UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CONTABILIDADE

Bruna Benita Weber Sanchez Lopez

As características do Conselho de Administração influenciam na divulgação de riscos cibernéticos?

Florianópolis, SC
2024

Bruna Benita Weber Sanchez Lopez

As características do Conselho de Administração influenciam na divulgação de riscos cibernéticos?

Dissertação submetida ao Programa de Pós-graduação em Contabilidade da Universidade Federal de Santa Catarina para a obtenção do título de Mestra em Contabilidade.

Orientadora: Profa. Denize Demarche Minatti Ferreira, Dra.

Florianópolis

2024

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC

Lopez, Bruna Benita Weber Sanchez
As características do Conselho de Administração influenciam na divulgação de riscos cibernéticos? / Bruna Benita Weber Sanchez Lopez ; orientador, Denize Demarche Minatti Ferreira, 2024.
61 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Contabilidade, Florianópolis, 2024.

Inclui referências.

1. Contabilidade. 2. Riscos Cibernéticos. 3. Conselho de Administração. I. Ferreira, Denize Demarche Minatti . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Contabilidade. III. Título.

Bruna Benita Weber Sanchez Lopez

O presente trabalho em nível de mestrado foi avaliado e aprovado, em 25 de março de 2024, pela banca examinadora composta pelos seguintes membros:

Presidente Profa. Suliani Rover, Dra.
Universidade Federal de Santa Catarina

Prof. Moacir Manoel Rodrigues Junior, Dr.
Universidade Federal de Santa Catarina

Prof. José Alonso Borba, Dr
Universidade Federal de Santa Catarina

Prof. Vagner Antônio Marques, Dr.
Universidade Federal do Espírito Santo

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Contabilidade atribuído pelo programa de Pós-Graduação.

Documento assinado digitalmente
Carlos Eduardo Facin Lavarda
Data: 08/07/2024 14:50:29-0300
CPF: ***.990.490-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Carlos Eduardo Facin Lavarda Dr.
Coordenador do Programa

Documento assinado digitalmente
Denize Demarche Minatti Ferreira
Data: 08/07/2024 09:30:29-0300
CPF: ***.985.407-**
Verifique as assinaturas em https://v.ufsc.br

Profa. Denize Demarche Minatti Ferreira, Dra.
Orientadora

Florianópolis, 2024

Este trabalho é dedicado à minha família.

AGRADECIMENTOS

Agradeço a Deus e aos meus pais Danira Weber e Pedro Fernando Sanchez que amo muito e sempre me apoiaram em todos os momentos da minha vida.

Agradeço ao meu noivo Guilherme Felipe dos Santos por valorizar e abraçar meus sonhos na mesma medida que os seus, pela paciência e compreensão durante a minha ausência no período das aulas ou para realização das atividades do mestrado, foi com ele que compartilhei todas as minhas ansiedades, surtos e desafios.

Agradeço ao Programa UNIEDU Pós-Graduação pela concessão da bolsa de pós-graduação em nível de mestrado, que visa contribuir para o fortalecimento de grupos de pesquisas que respondam às necessidades regionais e ampliem o comprometimento institucional com o desenvolvimento econômico e social e das potencialidades regionais.

À Universidade Federal de Santa Catarina, por proporcionar educação de qualidade em um ambiente inclusivo e respeitoso que promove o desenvolvimento do conhecimento e criatividade. Expresso a minha eterna gratidão à instituição na qual também realizei a minha graduação em Ciências Contábeis.

Aos meus colegas de classe que me incentivaram e compartilharam conhecimentos importantes para a área de contabilidade. Aos meus colegas de trabalho da Pwc, que sempre foram compreensíveis quanto aos meus compromissos com as aulas do mestrado. Aos professores Suliani Rover, Moacir Rodrigues, Luiz Alberton, Vagner Marques e José Alonso pelas contribuições e por terem participado da banca examinadora.

Agradeço a minha orientadora Denize Minatti pela paciência e compreensão sobre minhas limitações de horários e viagens por causa do trabalho. Que sempre me acalmou nos momentos de desespero e não me deixou desistir. A sua empatia e otimismo é admirável. Obrigada pela confiança e em acolher o desafio do tema de dissertação. Você tem toda a minha admiração e gratidão.

Dedico a meus irmãos Fernanda Weber Sanchez e Jakson Weber que amo muito. Não posso esquecer das minhas sobrinhas maravilhosas Isabelle, Mariana e Luna Celeste que deixaram de alguma forma meus dias mais leves e alegres.

Aos meus sogros Solenir e Paulo pelo apoio, compreensão e pelas caronas para Florianópolis. Muita gratidão. Amo vocês.

Agradeço a mim, pela coragem e persistência em realizar os meus sonhos e, que, de alguma maneira, possa contribuir para a ciência, pesquisa e educação do Brasil.

Agradeço a Katia Dalcero e Camila Sanfelice, pela disposição e contribuições, sem a ajuda não seria possível finalizar esta dissertação. Desejo que Deus sempre abençoe vocês.

Por fim, agradeço de coração aos demais familiares e amigos que de alguma forma me incentivaram e me apoiaram.

RESUMO

A segurança cibernética tem se tornado uma crescente preocupação para as empresas, governança corporativa, investidores e reguladores. Nesse contexto, esta pesquisa investiga a relação entre as características de diversidade do Conselho de Administração, como experiência em Tecnologia da Informação (TI), a presença feminina e Conselho de Administração idade, e a divulgação de riscos cibernéticos em relatórios corporativos no Brasil. A partir de uma amostra com 512 observações, no período de 2020 a 2022, e utilizando um modelo de regressão logística, constatou-se que a presença feminina no conselho aumenta 9,77 vezes as chances de divulgação de risco cibernético. Portanto, considerar aspectos de diversidade de gênero na formação e avaliação do Conselho de Administração pode ser crucial para uma divulgação transparente e confiável, fortalecendo a confiança dos investidores e partes interessadas. Esta descoberta contribui para a literatura sobre segurança cibernética e estudos sobre riscos corporativos, além de apoiar os reguladores em seus esforços para aumentar a representação feminina na composição dos Conselhos de Administração.

Palavras-chave: Divulgação de riscos cibernéticos, cibersegurança, Conselho de Administração.

ABSTRACT

Cybersecurity raises increasing concern for companies, corporate governance, investors and regulators. In this context, this research investigates the relationship between the diversity characteristics of the Board of Directors such as IT experience, the female presence on the Board of Directors and age can be determinants in the disclosure of cyber risks in corporate reports in Brazil. From a sample with 512 observations, in the period from 2020 to 2022, using the logistic regression model, it was found that the board's characteristic as a female presence increases the chances of cyber risk disclosure by 9.77 times. Therefore, considering aspects of gender diversity in the formation and evaluation of the Board of Directors can be crucial for transparent and reliable disclosure, strengthening the confidence of investors and stakeholders. This finding contributes to the literature on cybersecurity and studies on corporate risks, in addition to supporting regulators in greater efforts to increase female representation in the composition of Boards of Directors.

Keywords: Cyber risk disclosure, cybersecurity, Board of Directors.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

NIST	*National Institute of Standards and Technology*
AICPA	*American Institute of Certified Public Accountants*
SEC	Comissão de Valores Mobiliários dos Estados Unidos
CVM	Comissão de Valores Mobiliários do Brasil
B3	Bolsa de Valores do Brasil
ABNT	Associação Brasileira de Normas Técnicas
CMN	Conselho Monetário Nacional
ANEEL	Agência Nacional de Energia Elétrica
SMI	Superintendência de Relações com o Mercado de Intermediários
LGPD	Lei Geral de Proteção de Dados
TI	Tecnologia da Informação
FR	Formulário de Referência

SUMÁRIO

1 INTRODUÇÃO

A cibersegurança está cada vez mais se destacando como tema de pesquisas face às novas tecnologias empresariais, aumento do trabalho remoto, expansão das vendas *online* e recentes escândalos cibernéticos (Smaili et al., 2023). O crescimento exponencial das tecnologias digitais, dos dados e das necessidades empresariais expandem as superfícies de potenciais ameaças de ataque e trazem novos desafios que elevam a cibersegurança a uma questão estratégica de negócios (Deloitte, 2023). Portanto, a proteção das informações e a integridade dos relatórios financeiros estão vinculadas a manutenção de uma segurança cibernética adequada (Gordon et al., 2015).

Desta forma, a segurança das informações se tornou um tema importante para as empresas que operam na economia digital atual, e, com isso, uma quantidade significativa de empresas aumentaram as divulgações sobre segurança cibernética em relatórios anuais públicos nos últimos anos (Gordon et al., 2010). Por outro lado, as violações de dados *online* são incidentes cibernéticos recorrentes e prejudiciais para organizações em todo o mundo (Khipers & Schonheit, 2022). Somente no Brasil, o número de ataques cibernéticos cresceu desde 2001, tendo como alvo todos os setores frágeis em defesa cibernética (Lima, 2018). Os ataques cibernéticos são um dos principais riscos que as entidades precisam controlar devido a plena dependência às Tecnologias da Informação (TI) e das redes para o funcionamento de seus sistemas de gestão, inclusive os financeiros (Amir et al., 2018). Ainda, as empresas atingidas por ataques cibernéticos tendem a sofrer perdas econômicas e de reputação de longa duração (Agrafiotis et al., 2018; Janvrin & Wang, 2021; Kamiya et al., 2018).

Empresas de soluções de segurança cibernética tem se preocupado em transparecer seus dados em relatórios públicos. A *Fortinet* anunciou que o Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos no último ano, com base nos dados do *FortiGuard Labs* (Fortinet, 2023). A *Trend Micro* revelou, também em relatório, que o Brasil é o segundo país mais vulnerável a ataques cibernéticos e, no primeiro semestre de 2023, já correspondiam a 59% do total de ataques registrados no ano passado. Por sua vez, *SonicWall*, registrou, no seu relatório, que, 2023 se mostrou o segundo maior ano de tentativas globais de *ransomware*, bem como houve aumento de 87% no *malware* da Internet das Coisas (IoT).

Esses dados justificam uma série de incidentes cibernéticos que se apresentaram em grandes empresas. A Forbes Brasil (2021) aponta que organizações como a Renner, a CVC, a Porto Seguro, o Serasa *Experian* e as redes sociais *facebook* e *linkedin* já passaram por ataques cibernéticos e vazamento de dados. Adicionalmente, em 2022, empresas como a Americanas,

o banco de investimentos BR *Partners*, o Banco Pan, a empresa de saneamento Aegea e a ANP (Agência Nacional do Petróleo) também sofreram ataques de *hackers*, tendo a Americanas perdido 1 bilhão em vendas (Proofpoin, 2022). O ataque de cibercriminosos também compromete dados confidenciais das organizações (Eaton et al., 2019). Em 2022, a empresa Mercado Livre sofreu um ataque de *hacker* que expôs dados de 300 mil usuários ativos, de acordo com a divulgação pública da SEC (SEC, 2022). O banco INTER também sofreu ataque cibernético, o qual ocasionou o vazamento de dados pessoais de seus clientes, cerca de 19.961 correntistas, segundo o Ministério Público. Naquele período, o banco não divulgou essa informação para nenhum órgão público sobre o acontecimento, pois não existiam sanções como a Lei Geral de Proteção de Dados (LGPD) (Zandonai & Argiles, 2019).

Em vista disso, a *Pricewaterhousecoopers* uma das maiores multinacionais de consultoria e auditoria do mundo, com 7200 entrevistados em 123 países, demonstrou que em 2020, esses ataques trouxeram impacto econômico potencial, sendo que 66% no Brasil e 64% no mundo as perdas estimaram até US$ 1 milhão nos últimos dois anos (Pwc, 2020). Ademais, 31% das empresas brasileiras e 29% no mundo, afirmam ter gastado até duas vezes mais do que perderam com o crime além de custos, como investigações e intervenções (Pwc, 2020).

Khipers e Schoneit (2022) examinaram como as entidades podem mitigar a reputação e danos decorrentes de violações de dados por *hacking* a partir de estratégias de comunicação e divulgação e descobriram que as empresas tiveram melhor desempenho posteriormente. Nesse sentido, órgãos reguladores como AICPA (*American Institute of Certified Public Accountants*) começaram a incentivar a divulgação voluntária de relatórios de garantia de gerenciamento de riscos de segurança cibernética e introduziram orientações como a "*SOC for cybersecurity*" que estabelece estruturas de relatórios de gestão de riscos de segurança cibernética para auxiliar às organizações na comunicação de informações relevantes e úteis sobre a eficácia dos seus programas de gestão de riscos de segurança cibernética.

No Brasil, também houve um processo regulatório preocupado com a segurança das informações, sendo pautado na Resolução CVM nº 135/22, a qual orienta comunicar, por meio de um relatório final, à Superintendente de Relações com o Mercado de Intermediários (SMI) e ao Conselho de Administração a ocorrência de incidentes de segurança cibernética relevantes contendo a descrição, a avaliação do número de clientes afetados, as medidas tomadas para aperfeiçoamento dos controles e os relatórios internos de investigação produzidos por terceiros sobre a análise do incidente e as conclusões dos exames efetuados (CVM, 2022).

A cibersegurança tornou-se, portanto, uma preocupação para as empresas, bem como para outras partes interessadas, incluindo investidores e reguladores (Tsen et al., 2022). Diante das incertezas com o crescimento de ataques cibernéticos, o alívio dos investidores se efetua com o aumento da transparência sobre riscos, capaz de reduzir a assimetria das informações com as partes interessadas (Jiang et al., 2022). Assim, uma forma de minimizar as respostas às pressões externas é utilizar-se das divulgações como ferramenta para gerenciar a reputação e se adequar às expectativas dos investidores (Bansal & Clelland, 2004; Patten, 2002).

Diante da necessidade da evidenciação de informações nos relatórios anuais para os investidores, o papel dos Conselhos de Administração na governança se torna importante. A Teoria da Administração sugere que os conselhos orientem diversas práticas de gestão por meio de aconselhamento, colaboração e supervisão (Vicent et al., 2019), fato este validado pela Teoria da Agência (Fama & Jensen, 1983). Ademais, o envolvimento de um executivo de Tecnologia da Informação (TI) na equipe de gestão de topo diminui a possibilidade de violações de segurança da informação (Kwon et al., 2013).

1.1 PROBLEMA DE PESQUISA

O risco cibernético tem sido um tema recorrente na academia e nos fóruns de reguladores internacionais de mercado de capitais, além de ser pauta regulatória em diferentes países, representando uma ameaça significativa para organizações públicas e privadas. Inclusive, foi um dos principais assuntos na Reunião Anual do Fórum Econômico Mundial de 2023, realizada em Davos, na Suíça (Fórum Econômico, 2023).

No contexto brasileiro, os processos regulatórios de segurança cibernética são:

- Resolução CVM nº 135/22: obriga as empresas divulgarem incidentes cibernéticos ao Conselho de Administração e a Superintendência de Relações com o Mercado e Intermediários (“SMI”);
- Resolução CMN nº 4.893/2021: orienta a implementação de políticas de segurança cibernética em instituições financeiras;
- Resolução Normativa ANEEL nº 964/2021: aborda a Segurança Cibernética em empresas de energia elétrica;
- Lei Geral de Proteção de dados 13.709/2018.

Uma pesquisa da Global de Riscos realizada pela *PriceWaterHouseCoopers*, em 2022 evidenciou que um dos principais riscos observados pelos gestores mundialmente se relaciona ao gerenciamento de informações e riscos cibernéticos em todos os setores de atuação. As

consequências mais significativas incluem perdas financeiras, incapacidade de inovar e falta de resiliência operacional (PWC, 2022).

Outro fato que chama atenção, é o aumento do volume de ataques, tendo como principais motivos os impactos gerados pelas mudanças impostas pela pandemia do Covid-19, ou seja, a adoção do trabalho remoto ou híbrido, a relevância dos processos automatizados e a migração dos seus sistemas para provedores de nuvem (Cisco, 2021). Os ataques cibernéticos, como *phishing*, *ransomware* e ataques distribuídos de negação de serviço (DDoS) aumentaram e pouco se sabe se as empresas que sofreram ataques estão monitorando os seus riscos (PWC, 2021).

O *stakeholders*, em especial os externos às empresas, também possuem interesse sobre risco cibernético e seus possíveis impactos financeiros, exigindo mais da qualidade e assertividade das divulgações de informações nos relatórios publicados sobre o assunto, podendo esses dados serem reportados pela própria entidade ou, por exemplo, pela firma auditora em seu relatório de auditoria independente (Rosati et al., 2020). Outro grupo que, geralmente está à margem das discussões de riscos cibernéticos, são os gestores e auditores (Islam et al., 2018; Li et al., 2020; Rosati et al., 2019; Rosati et al., 2020; Smith et al., 2019; Sneller et al., 2016; Yen et al., 2018), pois consideram o tema relevante, considerando a repercussão a curto e longo prazo na reputação e sansões legais.

Nesse contexto, tendo em vista que o Conselho de Administração é um importante meio de governança corporativa e na mitigação de riscos (Kamiya et al., 2021), o tema de cibersegurança tornou-se prioridade (Li et al., 2018). Assim, devido à importância da segurança cibernética nas agendas corporativas e regulatórias, e à necessidade de entender como a governança corporativa influencia as práticas de comunicação sobre riscos cibernéticos às partes interessadas (Heroux & Fortin, 2022) e considerando aspectos de diversidade como experiência em Tecnologia da Informação (TI) , presença feminina e, idade, apresenta-se o seguinte problema de pesquisa: **Quais características do Conselho de Administração estão associadas às divulgações sobre risco cibernético ?**

1.2 OBJETIVOS

Para responder à pergunta de pesquisa, apresenta-se a seguir os objetivos geral e específicos.

1.2.1 Objetivo Geral

O objetivo geral da pesquisa é analisar as características do Conselho de Administração e sua relação com a evidenciação das informações sobre risco cibernético nos relatórios públicos das companhias brasileiras

1.2.2 Objetivos Específicos

Para alcançar o objetivo geral, estabeleceram-se os seguintes objetivos específicos:

a) Mensurar a probabilidade de divulgação das informações sobre risco cibernético das empresas brasileiras de capital aberto e;
b) Identificar as características do Conselho de Administração quanto a experiência, idade e gênero com a evidenciação das informações sobre risco cibernético.

1.3 JUSTIFICATIVA

A segurança cibernética é crucial para garantir a continuidade dos negócios, tornando a proteção de dados uma das principais preocupações dos diretores executivos (CEOs) auditores e comitês de administração e governança. Incidentes de segurança cibernética têm o potencial de afetar significativamente a materialidade das demonstrações financeiras, operações comerciais e, consequentemente, a reputação da empresa (Boss et al., 2022).

As pesquisas sobre segurança cibernética cresceram nos últimos anos à medida que as preocupações com a segurança das informações financeiras e a integridade dos sistemas contábeis se intensificaram. A literatura demonstra que os investidores valorizam as divulgações sobre segurança cibernética (Gordon et al., 2010; Wang, Kannan, & Ulmer, 2013), fato que incentiva os pesquisadores a compreenderem a qualidade dos dados que as empresas comunicam.

Revelar informações sobre riscos cibernéticos demonstra responsabilidade e disposição para enfrentar os desafios de segurança. Nessa linha, a divulgação voluntária de informações tem reações positivas no mercado financeiro. Por exemplo, Gordon et al. (2010) observaram que as divulgações voluntárias de segurança da informação no formulário 10-K estão associadas a um aumento no preço das ações, e este efeito é maior quando a divulgação descreve práticas de gestão de risco. Essa conclusão corrobora Wang et al. (2013) de que as

empresas que divulgam medidas de mitigação de riscos nos seus registros em formulários 10-K tem menor probabilidade de sofrer incidentes de segurança cibernética. Frank et al. (2019) fornecem evidências de que a eficácia dos relatórios voluntários de gestão de riscos de segurança cibernética e da garantia independente está relacionada ao aumento da atratividade de investimento desde que a empresa tenha divulgado um ataque cibernético anterior.

Em contrapartida, os gestores têm incentivos para reter informações negativas sobre segurança cibernética nas divulgações (Frank et al., 2019; Gigler & Hemmer, 2001) pois revelar dados negativos pode desencadear potenciais litígios e danos a reputação (Cui et al., 2018; Field et al., 2005; Leroy, 2022). Tal fato é um limitador para pesquisas empíricas sobre tendências e práticas de divulgação de riscos cibernéticos nas empresas (Gao et al., 2020), além da divulgação sobre a segurança cibernética ser, geralmente, pouco informativa, pouco legível e padronizada (Li et al., 2018; Gao et al., 2020).

A pesquisa em cibersegurança desempenha um papel fundamental ao comunicar informações sobre o tema às partes interessadas (Walton et al., 2021). Entender se as organizações comunicam adequadamente os riscos cibernéticos e incidentes podem contribuir para o desenvolvimento de estratégias eficazes de divulgação em cenários de crise.

A divulgação de riscos é uma prática essencial de governança corporativa, desempenhando um papel crucial nos relatórios financeiros das empresas. Esses dados oferecem *insights* valiosos sobre a possível ocorrência de diversos riscos, a abordagem adotada pela empresa diante dessas situações e os potenciais repercussões desses riscos no futuro do negócio (Almunawwaroh & Setiawan, 2023). Portanto, a importância desta pesquisa reside na compreensão de que a evidenciação de riscos cibernéticos oferece um panorama sobre a segurança de dados, o que pode demonstrar a integridade da empresa na mitigação de interrupções nos negócios e na manutenção da confiança dos clientes e investidores.

Além disso, a divulgação de riscos cibernéticos assume um papel cada vez mais importante diante do crescente grau de assimetria de informações entre gestores de TI e partes interessadas externas. Nesse contexto, os investidores estão cada vez mais atentos aos estudos sobre a evidenciação de riscos cibernéticos, utilizando essas informações para embasar suas decisões de alocação de recursos financeiros. Paralelamente, empresas de consultoria podem se valer dos resultados de pesquisas em segurança cibernética para informar suas recomendações e estratégias de segurança para os clientes (Alshirah et al., 2020; Khandelwal et al., 2020).

As partes interessadas, como acionistas, investidores, clientes e órgãos reguladores, demonstram uma crescente preocupação com a segurança cibernética (Sneller et al., 2016). No

entanto, a exposição de informações sobre TI ainda é limitada devido à falta de obrigatoriedade formal (Sneller et al., 2016). Em resposta a essas demandas por mais transparência, no Brasil, a resolução CVM nº 135/22, no art. 11, estabeleceu diretrizes para que as entidades administradoras de mercado organizado relatem, de forma oportuna, eventos críticos de segurança cibernética ao Conselho de Administração e à Superintendência de Relações com o Mercado de Intermediários (SMI).

Apesar do Brasil estar entre os líderes globais em ataques cibernéticos (Ribeiro et al., 2020), a resolução CVM nº 135/22 não obriga as empresas a divulgarem publicamente incidentes cibernéticos (CVM, 2022), o que preocupa os usuários, especialmente em termos contábil-financeiros (Ribeiro et al., 2020). Nesse sentido, o Conselho de Administração, segundo a resolução, é responsável por monitorar a segurança cibernética e garantir transparência nas divulgações de riscos cibernéticos (CVM, 2022), que deve estar atento aos riscos para garantir as melhores medidas de cibersegurança e maior transparência nas divulgações sobre riscos e violações cibernéticas materiais (Radu & Smaili, 2022).

Nesse sentido, destaca-se a responsabilidade dos Conselhos de Administração em relação ao risco cibernético, visando garantir a implementação de medidas apropriadas (Radu & Smaili, 2021). Esse aspecto se tornou uma prioridade (Li et al., 2018), especialmente considerando que os membros dos Conselhos de Administração frequentemente não estão suficientemente preparados para lidar com os riscos de segurança cibernética ou tem visões limitadas sobre o assunto (Hartmann e Carmenate, 2021).

Como resposta, espera-se que os conselhos promovam maior transparência por meio de programas eficazes de gestão da cibersegurança (Radu & Smaili, 2021), visto que o aumento de sua disseminação sinaliza a capacidade do Conselho de Administração de antecipar ataques cibernéticos e proteger os interesses das partes interessadas (Smaili et al., 2023).

De acordo com Bonime-Blanc (2016), é decisivo que os conselhos estejam plenamente informados e preparados para abordar as questões cibernéticas em suas atividades. Assim, no contexto da governança, os achados deste estudo têm o potencial de fornecer orientações úteis para os Conselhos de Administração e a alta gestão, ajudando-os a compreender os benefícios e diretrizes relacionadas aos riscos cibernéticos.

Por fim, há expectativas de que as discussões sobre segurança cibernética sejam abordadas nas reuniões de gestão e dos conselhos, visto que o risco cibernético é inerente e considerado como um dos maiores riscos que as empresas enfrentam (Fórum Econômico Mundial, 2023). Desta forma, se presume que o Conselho de Administração atue como um

mecanismo de governança corporativa que reduza a assimetria de informação em matéria de cibersegurança (Smaili et al., 2023).

Nessa linha, a literatura anterior sugere que as características dos membros do Conselho de Administração podem impactar as divulgações sobre segurança cibernética. Radu e Smaili (2022) descobriram que a composição com o conselho incluindo o gênero feminino pode influenciar positivamente a extensão das divulgações sobre segurança cibernética e aumento da extensão dos relatórios anuais. Por sua vez, Smaili et al. (2023) observaram que a independência do conselho e a experiência financeira impactam positivamente as divulgações. A experiência em TI no conselho também é uma característica importante, pois pode-se entender assim o nível de segurança cibernética de uma empresa e o que os gerentes de TI estão fazendo internamente (Al-Sartawi, 2020).

Heroux e Fortin (2020) destacam a importância de se investigar os fatores que influenciam a amplitude das práticas de divulgação de cibersegurança, contribuindo assim para preencher uma lacuna na literatura sobre o tema. Com isso, seria possível auxiliar na busca de conselhos mais proativos na supervisão e prevenção de futuros riscos cibernéticos (Chen et al., 2022; Lankton et al., 2021), pois, empresas que contam com o engajamento do Conselho de Administração na governança de TI estão mais bem preparadas para enfrentar esse desafio (Lankton et al., 2021).

Esta pesquisa tem o potencial de fornecer informações atualizadas sobre a divulgação de riscos cibernéticos no contexto brasileiro, além de abrir caminho para o desenvolvimento de hipóteses sobre as características do Conselho de Administração e sua relação com a divulgação de riscos cibernéticos nos Formulários de Referência. Considerando a rápida evolução do risco de cibersegurança e os substanciais recursos que as organizações investem, estudos sobre como essas organizações avaliam e gerenciam as ameaças à cibersegurança merecem uma análise mais aprofundada e atualizada (Janvrin & Wang, 2022).

Além disso, a divulgação dos riscos de segurança cibernética enfrentados pelas empresas públicas, bem como a forma como esses riscos são gerenciados, estão se tornando necessários para investidores, governos, consumidores, fornecedores e outras partes interessadas. Isso lhes permite fazer julgamentos informados, considerando os potenciais ataques cibernéticos materiais que a empresa pode enfrentar (Gao et al., 2020).

Por fim, esta pesquisa tem o propósito de atender às sugestões apresentadas por Janvrin e Wang (2022), que instigam os pesquisadores de contabilidade a explorarem a área de cibersegurança. Eles destacam a escassez de estudos empíricos na contabilidade que

investiguem os efeitos da divulgação de riscos de segurança cibernética, especialmente em comparação com pesquisas conduzidas por especialistas em sistemas de informação, sugerindo que a maioria dos estudos na área de contabilidade se concentra na reação dos investidores às divulgações (Janvrin e Wang, 2022). Adicionalmente, Haapamäki e Sihvonen (2019) também ressaltam a importância de preencher a lacuna na literatura sobre os determinantes da divulgação de segurança cibernética. Por último, Janvrin e Wang (2021) sugerem investigar a relação entre a presença feminina e a gestão de riscos de segurança cibernética, destacando a contribuição potencial deste estudo nesse contexto.

2 REVISÃO DA LITERATURA

2.1 SEGURANÇA CIBERNÉTICA: SÍNTESE DA ABORDAGEM NAS PESQUISAS

Embora a cibersegurança seja um termo utilizado por profissionais e investigadores, ainda não existe consenso na literatura sobre uma definição geral (Smaili et al., 2023). O termo cibersegurança é análogo ao termo segurança cibernética e segurança da informação (Haapamäki & Sihvonen, 2019). Os mesmos autores elucidam que a cibersegurança está relacionada a tecnologia, processos e controles implantados para proteger sistemas, redes e dados contra-ataques cibernéticos, reduzindo assim riscos de ataques de *hacker* e protegendo a sociedade, organizações e os clientes de invasões não autorizadas de dados e informações que se encontram nas redes e tecnologias (Haapamäki & Sihvonen, 2019).

No campo de sistemas de informações contábeis, Cram et al. (2023) definem segurança cibernética como a garantia, a governança e a restauração dos sistemas. O mesmo termo, segundo *National Institute of Standards and Technology* - NIST (2015) refere-se à prevenção de danos, uso não autorizado, exploração e, se necessário, restauração de sistemas eletrônicos de informação e comunicação, e das informações que eles contêm para fortalecer confidencialidade, integridade e disponibilidade.

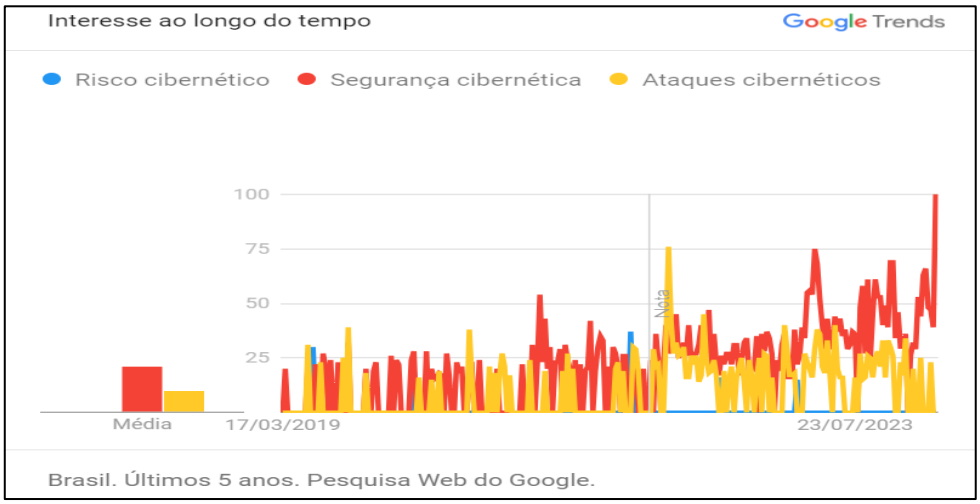
Por outro lado, quando informações confidenciais, segredos comerciais ou de propriedade intelectual são acessados, divulgados ou utilizados sem autorização podem ser caracterizadas como ataques cibernéticos (Gao et al., 2019). Ao passo que, esses ataques são definidos como subcategoria de violações de segurança que prejudicam a confidencialidade de um sistema por meio da obtenção de acesso não autorizado a informações confidenciais (Spanos & Angelis, 2016). Nestes casos, os ataques cibernéticos são realizados por indivíduos ou organizações com intenções políticas, criminosas ou pessoais que causam danos com controle ou acesso a documentos e sistemas de uma rede de computadores com informações confidenciais (Microsoft, 2023). Portanto, todas as empresas que armazenam dados pessoais e informações financeiras de partes interessadas são expostas ao risco cibernético (Kamiya et al., 2021; Walton et al., 2021).

No Brasil, o interesse pelo tema cresceu consideravelmente, conforme indicado pelo *Google Trends*. Palavras como "risco cibernético", "segurança cibernética" e "ataques cibernéticos" registraram um aumento significativo em popularidade nas pesquisas ao longo do período de 2018 a 2023.

O ponto mais alto no gráfico, em um dado período, representa o interesse de pesquisa e o valor de 100 representa o pico de popularidade do tema. (Figura 1).

Figura 1

Quantidade de pesquisas do Google Trends

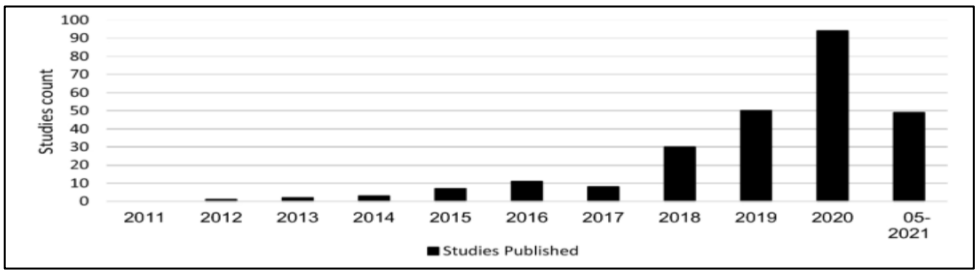


Adaptado de *Google Trends* (2024).

Diante da crescente preocupação com a segurança cibernética, Cremer et al. (2022) investigaram o estado da arte da literatura sobre o assunto. Os resultados revelaram um total de 255 artigos publicados nos últimos 10 anos, destacando a relevância e o interesse acadêmico nessa área (Figura 2).

Figura 2

Estudos publicados ao longo dos anos em segurança cibernética



Nota: Recuperado de *Cyber risk and cybersecurity: a systematic review of data availability* de Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S, 2022.

Assim, nota-se um aumento significativo nas pesquisas sobre segurança e riscos cibernéticos a partir de 2018, impulsionado pela necessidade de dados atualizados diante de eventos recentes (Cremer et al., 2022). Esse crescente interesse é corroborado por dados da Deloitte em 2023, que apontaram que 91% das empresas enfrentaram ao menos um incidente ou violação cibernética. Tais ataques, realizados por meio de diversas estratégias, incluem o

uso de *softwares* maliciosos como *malware*, DDoS, *ransomware*, *phishing*, SQL, entre outros (Microsoft, 2023).

Diferentes investigações concluem que as ameaças à segurança cibernética prejudicam a capacidade das organizações de inovar, conquistar e manter clientes (Berkman et al., 2018; Calderón & Gao, 2022). Deste modo, a crescente complexidade da conectividade dos sistemas de infraestrutura, dos riscos financeiros e de reputação geram aumento de custo e afetam a receita das empresas (NIST, 2015). Tais custos incluem despesas com advogados, litígios e consultoria jurídica, conformidade com regulamentações e leis e melhorias/restaurações dos sistemas de computadores, além da perda de reputação, propriedade intelectual e produtividade (Layton & Watters, 2014). Logo, havendo violação de segurança cibernética, uma empresa incorre em custos de curto prazo para investigar e remediar o problema (Frank et al., 2019).

Em virtude da sequência de violações de dados de empresas divulgados na *internet*, investidores, gestores, clientes e o público estão preocupados com as perdas financeiras decorrentes dos riscos de segurança cibernética (Hinz et al., 2015). A Deloitte (2023) em uma pesquisa com aproximadamente mil lideranças executivas com mais de US$ 500 milhões de receita em 23 países de todos os continentes, descobriu que 54% delas com 5 bilhões ou mais de receita relataram que gastam anualmente em média US$ 250 milhões em segurança cibernética, além de incluir as pautas de investimentos em planos estratégicos. Por isso, a gestão da cibersegurança é cada vez mais importante para as empresas na condução dos negócios no que diz respeito a criação de vantagem competitiva (Islam et al., 2018).

Diante dessa realidade, diversos autores, como Gao et al. (2020), Bodin et al. (2018), Hayel e Zhu (2015) e Tosh et al. (2017), ressaltam a importância do seguro de cibersegurança como meio de transferir e mitigar os riscos relacionados a possíveis violações cibernéticas. Esse tipo de seguro auxilia as empresas a transferirem parte do potencial de risco e exposição associados aos incidentes de cibersegurança (Gao et al., 2020).

Nessa linha, Bodin et al. (2018) propuseram um modelo para ajudar as empresas a selecionarem o conjunto ideal de apólices de seguro cibernético, visando minimizar custos e perdas esperadas. Hayel e Zhu (2015) investigaram o uso de seguros cibernéticos para promover medidas preventivas e melhores práticas em redes de computadores. Tosh et al. (2017) destacaram os benefícios do compartilhamento de informações de segurança cibernética e do seguro cibernético na defesa contra incidentes, enquanto examinavam os desafios e o potencial do mercado emergente de seguros cibernéticos. Eles enfatizaram a necessidade de produtos de seguros específicos para o ciberespaço e de melhores avaliações de riscos. Por sua vez, Biener

et al. (2015) investigaram a segurabilidade do risco cibernético através de uma revisão sistemática, concluindo que as características distintas dos riscos cibernéticos, comparados a outros riscos operacionais, apresentam problemas significativos devido a perdas altamente inter-relacionadas, falta de dados e graves assimetrias de informação.

Por outro lado, Janvrin e Wang (2021) afirmam que as pesquisas sobre segurança cibernética estão mais concentradas na área de contabilidade quando se trata de preocupações sobre as reações dos investidores e impactos financeiros. Essa descoberta se justifica porque as incertezas operacionais com a continuidade operacional desencadeiam reações negativas no mercado e aumentam riscos como perdas (Jeong et al., 2019; Li et al., 2020) visto que perdas financeiras e declínio de valor aos acionistas podem ser determinados pela reação do mercado (Calderon & Gao, 2022; Hinz et al., 2015).

Como resultado dessas pesquisas sobre a reação dos investidores, Richardson et al. (2019) mostraram que, em média, as violações resultam em menos de -0,3% de retornos anormais acumulados no curto período em torno da divulgação. Nessa linha, Kamiya et al. (2021) verificaram em 75 empresas com violações de dados entre 2005 e 2017, que os retornos anormais diminuem a riqueza dos acionistas em 1,09% no período de três dias em torno do ataque cibernético com perda de US$ 104 milhões. Tosun (2021) afirma que, em média, uma violação da segurança cibernética resulta num declínio permanente no preço das ações da empresa e afeta suas políticas em longo prazo, até cinco anos após o anúncio da violação. Michel et al. (2020), nos Estados Unidos, entre 2005 e 2017, encontraram uma reação adversa do mercado financeiro de janela curta pouco antes do anúncio da violação e uma reação positiva marginalmente significativa do mercado em uma janela de 20 dias após o anúncio.

Como elucidado, a literatura mostra que a resposta do mercado de ações a um anúncio de violação de dados é a categoria mais pesquisada e, em 75% dos estudos, têm respostas negativas a violação de dados (Richardson et al., 2019). Além dos efeitos nos preços das ações, os ataques cibernéticos também afetam o risco sistemático para as empresas e os seus investidores sendo base para tomada de decisões (Hinz et al., 2015). Complementando essa preocupação da perda de reputação, Leroy (2022) evidencia como recuperar o valor das ações ao propor ferramentas de gestão de reputação.

Escândalos contábeis de grandes empresas de capital aberto como Enron e Arthur Andersen, aumentaram a cautela dos investidores e das auditorias ao risco de erros materiais (Rosati et al., 2020). Recentemente, no Brasil, Americanas e Magazine Luiza apresentaram inconsistências contábeis com ajustes milionárias (Veja, 2023).

Como observado, nos últimos anos, os riscos associados ao vazamento de dados e aos ataques cibernéticos têm se tornado uma preocupação crescente para empresas em todo o mundo. Bisso et al. (2020) buscam aumentar a conscientização sobre essa questão ao apresentar casos práticos de multas aplicadas a empresas, destacando a importância de medidas preventivas e estratégias de segurança cibernética (Tabela 1).

Tabela 1

Penalidade aplicadas a empresas

Valor	Empresa	País	Ano
US$ 4 B	Facebook	EUA	2019
£ 183,39 M	Britinish Arways	Reino Unido	2019
US$ 148 B	Uber	EUA	2018
US$ 85 M	Yahoo	EUA/Israel	2018
€ 50 M	Google	França	2019
US$ 22,5 M	Google	EUA	2012
US$ 10 M	Blue Cross Blue Shield	EUA	2019
US$ 3,8 M	AMCA	EUA	2019
R$ 1,5 M	Banco Inter	Brasil	2018
€ 600 M	Uber	Holanda	2018
£ 385 M	Uber	Reino Unido	2018

Observação: B = bilhões, M = milhões
Fonte: Recuperado de *Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados*, Bisso, R., Kreutz, D., Rodrigues, G., & Paz, G, 2020.

Perante essas inseguranças no mercado, as firmas de auditoria que prestam serviços de consultoria de risco também estão preocupadas com as violações cibernéticas dos seus clientes (Bodin et al., 2018). Estudos detectaram aumento dos honorários de auditoria após violação de dados porque o risco inerente cresce e exige testes e trabalhos adicionais (Li et. al., 2020; Smith et al., 2019; Yen et al., 2018). Por sua vez, Smith et al. (2019) descobriram que as violações de dados estão associadas a aumento nos honorários de auditoria. A pesquisa ainda verificou que a presença de comitês de TI e de auditoria podem diminuir tais honorários visto que minimizam o risco de violação. Rosati et al. (2019) verificaram que as empresas violadas cobram honorários mais elevados, e aquelas que operam no mesmo setor da que foi invadida também enfrentam maiores valores, mas sugerem que o aumento é temporário. Yen et al. (2018) também mostram que os honorários de auditoria são elevados após a ocorrência da violação de segurança essa alteração é moderada quando é cliente de uma das *Big4*.

Embora os ataques cibernéticos possam não afetar diretamente os sistemas contábeis das empresas, os auditores externos devem estar vigilantes em relação às redes internas, uma vez que falhas nos controles gerais de TI podem indicar riscos (Li et al., 2020). Portanto, é

fundamental que os auditores considerem os controles de segurança de TI ao avaliar a confiabilidade das informações financeiras, pois isso influencia a percepção da qualidade da auditoria (Perols & Murthy, 2021). Deste modo, é necessário que os auditores estejam familiarizados com os controles automatizados sobre os relatórios financeiros, a fim de ajustar a avaliação dos riscos e planejar auditorias adicionais em caso de violações cibernéticas (Asthana et al., 2021), incluindo a possível provisão para passivos contingentes decorrentes de reclamações (Li et al., 2020).

Kahyaoglu e Caliyurt (2018) ofereceram suporte empírico à relação entre auditoria interna e segurança cibernética, fornecendo *insights* proativos e recomendações de valor agregado à gestão. Da mesma forma, No e Vasarhelyi (2017) ressaltaram a importância de considerar questões qualitativas de exposição cibernética no modelo de auditoria tradicional. Além disso, dada a experiência dos auditores na avaliação de riscos, eles podem contribuir para identificar exposições e vulnerabilidades nos negócios, capacitando-os a avaliar a probabilidade e a magnitude de diferentes ameaças (Eaton et al., 2019). Em suma, a auditoria independente desempenha um papel crucial como mecanismo externo de governança na gestão de riscos corporativos (Smith et al., 2019).

2.2 EVIDENCIAÇÃO SOBRE RISCOS CIBERNÉTICOS E SEGURANÇA DAS INFORMAÇÕES

Entender o cenário da evidenciação e como os diferentes aspectos corporativos podem ser influenciados são debates importantes para auxiliar órgãos fiscalizadores e as diferentes partes interessadas. Inicialmente, orientações sobre a divulgação de riscos de cibersegurança poderia avançar por meio de uma compreensão clara do conteúdo informativo das atuais divulgações de riscos relacionados (Chen et al., 2023). Logo, investigações como de Berkman et al. (2018) que constroem um índice de conscientização sobre segurança cibernética com base no conteúdo de todos os registros de formulários 10-K e descobrem que as empresas que demonstram conscientização sobre segurança cibernética têm maior valor de mercado, contribuem para esse desfecho.

Nesse pensamento, soma-se pesquisas que tratam sobre a divulgação de informações de segurança cibernética nos relatórios anuais das empresas. Ibrahim et al. (2021) e Eijkelenboom e Nieuwesteeg (2021) concentraram-se nas práticas de divulgação de empresas da Malásia e da Holanda. Os mesmos autores afirmam que, embora não exista obrigação legal de divulgar informações sobre segurança cibernética, uma percentagem significativa de

empresas menciona segurança nos seus relatórios anuais, porém, o nível de medidas específicas divulgadas é geralmente baixo, indicando a necessidade de divulgação mais abrangente.

Mesmo as companhias não sendo auditadas sobre a eficácia dos controles internos, Deumes e Knechel (2008) observaram que os investidores confiam em divulgações voluntárias, isso porque, segundo Gordon et al. (2010), os administradores compreendem os riscos associados ao seu negócio e tenta gerenciá-los ativamente. Posteriormente, Gordon et al. (2015) propuseram, a partir de uma perspectiva de "opções reais", que o compartilhamento de informações sobre riscos de segurança cibernética pode influenciar outras empresas a adotarem uma abordagem proativa em seus investimentos nessa área.

Esses resultados indicam a importância da divulgação voluntária para os gestores transmitirem informações quando não há exigência de divulgação obrigatória (Chen et al., 2023). Nesse sentido, Kelton e Pennington (2020) afirmam que as empresas podem empregar divulgações voluntárias como uma medida preventiva contra os impactos de futuras violações de segurança cibernética, investigando as percepções dos investidores sobre as divulgações de segurança feitas por uma empresa violada. Os autores concluem que divulgações que enfatizem o programa de gestão de riscos de segurança cibernética de uma empresa indicam aos investidores que ela possui controles de segurança eficazes.

Existe um consenso de que os investidores valorizam as divulgações voluntárias de segurança cibernética, o que impacta positivamente o mercado financeiro, resultando em aumento do valor das ações (Gordon et al., 2010). Esse impacto pode ser ainda maior quando as empresas divulgam suas práticas de gestão de risco (Wang et al., 2013).

Essas conclusões sobre divulgações voluntárias abrangem recepção positiva entre investidores e outras partes interessadas (Rennekamp, 2012; Hirst et al., 2007), pois, a pressão externa desempenha um papel significativo na divulgação de riscos de segurança cibernética (D'arcy & Basoglu, 2022), destacando a importância dessa divulgação para ajudar as partes interessadas a avaliarem os possíveis eventos adversos futuros (Li et al., 2018).

À medida que as empresas tomam decisões estratégicas de divulgação, as investigações sobre riscos de segurança cibernética podem impactar na probabilidade de violações futuras (Hughes et al., 2023). Além disso, empresas que compartilham medidas de mitigação de riscos têm menos probabilidade de sofrer incidentes de segurança cibernética e futuras violações divulgadas na mídia (Wang et al., 2013).

De acordo com Morse et al. (2017), algumas empresas ajustaram suas divulgações de riscos após observarem os efeitos negativos nos preços das ações de outras empresas que

enfrentaram incidentes de segurança cibernética. No entanto, nessa busca em compreender o cenário de divulgação de riscos após incidentes cibernéticos, Jiang et al. (2022) descobriram que nem todas as empresas violadas alteraram seu comportamento de divulgação.

Outras investigações sobre as práticas de evidenciação após ataques demonstraram que podem reduzir o custo do capital e melhorar a divulgação (He et al., 2022). Amir et al. (2018) confirmaram essa projeção ao concluir que as empresas que divulgaram imediatamente o ataque tiveram seus valores patrimoniais diminuídos em 0,33%, em média, nos três dias após a divulgação e 0,72% no mês seguinte. Nos casos em que as empresas não divulgaram o ataque, o impacto foi de 1,47% nos três dias após a descoberta do ataque e 3,56% no mês seguinte.

Explorando também a dinâmica pós-incidentes, D'arcy e Basoglu (2022) sugeriram na sua investigação que a pressão pública após uma violação de dados as leva a aumentarem as divulgações de informações sobre segurança cibernética, especialmente no caso de violações externas. Essa preocupação das organizações com a divulgação em caso de incidentes cibernéticos foi inclusive um dos principais temas das 52 cartas comentários sobre segurança cibernética enviadas a SEC (Tabela 2) segundo dados da pesquisa de Wang et al., (2022).

Outros autores como Wang et al., (2013), alegam que essa preocupação está vinculada às decisões de investimentos com custos altos e por isso pode causar impactos negativos. Essa constatação corrobora *PriceWaterHouseCoopers* (2023) que notou a violação cibernética custando de US$ 1 a 9 milhões para 27% dos entrevistados e de 10 a 19 milhões, para 7%. Além das implicações financeiras, divulgações dos riscos de segurança cibernética, é um importante meio de comunicação para investidores, governos, consumidores, fornecedores e outras partes interessadas e consequentemente tem efeito na reputação e no aumento dos litígios (Gao et al., 2020).

Tabela 2

Tópicos das cartas comentários enviados a SEC

Tópico da carta comentários	**Frequência**	**%**
Incidente de segurança cibernética	39	75%
Risco de segurança cibernética	15	28,85%
Controle de segurança cibernética	4	7,69%
Outros - Ambiente de segurança	1	1,92

Fonte: Recuperado de *Responses to SEC comment letters on cybersecurity disclosures: An exploratory study*, de Wang, T., Yen, J. C., & Yoon, K., 2022.

As diretrizes de segurança cibernética da *Securities and Exchange Commission* SEC nos EUA influenciaram a divulgação em formulários públicos das empresas americanas,

iniciando uma série de estudos sobre o tema. Wang et al. (2022) mostram que empresas respondem às cartas de comentários, ajustando suas divulgações de segurança cibernética para atender às exigências da SEC. Por outro lado, Li et al. (2018) afirmam que a presença e a duração dos fatores de risco de segurança cibernética divulgados nos formulários 10-K estavam relacionadas a incidentes de segurança cibernética relatados, mas a associação tornou-se insignificante após a emissão da orientação da SEC.

Quanto à legibilidade do conteúdo publicado sobre riscos cibernéticos, Li et al. (2018) destacam a importância de tornar todas as informações sobre riscos de cibersegurança compreensíveis, de forma a orientar as decisões dos investidores e fornecer *insights* aos reguladores para padronização e aumento da transparência. Esse aspecto também foi abordado por Gao et al. (2020), que observaram que a legibilidade tende a diminuir à medida que a dimensão da empresa aumenta e se torna mais clara quando há aumento dos ativos intangíveis ou após mudanças na liderança executiva.

Nessa mesma preocupação, Calderon e Gao (2022) realizaram comparações entre as divulgações de riscos de segurança cibernética de empresas norte-americanas e estrangeiras, utilizando análises textuais dos registros nos formulários 20-F e 10-K. Os resultados do estudo mostraram que as empresas estrangeiras tendem a divulgar mais informações, apresentando uma legibilidade maior, mais números, menos incerteza e uma linguagem menos litigiosa em relação aos seus riscos de segurança cibernética.

No Canadá, Héroux e Fortin (2020) avaliaram as práticas das empresas do índice S&P/TSX 60 em relação às diretrizes dos reguladores financeiros. Os resultados revelaram níveis baixos de divulgação, com falta de especificidade e linguagem padronizada. As conclusões indicam a necessidade de melhorias e de requisitos regulatórios mais rigorosos.

Na contabilidade, o aumento das ameaças virtuais representa uma preocupação crescente para as organizações, incluindo os escritórios que lidam com informações confidenciais de empresas e indivíduos. Esse cenário despertou o interesse de pesquisadores como Janvrin e Wang (2019), que exploraram as implicações da segurança cibernética nas informações contábeis e destacaram a importância de investigações adicionais para compreender melhor seu impacto. Além disso, no contexto da divulgação de informações, os contadores desempenham um papel importante, pois possuem habilidades para auxiliar as empresas na elaboração de narrativas descritivas para relatórios externos (Eaton et al., 2019).

2.3 GOVERNANÇA CORPORATIVA, RISCOS CIBERNÉTICOS E SEGURANÇA CIBERNÉTICA

Conforme o Instituto Brasileiro de Governança Corporativa – IBGC (2022), espera-se que 60% dos comitês de auditoria abordem a segurança cibernética em suas agendas trimestrais. Além disso, uma pesquisa realizada pelo mesmo órgão revelou que 62% dos entrevistados consideram a segurança cibernética um dos principais riscos. A discussão também tem se expandido ao incluir questões de governança relacionadas à segurança cibernética abordando o papel pela proteção das informações financeiras (Li et al., 2020).

Chen et al. (2022) analisaram empresas afetadas por violações de dados entre 2005 e 2018, constatando que a experiência em TI do comitê de auditoria está vinculada à redução de violações e à melhor supervisão de riscos cibernéticos. Da mesma forma, Ashraf et al. (2020) investigaram os efeitos de especialistas em TI no comitê de auditoria, observando reduções significativas em falhas materiais relacionadas à TI. Em um estudo sobre 110 falhas operacionais de TI em empresas financeiras dos EUA, Benaroch e Chernobai (2017) destacaram que o aumento da competência em TI nos Conselhos de Administração correspondeu a uma menor reação negativa do mercado.

Da mesma forma, a presença de especialistas em TI no Conselho de Administração está correlacionada a probabilidade de evidenciação sobre riscos cibernéticos e, por isso, elaborou-se a seguinte hipótese:

H1: A experiência em TI do Conselho de Administração está positivamente associada a divulgação sobre risco cibernético.

De acordo com Gul et. al, (2011), o Conselho de Administração com mais membros femininos tem uma associação positiva na qualidade das informações evidenciadas dos relatórios da empresa. A investigação mostra consistentemente que Conselhos de Administração com mais mulheres em sua composição têm impacto positivo em diversos aspectos do desempenho e nos relatórios empresariais.

Chen et al. (2016) descobriram que as empresas com maior representação feminina no conselho apresentaram menos deficiências de controle interno, com melhoria na qualidade dos relatórios financeiros. Estudos como de Ben-amar et al. (2023) concluem que os Conselhos de Administração com mulheres diretoras influenciam positivamente a legibilidade e a qualidade das divulgações financeiras corporativas.

Reddy e Rao (2016) contribuem para o debate sobre a importância da presença feminina nos conselhos ao acrescentar o conceito da influência positiva da heterogeneidade na

divulgação cibernética. Para chegar também nessa conclusão, Radu e Smaili (2021) utilizaram uma amostra de empresas listadas no índice S&P/TSX 60 entre 2014 e 2018 e alertam que o Conselho de Administração deve contar com pelo menos três mulheres para que este impacto possa ser observado. Logo, ter mulheres nos Conselhos de Administração aumentam as divulgações sobre informações relacionadas com a segurança cibernética, conforme anunciam Héroux e Fortin (2022) na sua pesquisa.

Diante dessa constatação, formulou-se a seguinte hipótese:

H2: A presença feminina no Conselho de Administração está positivamente associada a divulgação de risco cibernético pelas empresas.

Poucos estudos anteriores demonstraram relação entre idade do conselho e nível de evidenciação de informações voluntárias. Empiricamente, diretores mais jovens tendem a estar mais dispostos e preparados para divulgar informações relacionadas à segurança cibernética por estarem sincronizados no mundo digital e seus desafios (Héroux & Fortin, 2022). Em suma, os executivos mais jovens assumem mais riscos e os gestores mais velhos são menos suscetíveis a aderir decisões arriscadas e consequentemente a divulgar menos (Vroom & Pahl, 1971).

Post et al. (2011) verificaram que os conselhos com uma idade média de 56 anos têm mais probabilidade de divulgar informações sobre Responsabilidade Social Corporativa Ambiental. Nguyen et al. (2023) estudaram as influências dos atributos de diretores executivos no desempenho financeiro e, descobriram que dentre as características analisadas, a idade avançada contribui para a melhoria do desempenho das empresas.

Por outro lado, diretores ou membros, mais, velhos nos comitês apresentam menos apoio dos acionistas nas participações nas reuniões (Masulis et al., 2018) e na área de segurança cibernética. Na mesma linha, Héroux e Fortin (2022) desvendaram que a idade dos membros do conselho está negativamente associada à extensão de divulgação de segurança cibernética e a mitigação de riscos.

Com base nessa comprovação, elabora-se a seguinte hipótese:

H3: A presença de membros mais jovens do Conselho de Administração tende a influenciar positivamente o nível de evidenciação sobre risco cibernético.

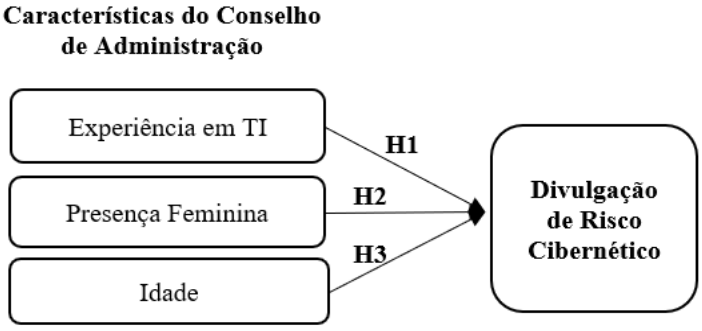
3 PROCEDIMENTOS METODOLÓGICOS

3.1 AMOSTRA E COLETA DE DADOS

A investigação documental verifica as associações entre o conteúdo de divulgação de risco cibernético com as hipóteses propostas (Figura 3).

Figura 3

Modelo e hipóteses da pesquisa



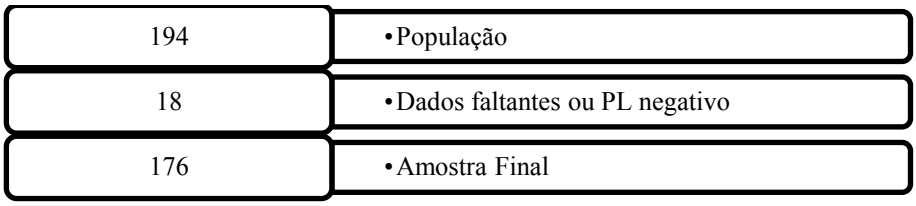
O instrumento de pesquisa utilizado é o Formulário de Referência (FR), visto que a maioria das pesquisas como as de Gordon et al. (2010), Wang et al. (2013), Li et al. (2018) e Calderon e Gao (2022) sobre evidenciação de risco cibernético utilizaram o formulário 10-K, que é um relatório anual que todas as empresas públicas devem apresentar à SEC, semelhante ao FR no Brasil.

Uma análise textual da variável dependente foi realizada, Nela foram utilizadas as palavras-chave da Tabela 3, desenvolvida com base em sugestões de estudos anteriores. Isso nos permitiu identificar os conteúdos cruciais nos Relatórios Financeiros relacionados à segurança cibernética.

A população da pesquisa são as empresas listadas na B3 e a amostra é formada por aquelas que compõe o segmento do Novo Mercado das carteiras dos anos de 2020, 2021 e 2022 que totalizaram 194 empresas (Anexo 1). As empresas foram selecionadas devido ao alto padrão de governança corporativa do Novo Mercado (B3, 2024). Além disso, Cruz et al. (2011) justificam essa escolha pelo compromisso dessas empresas com a qualidade e transparência na divulgação de informações. Foram excluídas da amostra as empresas com dados faltantes ou Patrimônio Líquido (PL) negativo, resultando em uma amostra final de 176 empresas, conforme mostrado na Figura 4.

Figura 4

Tratativas da amostra



Os dados textuais foram manualmente coletados dos FRs das versões mais recentes das empresas, de acordo com a metodologia utilizada por Radu e Smaili (2021), Héroux e Fortin (2022) e Smaili et al. (2023). A coleta ocorreu entre janeiro e fevereiro de 2024, acessando os documentos nos *websites* oficiais de cada empresa (Apêndice 1).

A identificação do conteúdo textual relevante para quantificar as variáveis dependentes seguiu palavras-chave predefinidas, de acordo com as descrições na Tabela 3, que segue os padrões estabelecidos na literatura anterior.

Tabela 3

Palavras-chaves para identificação do conteúdo de divulgação de riscos cibernéticos

Conteúdo de divulgação de riscos de segurança cibernética	Palavras-chaves	Referência
Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco	*Cyber*, cibersegurança, informações, cibernético, TI, tecnologia, proteção, informação, dados, ameaça, digital, *hacker*	Li et al. (2018) Smaili et al. (2023) Chen et al. (2023) Gao et al. (2020) Héroux e Fortin (2022) Héroux e Fortin (2020)

3.2 Variáveis do estudo e modelo econométrico da pesquisa

As variáveis dependentes, independentes e de controle selecionadas para o estudo, bem como a fundamentação teórica por trás de sua escolha estão apresentadas na sequência. Além disso, serão discutidos os critérios adotados para a construção do modelo econométrico, incluindo a especificação das relações entre as variáveis e a escolha das técnicas de estimação apropriadas.

A definição das variáveis e a especificação do modelo econométrico servem como base para a análise estatística e a interpretação dos resultados. Os dados coletados foram tabulados e compilados em uma planilha eletrônica em formato de painel e, em seguida, operacionalizados utilizando o *software* StudioR®. As variáveis que compõem o modelo

econométrico deste estudo estão listadas na Tabela 4 e foram selecionadas com base nos estudos de Héroux e Fortin (2022), Smaili et al. (2023) e Radu e Smaili (2022).

Por meio dessa análise, espera-se contribuir para uma compreensão mais profunda dos fenômenos estudados e para o avanço do conhecimento científico no campo da pesquisa empírica de segurança cibernética.

Tabela 4

Variáveis da regressão

	Variáveis dependentes	**Abreviações**	**Operacionalização**	**Coleta**
	Riscos cibernéticos sobre ameaças, vulnerabilidades, probabilidades e impactos no ambiente de TI	RISCO_CIBER	A companhia entende que há riscos sobre a segurança da informação? valor 1 para "sim" e "não" assume valor 0	Formulário de Referência
Hs	**Variáveis independentes**	**Abreviações**	**Operacionalização**	**Coleta**
H1	Experiência em TI do conselho	B_EXP	Porcentagem de membros do conselho com experiência em TI	Formulário de Referência
H2	Presença feminina no conselho	B_FEMININA	Porcentagem de mulheres no conselho	Formulário de Referência
H3	Idade do conselho	B_IDADE	Valor 1 para resultados baixo do 1° quartil da média de idade e para resultados acima do 1° quartil da média de idade assume o valor 0.	Formulário de Referência
	Variáveis de controle			
	Lucratividade	ROA	Lucro líquido/ativo total	ECONOMATICA®
	Tamanho	TAM	Logaritmo natural do ativo total	ECONOMATICA®
	Incidente Cibernético	ATAQUE	A companhia sofreu ataque cibernético. Valor 1 para "sim" e "não" assume o valor 0.	ECONOMATICA®
	Valor de Mercado	VM	Valor de mercado	ECONOMATICA®
	Alavancagem	ALAV	Empréstimos/PL	ECONOMATICA®

O suporte para as hipóteses é baseado na significância dos coeficientes de regressão das variáveis independentes e as regressões são realizadas para a variável dependente com a finalidade de verificar a associação com a divulgação de riscos cibernéticos.

3.2.1 Variável dependente

A variável dependente foi construída de acordo com as orientações em termos de melhores práticas do *Frameworks for Improving Critical Infrastructure Cybersecurity* (NIST)

(Tabela 5), desenvolvido pela agência dos Estados Unidos e que fornecem uma lista de padrões, diretrizes e práticas de segurança cibernética.

Tabela 5

Variável dependente

Conteúdo de divulgação de riscos de segurança cibernética	**Referência Informativa**
Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 /IEC 27001:2013 Cláusula 6.1.2

Fonte: Adaptado de *Framework for improving critical infrastructure cybersecurity* NIST, Barrent, 2018 & Public *compan'es' cybersecurity risk disclosures*.

3.2.2Variáveis Independentes

As variáveis independentes foram coletadas dos FRs de cada empresa da amostra, sendo verificadas por meio dos currículos disponíveis no tópico "Composição e experiência".

A variável independente (B_EXP) avalia se os membros do Conselho de Administração possuem experiência profissional ou formação acadêmica na área de TI. Alguns pesquisadores como Héroux e Fortin (2022) também utilizaram da mesma variável para verificar a extensão da divulgação de informações sobre segurança cibernética. Para esta categoria foram consideradas as porcentagens dos membros com experiência em TI em relação ao total de membros do Conselho de Administração.

A segunda variável (B_FEMININA) representa a igualdade de gênero e a justiça social no Conselho de Administração, sendo caracterizada na amostra pela proporção de mulheres nos conselhos. Espera-se com este componente ter resultados positivos assim como nos achados das pesquisas de Héroux e Fortin (2022) e Radu e Smaili (2022).

Por fim, para a variável idade (B_IDADE), calculou-se a média das idades dos membros do Conselho de Administração de cada empresa, em consonância com os resultados de Héroux e Fortin (2022). No entanto, para observar quais empresas apresentaram membros mais jovens, conforme descrito na H3, calculou-se o 1º quartil de todas as médias das idades dos membros dos conselhos de todas as empresas da amostra. A partir desse resultado, atribuiu-se uma variável *dummy*, com o valor 0 para resultados acima do 1° quartil da média das idades dos membros do conselho, e o valor 1 para os resultados abaixo do 1° quartil.

3.2.3 Variáveis de Controle

A base de dados para as variáveis de controle foram coletados do sistema Economatica® e calculados por meio de índices financeiros, conforme indicado em estudos anteriores que demonstraram ter influência na divulgação em matéria de riscos cibernéticos e cibersegurança, tais como: logaritmo natural do ativo da empresa (TAM), visto que as empresas maiores divulgam mais sobre segurança das informações (Radu & Smaili, 2021; .Heroux & Fortin, 2022; Smaili et al. 2023; Masoud Al-Utaibi, 2022; Gao et al., 2020; Evans et al., 2023); o retorno de lucratividade (ROA) que tem relação positiva com a divulgação (Gao et al., 2020; Evans et al., 2023; Heroux & Fortin, 2022); alavancagem (ALAV) (Smaili et al., 2023; Héroux e Fortin, 2022; Alshirash et al., 2020; Radu e Smaili, 2022); valor de marcado *market to book* (VM) (Radu e Smaili, 2022; Smaili et al., 2023; Héroux e Fortin, 2022; Radu e Smaili, 2022) e incidentes de segurança cibernética (ATAQUE) visto que na Resolução CVM nº 135, art. 111, existe uma obrigatoriedade da empresa divulgar incidentes cibernéticos para o Conselho de Administração.

3.3 MODELO DE REGRESSÃO

O método analítico utilizado nesta pesquisa foi a regressão logística, devido à sua capacidade de lidar com variáveis binárias ou dicotômicas, assim como nos estudos de Ashraf (2022); Héroux e Fortin (2022) e Radu e Smaili (2021) que buscaram entender a relação entre características do Conselho de Administração e a divulgação de riscos cibernéticos.

Ao focar em variáveis de resposta que indicam a presença ou ausência de divulgação de riscos cibernéticos, a regressão logística se torna apropriada para modelar essa relação, permitindo estimar a probabilidade de divulgação de riscos cibernéticos (ODDS Ratio) com base nas características do Conselho de Administração que compõem as hipóteses do estudo. Portanto, a escolha deste método estatístico se justifica pela sua adequação para lidar com a natureza das variáveis envolvidas e pela capacidade de oferecer interpretações claras e relevantes para os objetivos da pesquisa.

Assim, RISCO_CIBER é uma variável binária que indica a divulgação de riscos cibernéticos (1 para sim, 0 para não). Portanto, a equação de regressão logística pode ser formulada da seguinte maneira, conforme a Equação:

$$P(RISCO\_CIBER = 1) = 1/(1 + \varepsilon - (\beta_0 + \beta_1 B\_EXP_{it} + \beta_2 B\_FEMININA_{it} + \beta_3 B\_IDADE_{it} + \beta_4 ROA_{it} + \beta_5 TAM_{it} + \beta_6 ATAQUE_{it} + \beta_8 VM_{it} + \beta_9 ALAV_{it}$$

Em que:

- $\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7, \beta_8, \beta_9$ são os coeficientes utilizados para estimar a regressão por empresa *i* e ano *t*.
- B_EXP, B_FEMININA, B_IDADE, são as variáveis independentes por empresa *i* e ano *t*;
- ROA, TAM, ATAQUE, VM, ALAV são as variáveis de controle por empresa *i* e ano *t*;
- P(RISCO_CIBER =1) é a variável *dummy* com a probabilidade de divulgação de riscos cibernéticos.

Esta equação estima a probabilidade de uma empresa divulgar riscos cibernéticos com base nas características do Conselho de Administração (experiência em TI, presença feminina e idade), bem como a sua relação com os indicadores financeiros como ROA (Retorno sobre os ativos), TAMANHO (Logaritmo natural do ativo), ATAQUE (Histórico de Ataques), VM (Valor de Mercado) e ALAV (Alavancagem).

4 ANÁLISE DOS RESULTADOS

4.1 ANÁLISE DESCRITIVA DOS DADOS E REGRESSÃO

A análise descritiva dos dados envolve a compreensão inicial do perfil dos dados e revela informações importantes sobre a sua estrutura e variabilidade. Durante o período investigado neste estudo, a amostra final foi composta por 512 observações, abrangendo um total de 3.998 membros no Conselho de Administração, conforme Tabela 6.

Tabela 6

Estatística descritiva das variáveis independentes e de controle

Variáveis	Descrição	Média	Mediana	Desv. Padrão	Mínimo	Máximo
N=512						
Variáveis Independentes						
B_FEMININA	Porcentagem de mulheres no conselho	16%	14%	12%	0%	66%
B_EXP	Porcentagem de membros com experiência em TI	2%	0%	5%	0%	33%
B_IDADE	1° quartil da média de idade	56	56	7	39	78
Variáveis de controle						
ROA	Lucro líquido/ ativo total	0,03	0,03	0,09	-1,06	0,37
TAM	Logaritmo natural do ativo total	15,64	15,40	1,53	11,49	21,43
ALAV	Empréstimos/ PL	5,44	0,49	16,47	0,00	113,41
VM	Valor de Mercado	1,22	3,45	2,37	1,18	1,45
Variável dependente						
RISCO_CIBER	Riscos sobre segurança da informação	85,7%	1	0,37	0	1

Da análise da Tabela 6, observou-se que 85,7% das empresas divulgaram informações sobre risco cibernético. Houve um aumento de 17% de 2020 para 2022, semelhante ao 20% de crescimento observado por Smaili et al. (2023) de 2014 a 2018. Este resultado de evidenciação de risco cibernético está em linha com os achados de Héroux e Fortin (2020), que descobriram que 87% das empresas da amostra consideram a segurança cibernética como um fator de risco. Além disso, Gao et al. (2020), em sua pesquisa "*Cybersecurity risk disclosures by public companies*", afirmam que as divulgações aumentaram significativamente para todos os tipos de

riscos de segurança cibernética. Por sua vez, poucos membros do conselho apresentaram experiência em TI, especificamente apenas 2%.

O tamanho das empresas analisadas tem uma média de R$29.173,09 milhões. Destaca-se que o Banco do Brasil deteve o maior ativo da amostra, totalizando R$2.028.958,14 milhões, enquanto a Westing registrou o ativo mais baixo em 2020, com R$97.877 milhões. No que diz respeito ao Retorno sobre Ativos (ROA), a empresa que obteve o maior retorno em relação aos seus ativos totais foi o Banco do Brasil Seguridade, com 37%, enquanto a Nexpe apresentou o menor, com -106%, resultando uma média de 3,03%. Em relação ao valor de mercado, a Vale se destacou como aquela com maior valor, enquanto a Nexpe, o menor.

Em relação à divulgação de ataques cibernéticos, constatou-se que em 2022, 9% das empresas analisadas já foram vítimas de algum incidente. Assim, pode-se entender que o risco cibernético está sendo uma das maiores ameaças às empresas nos últimos anos (Radu & Smaili, 2021). No total, foram 17 empresas, das quais, 29% são do setor de comércio varejista (Tabela 7). Essa observação pode estar alinhada a grande volume de transações com as vendas *on-line* com o armazenamento de uma grande quantidade de base de dados pessoais dos seus clientes, importantes para os *hackers*.

Tabela 7

Características das empresas que divulgaram ter sofrido ataques cibernéticos

Setor	
Comércio Varejista	5
Petróleo, Gás e Biocombustíveis	3
Serviços Médico - Hospitalares, Análises e Diagnósticos	2
Material de Transporte	1
Agropecuária	1
Produtos de Cuidado Pessoal e de Limpeza	1
Transporte	1
Programas e Serviços	1
Construção Civil	1
Viagens e Lazer	1

Com a finalidade de controlar os valores extremos nos dados, foi realizada a *winzorização* a 1%, dessa forma as extremidades diminuem, uma vez que há substituição de valores discrepantes pelos valores menores e maiores remanescentes dos percentis mínimos e máximos a nível de 1%. Para avaliar a multicolinearidade, utilizou-se a estatística VIF (*Variance Inflation Fator*) conforme orientado por Montgomery et al. (2021) (Tabela 8). O VIF indica quanto a variância de um coeficiente de regressão é aumentada devido à distinção de

suas influências separadamente entre as variáveis independentes, como explicado por Montgomery et al. (2021). A multicolinearidade ocorre quando duas ou mais variáveis estão correlacionadas entre si, o que dificulta a distinção de suas influências separadamente no modelo de regressão. Para que a regressão seja considerada aceitável, é geralmente exigido que o fator de inflação da variância para os estimadores seja inferior a 4 (Fávero & Belfiori, 2017).

Tabela 8

VIF

Variáveis	VIF
B_FEMININA	1,05345
B_EXP	1,00623
B_IDADE	1,04522
TAM	1,13390
ROA	1,75742
ALAV	1,16574
VM	1,70765
ATAQUE	1,00000

Em geral, os valores de VIF estão abaixo de 4, o que indica que a Multicolinearidade não é um problema significativo neste modelo.

Para avaliar a qualidade do modelo de regressão logística utilizou-se o Pseudo-R Quadrado, que fornece uma medida relativa de ajuste do modelo em relação ao modelo nulo.

Tabela 9

Pressupostos da regressão

Descrição	Teste	Dif	Valor
Critério de Informação de Akaike	AIC	10	340,4797
Critério de Informação Bayesiano	BIC	10	378,5185
Nagelkerke R-squared	Nagelkerke		0,29614

Na interpretação do Nagelkerke (1991), o R-squared envolve compreender a proporção da variabilidade explicada pelo modelo em relação à variabilidade total dos dados. Um valor mais alto do que o Nagelkerke R-squared indica um melhor ajuste do modelo em comparação com um modelo nulo (Nagelkerke,1991). O Nagelkerke R-squared (Tabela 9) indica que aproximadamente 29% da variabilidade dos dados é explicada pelo modelo, o que representa um alto poder explicativo.

O *Akaike Information Criterion* (AIC) é uma medida de qualidade de ajuste de um modelo estatístico (Akaike, 1974). Quanto menor o valor do AIC, melhor o ajuste do modelo

aos dados observados, considerando o *trade-off* entre a complexidade do modelo e sua capacidade de explicar os dados (Akaike, 1974). Neste estudo com 10 graus de liberdade, o AIC é de aproximadamente 340,47 (Tabela 8).

O *Bayesian Information Criterion* (BIC) é usado para avaliar o ajuste de modelos estatísticos aos dados observados, levando em consideração a complexidade do modelo (Schwarz, 1978). Assim como o AIC, quanto menor o valor do BIC, melhor o ajuste do modelo aos dados observados

4.2 TESTE DE HIPOTESES

A partir dos testes de ajustes do modelo, considera-se adequada a regressão logarítmica realizada (Tabela 9).

Tabela 10

Resultados da Regressão – Risco Cibernético

Variáveis Independentes e de Controle	Regressão Logística Binária					Sinais Esperados
	Variável dependente	Medidas estatísticas				
	Estimate	z value	Pr(>|z|)	OR	P=valor	
(Intercepto) *(Erro Padrão)*	-4,73 1,99	-2,37	0,018	8,84	*	+
B_FEMININO *(Erro Padrão)*	6,88 1,49	4,61	4,03E-06	9,77	***	+
B_EXP *(Erro Padrão)*	1,76 9,40	1,87	0,06	4,43	.	+
B_IDADE *(Erro Padrão)*	3,52 3,43	1,02	0,3	1,42		+
TAM *(Erro Padrão)*	3,91 1,32	2,95	0,003	1,47	**	+
ROA *(Erro Padrão)*	-9,23 2,03	-4,53	5,68E-06	9,78	***	+
ALAV *(Erro Padrão)*	-3,10 1,06	-0,29	0,77	9,96		+
VM *(Erro Padrão)*	-7,09 7,21	-0,98	0,32	1,00		+
ATAQUE *(Erro Padrão)*	1,60 9,30	0,01	0,98	9,13		+

Nota: *, ** e *** indicam significância estatística, respectivamente, a 10%, 5% e 1%.

O teste de hipóteses tem por objetivo avaliar a evidência contra a hipótese nula H0 (de que não há influência da evidenciação de riscos cibernéticos com as características de experiencia em TI, participação feminina e idade). Por sua vez, o valor p é a probabilidade de observar um valor da estatística z se a hipótese nula H0 for verdadeira. Por outro lado, o *Odds*

Ratio (OR) indica a medida de associação entre as variáveis independentes (B_FEMININO, B_EXP e B_IDADE) com a variável dependente (RISCO_CIBER) do modelo de regressão logística. Ele representa a chance de ocorrência do risco cibernético para um aumento unitário das variáveis independentes, mantendo todas as outras variáveis constantes.

Com base nesses conceitos, os resultados indicam que **(H1**) a experiência em TI do Conselho não é estatisticamente significativa, portanto, rejeita-se **H1**, pois não está associado a evidenciação de riscos cibernéticos. Ao rejeitar **H1**, observa-se um contraste aos achados de Benaroch e Chernobai (2017), Heroux e Fortin (2022) e Smaili et al. (2023) de que a experiência em TI melhora a evidenciação de segurança cibernética

Por conseguinte, a presença feminina **(H2)** apresenta uma alta significância estatística de 1 % que a chance de haver uma maior divulgação de informações sobre risco cibernético é 9,77 vezes maior (OR = 9,770160) quando há a presença de mulheres na composição do Conselho de Administração, com um nível de confiança de 97,5**%.**

Portanto, em relação as demais hipóteses, não se rejeita **(H2)** e se pode afirmar que mulheres tem uma associação positiva com a divulgação de riscos cibernéticos. Essa conclusão é consistente com as evidências de Radu e Smaili (2021), que apontam associação positiva entre a presença e o nível de divulgação de segurança cibernética e a diversidade de gênero no Conselho de Administração quando há pelo menos três mulheres no conselho. Isso sugere que as mulheres promovem a cultura de cibersegurança ao direcionar a atenção para os riscos cibernéticos e ao destacar sua importância (Radu & Smaili, 2021).

Adicionalmente, a literatura mostra que as mulheres nos Conselhos de Administração têm uma inclinação para promover a transparência das empresas (Larkin et al., 2013). Portanto, conselhos com maior participação feminina podem tender a implementar mais mecanismos de divulgação para mitigar o risco de segurança cibernética (Radu e Smaili, 2021). Essa conclusão é reforçada pelos resultados de Héroux e Fortin (2022), que também encontraram uma associação positiva entre a presença de mulheres diretoras e divulgação de segurança cibernética.

Conforme destacado por Tao et al. (2020), Conselhos de Administração mais diversificados em termos de gênero impactam na clareza e no tom das divulgações financeiras corporativas, no contexto da Teoria dos Escalões Superiores. As autoras enfatizam a contribuição especialmente positiva das mulheres diretoras para a qualidade e transparência dessas divulgações financeiras.

Por sua vez, a B_IDADE não apresentou significância, isso sugere que membros mais novos do Conselho de Administração não estão associados a uma maior probabilidade de evidenciação sobre risco cibernético, o que contradiz a hipótese formulada, mantendo todas as outras variáveis constantes, portanto, a hipótese **H3** é rejeitada. Contrariamente à nossa expectativa, a idade do conselho não está significativamente associada à divulgação de segurança cibernética corroborando inclusive Héroux e Fortin (2022).

O ROA, que representa a rentabilidade dos ativos em relação à receita, revelou um aspecto surpreendente: empresas com um índice mais alto aumentam em 9,7 vezes as chances de divulgar riscos cibernéticos. Este achado confirma a expectativa inicial de que a rentabilidade das empresas estaria positivamente relacionada à divulgação da segurança cibernética. Comumente, espera-se que empresas lucrativas tenham mais capacidade de arcar com os custos associados à divulgação de informações relevantes para as partes interessadas (Smaili et al., 2023).

Por sua vez, a variável de controle (TAM) também apresentou significância a um nível de 5%. Esse resultado é consistente aos achados de Radu e Smaili (2021) de que o tamanho está positivamente associado ao nível de divulgação de segurança cibernética, porque as empresas de maiores enfrentam custos de agência mais elevados e mais pressão de divulgação por parte das partes interessadas e, consequentemente, fornecem mais divulgação para reduzir a assimetria de informação e legitimar as suas atividades (Radu & Smaili, 2021). Contrariamente aos achados de Héroux e Fortin, (2022) não encontraram resultados significativos entre o tamanho das empresas com a divulgação de riscos cibernéticos.

5 CONSIDERAÇÕES FINAIS

O risco cibernético emergiu como um dos principais focos de preocupação nas empresas. Consequentemente, a pesquisa sobre esse tema tem experimentado um notável avanço nos últimos anos, espelhando o crescente reconhecimento da relevância da segurança cibernética na guarda dos ativos de informações financeiras e na asseguração da integridade dos dados.

Por sua vez, para a governança corporativa, a identificação do risco cibernético nos Conselhos de Administração mostrou-se essencial na proteção contra ameaças cibernéticas, cumprimento de regulamentações, tomadas de decisões estratégicas, aumento da resiliência organizacional. Assim, a identificação e comunicação dos riscos cibernéticos demonstram transparência e responsabilidade corporativa, construindo confiança com os *stakeholders.*

Com base na literatura anterior, argumentou-se que características como experiência em TI, a presença feminina e idade no Conselho de Administração podem ser determinantes na divulgação de riscos cibernéticos. A partir de uma amostra com 512 observações, no período de 2020 a 2022, por meio do modelo de regressão logística, testou-se empiricamente as hipóteses sobre as características observáveis do Conselho de Administração e a sua associação com a divulgação de segurança cibernética.

Dos resultados, observou-se que a experiencia em TI não apresentou significância com a divulgação de risco cibernético, portanto, rejeitou-se **(H1).** A segunda hipótese **(H2)** apontou que a presença feminina está positivamente associada a maior divulgação sobre riscos cibernéticos, portanto, não se rejeita **(H2).** Ao passo que, a idade (H3) esta negativamente associada a divulgação de riscos cibernéticos, portanto, rejeita-se **(H3).**

Os achados deste trabalho complementam os resultados de estudos anteriores de conselho com experiência em TI (Ashraf et al., 2020); presença feminina nos conselhos (Radu & Smaili, 2021) e idade (Héroux & Fortin, 2022). Ademais, estas conclusões podem ser adicionadas a outros aspectos já estudados na literatura por outros pesquisadores, tais como a eficácia do conselho (Smaili et al., 2022), independência do conselho (Smaili et al.,2022; Héroux e Fortin, 2022); mandato do conselho (Héroux e Fortin, 2022); *expertise* financeira (Smaili et al., 2023) e comitê de TI (Héroux e Fortin, 2022) que se utilizaram de diferentes enquadramentos teóricos. Além disso, este estudo expande a análise sobre pesquisas como de Alshirah et al. (2020) e Khandelwal et al. (2020) que abordam as características do Conselho de Administração e a divulgação de riscos corporativos, ao incluir o risco cibernético como parte dos resultados.

Por conseguinte, este trabalho tentou diminuir a lacuna na literatura sobre divulgação cibernética, conforme demandado por Haapamäki e Sihvonen (2019), Walton et al. (2021) e Walton et al. (2022). Os resultados indicam um alto nível de divulgação sobre riscos cibernéticos, porém, as informações fornecidas são padronizadas e não específicas de cada empresa.

As descobertas contribuem também para o debate sobre a importância da governança corporativa para a evidenciação da segurança cibernética. As conclusões podem trazer reflexões para os membros do Conselho de Administração sobre a natureza e gerenciamento dos riscos cibernéticos. Além disso, os reguladores podem considerar o nível de divulgação encontrado para respaldar iniciativas regulatórias voltadas a promover uma representação mais equilibrada de mulheres nos Conselhos de Administração das empresas.

Para pesquisas futuras recomenda-se expandir a amostra de modo a incluir todas as empresas listadas na B3 para uma visão mais abrangente, além de analisar outras variáveis dependentes, tais como, seguros cibernéticos, treinamentos, políticas de TI, comitês de TI ou diretoria em TI para avaliar o nível de evidenciação de segurança cibernética.

REFERÊNCIAS

Akaike, H. (1974). A new look at the statistical model identification. *IEEE transactions on automatic control*, 19(6), 716-723.

Almunawwaroh, M., & Setiawan, D. (2023). Does audit committee characteristics a driver in risk disclosure?. *Cogent Business & Management*, 10(1), 2167551.

Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D. (2018), "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", *Journal of Cybersecurit*y, 4(1), 1-15.

Almunawwaroh, M. e Setiawan, D. (2023). As características do comitê de auditoria são um direcionador na divulgação de riscos?. Negócios e Gestão Cogente, 10 (1), 2167551.Alshirah, M. H., Rahman, A. A., & Mustapa, I. R. (2020). Board of directors' characteristics and corporate risk disclosure: the moderating role of family ownership. *EuroMed Journal of Business*, 15(2), 219-252.

Al-Sartawi, A. M. M. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructure*s, 16(2), 150-161.

Aneel. Resolução normativa nº 964/2022. (2022). Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Fonte: https://www2.aneel.gov.br/cedoc/ren2021964.html

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies,* 23, 1177-1206.

Ashraf, M., Michas, P. N., & Russomanno, D. (2020). The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *The Accounting Review*, 95(5), 23-56.

Al-Shammari, B. (2014). An investigation of the impact of corporate governance mechanisms on level of corporate risk disclosure: evidence from Kuwait. *International Journal of Business and Social Research*, Vol. 4 No. 6, pp. 51-70.

Bansal, P., & Clelland, I. (2004). Falando de lixo: legitimidade, gerenciamento de impressão e risco não sistemático no contexto do ambiente natural. *Academy of Management Journal*, *47*(1), 93-103.

Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, *NIST Cybersecurity Framework*, [online], https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov /cyberframework.

Ben-Amar, W., García-Meca, E., Francoeur, C., & Martínez-Ferrero, J. (2023). Do Gender-Diverse Boards Enhance the Linguistic Features of Corporate Financial Reporting?. *Accounting Horizons*, 1-25.

Benaroch, M. e Chernobai, A. (2017). Falhas operacionais de TI, destruição de valor de TI e mudanças na governança de TI no nível do conselho. *MIS trimestralmente*, 41 (3), 729-A6.

Bisso, R., Kreutz, D., Rodrigues, G., & Paz, G. (2020). Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação*, 3(1)

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice,* 40, 131-158.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of accounting and public policy*, 37(6), 527-544.

Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants, Cybersecuri'y Isn't Just for "Techies": Incorporating Cybersecurity into the Accounting Curriculum. *Issues in Accounting Education*, 37(3), 73-89.

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal,* 33(4), 360-376.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508-526.

Calderon, T. G., & Gao, L. (2022). Comparing the Cybersecurity Risk Disclosures of US and Foreign Firms. *Journal of Emerging Technologies in Accounting,* 19(2), 61-79.

Cisco. (2021). Proteção contra ransomware Segurança Zero Trust para uma força de trabalho moderna. Fonte: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/protecting-against-ransomware.pdf

Chen, Y., Eshleman, J. D., & Soileau, J. S. (2016). Board gender diversity and internal control weaknesses. *Advances in accounting,* 33, 11-19.

Chen, C., Hartmann, C., & Gottfried, A. (2022). The Impact of Audit Committee IT Expertise on Data Breaches. *Journal of Information Systems,* 36(3), 61-81.

Chen, N. X., Chi, S., & Shevlin, T. (2023). A tale of two forecasts: An analysis of mandatory and voluntary effective tax rate forecasts. *The Accounting Review,* 1-26.]

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199-224.

Cui, J., Jo, H., & Na, H. (2018). Does corporate social responsibility affect information asymmetry? *Journal of business ethics*, 148, 549-572.

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting,* 20(1), 15-38.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on risk and insurance-Issues and practice*, 47(3), 698-736.

Comissão Monetária Nacional Resolução n° 4.893 de 26/2/2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893

Comissão de Valores Monetário. Resolução nº 135/22. Fonte: https://conteudo.cvm.gov.br/legislacao/resolucoes/resol135.html

Cruz, A. P. C., Machado, E. A., Pereira, A. F., Oleiro, W. N., & Carvalho, L. N. (2014). Empresas brasileiras do novo mercado e suas práticas de evidenciação voluntária de informações por segmento. *SINERGIA-Revista do Instituto de Ciências Econômicas*, Administrativas e Contábeis, 18(2), 19-36.

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, 23(3), 779-805.

Deloitte. (2023). Futuro da Segurança Cibernética 2023. Fonte: https://www2.deloitte.com/br/pt/pages/risk/articles/futuro-seguranca-cibernetica.html.

Deumes, R., & Knechel, W. R. (2008). Economic incentives for voluntary reporting on internal risk management and control systems. *Audit Journal of practice & theory*, 27(1), 35-66.

Eaton, T., Grenier, J., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing* 13 (2): C1–C9.

Evans, C. A., Beyer, B., Mason, T. W., & West, A. N. (2023). Data Breach Severity and Debt Market Responses. *Accounting and the Public Interest*, *23*(1), 76-109.

Elshandidy, T., Fraser, I. and Hussainey, K. (2015), "What drives mandatory and voluntary risk reporting variations across Germany, UK and US?", *The British Accounting Review*, Vol. 47 No. 4, pp. 376-394.

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law & Security Review*, 40, 105513.

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The journal of law and Economics*, 26(2), 301-325.

Fávero, L. P., & Belfiore, P. (2017). Manual de análise de dados: estatística e modelagem multivariada com Excel®, SPSS® e Stata®. Elsevier Brasil.

Frank, ML, Grenier, JH, & Pyzoha, JS (2019). How Disclosure of a Previous Cyberattack Influences the Effectiveness of Cybersecurity Risk Management Reporting and Independent Assurance. *Journal of Information Systems*, *33*(3), 183-200.

Field, L., Lowry, M., & Shu, S. (2005). Does disclosure deter or trigger litigation? *Journal of Accounting and Economics*, 39(3), 487-507.

Forbes. (2021). 5 ataques cibernéticos no Brasil em 2021 que geraram alerta. Fonte: https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/

Fortinet (2022). Relatório de Cenário de Ameaças Global 2022. Fonte: https://www.fortinet.com/br/solutions/industries/power-utilities

Gigler, F. B., & Hemmer, T. (2001). Conservatism, optimal disclosure policy, and the timeliness of financial reports. *The Accounting Review*, 76(4), 471-493.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38, 100468.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS quarterly*, 567-594.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy,* 34(5), 509-519.

Gul, F. A., Srinidhi, B., & Ng, A. C. (2011). Does board gender diversity improve the informativeness of stock prices?. *Journal of accounting and Economics*, 51(3), 314-338.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management,* 52(3), 337-347.

Hayel, Y., & Zhu, Q. (2015). Attack-aware cyber insurance for risk sharing in computer networks. *I*n Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings 6 (pp. 22-34). Springer International Publishing.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834.

Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *Current Issues in Auditing,* 15(2), A9-A23.

Héroux, S., & Fortin, A. (2022). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance,* 1-46.

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, 19(2), 73-100.

Hirst, D. E., Koonce, L., & Venkataraman, S. (2007). How disaggregation enhances the credibility of management earnings forecasts. *Journal of Accounting Research*, 45(4), 811-837.

Hughes, H., Smith, T. J., & Walton, S. (2023). Material Contract Redactions and Cybersecurity Breaches. *Accounting Horizons*, 1-27.

Ibrahim, S. N. S., Shamsudin, A., Abdullah, S., Ibrahim, M. T., Jaaffar, M. Y., & Bani, H. (2021). Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia. *International Journal of Academic Research in Accounting, Finance and Management Sciences.*

Instituto Brasileiro de Governança Corporativa (IBGC). (2022). 5 tendências aos Comitês de Auditoria em 2022. Fonte: https://ibgc.org.br/blog/tendencias-comite-de-auditoria-2022#:~:text=A%20maioria%20(60%25)%20dos,de%20conhecimento%20adicional%20nessa%20%C3%A1rea.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journ*al, 33(4), 377-409.

ISO/IEC 27001:2013 (2013). Tecnologia da Informação—Técnicas de Segurança—Sistemas de Gerenciamento de Segurança da Informação—Requisitos. A Organização Internacional de Normalização (ISO): Genebra, Suíça.

Janvrin, D. J., & Wang, T. D. (2021). Linking Cybersecurity and Accounting: An Event, Impact, Response Framework Linking Cybersecurity and Accounting. *Accounting Horizons.*

Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems,* 36(1), 151-180.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management,* 56(5), 681-695.

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. *Journal of Information Systems*, 33(3), A1-A2.

Khandelwal, C., Kumar, S., Madhavan, V., & Pandey, N. (2020). Do board characteristics impact corporate risk disclosures? The Indian experience. *Journal of Business Research*, 121, 103-111.

Kamiya, S., Kang, J.K., Kim, J., & Milidonis, A. and Stulz, R.M. (2018), "What is the impact of successful cyberattacks on target firms?", *National Bureau of Economic Research*, working paper nº 24409.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719-749.

Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information System*s, 34(3), 133-157.

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems,* 27(1), 219-236.

Kuipers, S., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Revie*w, 25(3), 176-197.

Lankton, N., Price, J. B.; Karim, M. (2021). Cybersecurity Violations and the Role of Information Technology Governance in Audit Committee Bylaws. *Journal of Information Systems*, 35(1), 101-119.

Larkin, M. B., Bernardi, R. A., & Bosco, S. M. (2013). Does female representation on boards of directors associate with increased transparency and ethical behavior? *Accounting and the Public Interest*, 13(1), 132–150.

Lima.V. H. (2018). Hacktivismo e a Defesa Cibernética do Brasil. Centro de Estudos Estratégicos do Exército: Análise Estratégica, 8(2), 12-18.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40-55.

Leroy, I. (2022). The relationship between cyber-attacks and dynamics of company stock: the role of reputation management. *International Journal of Electronic Security and Digital Forensics*, 14(4), 309-317.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theor*y, 39(1), 151-171.

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, 19(6), 321-330.

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, 76(2), 131-140.

Masulis, R., Wang, C., Xie, F., & Zhang, S. (2018). Directors: older and wiser, or too old to govern?. *Journal of Financial and Quantitative Analysis*, 1-40.

Michel, A., Oded, J., & Shaked, I. (2020). Do security breaches matter? The shareholder puzzle. *European Financial Management*, 26(2), 288-315.

Microsoft (2023). Fonte: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a cyberattack#:~:text=Ataques%20cibern%C3%A9ticos%20s%C3%A3o%20tentativas%20de,se%20proteger%20contra%20esses%20ataques.

Montgomery, D. C., Peck, E. A., & Vining, G. G. (2021). Introduction to linear regression analysis. John Wiley & Sons.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2017). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *The Business Lawyer*, 73(1), 1-34.

Nagelkerke, N. J. (1991). A note on a general definition of the coefficient of determination. biometrika, 78(3), 691-692.

Nguyen, D. V., Nguyen, N. H. K., & Dinh, T. T. (2023). CEO attributes and firm performance: Evidence from companies listed on Ho Chi Minh Stock Exchange. *Cogent Economics & Finance*, 11(2), 2282838.

No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting*, 14(1), 1-12.

Patten, D. M. (2002). The relation between environmental performance and environmental disclosure: a research note. *Accounting, organizations and Society*, *27*(8), 763-773.

Perols, R. R., Murthy, U. S. (2021). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. Auditing: A *Journal of Practice & Theory*, 40(1), 73-89.

Peasnell, K. V., Pope, P. F., & Young, S. (2005). Board monitoring and earnings management: do outside directors influence abnormal accruals?. *Journal of business finance & accounting*, 32(7-8), 1311-1346.

PriceWaterHouseCoopers (2020). *Companhias nacionais chegaram a registrar perdas acima de US$ 50 milhões.* Fonte: https://www.pwc.com.br/pt/sala-de-imprensa/noticias/metade-das-empresas-brasileiras-foi-vitima-de-crimes-economicos-nos-ultimos-dois-anos.html#:~:text=J%C3%A1%20para%2066%25%20no%20Brasil,que%20perderam%20com%20o%20crime.

PriceWaterHouseCoopers (2021). *Pesquisa Global de Riscos*. Fonte: https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2022/pesquisa-global-com-investidores-2021.html

PriceWaterHouseCoopers (2023). O manual do C-suite: Colocar a segurança no epicentro da inovação. Fonte: https://www.pwc.com/us/em/services/55onsulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html.

Proofpoint (2023). Relatório Segurança cibernética: a perspectiva do conselho em 2023. Fonte: https://www.proofpoint.com/br

Post, C., Rahman, N., & Rubow, E. (2011). Green governance: Boards of directors' composition and environmental corporate social responsibility. *Business & society,* 50(1), 189-223.

Radu, C., & Smaili, N. (2021). Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure. *Journal of business ethics*, 1-24.

Reddy, D., & Rao, V. (2016). Cybersecurity skills: The moderating role in the relationship between cybersecurity awareness and compliance. *Twenty-second Americas Conference on Information Systems.*

Ribeiro, R., Krüger, C., de Freitas Michelin, C., & Raddatz, J. C. (2020). Cibersegurança e segurança da informação contábil: uma análise da percepção do profissional contábil. *RAGC*, 8(32).

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. The International *Journal of Accounting*, 54(03), 1950013.

Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-security incidents and audit quality. *European Accounting Review*, 31(3), 701-728.

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems,* 33(3), 227-265.

Rennekamp, K. (2012). Processing fluency and investors' reactions to disclosure readability. *Journal of Accounting Research*, 50(5), 1319-1354.

Schwarz, G. (1978). Estimating the dimension of a model. *The Annals of Statistics*, 6(2), 461-464.

Santos, A. D., & Grateron, I. R. G. (2003). Contabilidade criativa e responsabilidade dos auditores. *Revista Contabilidade & Finanças*, 14, 07-22.

Senado Federal (2023). Cota para mulheres em Conselhos de Administração é aprovada na CDH. Fonte: https://www12.senado.leg.br/noticias/materias/2023

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance,* 27(4), 1049-1071.

Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems*, 33(2), 177-204.

Sneller, L., Bode, R., & Klerkx, A. (2016). Do It matters matter? IT-related key audit matters in Dutch annual reports. *International Journal of Disclosure and Governance,* 14(2), 139-151.

SonicWall. (2023). Relatório de Ameaças Cibernéticas da SonicWall 2023. Fonte: https://www.sonicwall.com/pt-br/2023-cyber-threat-report/

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229.

Trend Micro Pesquisa Global de ameaças. (2023). Fonte: https://www.trendmicro.com/en_us/business.html

Tsen, E., Ko, R. K., & Slapnicar, S. (2022). Um estudo exploratório da resiliência cibernética organizacional, seus precursores e resultados. *Journal of Organizational Computing and Electronic Commerce*, 1-22.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 101795.

Tosh, D. K., Shetty, S., Sengupta, S., Kesan, J. P., & Kamhoua, C. A. (2017). Risk management using cyber-threat information sharing and cyber-insurance. In International conference on game theory for networks (pp. 154-164). Cham: Springer International Publishing.

Veja. (2023). Casos Magazine Luiza e Americanas acendem alerta no mercado. Fonte: https://veja.abril.com.br/economia/casos-magazine-luiza-e-americanas-acendem-alerta-no-mercado. Acesso em: Janeiro de 2024.

Vroom, V. H., & Pahl, B. (1971). Relationship between age and risk taking among managers. *Journal of applied psychology*, 55(5), 399.

World Economic Forum Annual Meeting (2023). Fonte: https://www.weforum.org/events/world-economic-forum-annual-meeting-2023

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. I*nformation systems research,* 24(2), 201-218.

Wang, T., Yen, J. C., & Yoon, K. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. *International Journal of Accounting Information* Systems, 46, 100567.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems,* 35(1), 155-186.

Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, 37(6), 489-507.

Zandonai, A. C., & Argiles, A. V. Incidente de Segurança: O vazamento de dados de clientes do Banco Inter sob a perspectiva da Lei 13.709/2018. *Justiça & Sociedade*, 4(1), 273-314.

Anexo 1

SEGMENTO	**Link**
3R PETROLEUM	https://ri.3rpetroleum.com.br/informacoes-financeiras/documentos-cvm/
COSAN	https://www.cosan.com.br/formulario-de-referencia-cadastral-e-20-f/
ENAUTA PART	https://ri.enauta.com.br/dados/documentos-cvm/
PETRORECSA	https://ri.petroreconcavo.com.br/informacoes-financeiras/documentos-cvm/
PETRORIO	https://ri.prio3.com.br/servicos-aos-investidores/formulario-cadastral-e-de-referencia/
ULTRAPAR	https://ri.ultra.com.br/divulgacoes-e-resultados/relatorios-anuais/
VIBRA	https://ri.vibraenergia.com.br/servicos-aos-investidores/central-de-downloads/
LUPATECH	https://lupatech.globalri.com.br/pt/formulario-cadastral-e-de-referencia
OCEANPACT	https://ri.oceanpact.com/informacoes-financeiras/documentos-entregues-a-cvm/
OSX BRASIL	https://www.osx.com.br/ListGroup.aspx?idCanal=+IXVlxxdIcYMqpIwJvGloA==&ano=2020&linguagem=pt
CBA	https://ri.cba.com.br/publicacoes-cvm/formulario-de-referencia/
VALE	https://ri-vale.mz-sites.com/informacoes-para-o-mercado/relatorios-anuais/formulario-de-referencia/
PARANAPANEMA	https://ri.paranapanema.com.br/informacoes-financeiras/formulario-de-referencia/
FER HERINGER	https://ri.heringer.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
VITTIA	https://ri.vittia.com.br/informacoes-financeiras/documentos-cvm/
DEXCO	https://ri.dex.co/informacoes-ao-mercado/documentos-entregues-a-cvm/
SUZANO S.A.	https://ri.suzano.com.br/Portuguese/Arquivamentos/Documentos-entregues-a-CVM/
IRANI	https://ri.irani.com.br/informacoes-ao-mercado/documentos-cvm/
ETERNIT	https://ri.eternit.com.br/List.aspx?idCanal=9KbhcDzPkGDnbSygmV2IZA==&ano=2023&linguagem=pt
PORTOBELLO	https://ri.portobello.com.br/ListGroup.aspx?idCanal=FzGlc6N1mRb5rC9MP9MaKg==&ano=2020&linguagem=pt
EMBRAER	https://ri.embraer.com.br/informacoes-financeiras/arquivadas-na-cvm/
TUPY	https://ri.tupy.com.br/informacoes-financeiras/formulario-de-referencia/
WEG	https://ri.weg.net/informacoes-financeiras/formulario-de-referencia-e-cadastral/
AERIS	https://www.ri.aerisenergy.com.br/informacoes-aos-investidores/documentos-cvm/
ARMAC	https://ri.armac.com.br/central-de-downloads/
KEPLER WEBER	https://ri.kepler.com.br/informacoes-financeiras/formulario-de-referencia-e-cadastral/
METALFRIO	https://ri.metalfrio.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
MILLS	https://ri.mills.com.br/ListGroup.aspx?idCanal=oYvLe43KuDQiSUmHG1TvgA==&ano=2023&linguagem=pt
ROMI	https://www.romi.com/investidores/informacoes-financeiras/formulario-de-referencia/
RUMO S.A.	https://ri.rumolog.com/divulgacoes-e-documentos/formulario-de-referencia-e-cadastral/
HIDROVIAS	https://ri.hbsa.com.br/informacoes-aos-acionistas/formulario-de-referencia/
LOG-IN	https://ri.loginlogistica.com.br/informacoes-aos-investidores/formulario-cadastral-e-de-referencia/
JSL	https://ri.jsl.com.br/informacoes-aos-investidores/formulario-de-referencia/
TEGMA	https://ri.tegma.com.br/en/financial-information/cvm-filings/
CCR SA	https://ri.grupoccr.com.br/esg/governanca/formulario-de-referencia-e-cadastral/
ECORODOVIAS	https://ri.ecorodovias.com.br/informacoes-aos-investidores/documentos-entregues-a-cvm/
TRIUNFO PART	https://www.triunfo.com/informacoes-financeiras/documentos-entregues-a-cvm/
SANTOS BRP	https://api.mziq.com/mzfilemanager/v2/d/cf449510-6b50-479e-aba7-6ab35d5a0c6f/c8f167bb-73d8-3a1e-792e-f5bd093edaee?origin=1
WILSON SONS	https://ri.wilsonsons.com.br/publicacoes/arquivamentos-cvm/

ESTAPAR	https://ri.estapar.com.br/informacoes-aos-investidores/documentos-cvm/
GPS	https://ri.gpssa.com.br/informacoes-financeiras/documentos-cvm/
PRINER	https://ri.priner.com.br/informacoes-aos-investidores/documentos-cvm/
SEQUOIA LOG	https://ri.sequoialog.com.br/informacoes-aos-acionistas/formulario-de-referencia/
VALID	https://ri.valid.com/arquivamentos-cvm/formulario-de-referencia/
3TENTOS	https://ri.3tentos.com.br/informacoes-finaceiras/documentos-cvm/
AGROGALAXY	https://ri.agrogalaxy.com.br/governanca-corporativa-e-sustentabilidade/formulario-de-referencia/
BOA SAFRA	https://ri.boasafrasementes.com.br/informacoes-aos-investidores/documentos-cvm/
BRASILAGRO	https://ri.brasil-agro.com/informacoes-financeiras/documentos-entregues-a-cvm-sec/
POMIFRUTAS	https://www.pomifrutas.com.br/central-de-downloads/
SLC AGRICOLA	https://ri.slcagricola.com.br/publicacoes-e-documentos/formulario-de-referencia-e-cadastral/
TERRASANTAPA	https://www.terrasantapa.com.br/ListGroup/Documentos-entregues-a-CVM-?=qUdcdxtITd0JV5nNjOCF9w==
JALLESMACHAD	https://ri.jalles.com/servicos-aos-investidores/documentos-cvm/
SAO MARTINHO	https://ri.saomartinho.com.br/ListGroup.aspx?idCanal=3kK+JHozjxal5isJwnwwEA==&ano=2020&linguagem=pt
BRF SA	https://ri.brf-global.com/informacoes-financeiras/relatorios-anuais/
JBS	https://ri.jbs.com.br/arquivos-cvm-e-sec/formulario-de-referencia-cadastral-e-prospectos/
MARFRIG	https://ri.marfrig.com.br/informacoes-financeiras/formulario-de-referencia/
MINERVA	https://ri.minervafoods.com/formulario-de-referencia/
CAMIL	https://ri.camil.com.br/informacoes-financeiras/formulario-de-referencia/
M.DIASBRANCO	https://ri.mdiasbranco.com.br/servicos-aos-investidores/central-de-downloads/
GRUPO NATURA	https://ri.naturaeco.com/documentos-regulatorios-e-assembleias/formularios/
ASSAI	https://ri.assai.com.br/informacoes-financeiras/documentos-cvm/
CARREFOUR BR	https://ri.grupocarrefourbrasil.com.br/informacoes-financeiras/arquivamentos-cvm/
GRUPO MATEUS	https://ri.grupomateus.com.br/relatorios-e-publicacoes/publicacoes-cvm/
P.ACUCAR-CBD	https://www.gpari.com.br/informacoes-financeiras/documentos-entregues-a-cvm-e-sec/
ALPHAVILLE	https://ri.alphaville.com.br/informacoes-aos-investidores/arquivamentos-cvm/
CURY S/A	https://ri.cury.net/informacoes-aos-investidores/documentos-cvm/
CYRELA REALT	https://ri.cyrela.com.br/cyrela-securitizadora/formulario-de-referencia/
DIRECIONAL	https://ri.direcional.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
EVEN	https://ri.even.com.br/formulario-de-referencia/
EZTEC	https://ri.eztec.com.br/arquivamentos-cvm/
GAFISA	https://ri.gafisa.com.br/informacoes-aos-investidores/publicacoes-cvm/
HELBOR	https://ri.helbor.com.br/documentos-cvm/documentos-entregues-a-cvm/
JHSF PART	https://ri.jhsf.com.br/informacoes-financeiras/fre/
LAVVI	https://ri.lavvi.com.br/servicos-aos-investidores/arquivamentos-cvm/
MELNICK	https://ri.melnick.com.br/ListGroup.aspx?idCanal=WsYVxqsuPj70ufB5XNKAUw==&ano=2023&linguagem=pt
MITRE REALTY	https://ri.mitrerealty.com.br/informacoes-aos-investidores/documentos-cvm/
MOURA DUBEUX	https://ri.mouradubeux.com.br/servicos-a-investidores/documentos-cvm/
MRV	https://ri.mrv.com.br/publicacoes-cvm/formulario-de-referencia/
PDG REALT	https://ri.pdg.com.br/List.aspx?idCanal=2ufxHYwuLl0t/+kndMi8XQ==&ano=2023&linguagem=pt
PLANOEPLANO	https://ri.planoeplano.com.br/informacoes-financeiras/formulario-de-referencia/
RNI	https://ri.rni.com.br/informacoes-financeiras/documentos-cvm/
ROSSI RESID	https://ri.rossiresidencial.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
TECNISA	https://ri.tecnisa.com.br/ListGroup/ListGroup.aspx?idCanal=lWyb2UCFYF7LCoAKgFWgfQ==&ano=2022&linguagem=pt
TENDA	https://ri.tenda.com/arquivamentos-cvm/formulario-de-referencia-e-cadastral/2021
TRISUL	https://ri.trisul-sa.com.br/publicacoes-cvm/
VIVER	https://ri.viver.com.br/informacoes-financeiras/formulario-de-referencia/
SPRINGS	https://ri.springs.com/servicos-aos-investidores/documentos-entregues-a-cvm/
GRENDENE	https://ri.grendene.com.br/PT/Informacoes-Financeiras/Formulario-de-Referencia
VULCABRAS	https://www.vulcabrasri.com/informacoes-financeiras/documentos-cvm/
TECHNOS	https://www.grupotechnos.com.br/pt/documentos-cvm

VIVARA S.A.	https://ri.vivara.com.br/informacoes-financeiras/documentos-cvm/
MOBLY	https://investors.mobly.com.br/documentos-cvm/
UNICASA	https://ri.unicasamoveis.com.br/informacoes-financeiras/prospecto-e-formulario-de-referencia-2022
WESTWING	https://ri.westwing.com.br/documentos-cvm/fre-e-fca/
IOCHP-MAXION	https://www.iochpe.com.br/informacoes-financeiras/formulario-de-referencia/
METAL LEVE	https://ri.mahle.com.br/informacoes-financeiras/formulario-de-referencia/
IMC S/A	https://ri.internationalmealcompany.com/informacoes-financeiras/documentos-entregues-a-cvm/
ZAMP S.A.	https://ri.zamp.com.br/list.aspx?idCanal=WLdm/nUI+PEal72OAtL8qw==&pagina=1#ancora&linguagem=pt
TIME FOR FUN	https://ri.t4f.com.br/servicos-aos-investidores/documentos-entregues-a-cvm/
CVC BRASIL	https://www.cvccorp.com.br/investidores/servico-aos-investidores/central-de-downloads/
SMART FIT	https://investor.smartfit.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
ANIMA	https://ri.animaeducacao.com.br/List.aspx?idCanal=6ql8C4wok4Z/nWa4YULT8w==&ano=2023&linguagem=pt
COGNA ON	https://ri.cogna.com.br/documentos-cvm/documentos-entregues-a-cvm-3/
CRUZEIRO EDU	https://ri.cruzeirodosuleducacional.com.br/informacoes-aos-investidores/documentos-cvm/
SER EDUCA	https://ri.sereducacional.com/informacoes-financeiras/documentos-entregues-a-cvm/
YDUQS PART	https://www.yduqs.com.br/List.aspx?idCanal=K/4NJa/VbSBGiLw4tgRJzQ==&ano=2023&linguagem=pt
LOCALIZA	https://ri.localiza.com/informacoes-aos-acionistas/formulario-de-referencia/
MOVIDA	https://ri.movida.com.br/informacoes-financeiras/documentos-cvm/?gad_source=1&gclid=Cj0KCQiAxOauBhCaARIsAEbUSQQSjfFzYucoG9Mw-Wy3SI6-g-58V6yQayHiwTsctapS-fXoJnKXPawaAkJiEALw_wcB&gclsrc=aw.ds
VAMOS	https://ri.grupovamos.com.br/servicos-aos-investidores/documentos-entregues-a-cvm/
DOTZ SA	https://ri.dotz.com.br/documentos-cvm/formulario-de-referencia-e-informe-de-governanca/
AREZZO CO	https://ri.arezzoco.com.br/informacoes-financeiras/documentos-cvm/
CEA MODAS	https://ri.cea.com.br/documentos-cvm/formulario-de-referencia/
GRUPO SOMA	https://www.somagrupo.com.br/investidores/formulario-cadastral-e-de-referencia/
GUARARAPES	https://ri.riachuelo.com.br/informacoes-financeiras/documentos-cvm/
LOJAS MARISA	https://ri.marisa.com.br/documentos-cvm/formulario-de-referencia/
LOJAS RENNER	https://lojasrenner.mzweb.com.br/doc-corporativos/formulario-de-referencia-e-cadastral/
VESTE	https://www.veste.com/documentos-cvm/formulario-de-referencia/
ALLIED	https://ri.alliedbrasil.com.br/ListGroup.aspx?idCanal=Xacd+ROi88zlkl70s6f0Nw==&ano=2023
CASAS BAHIA	https://ri.grupocasasbahia.com.br/informacoes-financeiras/formulario-de-referencia/
MAGAZ LUIZA	https://ri.magazineluiza.com.br/ListGroup/ListGroup.aspx?idCanal=ZNblHtomXlPEN1ssTVaUhQ==&ano=2024&linguagem=pt
AMERICANAS	https://ri.americanas.io/informacoes-aos-investidores/documentos-cvm/documentos-cvm-lasa/
ESPACOLASER	https://ri.espacolaser.com.br/documentos-cvm/
GRUPO SBF	https://ri.gruposbf.com.br/informacoes-financeiras/documentos-cvm/
PETZ	https://ri.petz.com.br/informacoes-financeiras/documentos-cvm/
QUERO-QUERO	https://ri.quero-quero.com.br/documentos-cvm/
OUROFINO S/A	https://ri.ourofino.com/ListGroup.aspx?idCanal=tIUN56TpBbmA8xm9cakqMQ==&ano=2023&linguagem=pt
ALLIAR	https://ri.allianca.com/documentos-cvm/formulario-de-referencia/
DASA	https://www.dasa3.com.br/atos-legais/formulario-de-referencia/
FLEURY	https://ri.fleury.com.br/documentos-regulatorios/formulario-de-referencia/
HAPVIDA	https://ri.hapvida.com.br/servicos-aos-investidores/central-de-downloads/
KORA SAUDE	https://ri.korasaude.com.br/informacoes-financeiras/publicacoes-cvm/
MATER DEI	https://ri.materdei.com.br/en/information-to-shareholders/reference-form/
ODONTOPREV	https://ri.odontoprev.com.br/informacoes-aos-acionistas/publicacoes-cvm/
ONCOCLINICAS	
QUALICORP	https://ri.qualicorp.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
REDE D OR	https://ri.rededorsaoluiz.com.br/informacoes-financeiras/formulario-de-referencia/
BLAU	https://ri.blau.com/informacoes-financeiras/formulario-de-referencia/
D1000VFARMA	https://ri.reded1000.com.br/ferramentas-de-analise/documentos-cvm/
DIMED	https://ri.grupopanvel.com.br/documentos-cvm/formulario-de-referencia/

HYPERA	https://ri.hypera.com.br/servicos-aos-investidores/central-de-downloads/
PAGUE MENOS	https://ri.paguemenos.com.br/informacoes-aos-investidores/formulario-de-referencia/?gclid=CjwKCAiA0PuuBhBsEiwAS7fsNfqQUMhp33jid7oebXYt9ux2GtaRBaRoIO0KHydLEMNvchTZ7_zTxhoCKQ8QAvD_BwE
PROFARMA	https://ri.profarma.com.br/informacoes-financeiras/formulario-de-referencia/
RAIADROGASIL	https://ri.rd.com.br/list.aspx?idCanal=M9eciSyHCkOXeOE9W1JJeA==
VIVEO	https://ri.viveo.com.br/central-de-downloads/formulario-de-referencia-e-formulario-cadastral/
INTELBRAS	https://ri.intelbras.com.br/informacoes-financeiras/documentos-cvm/
MULTILASER	https://ri.multilaser.com.br/informacoes-financeiras/formulario-de-referencia-cadastral-e-prospectos/
POSITIVO TEC	https://ri.positivotecnologia.com.br/informacoes-ao-mercado/formulario-de-referencia/
BEMOBI TECH	https://ri.bemobi.com.br/informacoes-financeiras/formulario-de-referencia/
ENJOEI	https://ri.enjoei.com/pt-br/informacoes-aos-investidores/documentos-cvm/
GETNINJAS	https://ri.getninjas.com.br/informacoes-financeiras/formulario-de-referencia/
INFRACOMM	https://ri.infracommerce.com.br/informacoes-aos-investidores/documentos-cvm/
LOCAWEB	https://ri.locaweb.com.br/outras-informacoes/formulario-de-referencia/
MELIUZ	https://ri.meliuz.com.br/list.aspx?idCanal=3nXgGaMscrlbIl/EGyfLJg==&ano=2024
NEOGRID	https://ri.neogrid.com/informacoes-aos-investidores/documentos-cvm/
PADTEC	https://www.padtec.com.br/investor/formulario-cadastral-e-de-referencia/
TC	https://ri.tc.com.br/documentos-cvm
TOTVS	https://ri.totvs.com/servicos-aos-investidores/central-de-downloads/
WDC NETWORKS	
BRISANET	https://ri.brisanet.com.br/servicos-aos-investidores/central-de-downloads
DESKTOP	https://www.ri.desktop.com.br/informacoes-financeiras/documentos-cvm/
TIM	https://ri.tim.com.br/informacoes-ao-mercado/arquivamentos/
UNIFIQUE	https://ri.unifique.com.br/informacoes-financeiras/documentos-entregues-a-cvm/
ELETROMIDIA	https://ri.eletromidia.com.br/servicos-aos-investidores/documentos-cvm/
AES BRASIL	https://ri.aesbrasil.com.br/informacoes-aos-investidores/documentos-cvm/formulario-de-referencia/
AUREN	https://ri.aurenenergia.com.br/arquivos-cvm/formulario-de-referencia-auren/
CPFL ENERGIA	https://ri.cpfl.com.br/list.aspx?idCanal=IekpSrgRp0EUlB698gUssQ==
ENEVA	https://ri.eneva.com.br/informacoes-ao-mercado/documentos-cvm/
ENGIE BRASIL	https://www.engie.com.br/investidores/
EQUATORIAL	https://ri.equatorialenergia.com.br/pt-br/divulgacao-e-resultados/formulario-cadastral-e-de-referencia/
LIGHT S/A	https://ri.light.com.br/divulgacoes-e-resultados/documentos-entregues-a-cvm/
NEOENERGIA	https://ri.neoenergia.com/resultados-e-indicadores/documentos-cvm/
OMEGAENERGIA	
AMBIPAR	https://ri.ambipar.com/informacoes-financeiras/fre/
COPASA	https://ri.copasa.com.br/formulario-de-referencia/
ORIZON	https://ri.orizonvr.com.br/publicacoes-cvm/formulario-de-referencia/
SABESP	https://ri.sabesp.com.br/informacoes-financeiras/submetidas-a-cvm/
BRASIL	https://ri.bb.com.br/publicacoes-e-comunicados/formularios-de-referencia/
B3	https://ri.b3.com.br/pt-br/documentos-regulatorios/
CIELO	https://ri.cielo.com.br/publicacoes-cvm/
CLEARSALE	https://ri.clear.sale/listgroup.aspx?idCanal=Qa/OaUtxVed8dzEuFOmp6w==
CSU DIGITAL	https://ri.csu.com.br/resultados-e-arquivos-cvm/formularios-fre-e-fca/
BBSEGURIDADE	https://www.bbseguridaderi.com.br/informacoes-ao-mercado/formularios-de-referencia/
CAIXA SEGURI	https://www.ri.caixaseguridade.com.br/informacoes-financeiras/formulario-de-referencia/
PORTO SEGURO	https://ri.portoseguro.com.br/informacoes-aos-acionistas/formulario-cadastral-e-formulario-de-referencia/
IRBBRASIL RE	https://ri.irbre.com/informacoes-financeiras/formulario-cadastral-e-formulario-de-referencia/
WIZ CO	https://ri.wiz.co/formulario-de-referencia/
ALLOS	https://ri.allos.co/servicos-aos-investidores/outros-documentos-entregues-a-cvm/
HBR REALTY	https://ri.hbrrealty.com.br/publicacoes-cvm/
LOG COM PROP	https://ri.logcp.com.br/documentos-cvm/formulario-de-referencia-e-formulario-cadastral/

SAO CARLOS	https://ri.scsa.com.br/informacoes-financeiras/documentos-cvm/
SYN PROP TEC	https://ri.syn.com.br/informacoes-financeiras/relatorios-anuais/
LOPES BRASIL	https://ri.lopes.com.br/informacoes-financeiras/formulario-de-referencia-e-formulario-cadastral/
NEXPE	https://www.nexpe.co/informacoes-financeiras/documentos-cvm/
SIMPAR	https://ri.simpar.com.br/formulario-de-referencia/