Um Modelo de Apoio à Gestão de Riscos Cibernéticos para o Negócio

Germano Fenner, Universidade Federal do Ceará
Fábio Lotti Oliva, Universidade de São Paulo

Resumo

Organizações estão cada vez mais dependentes dos serviços de tecnologia da informação (TI) para a realização de suas atividades e execução dos seus processos. Essa dependência aumentou com a COVID-19 que acelerou a transformação digital – fenômeno que incorpora o uso da tecnologia às soluções de problemas tradicionais. Empresas possuem dados sensíveis que se não forem protegidos, resultarão em prejuízos para o negócio. Este trabalho propõem um modelo para a gestão de riscos cibernéticos nas organizações visando promover a segurança cibernética para o negócio. Seu escopo considera a identificação e caracterização de agentes envolvidos no ambiente cibernético e suas relações com o negócio, a identificação dos riscos cibernéticos a eles associados, avaliação e mensuração dos impactos desses ricos na operação da empresa e apresenta um painel de controle, um *dashboard*, para apoiar os gestores na tomada de decisão em relação ao gerenciamento desses riscos.

Palavras-chave: Serviços de TI; dependência; ataques cibernéticos; segurança da informação; riscos cibernéticos.

Abstract

Organizations are increasingly dependent on information technology (IT) services to carry out their activities and execute their processes. This dependence has increased with COVID-19, which has accelerated digital transformation – a phenomenon that incorporates the use of technology into traditional problem-solving. Companies have sensitive data that, if not protected, will result in losses for the business. This paper proposes a model for cyber risk management in organizations, aiming to promote cyber security for the business. Its scope considers the identification and characterization of agents involved in the cyber environment and their relationships with the business, the identification of cyber risks associated with them, the assessment and measurement of the impacts of these risks on the company's operations, and presents a control panel, a dashboard, to support managers in decision-making regarding the management of these risks.

Keywords: Services; dependency; cyber-attacks; information security; cyber risks.

1. Introdução

Nos últimos anos empresas têm presenciado a transformação digital (TD) – fenômeno que incorpora o uso da tecnologia às soluções de problemas tradicionais – ocorrendo dentro das empresas. Com o evento da pandemia da Covid-19 em 2020, a TD foi acelerada, fazendo com que as instituições reavaliassem/mudassem sua forma de trabalho. Liu e Liu (2024) fazem considerações sobre a TD nas empresas e o aumento dos riscos. Segundo os autores, a TD é um

processo de longo prazo com alto investimento, alta dificuldade e alto risco. Nesta rápida mudança imposta pela pandemia, colaboradores e empresas não tiveram tempo hábil para se preparar e lidar com riscos cibernéticos (RC) ao qual a organização começou a ficar cada vez mais exposta. A necessidade de aprender a lidar com novas tecnologias e a ausência de uma preparação adequada em relação a segurança da informação (SI), criou um cenário propício para os criminosos cibernéticos explorarem vulnerabilidades nas soluções de tecnologia da informação (TI) que se materializaram em ataques cibernéticos (AC). Empresas passaram a ficar expostas a violações de dados, roubo de informações, investidas de *malware*, *ransomwares*, *phishing* e engenharia social. No ambiente informatizado moderno, o crime cibernético e os AC tornaram-se uma ameaça vital para as organizações (Rajan *et al*., 2021), a segurança cibernética (CS) tornou-se cada vez mais crucial nas organizações (Neeme, 2022).

A perspectiva de ocorrência de um AC faz com que as empresas despertem a preocupação em relação a continuidade dos serviços e a segurança das suas informações. Organizações possuem dados sensíveis e que precisam ser protegidos. Resguardar essas informações é de vital importância para a sobrevivência do negócio. Com a possibilidade de um AC cada vez mais eminente, as empresas precisam criar mecanismos para lidarem com os RC, garantindo a segurança de seus dados e sistemas computacionais.

Este artigo analisa a literatura relacionada aos tópicos de AC, RC e SI. O trabalho aqui apresentado contribui para o trabalho de Oliva (2016), entretanto, a ênfase de sua pesquisa está na área de TI. O foco principal deste estudo é propor um modelo para gestão de riscos cibernéticos que auxilie os gestores na tomada de decisões promovendo a segurança cibernética para o negócio.

2. Referencial Teórico

O referencial teórico adotado para esta pesquisa foi estabelecido em três temas inter-relacionados: AC, gerenciamento de riscos cibernéticos (GRCb) e SI. Essa base conceitual subsidiou o desenvolvimento dos instrumentos de pesquisa e o desenvolvimento da análise dos resultados. A teoria de GRCb é composta por conceitos, classificações, relações e modelos. Assim, buscou-se desenvolver um arcabouço conceitual para desenvolvimento do trabalho.

a) Ataques Cibernéticos

Pandey, Singh, Gunasekaran e Kaushik (2020) destacam que os AC estão se tornando um

fenômeno crescente. De acordo com Byres, Franz e Miller (2004) a maioria dos protocolos sistemas *ciber* físicos foi projetada muito antes de a segurança da rede ser percebida como um problema. Segundo De Coning e Mouton (2020) vários fatores contribuíram para o aumento de ataques entre eles: dependência crescente da sociedade na infraestrutura digital, treinamento deficiente dos trabalhadores transferidos para *home office*, sociedade dependente no que se refere a consumo de serviços *online*, falta de treinamento adequado para uma força de trabalho longe da proteção das redes corporativas. Para Demirkan e Mckee (2020) os ataques de segurança cibernética (SC) hoje se tornaram tão comuns que não são mais caracterizados como um "se" vai acontecer, mas agora é um "quando isso vai acontecer". De Coning e Mouton (2020) alertam que as ameaças cibernéticas tendem a continuar explorando vulnerabilidades para fins diversos, tais como espionagem, hacktivismo, terrorismo e ações perpetradas por estados nação, o que pode conduzir a cenários catastróficos de paralisia estratégica de países.

Nos últimos anos, os AC estão se tornando cada vez mais frequentes. Em setembro de 2017, o site da Google teve seus serviços comprometidos após ataques de DDoS (*Distributed Denial of Service*) ou ataque de negação de serviço, um tipo de ação que torna os recursos dos servidores *web* indisponíveis aos usuários. De acordo com o Canaltech (2020), esse foi o maior ataque de negação de serviço já registrado na história. O ano de 2017 também é marcado pelo *WannaCry*, um *crypto-ransomware* que afetou computadores que rodavam o sistema operacional Microsoft Windows 2007. Para o site Olhar Digital (2017), esse ataque infectou mais de 200 mil sistemas em 150 países. Empresas prestadoras de serviços como Vivo, Next e Net paralisaram suas atividades para lidar com o problema ou, como forma de se precaverem. Serviços públicos como INSS foram afetados e sistemas do Ministério Público e do Tribunal de Justiça de São Paulo ficaram inoperantes. O ataque de proporções globais atingiu hospitais públicos do Reino Unido, grandes corporações como Santander e Telefônica na Espanha e o Aeroporto Internacional na Ucrânia situado na capital Kiev. No dia vinte e oito de setembro de 2018, o *Facebook* sofreu uma pane global e como consequência teve a perda de suas funcionalidades. O problema afetou aplicativos como *Instagram* e *WhatsApp*. O ataque sofrido pela empresa é considerado por especialistas como o maior já realizado à privacidade da história e serve de alerta para usuários da internet. Segundo informações do site Tecnoblog (2019), estima-se que o ataque ao *Facebook* afetou 90 milhões de contas.

No Brasil, os ataques são frequentes e correm tanto em empresas privadas quanto em órgãos públicos. No dia 04 de novembro de 2021, os sistemas do Superior Tribunal de Justiça (STJ)

foram atacados deixando ministros e servidores sem conseguirem acessar aos seus próprios arquivos e e-mails (CONJUR, 2021). No dia 10 de dezembro do mesmo ano, foi a vez do site do Ministério da Saúde. De acordo com a CNN Brasil (2022), o site sofreu um ataque *hacker* na madrugada que o deixou inacessível. Estima-se que mais de 50 *terabytes* de dados foram excluídos. Em 30 de maio de 2021, a subsidiária da brasileira JBS nos Estados Unidos sofreu ataque *hacker* à sua operação naquele país. Segundo o G1 (2021), a empresa pagou US$ 11 milhões de dólares em *Bitcoin* para liberar o acesso ao sistema sequestrado e evitar vazamento de dados. No dia 30 de março de 2022, o TRF-3 (Tribunal Regional Federal da 3ª Região) foi alvo de um ataque cibernético que derrubou seu site e inviabilizou o atendimento à população (FOLHA UOL, 2022). Em dezembro do mesmo ano, *hacker* invade sistema da SPTrans (São Paulo Transporte S/A) e 13 milhões de usuários do bilhete único têm dados expostos (G1, 2022).

O ano de 2023 começa com o ataque cibernético a empresa Yum, proprietária das franquias KFC e Pizza *Hut*. Segundo a CNN Brasil (2023), o ataque virtual fechou 300 lojas no Reino Unido. No dia 12 de fevereiro, foi a vez da Organização do Tratado do Atlântico Norte (OTAN) ser atacada. Segundo a Microsoft (2023), vários websites ficaram temporariamente inoperante e no dia 21do mesmo mês, segundo o site Hardware.com.br (2023), um ataque cibernético ao App “Meu Correios”, expos os números de CPF e telefone dos usuários. 2024 revela um dado preocupante, segundo o site Olhar Digital (2024), AC crescem quase 70% no Brasil em um ano.

b) Gerenciamento de Riscos Cibernéticos

Em se tratando do gerenciamento de riscos (GR), existem diversas literaturas especializadas no tema como modelos tradicionais aplicados a gestão de projetos HERMES (OFCL, 2005), NBC (IPMA, 2012), *PRINCE2* (OGC, 2009), *PMBOK* (PMI, 2021), padrões especializados *M_o_R* (AXELOS, 2015), *Standard for Risk* (PMI, 2019) e o *The Orange Book Management of Risk* (2003), controles internos da empresa como COSO (2007) e as normas ABNT NBR ISO/IEC 27001 (2022), ISO/IEC 27002 (2022), ISO/IEC 27032 (2015) e ABNT ISO 31000 (2018).

Assim como o GR, o GRCb possui uma literatura especializada a saber:

- ***Cyber Security Body of Knowledge*** **(CyBOK)** – Modelo que busca disseminar o conhecimento em SC. Para o CyBOK (2019) a SC refere-se à proteção de sistemas de informação (hardware, software e infraestrutura associada), os dados sobre eles e os serviços que fornecem. O modelo é organizado em dezenove áreas de conhecimento

que o guia identifica por nível superior, ou KAs, que são agrupadas nas categorias (1) Aspectos humanos, organizacionais e regulatórios, (2) Ataques e Defesas, (3) Segurança de Sistemas, (4) Segurança de Software e Plataforma e (5) Segurança em Infraestrutura;

- ***CIS - Critical Security Controls* (CSC)** – Apresenta controles críticos organizados em grupo de informações e discute os complexos desafios enfrentados pelos profissionais responsáveis pela SC tanto no âmbito corporativo privado quanto no setor público. CSC está organizado em 18 grupos controles de alto nível que estão agrupados por ações prioritárias de cibersegurança e tem medidas e recomendações para proteção contra os AC mais comuns da atualidade. Para cada grupo existem três grupos de implementação, os chamados *Implementation Groups* (IGs) que contém medidas de segurança;
- **BSI-*Standard* 100-1** – Descreve como um sistema de gerenciamento de segurança da informação (SGSI) pode ser projetado. Leva em consideração as recomendações das normas ISO/IEC 27001 e 27002 e fornece um manual de instruções para implementação dos requisitos. Para o BSI (2008) o SGSI especifica os instrumentos e métodos que a gestão deve utilizar para gerir de forma clara (planejar, adotar, implementar, supervisionar e melhorar) as tarefas e atividades destinadas ao alcance da SI;
- **NIST *Privacy Framework*** – Fornece uma estrutura de gestão de riscos de privacidade publicada pelo *National Institute of Standards and Technology* (NIST). Tem por objetivo aperfeiçoar o GR de SC em infraestruturas críticas fornecendo uma linguagem comum e uma metodologia sistemática. Está organizado nas partes (1) *Framework Core*, (2) *Framework Implementation Tiers* e (3) *Framework Profile*. O NIST *Cybersecurity Framework* ajuda as organizações a prevenirem, detectar e responder a AC bem como melhorar as comunicações entre os stakeholders internos e externos.

A acadêmica tem dedicado considerável esforços no estudo e desenvolvimento de guias, modelos e padrões para GRCb. Dada a concretude e urgência em proteger as informações das empresas, preservar a sua imagem e garantir a sua SC, constatou-se que esses estudos relacionados para avaliar os riscos envolvidos na operação e nos processos do negócio despertam grande interesse no meio acadêmico e empresarial. Este trabalho pressupõe de que as organizações necessitam de uma gestão específica para lidar com a GRCb.

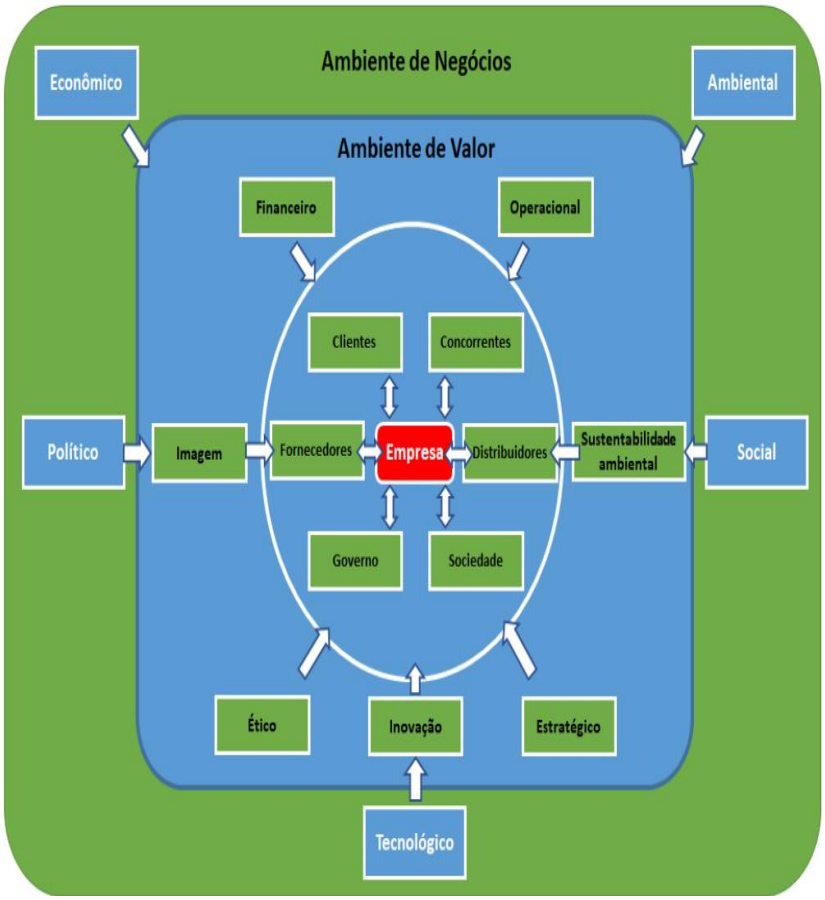
c) Segurança da Informação

Organizações possuem dados sensíveis que se não forem protegidos, resultarão em prejuízos que podem levar a crises e, em casos mais extremos, à falência da empresa. Nesse contexto,

surge a necessidade de proteger o negócio de AC. Empresas precisam desenvolver habilidades para se resguardarem e evitar que RC venham a ocorrer. Existem diversas literaturas orientando em como desenvolver a SC nas organizações. A norma ABNT NBR ISO/IEC 27002, por exemplo, orienta sobre técnicas de segurança e código de prática. Seu principal objetivo é estabelecer diretrizes e princípios para que a organização possa iniciar, implementar, manter e melhorar a gestão de segurança da informação (GSI). Já a ABNT NBR ISO/IEC 27032 (2015) fornece diretrizes para melhorar o estado de SC, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança, em especial a SI, a segurança de rede, a segurança de internet e a proteção da infraestrutura crítica de informação. Essa norma abrange as práticas básicas de segurança para as partes interessadas no espaço cibernético (EC) fornecendo uma visão geral de SC, explicação da relação e outros tipos de segurança.

Em um ambiente dinâmico a qual estamos inseridos, organizações precisam considerar novas abordagens em relação a SI. O trabalho de Oliva (2016), por exemplo, aborda as relações de risco da organização com seus agentes (Figura 1) para definir um nível de maturidade na Gestão de Riscos.

Figura 1 - Riscos corporativos no ambiente de valor



Fonte: Oliva (2016).

O autor conceitua o Ambiente de Valor da empresa como o conjunto dos agentes que tem relações com a organização podendo assim, gerar valor. Segundo Oliva (2016), a gestão de risco tem que avaliar todas essas relações de forma sistêmica para que não haja risco na relação de valor com esses agentes. Para Oliva (2016), as pesquisas devem estender sua a análise de forma sistêmica sobre ambos os ambientes que as organizações fazem parte de modo a alcançar uma visão holística na análise de riscos.

3. Metodologia

a) Aspectos Metodológicos

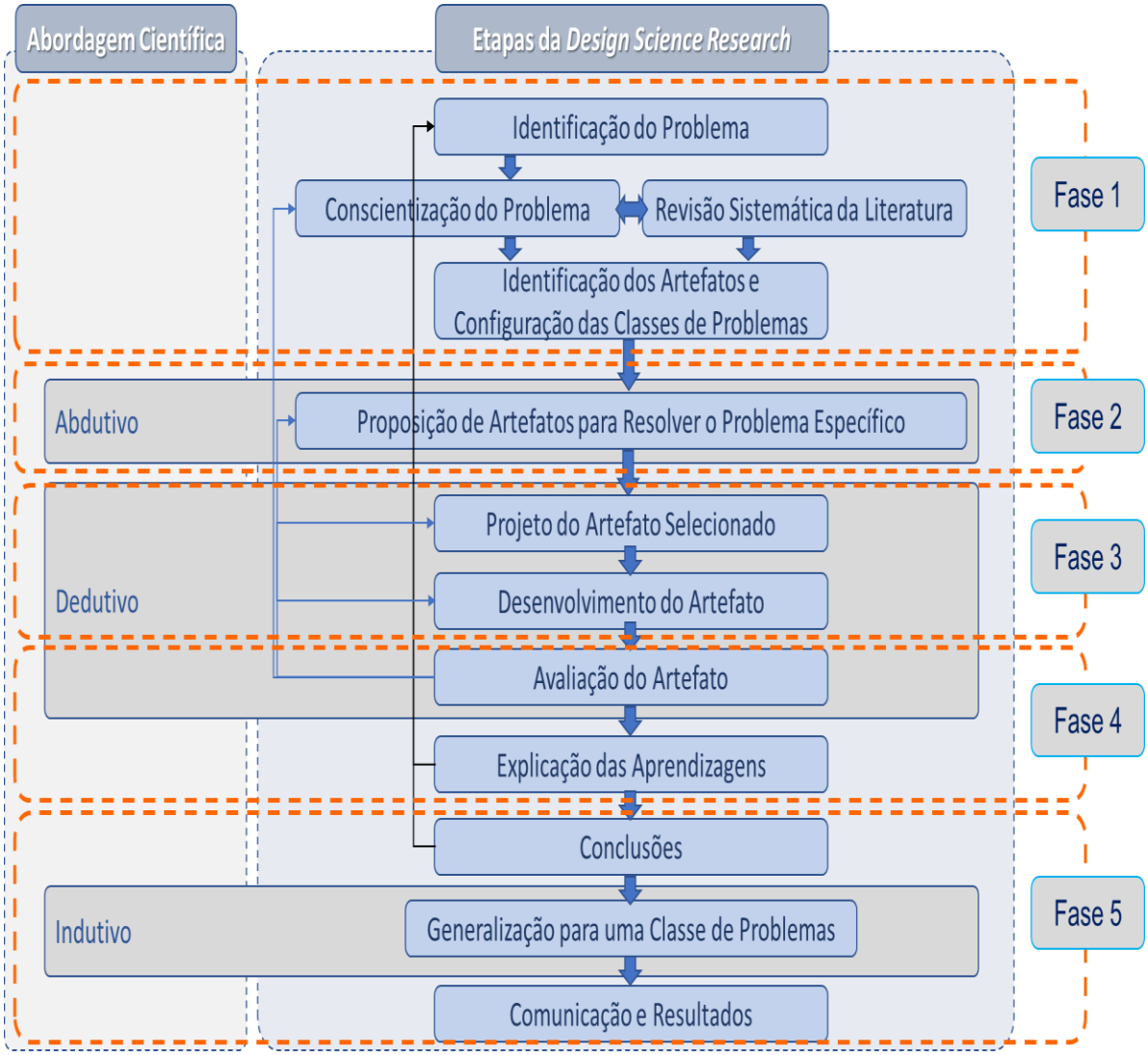
Considerando os objetivos da pesquisa, foram elaborados uma série de procedimentos metodológicos. Inicialmente, foram realizadas entrevistas com profissionais de diversas áreas que validaram as expectativas, hipóteses e opções sobre o objetivo geral do estudo, ou seja, propor um modelo para a GRCb em que o negócio possa utilizar visando promover a SI. Com base nessas informações e no modelo conceitual, foi desenvolvido o instrumento de pesquisa para realizar uma pesquisa quantitativa. As respostas nortearam a composição de um questionário com questões fechadas e de múltipla escolha com base no modelo conceitual e nos elementos teóricos advindos do referencial conceitual desenvolvido para o tema que foi aplicado a três gestores de grandes empresas. Buscou-se identificar quais são os agentes que se relacionam com a organização, os RC a eles associados, probabilidade de ocorrência, impacto ao negócio, características e respostas a serem adotadas. Com base nos dados coletados na pesquisa, foi proposto um artefato, um modelo de apoio ao GRC para o negócio.

b) *Design Science Research*

Para a construção da proposta metodológica foi utilizado o método *Design Science Research* (*DSR*) que combina as etapas de identificação do problema, revisão sistemática, conscientização e tem como resultado o desenvolvimento de um artefato como resultado do trabalho. Para Herbert Simon (apud PIMENTEL; FILIPPO; SANTORO, 2019), na abordagem *DSR* que encontramos fundamentos que legitimam o desenvolvimento de artefatos como um meio para a produção de conhecimentos científicos. Segundo Hevner (2004), trata-se de um processo rigoroso para projetar artefatos, resolver os problemas observados, fazer contribuições à pesquisa, avaliar os projetos e comunicar os resultados para o público adequado. Outro fator de escolha pelo *DSR* é método agregar robustez teórica à pesquisa. Segundo Dresch, Lacerda e

Junior (2013), o *DSR* é um método que parte de um problema teórico ou prático com repercussão para a organização e estabelece uma "conscientização" a respeito do mesmo para, a partir daí, buscar o desenvolvimento de uma solução. A Figura 1 apresenta as etapas da abordagem científica com o uso do método DSR.

Figura 2 - Abordagem Científica com o Método *Design Science Research*



Fonte: Adaptado de Goecks, De Souza, Librelato, Trento, (2021)

Considerando o objetivo dessa pesquisa, o *DSR* contribuiu com o aprimoramento do trabalho, uma vez que permite identificar os artefatos que possam auxiliar às organizações a identificarem soluções para o enfrentamento dos GRCb.

4. Modelo Proposto

a) Escopo, Variáveis e Componentes Arquitetônicos

O modelo permite avaliar o cenário dinâmico e complexo do GRCb em termos de ocorrência, probabilidade, impacto, monitoramento e respostas. Os cenários de simulação do modelo se conectam com a dinâmica dos comportamentos dos riscos e dos agentes a eles relacionados. Ao usar o modelo, gestores, gerentes de TI, analistas em SI, podem encontrar as condições sob as quais o processo de GRCb deve evoluir para contribuir com a SI do negócio. Muitas análises de riscos se resumem a números e resultados estatísticos. O modelo proposto complementa ao final da simulação, um painel de controle, um *dashboard* com informações sintetizadas de agentes de riscos e os riscos mais relevantes que a organização deve monitorar.

O escopo do modelo abrange:

1. Identificar e caracterizar os agentes envolvidos no ambiente cibernético e suas relações;
2. Identificar os RC a eles associados, avaliação e mensuração dos impactos para o negócio;
3. Apresentar um painel de controle, um *dashboard*, que apoie o negócio no GRCb.

O modelo utiliza variáveis organizadas nas perspectivas de amplitude, características do risco, criticidade, financeira, maturidade da organização, resposta e tempo que são divididas em quatro tipos: entrada, calibração, mediador e saída. Os valores de entrada são fornecidos pelos entrevistados ou coletados de ferramentas de monitoramento de RC. As variáveis relacionadas a perspectiva de amplitude, criticidade, tempo servem para personalizar o modelo de simulação (genérico) para que ele corresponda ao cenário operacional da organização. As variáveis das perspectivas maturidade, tipo de respostas, consideram aspectos político de gestão e diretrizes do negócio. Variáveis que consideram as características do risco aspectos financeiros, representam informações endógenas ao sistema. A Figura 2 apresenta os tipos de variáveis para simulação do modelo.

Figura 3 - Variáveis de entrada do modelo de simulação

		Características				AMPLITUDE			TEMPO		FINANCEIRO	MATURIDADE	RESPOSTA	CRITICIDADE
AGENTE	RISCO ASSOCIADO AO AGENTE	Duração do Risco	Pode ser Evitado	Gera Custos	Necessita de Tratado	Amplitude do Impacto	Área de Impacto	Possibilidade de Ocorrência	Exposição ao Risco	Tempo de Percepção	Impacto Financeiro	Resposta Clássica ao Risco	É Mitigável	SLA Acima de 99%?
Fornecimento	Problemas com suporte	Contínuo	Sim	Sim	Não	Regional	Tecnológico	Baixo	Médio	Instantâneo	Médio	Mitigar	Sim	Não
Fornecimento	Problemas com fornecimento	Temporal	Não	Sim	Sim	Nacional	Tecnológico	Baixo	Médio	Instantâneo	Alto	Mitigar	Sim	Não
Fornecedor de software	Sistemas vulneráveis	Contínuo	Não	Não	Sim	Nacional	Gestão	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Fornecedor de software	Concordar com termos de uso	Contínuo	Não	Não	Não	Local	Político-Legal	Muito baixo	Muito baixo	Instantâneo	Muito alto	Evitar	Não	Não
Fornecedor de software	Roubo de dados	Contínuo	Não	Não	Sim	Internacional	Imagem	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Fornecedor de hardware	Retenção de informações pelo fabricante	Contínuo	Não	Não	Não	Local	Político-Legal	Baixo	Muito baixo	Longo prazo	Médio	Evitar	Não	Não
Fornecedor de hardware	Defeitos no dispositivo	Temporal	Não	Não	Sim	Nacional	Tecnológico	Muito baixo	Baixo	Uso do dia a dia	Muito alto	Evitar	Não	Não
Fornecedor de internet	Vulnerabilidades do provedor	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Muito baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Provedor de Nuvem	Vulnerabilidades do provedor	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Muito baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Provedor de Sistemas Empresariais	Sistemas Offline	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Médio	Baixo	Instantâneo	Muito alto	Transferir	Sim	Sim
Provedor de Sistemas Empresariais	Bugs	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Provedor de Sistemas Empresariais	Perda de informações	Contínuo	Não	Não	Sim	Nacional	Imagem	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Provedor de Sistemas Empresariais	Imprecisão de informações	Contínuo	Não	Não	Sim	Nacional	Gestão	Médio	Baixo	Uso do dia a dia	Muito alto	Evitar	Não	Não
Provedor de Sistemas Empresariais	Dificuldades técnicas	Contínuo	Sim	Não	Sim	Nacional	Tecnológico	Médio	Muito baixo	Uso do dia a dia	Médio	Transferir	Sim	Não
Canais de Comunicação	Sistemas Offline	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Médio	Baixo	Instantâneo	Muito alto	Transferir	Sim	Sim
Canais de Comunicação	Vulnerabilidades do provedor	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Canais de Comunicação	Perda de Informações	Contínuo	Sim	Não	Sim	Nacional	Gestão	Baixo	Muito baixo	Longo prazo	Muito alto	Evitar	Não	Não
Sistemas Físico-Cibernéticos	Aparelhos defeitosos	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Baixo	Muito baixo	Instantâneo	Médio	Transferir	Sim	Não
Engenharia social	Vazar informações por chantagem	Contínuo	Sim	Não	Sim	Nacional	Político-Legal	Muito baixo	Muito baixo	Longo prazo	Muito alto	Evitar	Não	Não
Engenharia social	Golpes	Contínuo	Não	Não	Sim	Nacional	Imagem	Muito alto	Médio	Instantâneo	Muito alto	Evitar	Não	Não
Vazamento de dados	Vazamento de dados	Contínuo	Não	Não	Sim	Nacional	Imagem	Baixo	Muito baixo	Instantâneo	Muito alto	Evitar	Não	Não
Ambiente de Valor	Cadeia de suprimentos	Contínuo	Não	Não	Sim	Regional	Imagem	Alto	Médio	Instantâneo	Muito alto	Mitigar	Sim	Não
Crackers	Sequestro de sistemas	Contínuo	Não	Não	Sim	Internacional	Imagem	Baixo	Muito baixo	Instantâneo	Muito alto	Evitar	Não	Não
Crackers	Vazamento de dados	Contínuo	Não	Não	Sim	Nacional	Imagem	Baixo	Muito baixo	Longo prazo	Muito alto	Evitar	Não	Não
Crackers	Sequestro de dados	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Baixo	Baixo	Longo prazo	Muito alto	Evitar	Não	Não
Crackers	Pishing	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Médio	Médio	Longo prazo	Muito alto	Evitar	Não	Não
Crackers	Vírus	Contínuo	Não	Não	Sim	Nacional	Tecnológico	Médio	Médio	Longo prazo	Muito alto	Evitar	Não	Não

Fonte: Autor

O modelo simula os comportamentos e interações entre as variáveis para geração dos resultados de monitoramento e tomada de decisão.

b) Diagramas de modelo e implementação

O modelo foi implementado usando a linguagem de programação *Python* que oferece recursos de desenvolvimento de alto nível, interpretada de *script*, imperativa e orientada a objetos. O processo considera um *design* hierárquico (Agentes de Riscos – Riscos Cibernéticos – Tratamento dos Riscos). Os destaques do *design* do modelo são mostrados na Figura 4.

O resultado do processo é a geração de informações visuais dos RC que o negócio está exposto apresentadas nos seguintes modos:

- Gráfico de Funil - Apresenta a hierarquia dos 10 agentes com o maior número de riscos a eles associados;
- Cubo de Calor – Mostra as informações com diferentes combinações que são:
  - Tempo de Indisponibilidade: Considera o impacto das informações estarem indisponíveis. Quanto maior o tempo, maior o impacto do risco para o negócio;
  - Amplitude: Volume de abrangência dos dados comprometidos. Maior amplitude, mais áreas da empresa e mais *stakeholders* serão impactados;
  - Sensibilidade da Informação: Nível de confidencialidade dos dados. Exposição de informações sensíveis resulta em penalidades e danos à reputação da empresa.
- Gráfico *Treemap*: Possibilita a visualização dos dados hierárquicos referente aos agentes de riscos usando retângulos aninhados;
- Gráfico da Hierarquia de Riscos – Mostra os 10 maiores riscos que o negócio está exposto.

Figura 4 - Visão geral das variáveis, processos simulados e resultados gerados pelo modelo

Fonte: Autor

Essas informações visuais dos riscos ajudam o negócio na percepção doa assunto, aumentando a compreensão sobre o RC que a organização está exposta. Empresas podem ter uma noção de quais riscos existem, mas podem não saber quais são os principais que ela está exposta. Podem ter uma noção quando aso agentes, mas quais dessas são os mais recorrentes em relação aos riscos associas. O modelo proposto por essa pesquisa auxilia o negócio na GRCb proporcionando mais informações que auxiliem na tomada de decisão.

5. Casos de Estudo

O modelo foi apresentado para profissionais com diferentes *expertises* tais como analistas em SI, gestores de empresas, peritos forenses, especialistas em riscos corporativos e de TI. A escolha considerou diferentes segmentos de empresas como agricultura, educação, engenharia de mineração, saúde, transporte, varejo e porte (pequeno, médio e grande) das organizações. A opção por essa variedade de diferentes perfis profissionais, segmento e tamanho das empresas confirma que o modelo aqui apresentado pode ser aplicado a qualquer tipo de negócio, independente do seu porte e ramo de atividade. A pesquisa considera que as grandes organizações, quando comparadas com as de pequeno e médio porte, relacionam-se com um número maior de agentes em seu ambiente de negócio.

Todos os entrevistados relataram que a prática de identificar os riscos era baseada na

identificação e o impacto que eles podem causar. Os entrevistados também informaram que as raras ocasiões em que era feito um exercício no sentido de identificação e resposta a risco, consideravam como algo superficial e de pouca robustez. Nas poucas oportunidades que tiveram sobre o assunto, o tema foi tratado na forma de *brainstorming*, uso de ferramentas que eram mais voltadas a gestão da qualidade e na experiência dos gestores. Os entrevistados informaram que a proposta de uma visão mais externa (agentes e relações do ambiente de TI), proporciona uma abordagem mais profunda sobre o assunto.

A validação realizada junto aos entrevistados possibilitou inferir que o modelo aqui proposto se encontrava pronto para aplicação. Neste contexto, o modelo foi aplicado em três casos reais de avaliação que serão descritos a seguir.

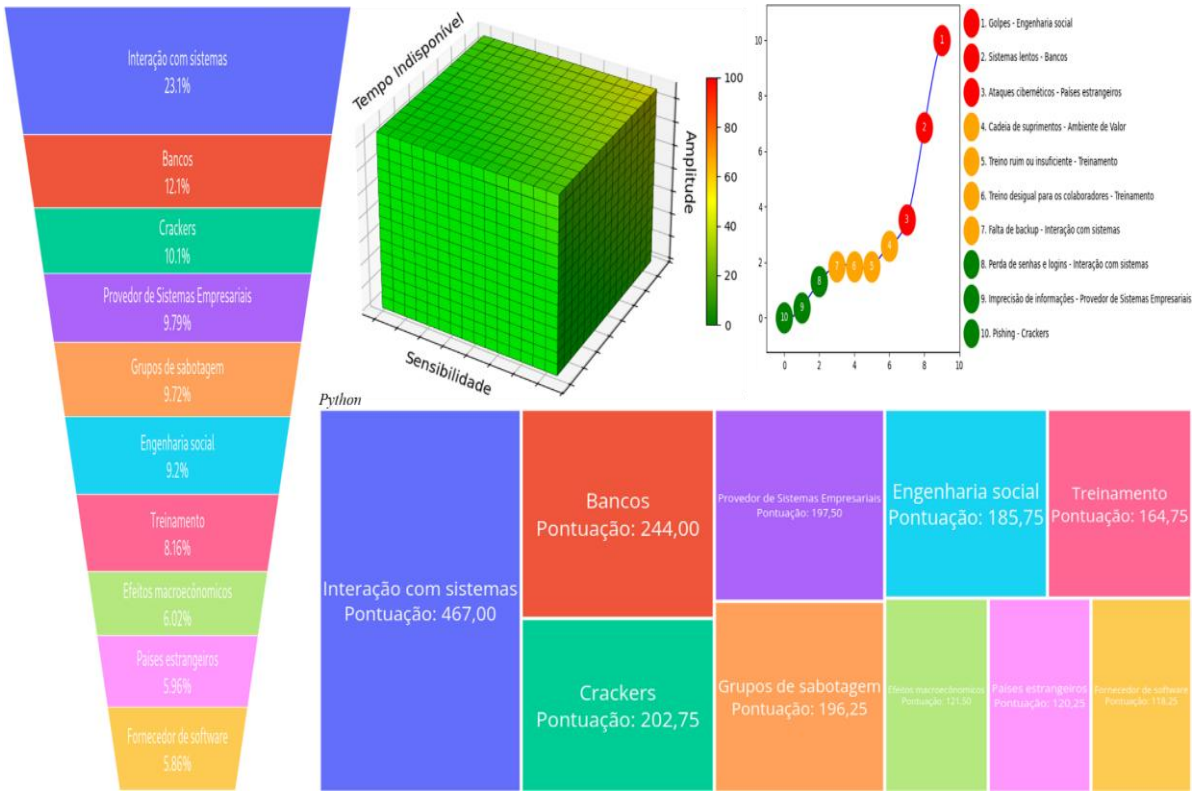
6. Resultados

a) Empresa do Segmento de Mineração

A empresa estudada atua na mineração e metalurgia de minerais industriais. Com atuação global, comercializa seus produtos para diversos países como China, França, Noruega entre outros, ela conta com mais de 2000 colaboradores da empresa e 1200 terceirizados.

Aplicando o modelo ao contexto da empresa, o fluxo do processo foi seguido dando início a identificação e caracterização dos agentes presentes no ambiente de TI da empresa. A partir das relações estabelecidas com os fornecedores, foram identificados os riscos de dependência de fornecedor (operação), corresponsabilidade por parada de sistema (produtividade/imagem), Roubo de dados (produtividade/imagem), ataque a serviços de TI (produtividade/imagem), sistemas vulneráveis (produtividade/imagem). A partir da aplicação do modelo, a organização percebeu a grande dependência em relação aos seus sistemas. Os provedores de sistemas empresariais viabilizam toda a operação contábil, fiscal, patrimonial, recursos humanos entre outros, da empresa. Existe uma interação muito grande entre os diversos sistemas que os fornecedores das soluções de ERP, CRM e soluções específicas para fins de engenharia disponibilizam para a instituição. Em razão de promover diversas operações internacionais, ela empresa também está exposta a grupos de sabotagens. Grupos de sabotagem podem dirimir ações simples, porém, de grande impacto para a operação do negócio como o rompimento intencional da comunicação de fibra óptica, por exemplo.

Figura 5 - Resultado do Painel de Gestão de Riscos Cibernéticos da Empresa 01



Fonte: Autor.

A primeira figura do painel de controle, Figura 5, apresenta os 10 principais agentes de risco que o negócio está exposto organizados por um gráfico de funil. A segunda figura apresenta um cubo de calor que apresenta as dimensões de tempo de indisponibilidade, sensibilidade e amplitude. O aspecto de amplitude é a característica de maior impacto para a organização. A terceira figura apresenta a hierarquia dos 10 maiores riscos que a organização está exposta e ao final, quarta figura do painel, é apresentado um gráfico de *treemap*, que possibilita visualizar os agentes de riscos organizados por dados hierárquicos usando retângulos.

b) Empresa do Segmento Público

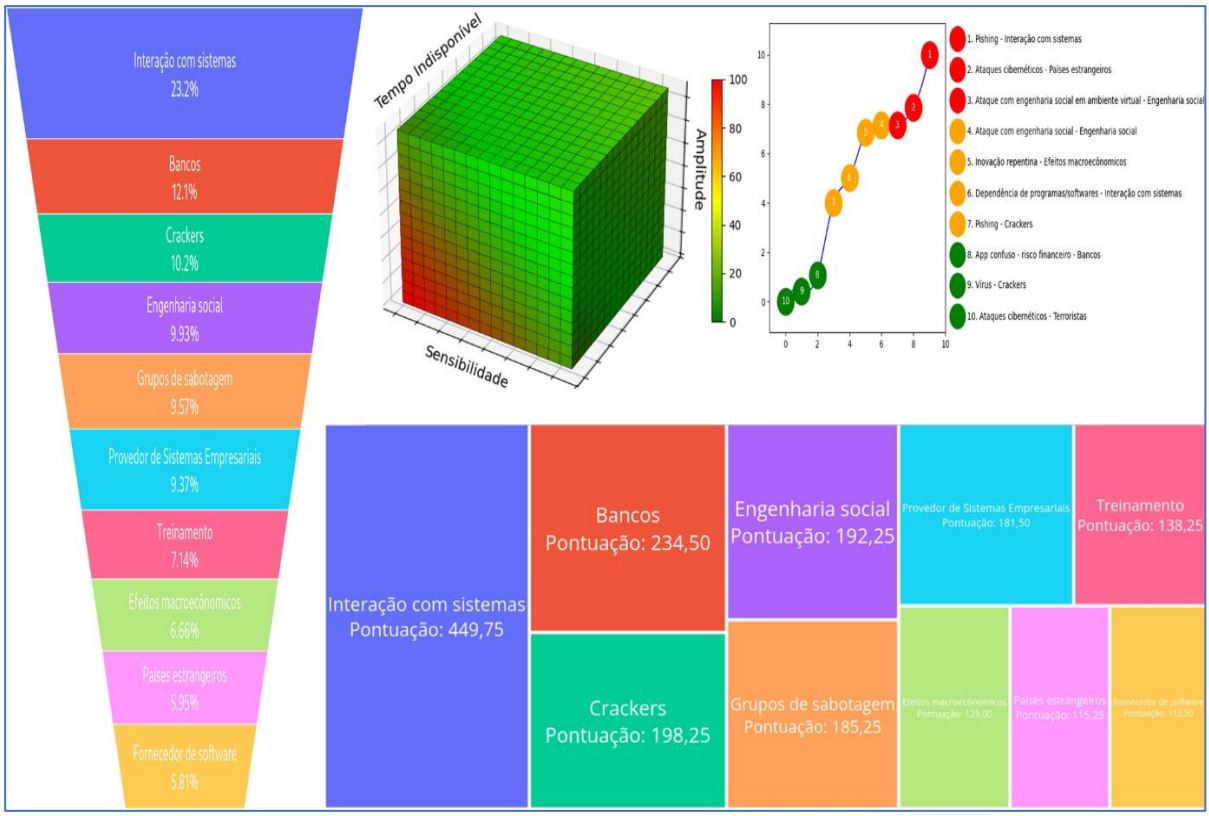
A segunda empresa em que o modelo foi aplicado é uma empresa de economia mista com capital aberto. Ela está presente em mais de 150 municípios do estado do Ceará, beneficiando cerca de 5 milhões de cearenses. Por ser uma empresa pública e prestando um benefício exclusivo a população, ela não possui concorrentes no seu segmento, porém, para atender aos usuários e manter a performance dos seus serviços, ela conta com uma complexa organização dos recursos de TI (software, hardware, processo, pessoas, regulamentos) que garantem o desempenho dos seus serviços.

Seguindo as etapas propostas no modelo, inicialmente foram identificados e caracterizados os

agentes presentes no ambiente de TI da empresa. A empresa destacou o nível de conhecimento variado que existe entre os colaboradores e o quanto isso impacta em relação a área da TI. Os fornecedores foram classificados nos grupos provedores de sistemas, que fornecem soluções específicas para o modelo de negócio, fornecedores de software que oferecem soluções voltadas a serviços de escritório e fornecedores de hardware oferecem computadores, impressoras, notebooks e *tablets*. A relação com esses agentes identificou o risco de dependência e obsolescência da solução. Os clientes têm uma elevada dependência dos seus serviços e para esse agente foram identificados riscos relacionados a comunicação, divergência quanto ao *report* de um problema que pode ser real ou fraude. Devido a empresa oferecer um serviço que é crítico para a população, esse agente também pode gerar o risco associado a imagem organização. Clientes acessam aos sistemas pela *web*, abrem chamados, reportam erros, fazerem solicitações de serviços. Os serviços de sistemas relacionados a parte de suporte aos usuários, é crítico para o negócio. No que diz respeito aos colaboradores, profissionais concursados e de carreira, a empresa possui tanto colaboradores *in loco* quando no modelo *home office*. Para ambos existe uma relação de poder de barganha, comprometimento e confiança. Foram identificados riscos de engenharia social, navegação por sites maliciosos, perdas de *login* e senha. Os colaboradores que estão no modelo de *home office*, tem recebido atenção redobrada da equipe de TI visto que eles estão em suas residências usando seus próprios equipamentos onde existe uma liberdade maior ao mesmo tempo que riscos de infecção por vírus, *phishing*, *malware* aumenta quando comparados aos colaboradores *in loco* aumenta. Os terceirizados tem riscos semelhantes aos dos colaboradores, porém, devido a rotatividade de pessoas pelas empresas contratadas, existe o risco de vazamento de dados, perda de informações e até sabotagem.

Ao final da entrevista e report dos dados, foi apresentado aos membros da empresa o painel de controle de riscos (Figura 6) mostrando as informações referentes aos agentes, os riscos associados a eles, em diversos aspectos para melhor entendimento e interpretação.

Figura 6 - Resultado do Painel de Gestão de Riscos Cibernéticos da Empresa 02



Fonte: Autor.

Pelo gráfico de funil, primeira figura do painel de controle, os entrevistados visualizaram os 10 principais agentes de risco que o negócio está exposto. O cubo de calor, segunda figura do painel, mostrou que o aspecto de sensibilidade é a característica mais vulnerável das informações do negócio. A terceira visão evidenciou os 10 maiores riscos que a organização está exposta e ao final, quarta figura do painel, o gráfico de *Treemap* possibilitou visualizar os agentes de riscos organizados por dados hierárquicos.

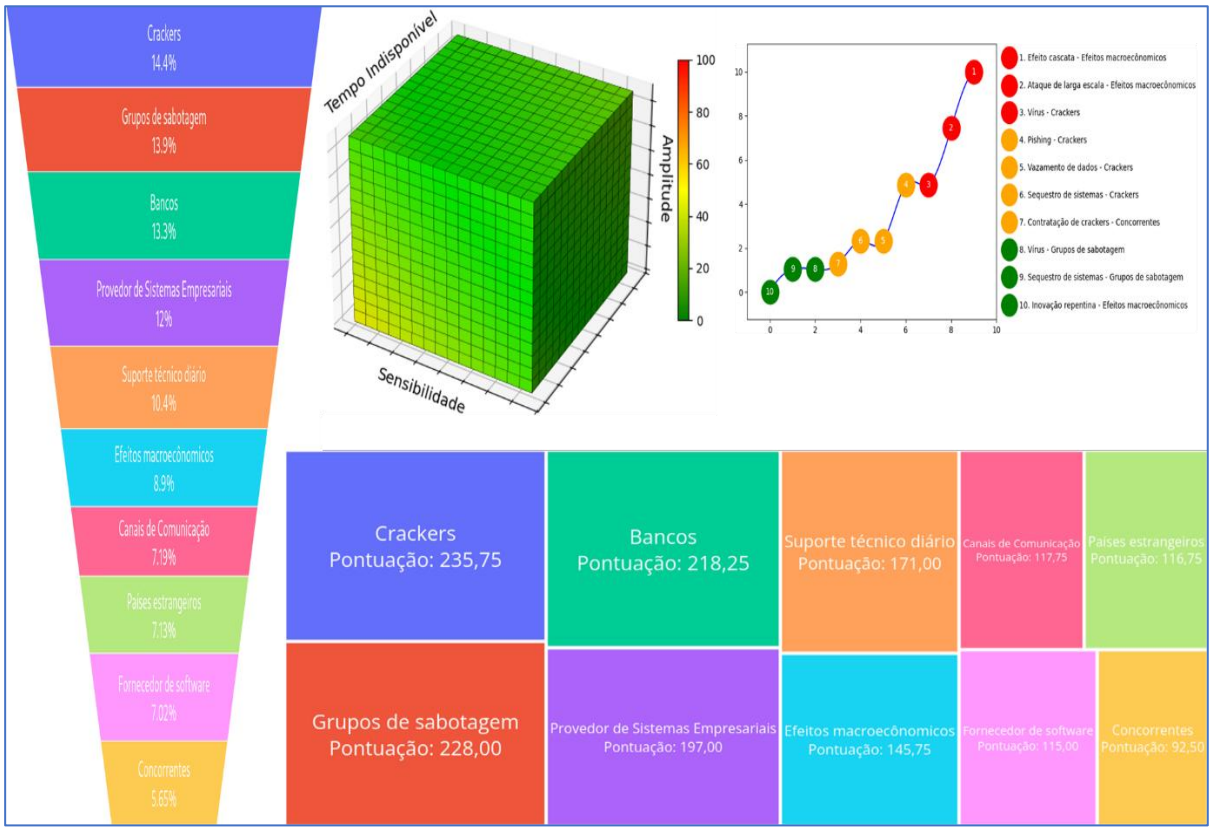
c) Empresa do Segmento de Segurança da Informação

A terceira empresa em que o modelo foi aplicado é especializada na oferta de serviços em segurança cibernética para organizações. Seu modelo de negócio considera um portfólio completo de serviços que vão desde consultoria em SI, treinamento de colaboradores, diagnósticos e auditorias. Atuando desde o ano de 2010, ela atende clientes locais e na região metropolitana da sua cidade. A empresa comercializa soluções de hardware e software incluindo serviços de instalação, configuração e manutenção.

Aplicando as etapas do modelo, durante processo de entrevista com os gestores, os agentes foram identificados e caracterizados. Dentre esses agentes identificados no modelo (Figura 7), estão fornecedores, clientes, concorrentes e *hackers*. Por ser um provedor de SI para diversas

organizações, ela é impactada pelos agentes de RC que ameaçam seus clientes. Dentre esses, destacam-se os grupos de sabotagens que por meio de diversos artifícios tais como engenharia social, ataques de DDoS, sequestro de sistemas e vazamento de informações.

Figura 7 - Resultado do Painel de Gestão de Riscos Cibernéticos da Empresa 03



Fonte: Autor.

A partir das relações estabelecidas com os fornecedores, apesar de existir uma relação de compartilhamento de conhecimento, coopetição e confiança, identificou-se os riscos de dependência, roubo de dados, retenção de informação pelo fabricante e defeito nos dispositivos. Os clientes são consumidores de pelo menos três soluções ofertadas pela empresa e a relação com eles começa em muitas das ocasiões após uma catástrofe que o negócio tenha sofrido, ou seja, o cliente foi vítima de um AC. Em relação aos clientes, um risco comum identificado é a obsolescência dos seus sistemas. Se por um lado a empresa contrata soluções atuais para SI por outro, ela deixa de manter atualizado suas soluções de ERP, CRM, CSM. O sistema operacional (SO) adotado pelos clientes, em sua grande maioria Microsoft Windows, está entre as soluções de software que mais tem versões obsoletas e em muitas vezes, sem suporte pelo fabricante.

Seus clientes pouco investem no aspecto comportamental dos seus colaboradores. Durante as entrevistas, os gestores comentaram sobre a possibilidade dos concorrentes, na intenção de

ganho de mercado, contratarem grupos de sabotagem. Segundo os entrevistados, esses grupos não precisam ser empresas próximas desejando atuar na região, não precisam gerar um AC. Suas ações podem vir por meio comentários na mídia, campanhas de marketing, degradação da imagem. O cubo de calor mostra que o aspecto de sensibilidade é a característica mais vulnerável das informações.

7. Conclusões

A informação visual do modelo proporcionou aos entrevistados uma experiência em gestão de ricos que vai além de números. Ela complementa o aprendizado dos entrevistados e proporciona uma compreensão mais efetiva sobre a GRCb. As considerações finais iniciam-se com a (1) apresentação do atendimento ao objetivo da pesquisa e aos aspectos metodológicos, (2) contribuições teóricas, (3) considerações finais da pesquisa e as sugestões para futuros estudos.

a) Atendimento ao Objetivo da Pesquisa e aos Aspectos Metodológicos

O trabalho teve como objetivo propor um modelo para fornecer apoio/suporte a GRCb nas organizações. Para seu alcance, três objetivos específicos foram propostos: (1) identificar e caracterizar os agentes envolvidos no ambiente cibernético; (2) identificar os riscos cibernéticos a eles associados, avaliação e mensuração dos impactos para o negócio; e (3) propor um modelo de apoio ao negócio. Alinhada ao problema e objetivo de pesquisa, a metodologia foi dividida em cinco etapas: (1) RSL; (2) proposta do modelo operacional; (3) aplicação do modelo com entrevistados; (4) aplicação de melhorias no modelo; (5) aplicação prática do modelo.

A primeira etapa desta pesquisa compreendeu a revisão sistemática da literatura (RSL) de modelos de análise em GRCb considerando assuntos relacionados aos temas de AC, RC e SI. Os resultados permitiram a identificação e caracterização dos agentes, as relações e os RC envolvidos no ambiente de negócios das empresas, possibilitando o avanço para a segunda que consistiu no desenvolvimento de um artefato, proposta de um modelo operacional para a GRCb. Na terceira etapa da pesquisa, foram realizadas entrevistas com quatorze profissionais que permitiu constatar que os agentes de riscos apresentados como exemplos eram aplicáveis as áreas dos entrevistados e os auxiliaram no exercício de identificação e caracterização desses agentes. Após as entrevistas, dúvidas e sugestões foram registradas permitindo assim, evoluir para a quarta etapa do modelo que compreendeu a aplicação de melhorias no processo. A quinta etapa da pesquisa que compreendeu a aplicação prática em três casos reais que considerou uma empresa no segmento de mineração, uma segunda empresa no segmento público e uma terceira

empresa do segmento de SC. A escolha por essas organizações com diferentes perfis foi para evidenciar que o modelo é aplicável a qualquer segmento de negócio, independente do seu porte e tamanho.

b) Contribuições Teóricas

Este estudo apresenta algumas contribuições teóricas para o avanço da literatura em GRCb. A RSL permitiu identificar e classificar, considerando os aspectos metodológicos, quais são os modelos para análise em GRCb existentes na literatura com os quais as empresas se relacionam em seu ambiente de negócios e quais as suas características. Os resultados indicaram 18 modelos com abordagem ao gerenciamento de riscos, dentre os quais 10 são conceituais e 08 são relacionados especificamente com a SI. Os modelos conceituais fazem uma abordagem generalizada quanto ao GR. Apenas 01 modelo abrange o GR no sentido mais amplo do assunto, 01 é voltado a Governança em TI, 02 são voltados ao estudo dos riscos corporativos, 04 são específicos para a área de gerenciamento de projetos, 03 são padrões especializados em GR, 03 são normas ISO/IEC relacionadas especificamente a SI e 04 são especializados em SC. Apesar de 08 desses modelos terem foco em SI, notou-se que muito pouco conduz a uma reflexão sobre os agentes envolvidos em um ambiente de TI e tão pouco abordam os tipos de relações entre os agentes e o negócio. Essa confirmação também foi constata nos quatro modelos especializados para riscos em gerenciamento de projetos e nos 03 padrões especializados em gerenciamento de riscos. Apenas nos 02 modelos para riscos corporativos pode-se perceber a ênfase dada em se identificar os agentes, a sua relação com o negócio e os riscos a eles associados. Existe muita literatura e conteúdo sendo produzido relacionado ao GR como um todo. Tem-se percebido a quantidade de eventos, congressos, pesquisas voltadas ao tema, treinamentos, certificações de mercado, workshops tratando sobre o assunto. Aliado a isso, diversas normas orientando sobre a matéria estão sendo produzidas – algumas de forma inédita – ou atualizadas. No entanto, percebe-se uma ênfase muito grande ao risco e sua consequência, deixando-se de considerar o seu causador que é o agente envolvido.

A revisão teórica sobre GRCb identificou alguns dos principais conceitos nesta área. Foram identificados os principais riscos tais como: ataques cibernéticos, roubo de dados, vazamento de informações, sequestro e sistemas, engenharia social, imagem da organização. Para cada risco foram avaliadas características como duração, possibilidade de ser eliminado, geração de resíduos pela solução adotada, necessidade de apoio para resposta, impacto, área mais afetada, possibilidade de ocorrência, exposição do negócio, tempo de percepção caso o risco ocorra,

impacto financeiro, resposta clássica (escalar, evitar, aceitar, transferir e mitigar) adotada pela organização, existência de SLA acima de 99% e o tempo de percepção da empresa (semanas, dias, minutos, segundos).

c) Considerações Finais e Sugestões para Futuros Estudos

Como primeira consideração à realização desta pesquisa, aponta-se para restrições do ponto de vista orçamentário, de logística e, principalmente, de acesso as informações e pessoas dispostas a viabilizar um processo mais rigoroso de validação. A metodologia adotada para a modelagem o GRCb é um processo iterativo, que demanda tempo e dedicação de todos os envolvidos. O esforço de modelagem, verificação e validação demandou o acesso a dados históricos, políticas, cultura e análise do ambiente organizacional em relação ao GR nas empresas entrevistadas. Este acesso foi bastante restrito, tanto pelo caráter estratégico das informações quanto pela falta da cultura do registro das empresas avaliadas. Tal restrição pode ser atribuída, em parte, à cultura organizacional tanto no GR quanto no gerenciamento dos RC. As contribuições geradas por esta pesquisa são de nível prático (modelo de apoio a GRCb para o negócio) e empírico (validação do modelo). A contribuição prática deste trabalho para os estudos em RC explora o potencial que a identificação de agentes, sua relação com o negócio e os riscos a eles associados.

Futuros estudos podem aplicar o modelo aqui proposto em outros setores, assim como monitorá-lo por um período a fim de verificar o impacto de sua aplicação. A natureza dos AC evolui constantemente. A grande variedade de soluções tecnológicas e uma dependência cada vez maior do negócio pelos serviços de TI facilita os AC as organizações. Este estudo buscou propor um modelo específico para fornecer apoio/suporte a GRCb nas empresas. As evidências desta pesquisa demonstram que as organizações precisam desenvolver mecanismos para líder com os RC. Estando o negócio cada vez mais dependente da TI e expostas a AC, adotar uma abordagem que possibilite a identificação dos agentes de riscos, suas relações com o negócio, os riscos a eles associados e o impacto que podem gerar às empresas, o estudo e avaliação desses riscos torna-se fundamental para a SC das organizações.

Referências

ABNT NBR ISO 31000. **Norma Brasileira ABNT NBR ISO 31000** - Gestão de Riscos – Diretrizes. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2018.

ABNT NBR ISO/IEC 27001. **Norma Brasileira ABNT NBR ISO/IEC 27001 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Sistema de Gestão da Segurança da Informação – Requisitos**. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2022.

ABNT NBR ISO/IEC 27002. **Norma Brasileira ABNT NBR ISO/IEC 27002 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Controles de Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2022.

AXELOS. **Management of Risk: Guidance for Practitioners 3rd Edition**. (ISBN 9780113312740). Published by TSO (The Stationery Office), 2010.

AXELOS. **RESILIA Cyber Resilience Best Practices is our guide to global best practice in cyber security for your organization**. (ISBN 9780113314638). Published by TSO (The Stationery Office), 2015.

BYRES, Eric J.; FRANZ, Matthew; MILLER, Darrin. ***The use of attack trees in assessing vulnerabilities in SCADA systems***. In: Proceedings of the international infrastructure survivability workshop. Citeseer, 2004.

CANALTECH – **Google Detalha como foi o Maior Ataque DDoS da história**. Disponível em: https://canaltech.com.br/seguranca/google-detalha-como-foi-o-maior-ataque-ddos-da-historia-173299/. Acessado em 04, abril 2022.

CONJUR - **Polícia Federal ainda está investigando ataque hacker ao STJ**. Disponível em: https://www.conjur.com.br/2021-jun-09/policia-federal-ainda-investigando-ataque-hacker-stj. Acessado em 04, abril 2022.

CNN BRASIL - Dona de KFC e Pizza Hut sofre ataque virtual e fecha 300 lojas no Reino Unido. Disponível em: https://www.cnnbrasil.com.br/economia/dona-de-kfc-e-pizza-hut-sofre-ataque-virtual-e-fecha-300-lojas-no-reino-unido/. Acessado em 21, jan. 2023.

COSO - **Gerenciamento de Riscos Corporativos - Estrutura Integrada**. *Price Waterhouse Coopers - PwC*, 2007.

DE CONING, Arno; MOUTON, Francois. **Bulk infrastructure management for facilities management**. In: 2020 Resilience Week (RWS). IEEE, 2020.

DEMIRKAN, Sebahattin; DEMIRKAN, Irem; MCKEE, Andrew. ***Blockchain technology in the future of business cyber security and accounting***. Journal of Management Analytics, 2020.

DRESCH, Aline; LACERDA, Daniel Pacheco; JÚNIOR, José Antonio Valle Antunes. ***Design Science Research*: Método de Pesquisa para a Engenharia de Produção. Gestão & produção**, v. 20, p. 741-761, 2020.

FOLHA UOL - **TRF-3 Aciona PF Após Ataque Hacker e Suspende Prazos Processuais**. Disponível em: https://www1.folha.uol.com.br/poder/2022/03/trf-3-aciona-pf-apos-ataque-hacker-e-suspende-prazos-processuais.shtml. Acessado em 04, abril 2022.

G1 - **Hacker invade sistema da SPTrans e 13 milhões de usuários do Bilhete Único têm dados expostos**. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/12/23/hacker-invade-sistema-da-sptrans-e-13-milhoes-de-usuarios-do-bilhete-unico-tem-dados-expostos.ghtml. Acessado em 27 Dez. 2022.

OFCL. **HERMES - Conduite et Déroulement de Projets Dans le Domaine des Technologies de l'information et de la Communication (TIC)**. Unité de stratégie informatique de la Confédération USIC, CH-3003 Berne. OFCL, CH-3003 Berne, 2005.

IPMA – **NBC - Referencial Brasileiro de Competências**. Tradução Raphael de Oliveira Albergarias Lopes. 1.ed. - Escola Politécnica/UFRJ, Rio de Janeiro: 2012.

LIU, F.; LIU, X. **Digital transformation is not a painless change: Evidence from corporate risk**. Pacific-Basin Finance Journal, p. 102427, 2024.

National Institute of Standards and Technology - NIST. ***/Framework for Improving Critical Infrastructure Cybersecurity***. Disponível em: https://doi.org/10.6028/NIST.CSWP.04162018. Acessado em: 24 set. 2023.

NEEME, Sara. **CYBER RESILIENCE: A GLOBAL CHALLENGE**. Technological Forecasting & Social Change, 2022.

NGUYEN, D. K.; VO, D. **Enterprise risk management and solvency: The case of the listed EU insurers**. Journal of Business Research, v. 113, p. 360-369, 2020.

OHAR DIGITAL - **Entenda o Ciberataque que Afetou mais de 200 mil PCs em 150 Países**. Disponível em: https://olhardigital.com.br/especial/wannacry/. Acessado em 04, abril 2022.

OLIVA, F.L. **Knowledge management barriers, practices and maturity model**. Journal of Knowledge Management, v. 18, n. 6, p. 1053–1074, 2014.

OLIVA, F. L.; SOBRAL, M. C.; DAMASCENO, F.; TEIXEIRA, H. J.; GRISI, C. C. H.; FISCHMANN, A. A.; SANTOS, S. A. dos. **Risks and strategies in a Brazilian innovation – flexfuel technology**. Journal of Manufacturing Technology Management, v. 25, n. 6, p. 916–930, 2014.

OLIVA, F. L. ***A Maturity Model for Enterprise Risk Management***. International Journal of Production Economics, v. 173, p. 66-79, 2016.

OLIVA, F.L.; KOTABE, M. **Barriers, practices, methods and knowledge management tools in startups.** Journal of Knowledge Management, v. 23, n. 9, p. 1838–1856, 2019.

OLIVA, F. L.; SEMENSATO, B. I.; PRIOSTE, D. B.; WINANDY, E. J. L.; BUTION, J. L.; COUTO, M. H. G.; BOTTACIN, M. A.; MAC LENNAN, M. L. F.; TEBERGA, P. M. F.; SANTOS, R. F.; da SILVA, S. F.; MASSAINI; SINGH, S. K. **Innovation in the main Brazilian business sectors: characteristics, types and comparison of innovation.** Journal of Knowledge Management, v. 23, n.1, p. 135–175, 2019.

OLIVA, F.L.; COUTO, M.H.G.; SANTOS, R.F.; BRESCIANI, S. **The integration between knowledge management and dynamic capabilities in agile organizations**. Management Decision, v. 57, n. 8, p. 1960-1979, 2019.

OLIVA, F. L.; TEBERGA, P. M. F.; TESTI, L. I. O.; KOTABE M.; GIUDICE, M. D.; KELLE, P.; CUNHA, M. P. **Risks critical success factors in the internationalization of born global startups of industry 4.0: A social, environmental, economic and institutional analysis**. Technological Forecasting and Social Change, v. 175, p. 121346, 2021.

OLIVA, F.L.; PAZA, A.C.T.; BUTION, J.L.; KOTABE, M.; KELLE, P.; VASCONCELLOS, E.P.G; de, GRISI, C.C. de H. e, *et al.* **A model to analyze the knowledge management risks in open innovation: proposition and application with the case of GOL Airlines**. Journal of Knowledge Management, v. 26, n. 3, p. 681–721, 2022.

OLIVA, F.L.; BUTION, J.L.; MOTTA, F.G.; FENNER, G.; RANDOLPH-SENG, B.; PAPA, M.; NAQSHBANDI, M.M. **Appetite for risk: theoretical framework and practical application in a technology-based environment.** Journal of Intellectual Capital, v. 26, n. 1, p. 71-103, 2025.

PANDEY, S., SINGH, R. K., GUNASEKARAN, A., & KAUSHIK, A. (2020). ***Cyber security risks in globalized supply chains: conceptual framework***. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128.

PMI. ***The Standard for Risk Management in Portfolios, Programs, and Projects***. PMI: Philadelphia, Pennsylvania - USA, 2019.

PMI. ***A Guide to the Project Management Body of Knowledge and the Standard for Project Management Seventh Edition***. PMI: Filadélfia, Pensilvânia - USA, 2021.

RAJAN, R.; RANA, N. P.; PARAMESWAR, N.; DHIR, S.; DWIVED, Y. K. **Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management**. Technological Forecasting and Social Change, v. 170, p. 120872, 2021.

TECNOBLOG – **O que Sabemos Sobre o Ataque ao Facebook que afetou 90 milhões de contas**. Disponível em: https://tecnoblog.net/especiais/melissa-cruz-cossetti/o-que-sabemos-sobre-o-ataque-ao-facebook/. Acessado em 04, abril 2022.

The Cyber Security Body of Knowledge **- CyBOK**. University of Bristol, 2019. Disponível em: https://www.cybok.org/. Acessado em: 29 set. 2023.

The Orange Book Management of Risk. ***The Orange Book Management of Risk - Principles and Concepts***. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf. Acessado em: 24 set. 2023.

Agradecimentos:

O artigo é baseado em estudo apoiado por:

Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

Faculdade de Economia, Administração, Contabilidade e Atuária - FEAUSP.

Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP.

Fundação Instituto de Administração - FIA.

Universidade de São Paulo – USP.

Universidade Federal do Ceará - UFC.