18th CONTECSI USP – International Conference on Information Systems and Technology Management

Consórcio Doutoral

Título: RISCOS CIBERNÉTICOS E ESTRUTURAS DE GOVERNANÇA: ESTUDO DA MITIGAÇÃO DE RISCOS NO SETOR DE SERVIÇOS

Márcia Cristiane Rossi
e-mail: marciarossi@hotmail.com
Contato: (11) 99483-9448

PPGA - Programa de Pós-Graduação em Administração
Universidade Presbiteriana Mackenzie
Prof. Dr. Gilberto Perez
e-mail: gilbertoperez@mackenzie.br

Área Temática
SEC – Segurança em SI e TI, Computação Forense

RISCOS CIBERNÉTICOS E ESTRUTURAS DE GOVERNANÇA: ESTUDO DA MITIGAÇÃO DE RISCOS NO SETOR DE SERVIÇOS

RESUMO

Com este estudo pretende-se analisar os riscos cibernéticos, compreendendo como as estruturas de governança podem afetar o setor de serviços. A temática do risco cibernético tem sido caracterizada pelos danos e perdas financeiras na ocorrência do mau funcionamento no ambiente digital ou quando dados são negligenciados, subtraídos ou compartilhados ilegalmente. Partindo dos trabalhos desenvolvidos por Williamson, apresenta-se neste estudo a oportunidade de compreensão da influência dos custos de transação, acrescentando o ambiente cibernético como um dos tipos das especificidades das transações. Igualmente, será compreendido os custos de transação sob as dimensões da incerteza e da frequência, além dos pressupostos comportamentais mediante as ocorrências de ameaças cibernéticas. Pretende-se realizar uma pesquisa exploratória com entrevistas semiestruturadas com atores do setor de serviços. Os objetivos específicos propostos são: (i) analisar as formas complexas de contratação e os mecanismos de mitigação de riscos cibernéticos; (ii) avaliar os mecanismos utilizados pelas organizações; (iii) avaliar a influência dos riscos cibernéticos sobre os custos de transação. Pretende-se que este estudo contribua para o desenvolvimento das organizações, inclusive pequenas e médias, à medida em que os recursos vinculados às perdas possam ser realocados para a atividade econômica da organização, enquanto blinda processos contra crimes cibernéticos.

Palavras-chave: Riscos cibernéticos. Estruturas de Governança. Teoria dos Custos de Transação. Mitigação de Riscos. Setor de Serviços.

1. INTRODUÇÃO

As organizações têm manifestado a necessidade de melhor posicionamento perante a sociedade e muitas delas passaram a compreender que sustentabilidade não é uma ação isolada, mas necessária para gerenciar e mitigar quaisquer riscos, sejam eles do próprio negócio bem como, advindos da sua cadeira de valor. Tal assunto demanda importância pela crescente complexidade e expansão dos mercados, ao exigirem que as empresas busquem conformidade e qualidade em seus processos.

No entanto, a preocupação com ameaças digitais em riscos cibernéticos tem permanecido em segundo plano na agenda dos CEOs no mundo. Esta constatação ganha reforço em estudos, dentre eles, uma pesquisa realizada pela Marsh em parceria com a Microsoft que envolveu 168 empresas brasileiras num total de 600 globais, cujo resultado revelou que 61% destas empresas não possuem seguro com cobertura de risco cibernético, enquanto 22% não souberem responder se a empresa investe neste tipo de seguro (Funke, 2021).

Ainda que haja investimento na criação de processos de controles, normas, políticas internas, treinamentos, além das tecnologias como suporte no combate aos riscos cibernéticos, estes mecanismos demonstram ser pouco efetivos ou negligenciados, permitindo que terceiros possam apropriar-se de informações confidenciais e/ou desviem recursos financeiros.

Risco cibernético pode ser considerado um conceito amplo e utilizado de forma multidisciplinar, tanto que não há consenso teórico sobre esta temática, sendo a complexidade envolvida em seu processo operacional um dos motivos mais aceito. Neste aspecto, a indústria de serviços cuja nomenclatura é reconhecida mundialmente, baseia-

se num setor que está presente em todos os demais segmentos do mercado, e por isso, assume-se que são disponibilizados e distribuídos para todas as pessoas.

Em constante migração de mão-de-obra desde a revolução industrial, o setor de serviços configura-se como a coprodução de valores por pessoas, tecnologia, sistema de serviços internos, externos e informações compartilhadas. A representatividade deste setor pode ser destacada por sua participação das atividades de serviços no Produto Interno Bruto (PIB) do Brasil, que passou de 55,7% em 1947 para 74% em 2020 (CNC, 2020).

Pretende-se analisar os processos existentes na gestão de riscos cibernéticos por meio da questão de pesquisa: **Como as estruturas de governança podem impactar na mitigação dos riscos cibernéticos no setor de serviços?** A resposta à esta questão permitirá identificar as formas complexas de contratação que permitam compreender a relação entre a sua gestão e os mecanismos de mitigação de riscos cibernéticos.

Os custos de transações estão associados à busca de política de pública que atenda às normas e leis claras, aplicáveis e efetivas (Peres, 2007). No entanto, a ocorrência da incerteza, oportunismo e racionalidade limitada podem impactar o cumprimento dos objetivos regulatórios, inclusive, pelo custo de agência entre órgãos reguladores, burocracia e organizações (Simon, 1980; Miller, 1992; Frant, 1996; Dixit, 2002; Peres, 2007).

Os impactos vão além do financeiro, tais como a exposição de informações de clientes, exposições para espionagem, seja comercial ou política, fazendo com que as organizações necessitem reparar a imagem perante o mercado devido à falta de confiança em seus processos de segurança operacional e cibernética (Norton, 2020). Para obtenção da resposta à questão de pesquisa, busca-se atingir os seguintes objetivos específicos:

1. Analisar as formas complexas de contratação que permitam compreender a relação entre atores e os mecanismos de mitigação de riscos cibernéticos;
2. Avaliar os mecanismos utilizados pelas instituições (informações, processos, conhecimento e consequências) para lidar com os problemas associados às transações que permeiam o espaço cibernético;
3. Avaliar a influência do riscos de cibernéticos sobre os custos de transação, considerando o setor de serviços cada vez mais orientados para a inovação e tecnologias emergentes.

Como contribuição teórica, cita-se o ineditismo deste trabalho ao tratar de riscos cibernéticos, estruturas de governança em custos de transação e setor de serviços. Tanto que, espera-se ainda, propor um modelo conceitual a partir da exploração das aplicações da economia dos custos de transação nos riscos cibernéticos. Isto porque o gerenciamento eficaz de riscos é conduzido não apenas pela teoria sólida, mas também pela prática sólida (Lam, 2014). As melhores práticas em gerenciamento de riscos só podem surgir quando as teorias e modelos são testados nos limites do mundo real, aumentando o valor da empresa (Olson e Wu, 2008) e do sistema no qual ela está inserida.

Este estudo não considera o risco cibernético sobre o prisma da tecnologia em si, mas como um sub-risco dos riscos operacionais aos quais uma organização pode estar exposta. Uma das principais motivações da pesquisa sobre riscos cibernéticos está na análise de políticas e normas de segurança cibernética que estão sob os aspectos formais das organizações (objetivos, indicadores, estratégias, recursos e estrutura organizacional), bem como os informais (lacuna de conhecimento, resistência às mudanças e liderança). No entanto, há de se destacar que o risco que reverbera das instituições e organizações para a sociedade tem tornado a discussão de combate à fraude e ao cibercrime de maneira frequente.

2. REFERENCIAL TEÓRICO

2.1 A Nova Economia Institucional

Custos de Transação. Quanto maior a especificidade, maior serão os riscos, os problemas de adaptação e maior os custos de transação (Farina, Saes e Azevedo, 1997). Neste sentido, Williamson (1985, 1991) distinguiu seis tipos de especificidade das transações que não se esgotam e explicam grande parte dos problemas de dependência bilateral, além das consequências no custo de transação, tais como: locacional, ativos físicos/digitais, ativos de humanos, ativos dedicados, especificidade de marca e especificidade temporal.

No entanto, neste estudo pretende-se avaliar um sétimo tipo de especificidade para analisar as transações no contexto das estruturas de governança: o ambiente cibernético, considerando que Willianson (1996) entende que formas híbridas são uma estrutura de governança, mas não chegou a incluir práticas inovativas nas relações comerciais (Grassi, 2002) e tampouco as cibernéticas.

Pressupostos Comportamentais. "O risco humano é considerando o elo mais fraco da segurança da informação" (Dodel e Mesch, 2019, p. 75). O oportunismo pode ser identificado pelas ações que visam burlar o sistema por meio de comportamento malicioso e a racionalidade limitada pelas habilidades e conhecimento atomizados quando se tratar de proteção contra ameaças cibernéticas.

A partir dos conceitos de racionalidade limitada e oportunismo, tem-se que o estabelecimento de contratos para regulamentação das transações sempre será complexo e incompleto (Peres, 2007). Sarto e Almeida (2015) destacam que a racionalidade limitada decorre da necessidade de considerar as incertezas relativas à evolução do ambiente econômico, enquanto o oportunismo exige uma avaliação estratégica das possíveis condutas dos participantes da transação diante de acontecimentos imprevistos.

O comportamento oportunista conforme Santos, Lourenzani e Lourenzani (2019, p.115) "não é previsível, e nem mesmo assume padrões convencionais constatados no ambiente organizacional" podendo ocorrer *ex ante* ou *ex post* à elaboração dos contratos. o que faz jus trazer a análise de formas híbridas (Williamson, 1991; Zylbersztajn, 1995; Ménard, 2004; da Silva, 2020) consideradas meios complexos de contratação, tais como: contratos, joint-ventures, subcontratação, redes, franquias, parcerias, cooperativas e alianças, caracterizadas por aspectos de competição e cooperação serão avaliados, considerando os novos modelos de negócios que surgem no âmbito do segmento de serviços (Grassi, 2002).

2.2 O Ambiente Cibernético e seus Riscos

O ambiente cibernético vai além da *Internet*, incluindo não apenas o *hardware, software* e sistemas de informações (Silva e Nogueira, 2019), mas também pessoas e suas interações sociais nas redes de computadores (Klimburg, 2012). A alta competitividade tem forçado mudanças constantes nos processos das organizações, justamente para melhorar seu posicionamento no mercado (Sacramento, Perez e Nagano, 2016), mesmo que diante de riscos desconhecidos e incertezas.

Riscos podem assumir duas formas: (i) de natureza estática ou pura, caracterizado pelo risco que resulta somente a chance de perda (ii) de natureza especulativa ou dinâmica, em que envolve a possibilidade de perda de uma partes enquanto a outra obtém algum ganho (Powers, 2006; Durak, 2020). O risco dependerá das ameaças maliciosas (ou não) que a organização enfrenta e como as organizações mitigam os riscos por meio de decisões de negócios e estratégicas (Egan et al., 2019).

O risco tem por característica a incerteza ou imprevisibilidade (Olson; Wu, 2008) e as empresas têm operado em um ambiente marcado por informação imperfeita, assimetria de informação, externalidades, fatores de riscos comuns na operacionalização e de não previsibilidade (Böhme et al, 2019) em relação aos resultados das estratégias escolhidas.

O risco cibernético é uma temática recente no discurso científico ao tempo em que sua diversidade promovida pela mudança exponencial nos âmbitos da cibersegurança e ameaças cibernéticas tem ganhado atenção por meio da digitalização acelerada da economia e das relações sociais (Strupczewski, 2021).

Como práticas organizacionais, situações de enfrentamento exigem conhecimento sobre a segurança e proteção cibernética que permitam identificar as formas complexas de contratação que permitam compreender a relação entre a sua gestão e os mecanismos de mitigação de riscos cibernéticos:

Operacional. O risco cibernético abrange ameaças decorrentes do uso e transmissão de dados, tais como: (i) internet e redes de telecomunicações; (ii) dano físico causado por ataques cibernéticos (iii) fraude pelo uso indevido de dados (iv) qualquer responsabilidade decorrente do uso, armazenamento e transferência de dados e (v) disponibilidade, integridade e confidencialidade de indivíduos, empresas ou governos (CRO Forum, 2014, p. 5).

Financeiro. Um dos elementos do impacto financeiro a ser destacado é em função da inclinação dos investidores venderem ações com alto risco cibernético e comprar aquelas que oferecem menor risco. Inclusive, essa tendência é mais forte durante os períodos com maiores preocupações com violação de dados. Neste sentido, Jiang, Khanna e Yang (2020) revelaram que a obtenção de ações com maior risco cibernético afeta e eleva o custo de capital próprio ex-ante.

Reputacional. Risco cibernético pode ser definido como impacto negativo na operação da organização envolvendo elementos informais, pautados em missão, imagem e reputação, das quais recursos e capital intelectual são os "meios" de uso de sistema de informação.

Sendo assim, o risco cibernético pode ser entendido como aquele que ocasiona o dano físico ou impacta na perdas financeiras quando há ocorrência de mau funcionamento no ambiente digital ou quando dados são negligenciados ou compartilhados ilegalmente (Nieuwesteeg e Waard, 2018), em situações de ameaças cibernéticas (Smidt e Botzen, 2017; Dan Geer, Eric Jardine e Eireann Leverett, 2020), ocorrência de crimes financeiros e fraudes (Dudin et al, 2018; Santucci, 2018), ampliação da cibersegurança (Böhme, 2005), incidência de desvantagens informacionais (Shetty, 2018) e riscos econômicos em Internet das Coisas (Lee, 2020; Radanliev et al, 2020) constituindo como principais elementos do risco que têm permeado todo o espaço cibernético.

2.3 O Setor de Serviços

A compreensão sobre a responsabilidade pela cibersegurança compartilhada entre diferentes atores em iniciativas inseridas por meio das tecnologias no setor de serviços, tais como: compartilhamento de espaços, provedores, economias de escala, inovação aberta, dentre outros, é considerada muito fragmentada, e ainda não se chegou a um consenso mínimo entre as diversas áreas do conhecimento.

Considerando-se a infinidade de perspectivas que poderiam ser desenvolvidas partindo da amplitude do setor de serviços, este estudo procurará traçar a análise dos principais atores envolvidos neste segmento:

1) Agências ou órgãos reguladores. Destaque para a importância de analisar as transações das organizações do setor de serviços com o setor público, trazendo luz ao

contexto dos reguladores e órgãos fiscalizadores que possuem como premissas criar, executar, monitorar e fiscalizar as interação dos atores envolvidos nos riscos cibernéticos. Destaca-se aqui, a burocracia que resulta muitas vezes em comportamentos e estratégias oportunistas que são analisados como pressupostos comportamentais da Teoria de Custos de Transação (Williamson, 1991 e 1993).

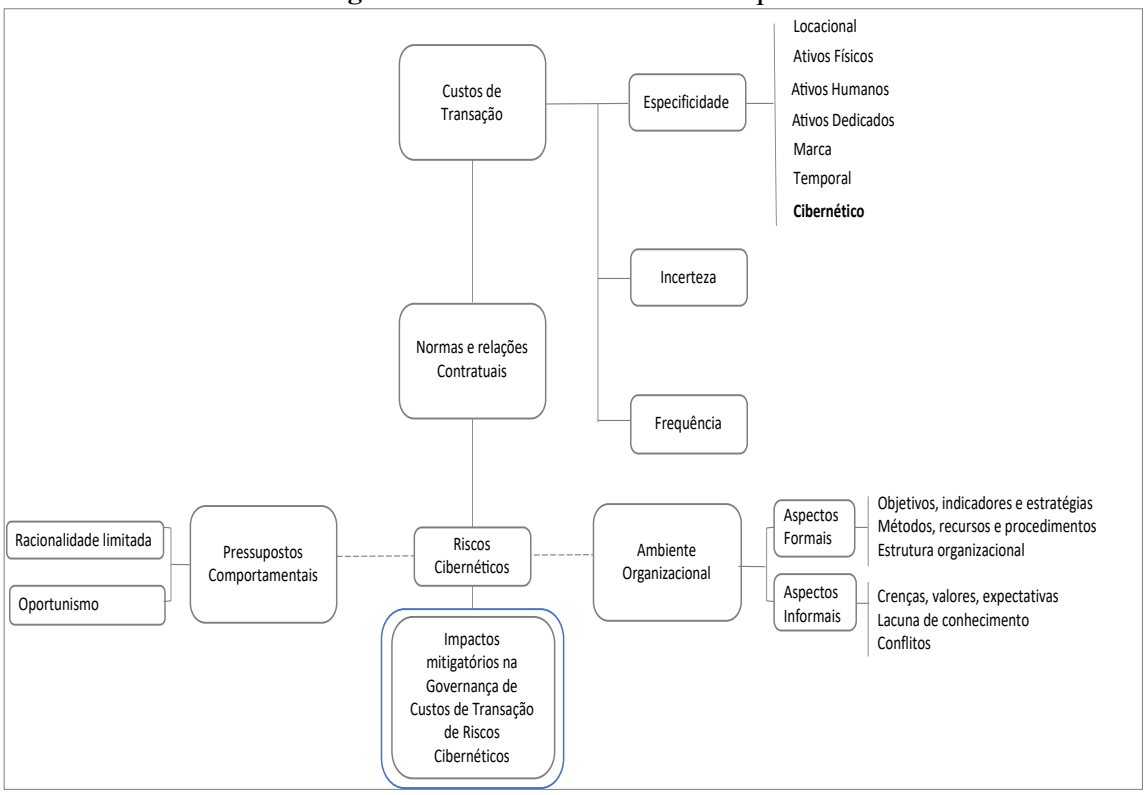
2) Instituições ou organizações inseridas no setor de serviços. No contexto da organização contratante ou prestadora do serviços, ambas serão pesquisadas sob o prisma de que o gerenciamento do risco tende facilitar a integração e fornecimento de apoio para detecção de eventos maliciosos e ou ocasionados pela lacuna de conhecimento ou gestão nas transações contratuais ou processos.

O conhecimento pode tornar o tomador de decisão mais consciente do tipo de ataque cibernético (Ben-Asher e Gonzalez, 2015), justamente pela dinâmica em que o ambiente competitivo cria mudanças externas que geram novas demandas, às quais as organizações precisam se adaptar (Bataglia e Meirelles, 2009).

3) Clientes. Por fazerem uso e experiência do serviço prestado**.**

Portanto, pretende-se desenvolver este estudo conforme o esquema representado pela Figura 1, em que são expostos os principais aspectos teóricos que serão trabalhados por meio da pesquisa focalizada.

Figura 1: Estrutura Teórica da Pesquisa



Fonte: Autora (2021)

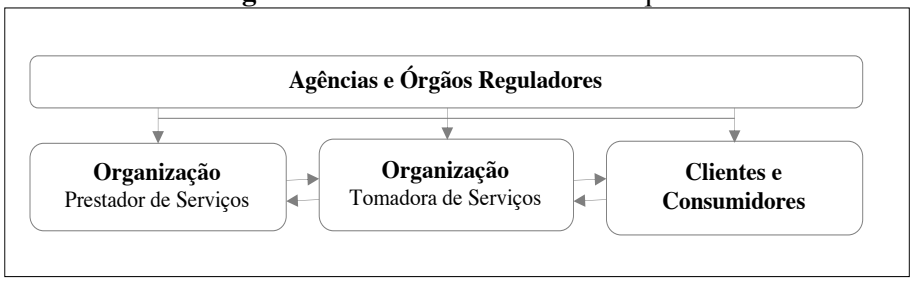
3 PERCURSO METODOLÓGICO

Este projeto seguirá por meio de investigação exploratória com o objetivo de se obter evidências e as particularidades da temática, em função da escassez da literatura

envolvendo riscos cibernéticos, estruturas de governanças, dentro das perspectivas corporativa e econômica da transação de custos.

O gerenciamento de riscos demanda práticas e práticas incorporam padrões de significado que podem ser importantes para o entendimento de como operacionaliza o setor de serviços por meio dos seguintes atores, conforme ilustra a Figura 2:

Figura 2: Atores envolvidos na Pesquisa



Fonte: Autora (2021)

Além da conceituação, indispensável para o sucesso da investigação e coleta de informações por meio de documentos, para a realização deste trabalho, também será realizada entrevista distinta para cada ator do setor de serviços (conforme Figura 2), respeitados os critérios de aderência à temática que permita alcançar os objetivos específicos traçados para este estudo. Em duas etapas, a pesquisa será desenvolvida considerando a seguinte ordem:

i) a primeira etapa da pesquisa consistirá em identificar os mecanismos mitigatórios de riscos implementados ou executados pelos atores, bem como, as perdas e/ou investimentos financeiros em virtude dos riscos cibernéticos inerentes aos negócios e processos da empresa, por meio de:

a) *entrevista semiestruturada* abrangendo CEOs, diretores, superintendentes, delegados, gerentes, analistas e clientes. O público para empreender a entrevista é amplo, mas focalizada (Kvale e Brinkman, 2009), considerando que o risco cibernético permeia todos os ambientes administrados, controlados e ou acessados por estes atores. Entende-se ainda, que a entrevista, segue um roteiro de perguntas pré-estabelecidas (Patton, 1999), permitindo a captura das respostas abertas dos respondentes;

b) *análise de conteúdo da entrevista*. A técnica de análise de dados está assentada na análise da bibliográfica, revisões da literatura e bibliométricas, bem como na análise de conteúdo das entrevistas e bases documentais obtidas na pesquisa de campo (Bardin, 2016).

c) *os resultados serão adequados ao referencial teórico*.

ii) em relação à segunda etapa, esta procurará identificar e analisar informações e exemplos que proporcionem maior compreensão sobre o estudo. Importante destacar que, para a definição de qualquer estudo de pesquisa é importante identificar a rede de relação entre as variáveis consideradas importantes para o estudo de qualquer situação problema, (Sekaran e Bougie, 2016) que serão exploradas por meio das entrevistas e documentações fornecidas pelos entrevistados.

Por meio da abordagem qualitativa, Godoy (1995, p. 58) expõe que "envolve a obtenção de dados descritivos sobre pessoas, lugares e processos interativos pelo contato direto do pesquisador com a situação estudada, procurando compreender os fenômenos". Tais fenômenos são buscados neste trabalho considerando a perspectivas dos atores da situação em estudo conforme a Tabela 1:

Tabela 1: Características da Pesquisa

Abordagem	Qualitativa
Tipo de Pesquisa	Exploratória
Paradigma de Pesquisa	Positivismo
Método de Pesquisa	Entrevistas semiestruturadas
Natureza	Teórica
Epistemologia	Objetivista
Técnica de Análise	Análise de Conteúdo
Espaço Amostral	**Expectativa de quantidade mínima:** Agência e Órgãos reguladores: cinco entrevistas Organizações tomadoras e prestadoras de serviços: dez entrevistas para cada Clientes (consumidores): 20 entrevistas

Fonte: Autora (2021)

Entende-se ainda, que nas etapas de análise das entrevistas será possível compreender os constructos motivacionais que permitem a interação entre tecnologia e pessoas, mediante o risco cibernético no setor de serviços. Baseando-se no rigor e na descoberta dos instrumentos de investigação, Bardin (2016, p. 29) sugere dois polos importantes que traduzem a subtileza dos métodos de análise de conteúdo, corresponde aos objetivos traçados:

1. Ultrapassagem da incerteza, ao questionar-se sobre a imparcialidade da mensagem auto julgada e sobre a leitura do pesquisador, se seria válida ou generalizável.
2. Enriquecimento da leitura: por meio da leitura atenta, aumentar a produtividade e a pertinência. "Pela descoberta de conteúdos e de estruturas que confirmam (ou infirmam) o que se procura demonstrar o objetivo das mensagens, ou significações de que até então, não se detinha a compreensão.

Entende-se que nas etapas de entrevistas será possível identificar e compreender os constructos e elementos que permitem a relação entre atores e os mecanismos de mitigação de riscos cibernéticos no setor de serviços permitindo assim, desenvolver um modelo conceitual. Para a análise dos dados qualitativos obtidos nas entrevistas será utilizado o Software NVIVO® V10.

4 CONTRIBUIÇÃO ESPERADA E RELEVÂNCIA DA PESQUISA

Independente de quaisquer campos de atuação, a produção científica desenvolvida por um pesquisador deve ter "um compromisso social e ser conhecida como de utilidade para a comunidade acadêmica e a sociedade em geral" (Barrancos e Duarte, 2013, p. 108).

A contribuição da empresa para melhor inclusão da sociedade, geração de riqueza local enquanto seus negócios são realizados por meios digitais, têm fomentado cada vez mais uma proposta de agenda em que as organizações sejam mais ambiciosas em um compromisso social-econômico.

Neste sentido, Kuhn (1970, p. 21) explicita que o conhecimento é uma empreitada fundamentalmente coletiva, desenvolvida por grupos, sob o entendimento de que "a ciência não se desenvolve pela acumulação de descobertas individuais", e a existência de um paradigma há de colocar sempre um problema a ser resolvido.

Amit e Schoemaker (1993) advertem que gestores devem antecipar-se ao futuro, avaliar as interações competitivas, bem como, superar a inércia organizacional por meio

de decisões estratégicas. Ambientes que demandam preocupação constante com sustentabilidade, responsabilidade social e cidadania corporativa (Hays, 2008) e diplomacia da inovação (Nye, 2011; Peterkova, 2020) aceleram mudanças, ao mesmo tempo que geram incertezas.

Rooney e McKenna (2007, p. 126) argumentam que os negócios precisam ser mais sábios, não apenas por razões intelectuais ou comerciais, mas também por razões éticas, porque os negócios são um mediador-chave entre a esfera econômica e a social, entre as esferas ambientais e tecnológicas. Neste aspecto, os sistemas de informação codificam e armazenam quaisquer dados para uso posterior, e as pessoas que coletam estes dados precisam compreender o quanto são essenciais e úteis (Rowley, 2007).

Os processos de digitalização da economia e da sociedade e tem constituído elemento essencial, cujo impacto é potencialmente significativo na prosperidade global. Younan et al. (2020), apresentaram uma visão geral exaustiva para o futuro da *internet* das coisas e desafios relacionados sob a luz da ciência e informação de dados necessárias nas tecnologias de comunicação, como inteligência artificial, computação em nuvem, dentre outros – estas, abrangendo tanto o setor público como o privado.

Portanto, mediante a alta competitividade do mercado, forçando as mudanças das organizações a melhorar o posicionamento da empresa mediante riscos e incertezas, além da crescente complexidade e expansão dos mercados em que exigem a conformidade e perenidade dos seus processos, considera-se a relevância do impacto social e econômico do setor de serviços para este estudo.

Com os resultados deste estudo, busca-se também atrair o interesse dos pesquisadores em uma variedade de áreas, como administração, tecnologia e sociologia, indo além dos referenciais teóricos com foco na aplicação e operacionalização no contexto organizacional, em destaque, a indústria de serviços em quaisquer outros países, considerando seu potencial impacto econômico e social.

REFERÊNCIAS

Amit, R., & Schoemaker, P. J. H. (1993). Strategic Asset and Organizational Rent Strategic. Management Journal.

Barrancos, J. E., & Duarte, E. N. (2013). Inteligência Competitiva e as Práticas de Gestão do Conhecimento no Contexto da Administração e da Ciência da Informação: revelações da produção científica. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, 18(38), 107-126.

Bataglia, W., & Meirelles, D. (2009) Population ecology and evolutionary economics: toward an integrative model. Management Research: Journal of the Iberoamerican Academy of Management, v. 7, n. 2, p. 87-101.

Bardin, L. (2016). Análise de conteúdo. Lisboa: Edições 70.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, v. 48, p. 51-61

Böhme, R. (2005). Cyber-Insurance Revisited. In WEIS.

Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. Variance, 12(2), 161-185.

CNC. (2020) Confederação Nacional do Comércio de Bens e Turismo. 75 anos da CNC espelham trajetória do comércio e serviços no Brasil. Disponível em https://www.portaldocomercio.org.br/noticias/75-anos-da-cnc-espelham-trajetoria-do-comercio-e-servicos-no-brasil/322895, acessado em 28 jun 2021.

CRO Forum (2014). Cyber resilience - the cyber risk challenge and the role of insurance, Chief Risk Officers (CRO) Forum, December 2014.

https://www.thecroforum.org/2014/12/19/cyber-resilience-cyber-risk-challenge-role-insurance/ Acessado em 26 de junho 2021

da Silva, A. A. (2020). Custos de Transação no varejo farmacêutico: impactos do oportunismo e das dimensões analíticas das transações. Conference: XIV Congresso da ANPCont.

Durak, T. (2020). Innovation Spaces: the New Campus Risk Paradigm. In Challenges for Health and Safety in Higher Education and Research Organisations (pp. 304-336). Royal Society of Chemistry.

Dodel, Matias, Mesch, Gustavo, (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic, and digital determinants affect diverse safety practices. Comput. Security 86, 75–91.

Dudin, M. N., Zasko, V. N., Frolova, E. E., Pavlova, N. G., & Rusakova, E. P. (2018). Mitigation of cyber risks in the field of electronic payments: organizational and legal measures. J. Advanced Res. L. & Econ., 9, 78.

Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. Journal of Cyber Policy, 5(1), 9-29.

Dixit, A. (2002). Incentives and organizations in the public sector: An interpretative review. Journal of human resources, 696-727.

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic, and digital determinants affect diverse safety practices. Computers & Security, 86, 75-91.

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., ... & Ang, K. (2019). Cyber operational risk scenarios for insurance companies. British Actuarial Journal, 24.

Farina, E. M. M.; Saes, M. S. M. & Azevedo, P. F.(1997) Competitividade: mercado, estado e organizações. São Paulo: Singular.

Frant, H. (1996). High-powered and low-powered incentives in the public sector. Journal of Public Administration Research and Theory, 6(3), 365-381.

Funke, Martha. (2021) Empresas lançam soluções voltadas a riscos cibernéticos. Jornal Valor.Disponível:https://valor.globo.com/publicacoes/suplementos/noticia/2021/03/25/empresas-lancam-solucoes-voltadas-a-riscos-ciberneticos.ghtml. Acesso em 29 de abr 2021.

Godoy, A. S. (1995). Introdução à pesquisa qualitativa e suas possibilidades. Revista de administração de empresas, 35(2), 57-63.

Grassi, R. A. (2002). Williamson e "formas híbridas": uma proposta de redefinição do debate. Economia e sociedade, 12(1), 43-64.

Jiang, H., Khanna, N., & Yang, Q. (2020). The Cyber Risk Premium. Available at SSRN 3637142.

Hays, J. (2008). Dynamics of organizational wisdom. Australian National University, School of Management, Marketing, and International Business. Working paper series.

Kvale, S., & Brinkmann, S. (2009). Interviews: Learning the craft of qualitative research interviewing. sage.

Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence.

Kuhn, T. S. (2000). A estrutura das revoluções científicas. 3. ª edição. São Paulo.

Lam, J. (2014). Enterprise risk management: from incentives to controls. John Wiley & Sons.

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157.

Miller, G. J. (1992). Managerial dilemmas: The political economy of hierarchy. Cambridge University Press.

Norton. (2020) Cybersecurity Insights Report. Disponível em: https://br.norton.com/norton-cybersecurity-insights-report-brazil Acesso em 15 mai 21.
Nieuwesteeg, B., & de Waard, B. (2018). The Law and Economics of Cyber Insurance Contracts: A Case Study. European Review of Private Law, 26(3).
Nye, J. S. (2011). The future of power. Public Affairs.
Olson, D. L., & Wu, D. (Eds.). (2008). New frontiers in enterprise risk management. Springer Science & Business Media.
Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. Health services research), v. 34, n. 5, p. 1189.
Peres, U. D. (2007). Custos de transação e estrutura de governança no setor público. Revista Brasileira de Gestão de Negócios-RBGN, 9(24), 15-30.
Peterkova, J. (2020). Innovation and Industry 4.0 as a part of small state diplomacy. In SHS Web of Conferences (Vol. 74, p. 02013). EDP Sciences.
Powers, M. R. (2006). Pure vs speculative risk: False choice; sham marriage. The Journal of Risk Finance.
Radanliev, P., De Roure, D. C., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2019). Cyber Risk in IoT Systems.
Rooney, D., & McKenna, B. (2007). Wisdom in organizations: Whence and whither. Social Epistemology, v. 21, n. 2, p. 113-138.
Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. Journal of information science, 33(2), 163-180.
Sarto, V. H., & Almeida, L. T. (2015) A teoria de custos de transação: uma análise a partir das críticas evolucionistas. Revista Iniciativa Econômica, v. 2, n. 1.
Sekaran, U., & Bougie, R. (2016). Research Methods for Business, A Skill Building Approach. NY: John Willey & Sons.
Sacramento, K; Perez, G. & Nagano, C. (2016) 50 anos de inteligência competitiva: análise bibliométrica da produção cientifica de 1965 a 2015.XIX Semead. ISSN 2177-3866.
Santos, E. J., Lourenzani, W. L., & Lourenzani, A. E. B. S. (2019). Coordenação do sistema agroindustrial do urucum na Microrregião de Dracena, Estado de São Paulo. Revista Brasileira de Gestão e Desenvolvimento Regional, 15(1).
Santucci, L. (2018). Quantifying cyber risk in the financial services industry. FRB of Philadelphia Payment Cards Center Discussion Paper, (18-3).
Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(2), 224-238.
Simon, H. (1980). A racionalidade do processo decisório em empresas. Edições Multiplic, 1(1), 25-60.
Silva, W. R., & Nogueira, J. M. (2019). Ataques cibernéticos e medidas governamentais para combatê-los. O Comunicante, 9(1), 42-57.
Smidt, G., & Botzen, W. J. (2017). Perceptions of Corporate Cyber Risks and Insurance Decision-making (Working Paper# 2017-18). Risk Management and Decision Processes Center, University of Pennsylvania.
Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143.
Williamson O. E. (1985) Transaction cost economics: The governance of contractual arrangements.
Williamson O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. Administrative science quarterly, p. 269-296, 1991.
Williamson, O. E. (1993). Transaction cost economics and organization theory. Industrial and corporate change, 2(2), 107-156.

Williamson, O. E. (1996). The mechanisms of governance. Oxford University Press.
Younan, M., & et al. (2020). Challenges and recommended technologies for the industrial internet of things: A comprehensive review. Measurement, v. 151, p. 107198.
Zylbersztajn, D. (1995). Estruturas de governança e coordenação do agribusiness: uma aplicação da nova economia das instituições.