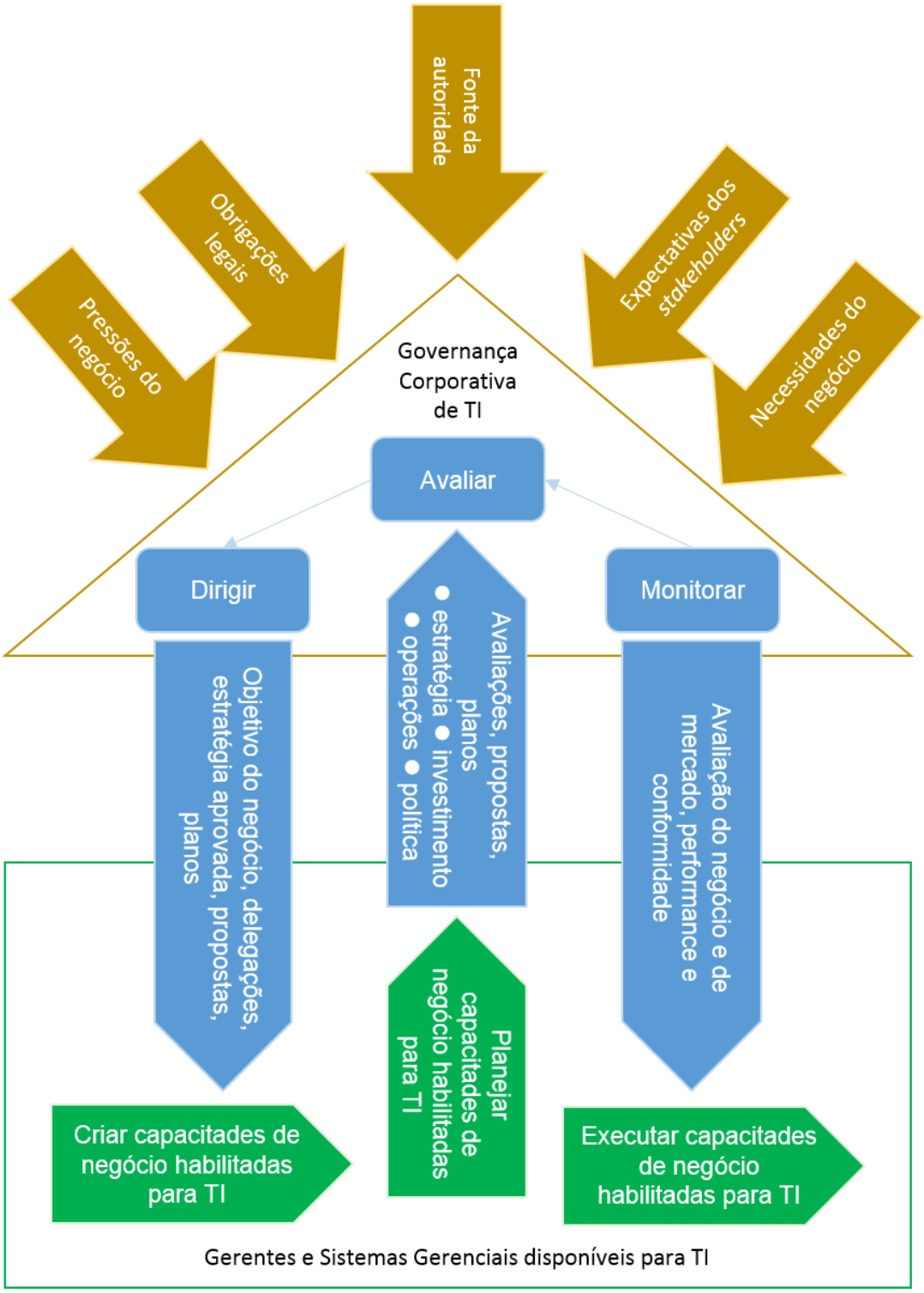
Baseando-se na norma supracitada, a Associação Brasileira de Normas Técnicas (ABNT) elaborou a NBR ISO/IEC 38500/2009, cujo objetivo é fornecer uma estrutura de princípios que possam ser utilizados pelos dirigentes na avaliação, tomada de decisão, gerenciamento e monitoramento do uso da Tl em suas organizações.

Os princípios elencados pela norma são:

- Responsabilidade: Os indivíduos e grupos da organização compreendem suas responsabilidades e atuam respeitando a demanda de TI.
- Estratégia: A estratégia de negócio considera as capacidades atuais e futuras de TI
- Aquisição: As aquisições de TI possuem razões válidas embasadas em análises transparentes, contínuas e apropriadas.
- Desempenho: A TI se adequa e apoia a organização fornecendo serviços baseados em níveis e com qualidade.
- Conformidade: A TI cumpre com toda a legislação e regulamentos obrigatórios, possuindo políticas e práticas claramente definidas, implementadas e fiscalizadas.
- Comportamento humano: As políticas, práticas e decisões de TI demonstram respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas.

Juiz e Toomey (2015) destacam em seus estudos que agregar valor envolve planejamento, liderança, controle e corroboram com a abordagem destes princípios de modo a orientar a governança de TI e apoiar líderes no planejamento, construção e execução das capacidades de TI. Baseando-se na norma ISO/IEC 38500, apresentam um modelo conceitual de governança de TI, que ilustra, conforme a Figura 3, as atividades de governança, gerenciamento e objetivo do negócio para a utilização efetiva de TI pela perspectiva dos diretores.

Figura 3 – Modelo para a governança de TI baseado na norma ISO/IEC 38500



Fonte: Modificado por Juiz e Toomey (2015), p.61

A TI se tornou, portanto, uma espécie de habilitador estratégico de negócio, sendo interessante que organizações ampliem ainda mais sua abrangência de modo a agilizar o alinhamento dos objetivos do negócio e aprimorar produtos e serviços (LUNARDI et al. 2014).

Segundo Raghupathi (2007), a governança de TI reflete na liderança, nas estruturas organizacionais e nos processos, certificando-se de que a TI apoie e amplie as estratégias e

objetivos organizacionais e, Lunardi et al. (2012) aponta para o fato de que algumas empresas que podem melhorar seu desempenho por meio da governança de TI. Seus estudos permitiram concluir que o desempenho organizacional de um grupo de empresas que havia adotado mecanismos formais de governança de TI melhorou significativamente quando comparado ao grupo que não adotava tais mecanismos, os quais vêm sendo essencialmente adotados por empresas para aumentar sua eficiência, reduzir custos e aprimorar a utilização da infraestrutura de TI.

Em diversos países, mais de um terço da economia consiste em organizações governamentais incluindo educação, saúde e serviços que, de forma similar às organizações com fins lucrativos, utilizam serviços e infraestrutura de TI adquiridos por meio de seus recursos. Porém, o desempenho da governança nestas organizações é geralmente baixo e, uma governança de TI efetiva deve abordar os seguintes questionamentos: Quais decisões devem ser tomadas? Quem deveria tomar estas decisões? Como tomadas e monitorar essas decisões? (WEILL, 2004).

Weill e Woodham (2002) reiteram que a governança de TI não pode ser considerada de forma isolada, pois relaciona a governança de outros ativos da empresa que, por sua vez, estão interligados à governança corporativa, destacando as 5 (cinco) principais decisões a serem tomadas pela governança de TI:

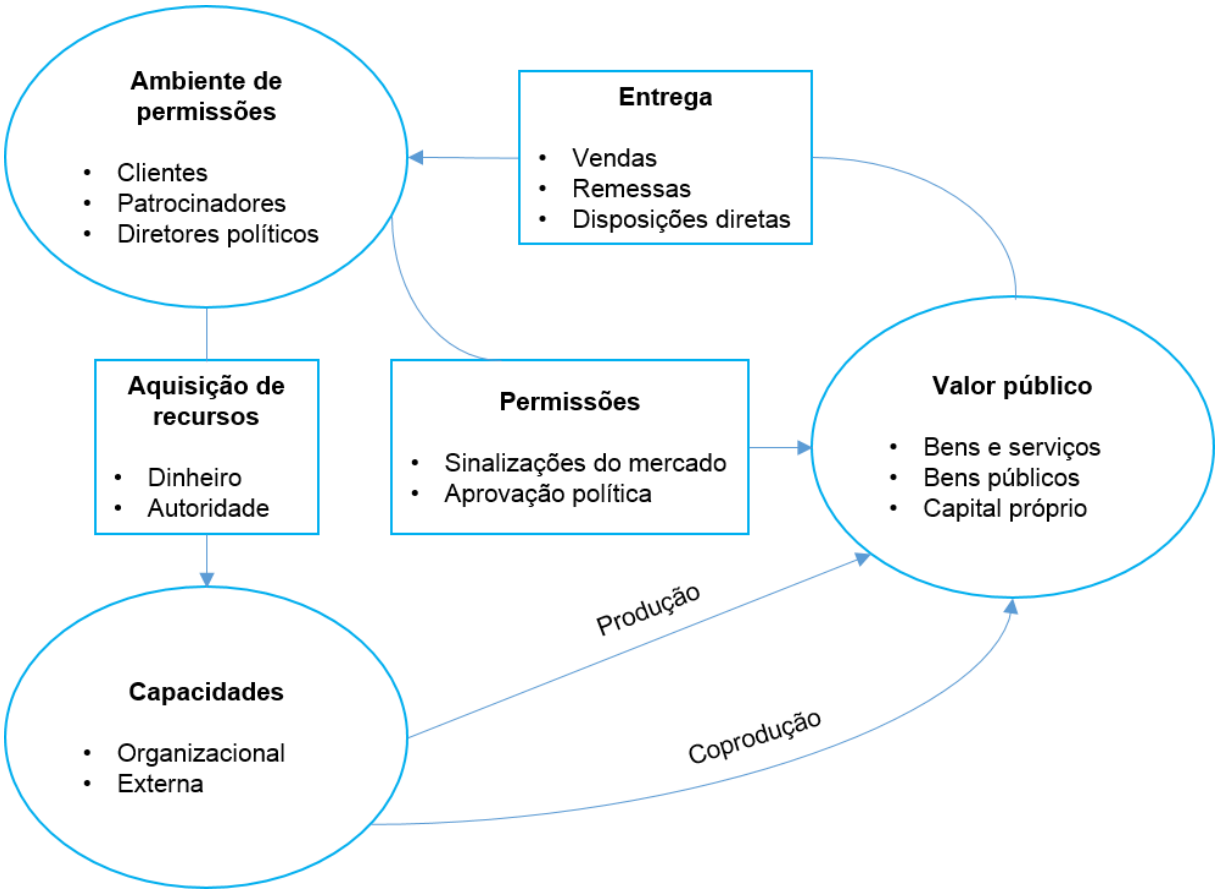
- Princípios de TI: Demonstrações de alto nível quanto à utilização de TI nos negócios.
- Arquitetura de TI: Organização lógica para os dados, aplicações e infraestruturas visando integrar os negócios à tecnologia de forma padronizada.
- Infraestrutura de TI: Serviços de TI centralizados e coordenados como alicerces das capacidades de TI da organização.
- Aplicações de TI: Especificação das necessidades do negócio para a aquisição de aplicações de TI ou implementação de aplicações de TI internas.
- Priorização de investimentos em TI: Quando e onde investir em TI, incluindo aprovações de projetos e justificativas técnicas.

Diante destas decisões, percebe-se que criar valor por parte da TI é bastante complexo. O conceito de valor no ambiente público é extremamente amplo e, segundo Weill e Ross (2004), as complexidades a serem mensuradas podem abordar performance, transparência, investimento em infraestrutura, liberdade de atuação, redução de custos e outros. As habilidades, o conceito de valor e o ambiente no qual atuam estas organizações cria desafios para a governança de TI e, buscando alinhar estes fatores, os autores adaptaram um modelo, ilustrado pela Figura 4, de criação de valor voltado a gerentes de organizações públicas.

Thompson et al. (2013) afirma que é papel dos gestores alinhar os investimentos de TI com a estratégia da organização, buscando minimizar custos de tecnologia, assegurando que a infraestrutura de TI possa acomodar e se adequar à utilização crescente de novas aplicações.

Desta forma, para manter a organização alinhada ao seu negócio estratégico, os diretores, gerentes executivos e gestores devem entender como atuar em relação à governança de TI, dando a esta o mesmo nível de atenção desprendido aos demais ativos da organização.

Figura 4 – Modelo de criação de valor voltado a gerentes de organizações públicas



Fonte: Weill e Ross (2004), p.191

2.3 Gestão de riscos de segurança da informação

O risco é inerente a toda atividade humana. A capacidade de definir o que acontecerá no futuro e optar entre várias alternativas é central às sociedades contemporâneas. A administração do risco nos guia por uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros e isto inclui a informação e a complexa tecnologia envolvida em seu processo (BERNSTEIN, 1997).

As organizações enfrentam influências de fatores e externos incertos que afetam seus objetivos. De modo a reduzir incertezas, é necessário monitorar e identificar o risco de modo a avaliar se este deve ser modificado ou tratado, uma vez que sua compreensão nos permite tomar decisões de modo racional. (ISO, 2009)

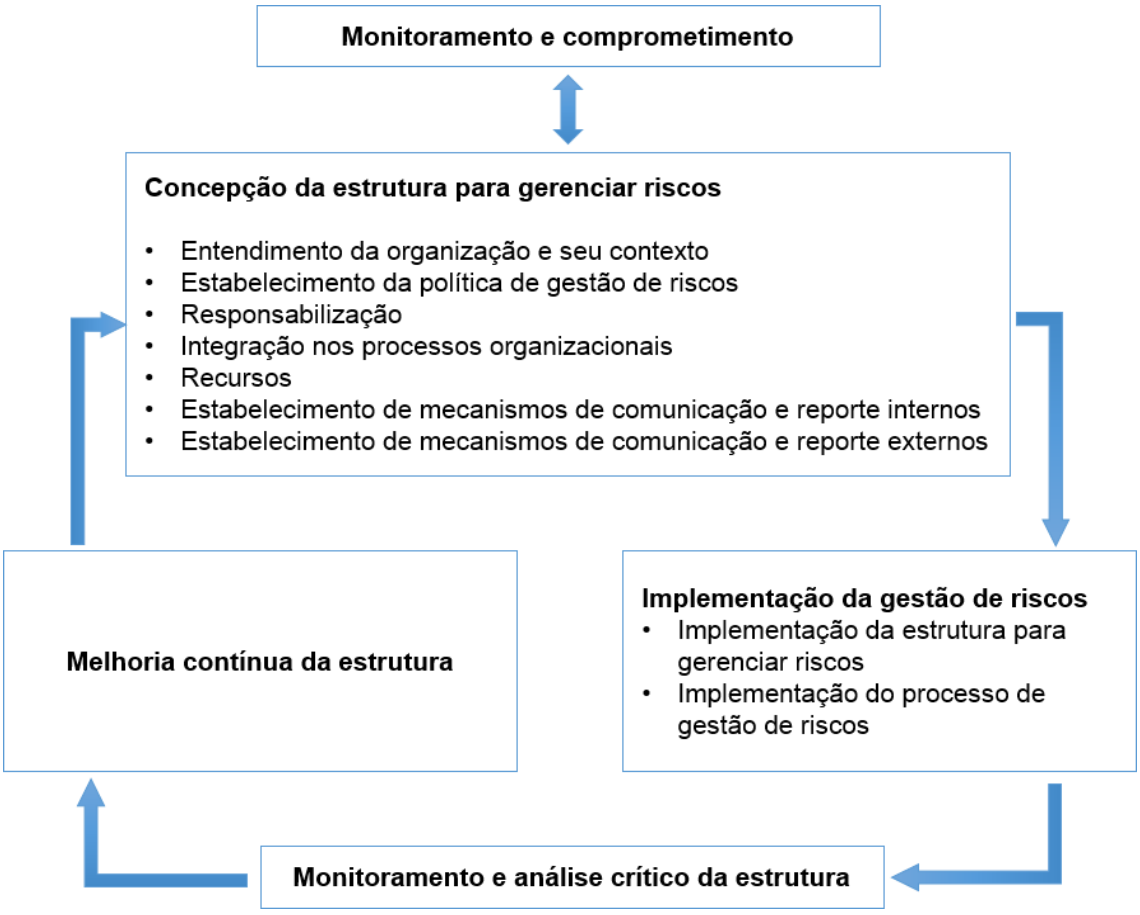
Atualmente, os padrões de governança de risco tendem a ser de alto nível, porém existe margem para sua aplicação em diferentes empresas e situações. Bromiley et al. (2015), destacam que as potenciais particularidades e desafios na avaliação do risco oferecem também oportunidades para que as organizações observem problemas em seus processos internos.

Segundo a OECD (2014), as instituições públicas podem adotar práticas de governança similares às adotadas por empresas privadas, sendo crucial que haja o controle de risco tanto

pela ação direta dos gestores, assim como por delegações dos diretores, que podem se utilizar de qualquer oportunidade para formular diretivas estratégicas e de liderança. O objetivo da governança é criar valor por meio da realização de benefícios e otimização dos riscos e recursos, portanto uma governança de TI eficiente gerencia e avalia constantemente as atividades e os riscos relativos à TI de modo a mantê-los em um nível aceitável (ITGI, 2007; ISACA, 2012).

A norma ABNT NBR ISO 31000/2009 fornece princípios e diretrizes para a gestão de riscos e pode ser aplicada tanto no setor público ou privado, assim como avaliar qualquer tipo de risco, independentemente de sua natureza. Segundo a norma, o sucesso da gestão de riscos depende da estrutura de gestão – ilustrada pela Figura 5 –, que irá fornecer fundamentos e arranjos de modo a incorporar este processo a toda a organização, auxiliando a gerenciar os riscos de maneira eficaz por meio de sua aplicação em diferentes níveis e contextos organizacionais e assegurando que o risco seja adequadamente identificado e reportado, podendo, assim, ser utilizado como base na tomada de decisões.

Figura 5 – Relacionamento entre os componentes da estrutura de gerenciamento de riscos



Fonte: ABNT (2009), p.9

Hardy (2006) afirma que uma pequena brecha, roubo, erro, violação de sistema ou ataque de vírus na TI pode resultar em sérios danos ao orçamento e reputação da organização. Por consequência disto, os gerentes, *stakeholders*, funcionários e clientes se preocupam com a segurança das informações. Os diretores e os conselhos de administração devem, portanto, buscar meios de assegurar a proteção dos ativos de informação organizacional.

A norma ABNT NBR ISO/IEC 27005/2011 por sua vez apresenta diretrizes para o processo de Gestão de Riscos de Segurança da Informação (GRSI) e pode ser aplicada em

organizações públicas ou privadas que pretendam gerir riscos relacionados à segurança da informação organizacional.

Segundo a referida norma, o processo de GRSI pode ser utilizado de forma iterativa na avaliação ou para atividades de tratamento de risco. Seu enfoque iterativo torna possível o detalhamento da avaliação a cada repetição, minimizando o tempo e esforço necessários na identificação de controles, assegurando que riscos de alto impacto e probabilidade sejam adequadamente avaliados.

A gestão de risco pode ser vista, portanto, como uma atividade holística que envolve todos os aspectos da organização NIST (2010), e seu processo de gestão busca fornecer uma base sólida para que seja possível determinar quais riscos são aceitáveis, assim como obter informações necessárias ao seu tratamento (PURDY, 2010). Não obstante, prevenir perda, dano, destruição ou acesso não autorizado à informação organizacional é um processo contínuo, uma vez que a constante evolução dos riscos internos e externos podem resultar em violações e perdas para a organização como um todo (VEIGA; MARTINS, 2015).

3. Metodologia

A pesquisa realizada neste trabalho pode ser classificada como qualitativa e exploratória que, segundo Sampieri et al. (2006), é baseada em um processo indutivo que explora, descreve e em seguida gera perspectivas teóricas.

Akabane (2012) destaca que uma das metodologias utilizadas na gestão de riscos e protocolos de segurança leva em conta processo de definição e análise dos perigos inerentes os indivíduos, empresas e agências governamentais, os quais ser provocados pelo agente natural e/ou humano e causados por eventos adversos, podendo ainda ser de natureza quantitativa ou qualitativa. A análise qualitativa de riscos, utilizada com maior frequência, envolve a definição de várias ameaças e seu grau de vulnerabilidade, podendo ser utilizada em TI para alinhar os objetivos relacionados à tecnologia aos objetivos de negócio da empresa.

Desta forma, o levantamento de dados em bases acadêmicas, livros, artigos, periódicos, congressos e normas técnicas apresentada no item 2, buscou proporcionar uma visão de como Gestão de Riscos de Segurança da Informação poderá ser apresentada à Governança de TI do setor público.

4. Apresentação e Análise dos Resultados

Para algumas organizações a informação e a tecnologia que a suporta representam o seu bem mais valioso. Elas reconhecem os benefícios da tecnologia da informação e a utilizam para direcionar os valores das partes interessadas no negócio. No mercado global atual, capacitado pela Internet e tecnologias avançadas, a dependência crítica de muitos processos de negócios da TI exige que as organizações gerenciem os riscos associados e cumpram um crescente número de exigências legais e regulatórias. (ITGI, 2012)

Valor, risco e controle constituem a essência da governança de TI e, a necessidade da avaliação do valor, o gerenciamento dos riscos e as crescentes necessidades de controle sobre as informações de TI são agora vistos como elementos-chave da governança corporativa. (ITGI, 2007)

Deste modo, na Administração Pública cabe à Governança de TI atender às normas e aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência (BRASIL, 1988), para que a TI agregue valor ao negócio. Normas como a ABNT NBR ISO/IEC 38500/2009 e ABNT NBR ISO/IEC 31000/2009 apresentam diretrizes que auxiliam órgãos públicos a atenderem alguns destes estes princípios.

Este estudo se justifica pela dificuldade encontrada por algumas organizações em avaliar os riscos inerentes às suas atividades, especialmente no que tange à segurança de seus ativos de informação e as possíveis vulnerabilidades da TI, buscando, ainda, contribuir para que as incertezas envolvidas neste processo possam ser mitigadas.

Para a verificação de como Gestão de Risco de Segurança da Informação (GRSI) está sendo implementada e a forma como ela é apresentada na Governança de TI (GTI), sugere-se o levantamento de indicadores e a verificação de conformidade às boas práticas.

Os indicadores poderiam ser fragmentados em de 2 (dois) grupos de indicadores obtidos por meio de questionamentos elaborados e fundamentados com base em pesquisas científicas e nas normas NBR ISO/IEC 38500, 31000 e 27005.

- 1º grupo de indicadores: GTI
- 2º grupo de indicadores: GRSI

Para o levantamento dos indicadores do primeiro grupo, poderiam ser considerados os princípios elencados pelo ISACA (2012) em seu modelo corporativo para governança e gestão de TI (COBIT 5), os quais estão em conformidade com a norma e ISO/IEC 38500 e permitirão uma avaliação de alto nível do comprometimento da organização com a Governança de TI.

Exemplo de questionamentos para o 1º grupo:

- Os indivíduos e grupos da organização compreendem suas responsabilidades e atuam respeitando a demanda de TI?
  - Indicador: Responsabilidade
- A estratégia de negócio considera as capacidades atuais e futuras de TI?
  - Indicador: Estratégia
- As aquisições de TI possuem razões válidas embasadas em análises transparentes, contínuas e apropriadas?
  - Indicador: Aquisição
- A TI se adequa e apoia a organização fornecendo serviços baseados em níveis e com qualidade?
  - Indicador: Desempenho
- A TI cumpre com toda a legislação e regulamentos obrigatórios, possuindo políticas e práticas claramente definidas, implementadas e fiscalizadas?
  - Indicador: Conformidade
- As políticas, práticas e decisões de TI demonstram respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas?
  - Indicador: Comportamento humano

Para o levantamento dos indicadores do segundo grupo, poderia ser feita uma avaliação de alto nível que, conforme a normas ABNT ISO/IEC 31000/2009 e 27005/2011, permite identificar os riscos com alto potencial impacto ao negócio e, consequentemente, o nível de comprometimento da organização com a GRSI.

Exemplo de questionamentos para o 2º grupo:

- Qual o nível de apoio e compreensão dos diretores quanto aos riscos inerentes à TI e seus impactos para o negócio?
  - Indicador: Nível de apoio e entendimento da governança
- Os controles implementados pelos gerentes de TI atendem aos requisitos do negócio?
  - Indicador: Conformidade dos controles com o objetivo do negócio
- A organização atende aos requisitos legais e normativos de segurança da informação?

    - Indicador: Conformidade legal e normativa
- Em que nível a segurança da informação relacionada aos ativos de informação atende as expectativas e percepções dos *stakeholders*?
    - Indicador: Conformidade com os interesses dos *stakeholders*
- Qual o valor estratégico do processo que trata as informações do negócio?
    - Indicador: Valor estratégico das informações
- Qual a criticidade dos ativos de informação envolvidos com as informações do negócio?
    - Indicador: Valor crítico das informações
- Qual a importância, do ponto de vista do negócio, da disponibilidade, confidencialidade e integridade das informações?
    - Indicador: Importância da informação para o negócio
- Qual a importância, do ponto de vista operacional, da disponibilidade, confidencialidade e integridade das informações?
    - Indicador: Importância da informação para o operacional
- Com que frequência ocorrem perdas da disponibilidade, confidencialidade e integridade de informações?
    - Indicador: Frequência de perda de informações
- Qual o nível de importância das operações comprometidas com a TI?
    - Indicador: Nível de comprometimento operacional com a TI
- Qual o nível do impacto para o negócio da perda de informação causada por um incidente de segurança da informação?
    - Indicador: Impacto da perda de informações
- Qual o impacto para da interrupção do negócio causado por um incidente de segurança da informação?
    - Indicador: Impacto da interrupção do negócio
- Qual o nível do impacto causado por um incidente de segurança da informação para a reputação da organização?
    - Indicador: Impacto na reputação
- Qual impacto o não atendimento de requisitos legais e normativos de segurança da informação trariam para o negócio?
    - Indicador: Impacto de violação legal

Para cada um dos grupos, poderá ser atribuído aos respectivos indicadores um valor de escala numérica, de modo que a análise dos resultados permitiria ao pesquisador verificar como a Gestão de Risco de Segurança da Informação pode ser apresentada na governança de TI.

5. Considerações finais

Apesar das dificuldades de detecção e prevenção de ameaças e oportunidades, Akabane (2012) destaca que uma das metodologias utilizadas na gestão de riscos e protocolos de segurança leva em conta processo de definição e análise dos perigos inerentes os indivíduos, empresas e agências governamentais, os quais ser provocados pelo agente natural e/ou humano e causados por eventos adversos, podendo ainda ser de natureza quantitativa ou qualitativa. A análise qualitativa de riscos, utilizada com maior frequência, envolve a definição de várias ameaças e seu grau de vulnerabilidade, podendo ser utilizada em TI para alinhar os objetivos relacionados à tecnologia aos objetivos de negócio da empresa.

Futuros estudos podem utilizar-se da ferramenta do estudo de caso que, segundo Yin (2001), permite uma investigação que preserva as características holísticas e significativas dos eventos da vida real – tais como ciclos de vida individuais, processos organizacionais e

administrativos, mudanças ocorridas em regiões urbanas, relações internacionais e a maturação de alguns setores.

Há ainda, portanto, vasto campo de trabalho quanto à avaliação e aplicação prática deste estudo em futuras pesquisas.

Referências

ABNT. **NBR ISO 31000 – Governança corporativa de tecnologia da informação**. Associação brasileira de normas técnicas. Rio de Janeiro, 2009. 32p

ABNT. **NBR ISO/IEC 38500 – Governança corporativa de tecnologia da informação**. Associação brasileira de normas técnicas. Rio de Janeiro, 2009. 21p.

ABNT. **NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação**. Associação brasileira de normas técnicas. Rio de Janeiro, 2011. 87p.

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

ALEXANDER, Lucy. *Corporate governance and cross-border mergers.* ***Conference Board Research Report***, Nova York, jun. 2000.

ARTERO, Juan P.. ***Corporate Governance: The revival of an academic, professional and policy field***. Bronx, NY, p.1-25, dez. 2007.

BERNSTEIN, Peter L.. **Desafio aos Deuses**: A fascinante história do risco. Rio de Janeiro: Campus, 1997. 212 p. Tradução de: Ivo Korytowski.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRIS, Arturo; BRISLEY, Neil; CABOLIS, Christos. *Adopting better corporate governance: Evidence from cross-border mergers.* ***Journal of Corporate Finance***, Grécia, v. 3, n. 14, p.224-240, fev. 2008.

BROMILEY, Philip et al. *Enterprise Risk Management: Review, Critique, and Research Directions.* ***Long Range Planning***, [S.l.], v. 48, n. 1, p.265-276, jan. 2015.

CADBURY, Adrian. ***The Financial Aspects of Corporate Governance***. Londres: *Committee on the Financial Aspects of Corporate Governance*, 1992. 90 p.

CHAU, S L. ***An Anatomy of Corporate Governance***. *Hang Seng Management College*, Hong Kong, p.1-16, dez. 2011.

HARDY, Gary. *Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges.* ***Information Security Technical Report***, [S.l.], v. 11, n. 1, p.55-61, jan. 2006. Disponível em: <http://dx.doi.org/10.1016/j.istr.2005.12.004>. Acesso em: 03 jun. 2015.

IBGC. **Governança Corporativa**. Instituto Brasileiro de Governança Corporativa, 2015. Disponível em: <http://www.ibgc.org.br/>. Acesso em: 12 jun. 2015.

ISACA. **COBIT 5: Modelo Corporativo para Governança e Gestão de TI**. Rolling Meadows, IL (EUA): *Information Systems Audit and Control Association*, 2012. 98p.

ISO. ***ISO 31000 – Risk Management: Principles and guidelines***. Suiça: *International Organization for Standardization*, 2009. 36 p.

ITGI. ***Board Briefing on IT Governance***, *Second Edition*. Rolling Meadows, IL (EUA): *IT Governance Institute,* 2003. 7 p.

ITGI. **COBIT 4.1: Objetivos de Controle para Informações e Tecnologias Correspondentes**. Rolling Meadows, IL (EUA): *IT Governance Institute*, 2007. 212 p.

ITGI. ***Enterprise Value Governance of IT Investments – The Val IT Framework 2.0 Extract***. Rolling Meadows, IL (EUA): *IT Governance Institute*, 2008. 45p.

JUIZ, Carlos; TOOMEY, Mark. *To govern IT, or not to govern IT?* ***Communications of the ACM***, [S.l.], v. 58, n. 2, p.58-64, fev. 2015.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Um estudo empírico do impacto da governança de TI no desempenho organizacional. **Produção**, v. 22, n. 3, p. 612-624, maio/ago 2012.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G.; DOLCI, P. C.. *The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms.* ***International Journal of Accounting Information Systems***, [S.I,], v. 15, n. 1, p.66-81, mar. 2014.

NIST. ***Guide for Applying the Risk Management Framework to Federal Information Systems****: A Security Life Cycle Approach*. 800-37 ed. Gaithersburg, *National Institute of Standards and Technology*, 2010. 93 p.

OECD. ***Principles of Corporate Governance***. *Organization for Economic Co-operation and Development. OECD Publishing*. Disponível em: <http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf>. Acesso em: 10 jun. 2015.

OECD. ***Risk Management and Corporate Governance***. *Organization for Economic Co-operation and Development. OECD Publishing*. Disponível em: < http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf>. Acesso em: 09 jun. 2015.

PURDY, Grant. ISO 31000: 2009 - *Setting a New Standard for Risk Management.* ***Risk Analysis***, [S.l.], v. 30, n. 6, p.881-886, 8 abr. 2010.

RAGHUPATHI, W. *Corporate governance of IT: A framework for development.* ***Communications of the ACM***, [S.l.], v. 8, n. 1, p.94-99, ago. 2007.

SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, Maria P. B.. ***Metodología de la Investigación***. 4ª ed. México, MX. Mac Graw Hill, 2006. 736 p.

THOMPSON, Steven et al. *A model to support IT infrastructure planning and the allocation of IT governance authority.* ***Decision Support Systems***, [S.l.], v. 59, n. 1, p.108-118, nov. 2013.

VEIGA, Adéle da; MARTINS, Nico. *Information security culture and information protection culture: A validated assessment instrument.* ***Computer Law & Security Review***, [S.l.], v. 31, n. 2, p.243-256, abr. 2015.

WEILL, Peter. *Don't just lead, govern: How top-performing firms govern IT*. ***Center For Information Systems Research***, Massachusetts, v. 3, n. 1, 17p, mar. 2004.

WEILL, Peter; ROSS, Jeanne W. ***IT governance: how top performers manage IT decisions rights for superior results***. Boston: HBS Press, 2004.

WEILL, Peter; WOODHAM, Richard. *Don't Just Lead, Govern: Implementing Effective IT Governance.* ***Center For Information Systems Research***, Massachusetts, v. 326, n. 1, 20 p, abr. 2002.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. Porto Alegre: Bookman, 2001.