Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração

RODRIGO SANTOS DOS REIS

SEGURANÇA CIBERNÉTICA NO SETOR BANCÁRIO: uma análise da produção internacional de artigos científicos em bases de dados da área de Administração

Brasília – DF
2021

RODRIGO SANTOS DOS REIS

SEGURANÇA CIBERNÉTICA NO SETOR BANCÁRIO: uma análise da produção internacional de artigos científicos em bases de dados da área de Administração

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Dr. Carlos André de Melo Alves

Brasília – DF

2021

RODRIGO SANTOS DOS REIS

SEGURANÇA CIBERNÉTICA NO SETOR BANCÁRIO: uma análise da produção internacional de artigos científicos em bases de dados da área de Administração

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do aluno

Rodrigo Santos dos Reis

Doutor, Carlos André de Melo Alves
Professor-Orientador

Doutor, Rafael Rabelo Nunes
Professor-Examinador

Mestre, Roque Magno de Oliveira
Professor-Examinador

Brasília - DF, 12 de fevereiro de 2021

Dedico este trabalho aos meus pais, pelo amor e incentivo que sempre me deram durante toda a vida. A todos os professores e professoras que tive ao longo dos anos, em especial aqueles e aquelas do Ensino Médio que, por meio da educação e da ciência, instigaram-me a buscar mais conhecimento para ajudar a tornar o mundo um lugar melhor.

AGRADECIMENTOS

Agradeço à minha esposa, Juliana, por toda a compreensão, paciência e amor durante a minha jornada na universidade. Ao meu orientador, Prof. Dr. Carlos André de Melo Alves, pela dedicação, disponibilidade e profissionalismo. Sua atuação foi fundamental para a elaboração deste trabalho. À Universidade de Brasília, pela diversidade e excelência no ensino. Aqui aprendi lições que levo para a vida.

RESUMO

O objetivo geral deste trabalho é analisar a produção internacional de artigos científicos sobre o tema ‘segurança cibernética no setor bancário’ em bases de dados da área de Administração. Para tal finalidade, realizou-se uma pesquisa descritiva com abordadem qualitativa e quantitativa com análise de 72 artigos por meio de um estudo bibliométrico. Os artigos foram coletados no período de 28.01.2020 até 08.07.2020 em períodicos disponíveis em quatro bases de dados da área de Administração, indexadas pelo Portal de Periódicos da CAPES, sendo elas: EBSCOhost, ProQuest, Scopus - Elsevier e *Web of Science* - WoS. O tratamento dos dados empregou a estatística descritiva, a técnica de elaboração de nuvens de palavras, a análise de co-ocorrência de palavras-chaves e a análise de coautoria. Adicionalmente, para a classificação dos artigos conforme a ótica predominante em ‘Negócios’, ‘Legal’ ou ‘Técnico’, foi utilizada a análise de conteúdo, baseado na taxonomia descrita por Evesti, Kanstrén e Frantti (2017). Os principais resultados encontrados indicaram que 73,61% da produção de artigos científicos ocorreu entre os anos de 2017 e 2020. Além disso, o continente europeu figurou com 41,12% do total de instituições às quais os autores dos artigos estão vinculados. Entre as palavras-chaves recorrentes, destacaram-se ‘*cyber crime*’, ‘*cyber security*’ e ‘*phishing’.* Notou-se, também, que a abordagem metodológica predominante foi a qualitativa, com 44 artigos (61,11%) e que a ótica predominante em estudos foi a de ‘Negócios’, com 50,00% do total da amostra. Com esta pesquisa, espera-se contribuir academicamente para a compreensão do tema ‘segurança cibernética no setor bancário’ e trazer reflexões para acadêmicos, instituições financeiras, órgãos reguladores do setor bancário que tratam sobre o assunto, pesquisadores e clientes de instituições financeiras interessados em melhor entender o tema.

Palavras-chave: segurança cibernética, bancos, bibliometria, análise de conteúdo

LISTA DE ILUSTRAÇÕES

Figura 1 - Buscas pelos termos ‘cyber security’ e ‘cybersecurity’ no Google 13
Figura 2 - Métricas de Segurança Cibernética por Região.......................................21
Figura 3 - Detecção de e-mails maliciosos com o tema ‘Coronavírus’ no período de 01 de março a 26 de abril de 2020.. 22
Figura 4 - Número de jurisdições que reportam esquemas de regulamentação ou de supervisão, por setor financeiro 29
Figura 5 - Etapas para a seleção da amostra...41
Figura 6 - Quantidade de artigos publicados por ano..44
Figura 7 - Quantidade de autores por artigo publicado 46
Figura 8 - Mapa de coautoria entre os autores da amostra.......................................47
Figura 9 - Nuvem de palavras-chaves presentes nos artigos da amostra.................51
Figura 10 - Mapa de co-ocorrência de palavras-chaves presentes nos artigos da amostra 52
Figura 11 - Quantidade de artigos quanto à metodogolia empregada 53
Figura 12 - Classificação dos artigos de acordo com a ótica 54

LISTA DE QUADROS

Quadro 1 - Tipos de Crimes Cibernéticos 22
Quadro 2 - Estudos selecionados sobre taxonomia para Segurança Cibernética 24
Quadro 3 - Taxonomia da Conscientização Situacional em Segurança Cibernética. 26
Quadro 4 - Elementos fundamentais de Segurança Cibernética no
Setor Financeiro 31
Quadro 5 - Itens considerados para analisar os artigos 43
Quadro 6 - Instituições com mais aparições na filiação acadêmica 50

LISTA DE TABELAS

Tabela 1 - Quantidade de artigos por periódico 45
Tabela 2 - Quantidade de artigos publicados por continente em que estão localizadas as instituições a que estão vinculados os autores 49

LISTA DE ABREVIATURAS E SIGLAS

BCB	Banco Central do Brasil
BCBS	*Basel Committee on Banking Supervision*
BIS	*Bank for International Settlements*
CMN	Conselho Monetário Nacional
CPMI	*Committee on Payments and Market Infrastructures*
CSSC	Conscientização Situacional em Segurança Cibernética
DDoS	*Distributed Denial of Service*
DHS	*Department of Homeland Security*
EUA	Estados Unidos da América
FSB	*Financial Stability Board*
FSI	*Financial Stability Institute*
IAIS	*International Association of Insurance Supervisor*
Interpol	*The International Criminal Police Organization*
IOSCO	*International Organization of Securities Commissions*
ITU	*International Telecommunication Union*
NIST	*National Institute of Standards and Technology*
ORG	*Operational Resilience Working Group*
P&D	Pesquisa e Desenvolvimento
PDG	*The Policy Development Group*
TICs	Tecnologias da Informação e Comunicação
WoS	*Web of Science*

SUMÁRIO

1. INTRODUÇÃO....12
1.1. Contextualização 12
1.2. Formulação do Problema....14
1.3. Objetivo Geral....15
1.4. Objetivos Específicos....15
1.5. Justificativa 16
2. REFERENCIAL TEÓRICO 18
2.1. Segurança Cibernética: Conceito e Taxonomia....18
2.2. Segurança Cibernética e o Setor Bancário....26
2.3. Análise Bibliomética e Segurança Cibernética 34
3. MÉTODOS E TÉCNICAS DE PESQUISA....39
3.1. Tipologia e descrição geral dos métodos de pesquisa 39
3.2. Caracterização da área de estudo....39
3.3. População e amostra....40
3.4. Procedimentos de coleta e de análise de dados 41
4. RESULTADOS E DISCUSSÕES....44
4.1. Quantidade de artigos publicados por ano de publicação 44
4.2. Quantidade de artigos publicados por periódicos 45
4.3. Classificação dos artigos conforme a quantidade de autores e análise de coautoria....46
4.4. Quantidade de artigos por filiação acadêmica ou instituição a que estão vinculados os autores....48
4.5. Distribuição das palavras-chaves dos artigos e análise de co-ocorrências 50
4.6. Categorização dos artigos segundo à abordagem metodológica empregada 53
4.7. Classificação dos artigos de acordo com a ótica 53
5. CONCLUSÕES E RECOMENDAÇÕES....55
REFERÊNCIAS....59
APÊNDICE A – Relação dos artigos coletados....67

1. INTRODUÇÃO

1.1. Contextualização

O advento da *Internet* e de novas tecnologias permitindo o uso de dispositivos móveis, por exemplo, trouxe mais praticidade para a vida das pessoas e oportunidades de negócios para as organizações. A interconectividade entre computadores e esses dispositivos móveis permitiu o avanço do comércio eletrônico, do *Internet Banking*, do *Mobile Banking*, entre outros, facilitando as trocas comerciais e as transações financeiras.

Apesar das facilidades trazidas pelas novas tecnologias, é importante preocupar-se com um tema que tem relação com uso adequado delas, a segurança cibernética, que é a “preservação da confidencialidade, integridade e disponibilidade de informações no espaço cibernético” (ISO/IEC, 2012).

Segurança Cibernética é um tema de interesse internacional e vem, assim, tornando-se cada vez mais uma função estratégica de governos e essencial à manutenção e preservação das infraestruturas críticas de um país como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outros (CANONGIA; MANDARINO, 2009).

O termo Segurança Cibernética tem sido usado durante muitos anos, mas sua popularidade aumentou consideravelmente quando o ex-presidente dos Estados Unidos, Barack Obama, em 2009, convidou as pessoas a reconhecerem a importância do tema, incentivando a realização de eventos e treinamentos para aprimorar a segurança nacional do país (SCHATZ; BASHROUSH; WALL, 2017).

O impacto disso pode ser observado na Figura 1, que mostra os resultados de buscas feitas por meio da ferramenta Google Trends de janeiro de 2004 e maio de 2020. As linhas no gráfico mostram o total de procura pelos termos relativo ao total de pesquisas feitas no Google ao longo do tempo. No gráfico da figura, observa-se que a partir de 2009 as buscas pelo termo ‘*cyber security*’ e ‘*cybersecurity*’, ou segurança cibernética em português, aumentaram significativamente no mundo todo. Esse resultado é apenas indicativo, mas mostra que a importância dada ao tema Segurança Cibernética tem aumentado significativamente.

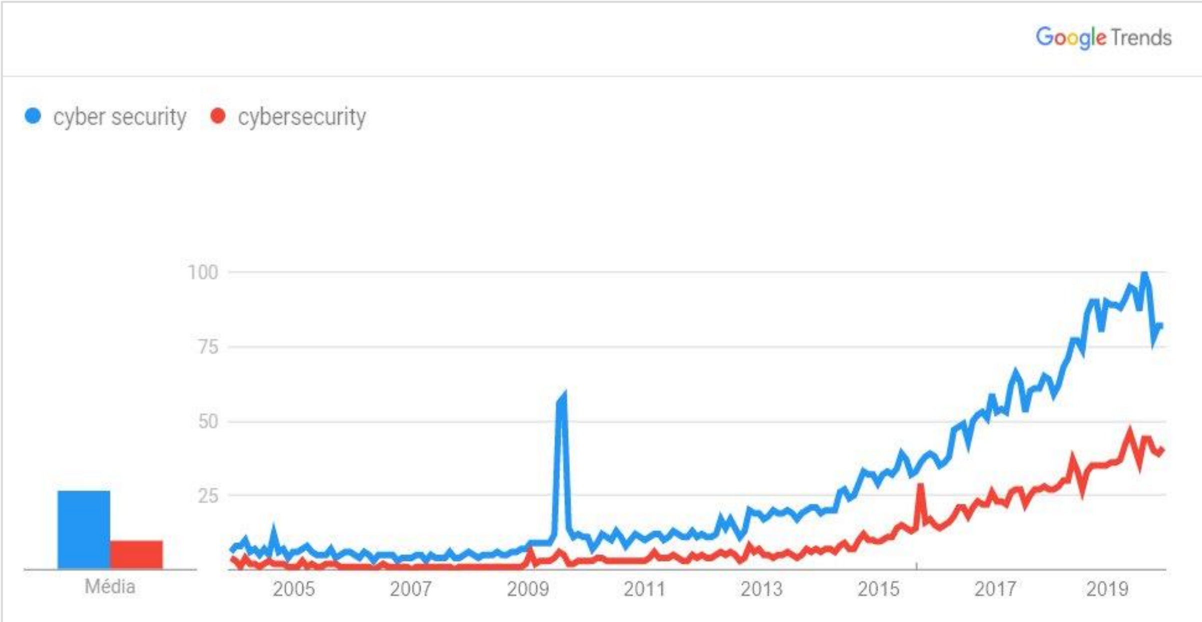

FIGURA 1 – Buscas pelos termos ‘cyber security’ e ‘cybersecurity’ no Google
Fonte: Google, 2020.

Evesti, Kanstrén e Franti (2017), ao explorar a temática da Conscientização Situacional em Segurança Cibernética – CSSC[1], contribuem com uma sugestão de taxonomia, classificando as situações de segurança cibernética conforme sua ótica em ‘Negócios’, ‘Legal’ ou ‘Técnica’. Com a intenção de categorizar os assuntos relevantes à segurança cibernética, este estudo busca auxiliar na delimitação e organização do conhecimento científico sobre o assunto.

Além disso, a segurança cibernética tem chamado a atenção do setor financeiro. Neste sentido, o *Financial Stability Board* – FSB[2] dedica esforços, entre outros, para orientar a regulamentação e a supervisão no sistema financeiro no que se refere à segurança cibernética. Em outubro de 2017, por exemplo, apresentou aos Ministros de Finanças e presidentes dos Bancos Centrais do G20 um relatório com conclusões de uma avaliação sobre segurança cibernética, com o objetivo de melhorar a cooperação transfronteiriça (FSB, 2018).

---

[1] A Conscientização Situacional em Segurança Cibernética - CSSC, ou *Cybersecurity Situational Awareness,* tem relação com o conhecimento, por parte dos tomadores de decisão de uma organização, sobre o que está acontecendo nos sistemas em rede no que se refere aos níveis de segurança (EVESTI; KANSTRÉN; FRANTI, 2017). Uma melhor discussão sobre o tema é apresentada na seção 2.1.

[2] Nota do autor: O FSB é um órgão internacional que monitora e faz recomendações sobre o sistema financeiro no mundo todo com o objetivo de promover a estabilidade financeira internacional.

Considerando o setor bancário, a segurança cibernética tem chamado a atenção de organismos internacionais com foco em bancos. A este respeito, o *Basel Committee on Banking Supervision* – BCBS[3] também preocupa-se com o tema, principalmente por meio do *The Policy Development Group* – PDG, um dos grupos do BCBS. O PDG é subdivido em grupos de trabalho, sendo um deles dedicado a riscos cibernéticos: o *Operacional Resilience Working Group* – ORG (BIS, 2020ª).

Ainda no âmbito internacional, Camillo (2017) trouxe como contribuição uma discussão sobre os riscos e o gerenciamento de riscos em bancos e instituições financeiras no escopo da segurança cibernética. Preocupado com o crescimento das ameaças cibernéticas a instituições financeiras, estudou dois assuntos que estão relacionados ao tema deste trabalho: riscos cibernéticos e crimes cibernéticos em instituições financeiras.

Já no Brasil, o Conselho Monetário Nacional – CMN, por meio da Resolução nº 4.568, de 26 de abril de 2018 (CMN, 2018), e o Banco Central do Brasil – BCB, por meio da Circular nº 3.909, de 16 de agosto de 2018 (BCB, 2018), regulamentaram e determinaram, entre outros pontos, a obrigatoriedade de uma política de segurança cibernética por parte das instituições financeiras e instituições de pagamento autorizadas a funcionar pelo BCB. O BCB dispôs, ainda, sobre remessa de informações ao BCB sobre risco operacional[4] e sobre risco cibernético, por meio da Circular nº 3.979, de 30 de janeiro de 2020 (BCB, 2020).

1.2. Formulação do Problema

Nota-se que a temática da Segurança Cibernética engloba vários setores de interesse, inclusive o financeiro e o bancário. Para fins deste trabalho, optou-se por enfatizar o setor bancário. Dado o crescente interesse na segurança cibernética neste setor, é possível efetuar levantamentos bibliométricos sobre a temática, uma vez que este tipo de estudo pode ajudar a melhor entender como tem evoluído a publicação de artigos sobre segurança cibernética, inclusive em periódicos cujo acesso é

[3] O BCBS é o fórum internacional para discussão e formulação de recomendações para a regulação prudencial e cooperação para supervisão bancária, composto por 45 autoridades monetárias e supervisoras de 28 jurisdições (BCB, 2020?)

[4] O risco operacional é o risco de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou mesmo de eventos externos. Aqui, inclui-se o risco legal, mas exclui-se os riscos estratégicos e de reputação (BCBS, 2003; MIRANDA; ALVES, 2019).

disponibilizado por meio de bases de dados da área de Administração.

Tais estudos bibliométricos podem, entre outros, permitir o exame de artigos publicados em diferentes continentes, na ótica de diferentes autores, e diferentes filiações acadêmicas, auxiliando o entendimento de quais assuntos associam-se à temática da segurança cibernética. Em adição, taxonomias sobre segurança cibernética podem ser empregadas para melhor delimitar e organizar o conhecimento científico sobre o assunto, a exemplo daquela citada na contextualização e atribuída a Evesti, Kanstrén e Fantti (2017).

Por fim, considerando o que foi apresentado na contextualização e nesta seção, o problema de pesquisa proposto é o seguinte: **qual é a produção internacional de artigos científicos sobre o tema ‘segurança cibernética no setor bancário’ constante em bases de dados da área de Administração?**

1.3. Objetivo Geral

Investigar a produção internacional de artigos científicos sobre o tema ‘segurança cibernética no setor bancário’ constante em bases de dados da área de Administração.

1.4. Objetivos Específicos

Com o intuito de alcançar o objetivo geral, foram propostos os seguintes objetivos específicos:

- Verificar a quantidade de artigos por ano de publicação;
- Mensurar a quantidade de artigos publicados por periódico;
- Classificar os artigos conforme a quantidade de autores;
- Analisar os artigos conforme as relações de coautoria;
- Verificar a quantidade de artigos segundo a filiação acadêmica dos autores;
- Analisar a distribuição e co-ocorrência de palavras-chaves dos artigos;
- Categorizar os artigos segundo à abordagem metodológica empregada; e
- Classificar os artigos de acordo com a ótica de negócios, legal ou técnica.

1.5. Justificativa

Entende-se que a temática Segurança Cibernética é relevante, pois como foi visto na contextualização há uma preocupação internacional sobre o assunto. Ao analisar o tema com foco no setor bancário a discussão torna-se mais específica, podendo despertar o interesse das partes que atuam nessa área. Assim sendo, estudos acadêmicos podem ser importantes por explorar o tema de um ponto de vista científico, trazendo contribuições tanto teóricas quanto práticas.

Este estudo possui relevância teórica por diferenciar-se de outras pesquisas ao propor uma investigação da produção acadêmica por meio de uma pesquisa bibliomética, evidenciando as características dos artigos científicos produzidos sobre o tema segurança cibernética ligada ao setor bancário. Além disso, propõe uma categorização dos artigos de acordo com a ótica predominante em ‘Negócios’, ‘Legal’ ou ‘Técnico’, baseada em Evesti, Kanstrén e Fantti (2017).

Quanto à importância prática, este estudo pode ser útil para as instituições financeiras, em especial aquelas atuantes no setor bancário, tendo em vista que a segurança cibernética é um assunto relevante para a tomada de decisões estratégicas. Também pode ser útil para órgãos reguladores do setor bancário que tratam sobre o assunto, para pesquisadores e clientes de instituições financeiras interessados em melhor entender o tema.

Este trabalho foi produzido enquanto a doença COVID-19 estava caraterizada como pandemia[5] (WHO, 2020), tendo sido constatadas recomendações sobre isolamento social como uma das medidas para combate à referida pandemia. Considerando esse fato, entende-se haver incentivos para a adoção do comércio eletrônico[6] inclusive para a realização de transações financeiras por meio do *Internet banking* e do *mobile banking*. As referidas transações podem ser alvos de ações maliciosas, acarretando crimes financeiros por meio do ambiente cibernético,

[5] A COVID-19 é uma doença causada pelo coronavírus SARS-CoV-2. Essa doença, cujos efeitos estão em estudo na comunidade científica, foi classificada como pandemia pela *World Health Organization* em 11.3.2020 (WHO, 2020).

[6] A este respeito, cabe constatar que períodos de epidemias, como ocorridas na China em 2003 com a gripe SARS, podem incentivar a adoção de novas tecnologias e o emprego do comércio eletrônico (CARLSSON-SZLEZAK; REEVES; SWARTZ, 2020).

conforme apontado pelo *Financial Stability Institute* – FSI[7] (CRISANTO; PRENIO, 2020). Tais crimes afetam negativamente o funcionamento do setor bancário. Assim, o estudo bibliométrico abordando a segurança cibernética trata-se de tema atual, permitindo uma oportuna análise da produção científica no referido setor.

[7] O FSI foi criado em 1998 para ajudar os supervisores em todo mundo a melhorar e fortalecer seus sistemas financeiros (BIS, 2020c).

2. REFERENCIAL TEÓRICO

Este capítulo apresenta o referencial teórico do estudo e é dividido em três seções. A Seção 2.1 é uma contextualização, com conceitos e apresentação de alguns estudos sobre taxonomia relativos à Segurança Cibernética. Já a Seção 2.2 discorre sobre o tema no sistema financeiro e, especialmente, no setor bancário. Por fim, a Seção 2.3 trata de uma exposição de conceitos sobre análise bibliométrica relacionados à Segurança Cibernética.

2.1. Segurança Cibernética: Conceito e Taxonomia

O termo *Cyber Security*, ou Segurança Cibernética, é amplamente utilizado e sua definição é variável. As definições podem mudar a depender do contexto em que o assunto está inserido, podendo ter relação com áreas como ciência da computação, engenharia, estudos policiais, psicologia, estudos sobre segurança, administração, educação e sociologia. (CRAIGEN; DIAKUN-THIBAULT; PURSE, 2014).

O *Department of Homeland Security* – DHS[8] informa que a segurança cibernética inclui a prevenção de danos, o uso não autorizado de sistemas eletrônicos de informação e comunicação e as informações neles contidas. Isso tudo é relevante para garantir a confidencialidade, integridade e disponibilidade da informação. Também inclui a restauração de sistemas eletrônicos de informação e comunicação em caso de ataque terrorista ou desastre natural (DHS, 2009).

Adicionalmente, o estudo da Segurança Cibernética está inserido no contexto do c*yberspace*, ciberespaco ou espaço cibernético, que seria o conjunto de sistemas de informação interconectados (*hardware*, *software* e as mídias que os conectam), e a relação desses sistemas com os usuários humanos que interagem com eles. (OTTIS; LORENTS, 2010).

Para Craigen, Diakun-Thibault e Purse (2014), a segurança cibernética pode ser entendida como a organização e coleção de recursos, processos e estruturas usadas para proteger o espaço cibernético e sistemas de ocorrências que violem os

[8] O DHS é um organismo internacional que tem como objetivo proteger os Estados Unidos da América – EUA contra ameaças diversas. Para isso, conta com a dedicação de funcionários em trabalhos que variam da segurança da aviação e das fronteiras, como analistas da segurança cibernética e inspetores de instalações químicas (DHS, 2020).

direitos de propriedade dos indivíduos, sendo incluídos os direitos de acesso, retirada, administração, exclusão e alienação dos ativos digitais.

Já para o FSB, em concordância com a ISO/IEC, a segurança cibernética é assim definida:

> (...) a preservação da confidencialidade, integridade e disponibilidade de informações e/ou sistemas de informações no espaço cibernético. Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidas (ISO/IEC, 2012; FSB, 2018).

Segundo Solms e Niekerk (2013), Segurança Cibernética e Segurança da Informação, por vezes, são confundidas, já que ambas tratam sobre questões semelhantes. Entretanto, entender suas diferenças é importante. A Segurança da Informação não é um produto ou uma tecnologia, mas um processo. Além disso, segurança é um problema referente a pessoas e administração, não é um problema apenas tecnológico (MITNICK; SIMON, 2003).

Segurança da Informação é tudo aquilo que se refere à proteção da informação, geralmente focado na confidencialidade, integridade e disponibilidade da informação, semelhante ao que disseram Solms e Niekerk (2013), enquanto que a Segurança Cibernética trata sobre a segurança das coisas que podem ser vulneráveis ao se utilizar as Tecnologias da Informação e Comunicação - TICs, incluindo coisas que são informações, físicas ou digitais, e coisas que não são informações, como aplicações eletrônicas. Também considera, conforme Eswaran e Vinayagamoorthi (2019), onde os dados são armazenados e as tecnologias usadas para garantir sua segurança.

O aumento da utilização das TICs permitiu também o aumento dos eventos cibernéticos[9], o que reforça a importância da segurança cibernética. Dentro desse contexto, dois subtemas são importantes: os *cyber risks*, ou riscos cibernéticos, e os *cybercrimes*, ou crimes cibernéticos.

Conforme Biener, Eling e Wirfs (2015), organizações de todos os tamanhos, públicas ou privadas, dependem cada vez mais de aparato de informação e tecnologia para melhor prestação de seus serviços. Na ocorrência de falhas, há impacto negativo nos processos que sustentam os negócios, podendo trazer problemas no

[9] Como eventos cibernéticos entende-se qualquer ato natural, humano ou uma combinação destes que impactam negativamente a disponibilidade, integridade ou confidencialidade dos sistemas de TI em rede e informações (BJORCK *et al.*, 2015). O conceito vai de acordo com aquele apresentado pelo FSB (2018), que diz que evento cibernético é qualquer ocorrência observável em um sistema de informação.

fornecimento de serviços, por exemplo. Esse tipo de ocorrência é chamado de risco cibernético, cuja definição é “a combinação da probabilidade de ocorrência de incidentes cibernéticos[10] e seu impacto” (FSB, 2018).

Os riscos cibernéticos também se referem às diferentes fontes de riscos que podem afetar os ativos de informação e de tecnologia de uma empresa, e podem ser divididos em quatro classes: (i) ações de pessoas; (ii) falhas de sistemas e tecnologias; (iii) falha interna de processoes; e (iv) eventos externos (BIENER; ELING; WIRFS, 2015). Adicionalmente, os riscos cibernéticos podem ser estudados como incorporados aos riscos operacionais que são relevantes e que trazem consequências para a confidencialidade, disponibilidade ou integridade da informação ou dos sistemas de informação (CEBULA; YOUNG, 2010).

Questões que envolvem riscos cibernéticos podem ser prejudiciais para organizações do mundo todo, seja no comércio internacional, na eficiência dos serviços ou no *marketing*. Os incidentes cibernéticos criam problemas para essas organizações e para seus clientes. Como a informação hoje é um ativo importante, caso seja acessada por pessoas não autorizadas pode ser um risco para as organizações (BAGHERI; RIDLEY, 2017).

De modo a aumentar a conscientização sobre a importância e as diferentes dimensões do tema, o *International Telecommunication Union* – ITU[11] criou o *Global Cybersecurity Index* – GCI, ou Índice Global de Segurança Cibernética, para ser uma fonte confiável que mede o compromisso dos países com a segurança cibernética em nível global. Na edição de 2018, a ITU trouxe, entre outros, um levantamento sobre as métricas de segurança cibernética para avaliação de risco cibernético por região (Figura 2).

O indicador sobre as métricas de segurança cibernética é qualquer *benchmarking* nacional ou setorial utilizado para medir o desenvolvimento da segurança cibernética, estratégias de avaliação de riscos, auditorias em segurança cibernética e outras ferramentas e atividades para classificar ou avaliar o desempenho resultante para melhorias futuras (ITU, 2018). Como exemplo, baseado na ISO/IEC

---

[10] Incidente Cibernético é um evento cibernético, ou seja, qualquer ocorrência em um sistema de informação que põe em risco a segurança cibernética de um sistema de informações ou as informações que o sistema processa, armazena ou transmite. Pode ser caracterizado, também, como um evento cibernético que viole as políticas de segurança, procedimentos de segurança ou políticas de uso aceitável, resultantes de atividades maliciosas ou não (FSB, 2018).

[11] O ITU é a agência especializada das Nações Unidas em tecnologias de informação e comunicação.

27002:2013, um padrão nacional de segurança cibernética pode promover uma resposta nacional aos requisitos de segurança cibernética (ISO/IEC, 2013).

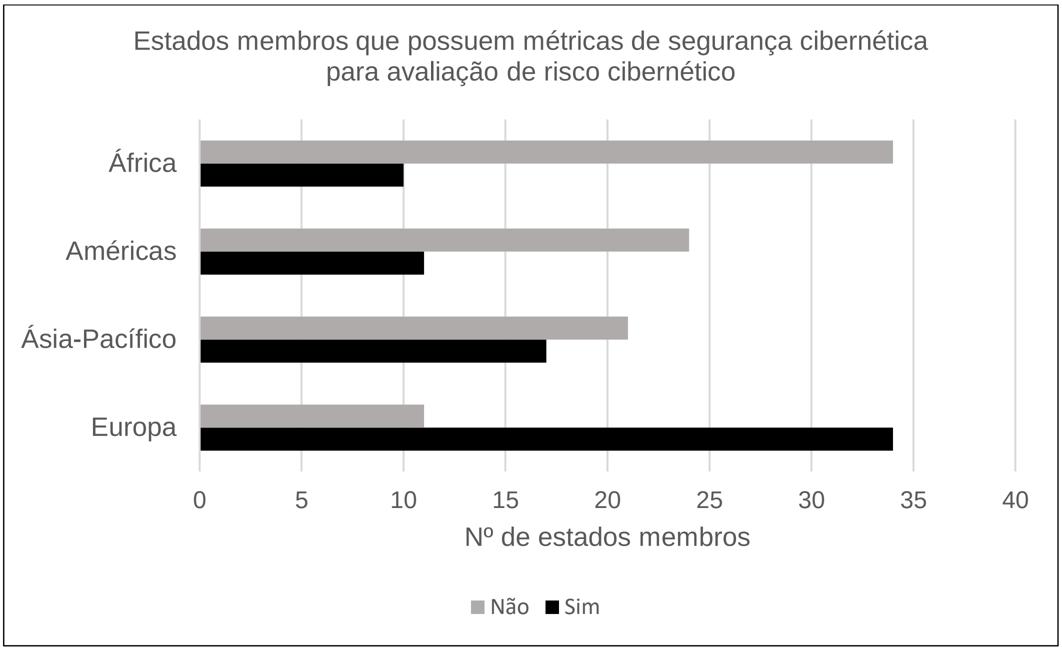

FIGURA 2 – Métricas de Segurança Cibernética por Região
Fonte: Adaptado de ITU, 2018.

Destaca-se, na Figura 2, que a maioria dos estados membros da Europa possui métricas de segurança cibernética para avaliação de risco cibernético, enquanto as regiões da África e das Américas apresentam menor quantidade de estados membros nesta condição, proporcionalmente à quantidade de estados membros de cada região. Os resultados sugerem que há espaço para melhorias das métricas por meio da governança e do gerenciamento de riscos, além do devenvolvimento, implementação, monitoramento e atualização das métricas (ITU, 2018).

Por sua vez, os crimes cibernéticos possuem diferentes manifestações e ocorrem em muitos cenários e ambientes, podendo ser entendidos como qualquer crime que é facilitado ou cometido utilizando-se um computador, a *Internet* ou dispositivo de *hardware*. Aqui, o computador ou dispositivo pode ser o agente do crime, o facilitador ou o alvo. Dessa forma, o crime cibernético pode ocorrer apenas no computador ou em outros locais não virtuais (GORDON; FORD, 2006).

Devido à amplitude da definição, pode-se subdividir o crime cibernético em dois tipos distintos, conforme Quadro 1, em Tipo 1 e Tipo 2. De notar que o Tipo 1 apresenta o *phishing*, um tipo de ataque de engenharia social em que os criminosos uitilizam mensagens falsas para induzir as pessoas a compartilhar informações confidenciais ou instalar programas maliciosos em seus computadores (HONG, 2012).

QUADRO 1
Tipos de Crimes Cibernéticos

Tipo 1	**Tipo 2**
O primeiro tipo de crime cibernético tem as seguintes características: (1) é discreto, da perspectiva da vítima, ou seja, pode não ser percebido de imediato; (2) geralmente é facilitado pela introdução de softwares maliciosos no sistema de computador do usuário que ajudam a capturar dados e informações da vítima; e (3) estes softwares podem ser introduzidos, não necessariamente, por vulnerabilidade dos sistemas das vítimas. Exemplos: tentativas de *phishing*, roubo ou manipulação de dados ou serviços por meio de vírus, roubo de identidade e fraude bancária etc.	As características do segundo tipo de crime cibernético são: (1) geralmente são facilitados por programas que não foram criados especificamente para fins maliciosos. Por exemplo, conversas podem ser realizadas por meio de aplicativos de mensagens assim como a transferência de arquivos; (2) da perspectiva da vítima, geralmente ocorrem contatos ou eventos frequentes, como uma espécie de espionagem, podendo a vítima estar ou não ciente disso. Exemplos: perseguição e assédio cibernético, extorsão, chantagem, manipulação do mercado de ações, espionagem corporativa etc.

Fonte: Adaptado de Gordon e Ford, 2006.

A título de exemplo, a Figura 3 apresenta um gráfico com a evolução da detecção de e-mails maliciosos contendo o tema ‘Coronavírus’ e ilustra como esse tipo de evento cibernético evoluiu com a pandemia de Covid-19, o que pode contribuir para a incidência de crimes cibernéticos (CRISANTO; PRENIO, 2020).

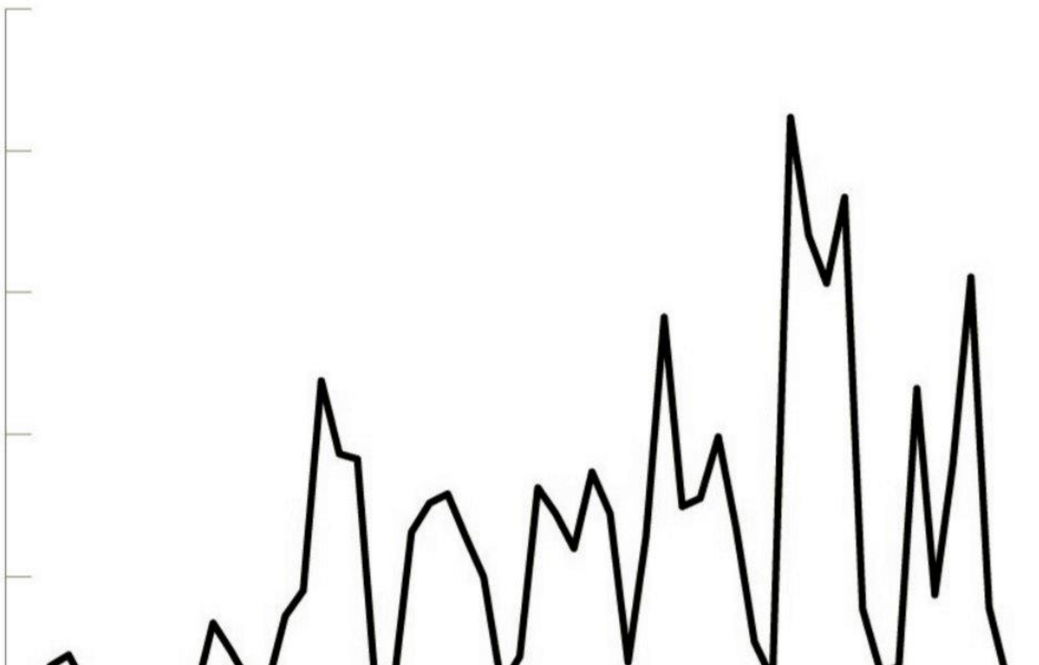

FIGURA 3 – Detecção de e-mails maliciosos com o tema ‘Coronavírus’ no período de 01 de março a 26 de abril de 2020.
Fonte: Crisanto e Prenio, 2020.

Outro conceito a ser considerado neste estudo é o da resiliência cibernética, que pode ser definida como sendo “a habilidade de uma organização de manter os resultados, apesar dos eventos cibernéticos” (BJORCK *et al.*, 2015, p. 312). Neste sentido, resiliência tem relação com a capacidade dos sistemas de lidar, adaptar-se e recuperar-se de perturbações (LEI *et al.*, 2014).

O conceito de segurança cibernética difere de resiliência cibernética, pois esta tem relação com a capacidade de um sistema ter um desempenho efetivo, independentemente dos riscos no ambiente de negócios. Entretanto, as soluções em segurança cibernética sem resiliência cibernética não minimizam os crimes cibernéticos (BAGHERI; RIDLEY, 2017).

De acordo com Evesti, Kasntren e Frantti (2017), no mundo digitalizado é preciso estar ciente dos ativos mais críticos a serem protegidos, ameaças e vulnerabilidades relacionadas, contramedidas válidas e técnicas de mitigação de riscos. A CSSC está inserida neste contexto, pois é importante saber o que acontece nos sistemas em rede, qual o nível estimado de segurança atual e quais são as relações causais dos riscos observados. A CSSC baseia-se em dados extraídos de sistemas internos e de seu ambiente geral para descobrir qual é o cenário de segurança:

> (...) Isso permite definir medidas eficazes e eficientes para proteger o sistema contra ameaças e ataques, para mitigar seus efeitos negativos e se recuperar de ataques passados. Uma CSSC imprecisa pode levar à falsa sensação de segurança, portanto possíveis falhas podem trazer consequências no mundo real (EVESTI; KASNTRÉN; FRANTTI, 2017, p. 1)

É notável que o estudo da segurança cibernética pode ser estendido a diversos contextos e situações, como foi visto até aqui. Isso pode trazer alguma dificuldade para o etendimento do tema. Com a intenção de categorizar os assuntos relevantes à segurança cibernética, estudos contribuíram com algumas taxonomias, que serão apresentadas no Quadro 2. Os estudos foram organizados por data de publicação.

QUADRO 2
Estudos selecionados sobre taxonomia para Segurança Cibernética

Autor (es)	Contexto	Taxonomia
Cebula e Young (2010)	Apresenta uma taxonomia de riscos operacionais no contexto da segurança cibernética e organiza as fontes de riscos operacionais em classes	(i) Ações de Pessoas; (ii) Falhas de Sistemas e Tecnologia; (iii) Falha Interna de Processos; (iv) Eventos Externos
Klaper e Hovy (2014)	Apresenta duas ideias que visam melhorar o ensino sobre segurança cibernética. Primeiro, estabelece uma taxonomia para segurança cibernética. Depois, apresenta um portal que serve como plataforma para os usurários discutirem a segurança de sites específicos.	(i) Ações de pessoas; (ii) Falhas de Sistemas e Tecnologia; (iii) Falha Interna de Processos; (iv) Eventos Externos (i) Verificação de Integridade dos Dados; (ii) Criptografia; (iii) Detecção de Intrusão e Mitigação de riscos; (iv) Autenticação e Autorização; (v) Análise Automática de Padrões de Uso Legítimo (i) História; (ii) Ativismo Social; (iii) Política e Direito; (iv) Educação; (v) Impacto Econômico; (vi) Esforços de Conscientização: iniciativas e ferramentas
Burger *et al.* (2014)	Propõe uma taxonomia para classificar tecnologias existentes contra ameaças cibernéticas, além de identificar lacunas nas tecnologias existentes e explicar suas diferenças de uma perspectiva cientifica	(i) 5W's; (ii) Inteligência; (iii) Indicadores; (iv) Sessão; (v) Transporte
Elnagdy e Gai (2016)	Discussão sobre taxonomia de riscos cibernéticos em segurança da informação ligados ao setor de seguros no contexto da computação em nuvem	(i) Perspectivas Internas; (ii) Perspectivas Externas (i) Atributos; (ii) Recursos
Ibrahim (2016)	Tem o objetivo de estabelecer as particularidades do crime cibernético na Nigéria e se isso sugere problemas com as taxonomias prevalecentes do crime cibernético	(i) Socioeconômico; (ii) Psicossocial; (iii) Geopolítico
Guaman *et al.* (2017)	O artigo faz uma revisão sistemática de estudos sobre taxonomias de riscos cibernéticos. Ao fim, apresenta os resultados dos artigos e sugere cinco perspectivas	(i) Ativos; (ii) Serviços; (iii) Comercial; (iv) Ataques; (v) Externo
Evesti, Kanstrén e Frantti (2017)	Constrói uma taxonomia sobre consciência situacional em segurança cibernética. Antes disso, apresenta os objetivos da conscientização situacional em segurança cibernética.	A. Escopo: (i) Nacional. (ii) Organizacional B. Nível: (i) Estratégico; (ii) Operacional C. Ótica: (i) Negócios; (ii) Legal; (iii) Técnico D. Tomada de Decisão: (i) Automática; (ii) Humana
Agrafiotis *et al.* (2018)	Sugere uma reflexão sobre danos cibernéticos e como isso foi conceituado em disciplinas como criminologia e economia, e investiga como outras noções, como risco e impacto, estão relacionados a danos cibernéticos. Além disso, cria uma taxonomia para danos cibernéticos.	(I) dano físico ou digital; (ii) dano econômico; (iii) dano psicológico; (iv) dano à reputação; (v) danos sociais e societais

Fonte: Dados da pesquisa.

Nota-se que as taxonomias citadas no Quadro 2 são variadas, a depender do contexto dos estudos, pois cada classificação atende a necessidades diferentes. Os estudos, citados de maneira geral no referido quadro, tangenciam a temática da segurança cibernética de forma específica ou correlata. Para atingir os objetivos propostos neste trabalho, optou-se por detalhar a taxonomia proposta por Evesti, Kanstrén e Frantti (2017).

Evesti, Kanstrén e Frantti (2017) apresentam uma taxonomia para CSSC a partir da apresentação de quatro finalidades sugeridas por eles, citadas no Quadro 2: (A) Escopo; (B) Nível; (C) Ótica; e (D) Tomada de Decisão. O Escopo é dividido em ‘Nacional’ (subdivido em militar e civil) e ‘Organizacional’, que se refere ao monitoramento de eventos e tendências em segurança cibernética. O Nível subdivide o objetivo da CSSC em ‘Estratégico’, que produz informações de longo prazo para tomada de decisões, e ‘Operacional’, que produz informações de curto prazo. A Ótica é subdividida em ‘Negócios’, ‘Legal’ e ‘Técnico’, a depender do contexto. Já a Tomada de Decisões é dividida em decisões ‘Automáticas’ e ‘Manuais’.

Das quatro finalidades da CSSC sugeridas por Evesti, Kanstrén e Frantti (2017) e citadas no Quadro 2, para fins deste trabalho enfatiza-se a da Ótica, citada no parágrafo anterior. O Quadro 3 apresenta uma descrição mais detalhada dessas óticas com suas definições e exemplos:

QUADRO 3
Taxonomia da Conscientização Situacional em Segurança Cibernética

Ótica	Definição	Exemplos
Negócios	Esta ótica aborda os seguintes aspectos: requisitos do cliente, preferências do cliente e ameaças específicas do domínio comercial. Tem uma visão voltada para o cliente para quem a organização presta serviços ou comercializa seus produtos.	Requisitos do cliente: um cliente que precisa seguir alguma regulamentação legal na definição de controle de segurança; Preferências dos clientes: clientes que passam a preferir os serviços em nuvem domésticos; Ameaças específicas do domínio comercial: vulnerabilidades, tais como o Ataque de Negação de Serviço*, que pode aparecer em áreas geográficas específicas ou em um setor comercial específico.
Legal	Esta ótica aborda aspectos a partir de uma perspectiva jurisdicional. Contempla informações necessárias ao tomador de decisão que se referem à regulamentação atual e futura e como isso afeta a organização. Tem uma visão voltada para a organização.	Uma organização que precisa seguir as normas de proteção de dados dos clientes. Para isso, há uma previsão legal de ações presumidas em caso de violação da regulamentação por parte da organização e sanções por possíveis violações.
Técnico	Esta ótica aborda as soluções e pesquisas tecnológicas envolvidas na conscientização situacional em segurança cibernética. Tem uma visão voltada para a organização.	Vulnerabilidades encontradas em produto de *software* utilizados e/ou produzidos pela organização e atividades contínuas de varredura de portas.

Fonte: Adaptado de Evesti, Kanstrén e Frantti, 2017.

*Nota. *Distributed Denial of Service* – DdoS, ou Ataque de Negação de Serviço, em português, é um tipo de ataque em sistemas que tem o objetivo de interromper os trabalhos de uma organização ou o funcionamento de serviços, inutilizando recursos. Trata-se de um ataque com várias origens, tornando-o "distribuído", o que faz com que a defesa seja mais difícil, pois um ataque originado de um único ponto pode ser mais facilmente bloqueado (CMU, 2016).

2.2. Segurança Cibernética e o Setor Bancário

Na Seção 2.1, foi visto que a segurança cibernética é um tema de interesse de vários setores da sociedade. Nesta seção, primeiramente faz-se uma descrição sobre como o tema relaciona-se com o setor financeiro em geral, descrevendo-se, na sequência, aspectos pertinentes à segurança cibernética no setor bancário.

Muitas nações reconhecem que o setor financeiro é essencial para suas estruturas críticas e economias. Este setor tem sido cada vez mais alvo de incidentes, inclusive crimes cibernéticos. Nos EUA, para exemplificar, já houve incidentes de segurança em empresas que prestam serviços financeiros e de pagamento, como JP Morgan, Card Services e Target (CATOTA *et al.*, 2018). Em 2016, um incidente direcionado ao Banco de Bangladesh resultou em um prejuízo de US$ 81 milhões; em 2017, a instituição financeira de crédito, Equifax, dos EUA, foi alvo de incidente provocado por *hackers*, o que resultou no comprometimento de informações pessoais de mais de 146 (cento e quarenta e seis) milhões de indivíduos (FSB, 2018). Outro exemplo ocorreu em 2016, quando clientes de um grande banco foram impedidos de acessar o *Internet Banking* por várias horas depois de um ataque configurado como crime cibernético (CAMILLO, 2017).

O comprometimento da segurança cibernética em instituições financeiras é impulsionado por vários fatores, incluindo a evolução da tecnologia. Esta evolução tecnológica, quando inadequadamente conduzida, pode aumentar ou causar: novas vulnerabilidades; interconexões entre instituições financeiras ou entre instituições financeiras e partes externas, como provedores de serviços de computação em nuvem e *FinTechs*[12], que podem não estar sujeitas à regulamentação das atutoridades do setor financeiro; novos métodos encontrados por criminosos cibernéticos para comprometer os sistemas baseados nas TICs; e a atratividade que as instituições financeiras têm para criminosos cibernéticos buscando ganhos financeiros ilícitos (FSB,2018).

O FSI e pesquisadores do sistema financeiro apontam que a pandemia de Covid-19 também foi um fenômeno que trouxe a emergência de crimes financeiros por meio do ambiente cibernético. A *The International Criminal Police Organization* – Interpol, por exemplo, emitiu em 2020 uma avaliação global de ameças sobre crimes e policiamento a seus 194 países membros, destacando um aumento acentuado de ameaças cibernéticas relacionadas a domínios e programas maliciosos de computadores (CRISANTO; PRENIO, 2020).

A lavagem de dinheiro também é um problema relacionado aos crimes cibernéticos e ao sistema financeiro e bancário. Com novos métodos de pagamento e com a introdução de serviços descentralizados, as possibilidades de lavagem de dinheiro mudaram e transformaram-se significativamente. A *Internet*, associada ao sistema financeiro, pode ser utilizada para fazer a lavagem de dinheiro de qualquer atividade ilegal realizada dentro e fora do espaço cibernético, mas grande parte dos casos está associada às atividades de criminosos cibernéticos (TROPINA, 2014).

Por sua vez, os riscos cibernéticos estão vinculados aos riscos operacionais no setor financeiro. As perdas decorrentes de incidentes cibernéticos representam uma parcela pequena das perdas operacionais. Além disso, a frequência com que ocorrem

---

[12] O termo *FinTech* é uma contração de '*financial techonology'*, que conceitua instituições que oferecem soluções financeiras inovadoras utilizando tecnologia da informação (PUSCHMANN, 2017).

é menor do que as demais perdas operacionais. No entanto, houve um aumento dessas perdas decorrentes dos incidentes cibernéticos nos últimos anos, em especial em 2016, quando houve um forte pico. Após esse período, houve um declínio, que pode ser explicado pelo aumento dos esforços e recursos gastos pelas instituições financeiras para diminuir os riscos cibernéticos. Apesar de representar uma parcela relativamente pequena de perdas operacionais, as perdas decorrentes de incidentes cibernéticos podem ser responsáveis por até um terço do valor operacional associado ao risco total (BIS, 2020d).

A preocupação com os riscos cibernéticos deu origem a várias iniciativas estratégicas para combatê-los no setor financeiro, como o uso da estrutura de segurança cibernética proposta pelo *National Institute of Standards and Technology* – NIST, programas de compartilhamento de informações e outras estratégias. Internacionalmente, os paises mais desenvoldidos já adotaram abordagens semelhantes (CATOTA *et al.*, 2018).

A respeito do risco cibernético no setor financeiro, o FSB diz o seguinte:

> (...) Reconhecendo os riscos de incidentes cibernéticos, autoridades em todo o mundo adotaram medidas regulatórias e de supervisão projetadas para facilitar a mitigação do risco cibernético pelas instituições financeiras e oferecer respostas eficazes, além de iniciativas para recuperação de incidentes cibernéticos (FSB, 2018).

Em reunião ocorrida de março de 2017, que contemplou ministros de finanças e presidentes dos bancos centrais do G20 em Baden-Baden, Alemanha, discorreu-se que o uso malicioso das TICs poderia interromper os serviços financeiros essenciais para os sistemas financeiros nacionais e internacionais, minar a segurança e a confiança, além de comprometer a estabilidade financeira. Buscando evitar tudo isso, e com o objetivo de melhorar a cooperação transfronteiriça, foi solicitado ao FSB, como um plano inicial, que fizesse uma avaliação das regulamentações e práticas de supervisão que eram praticadas nas suas jurisdições, inclusive para identificar aquelas que fossem eficazes. Em outubro de 2017, o FSB entregou o relatório de avaliação solicitado (FSB, 2018). No relatório, o FSB reuniu as respostas da pesquisa feita com as 25 (vinte e cinco) jurisdições membros do FSB e de organismos internacionais relacionados com o setor financeiro. Entre as conclusões citadas no relatório, destacam-se as seguintes (FSB, 2017):

- Todas as jurisdições membros do FSB haviam atuado ativamente no tratamento da segurança cibernética para o setor financeiro;
- Os organismos internacionais também haviam atuado ativamente na abordagem da segurança cibernética para o setor financeiro;
- As jurisdições relataram que seus esquemas regulatórios adotaram mais abordagens direcionadas à segurança cibernética e/ou riscos relacionados à tecnologia da informação (66% dos esquemas relatados) e menos abordagens direcionadas aos riscos operacionais em geral (34% dos esquemas relatados);
- Existiam muitas semelhanças entre as orientações internacionais, com muitos dos mesmos tópicos abordados;
- As jurisdições permaneceram ativas na área da segurança cibernética.

Uma constatação deste relatório diz respeito ao setor bancário, pois este foi o único setor de serviços financeiros para o qual todas as jurisdições membros do FSB emitiram pelo menos um regulamento, orientação ou prátcias de supervisão. A Figura 4 apresenta os dados agregados sobre este levantamento.

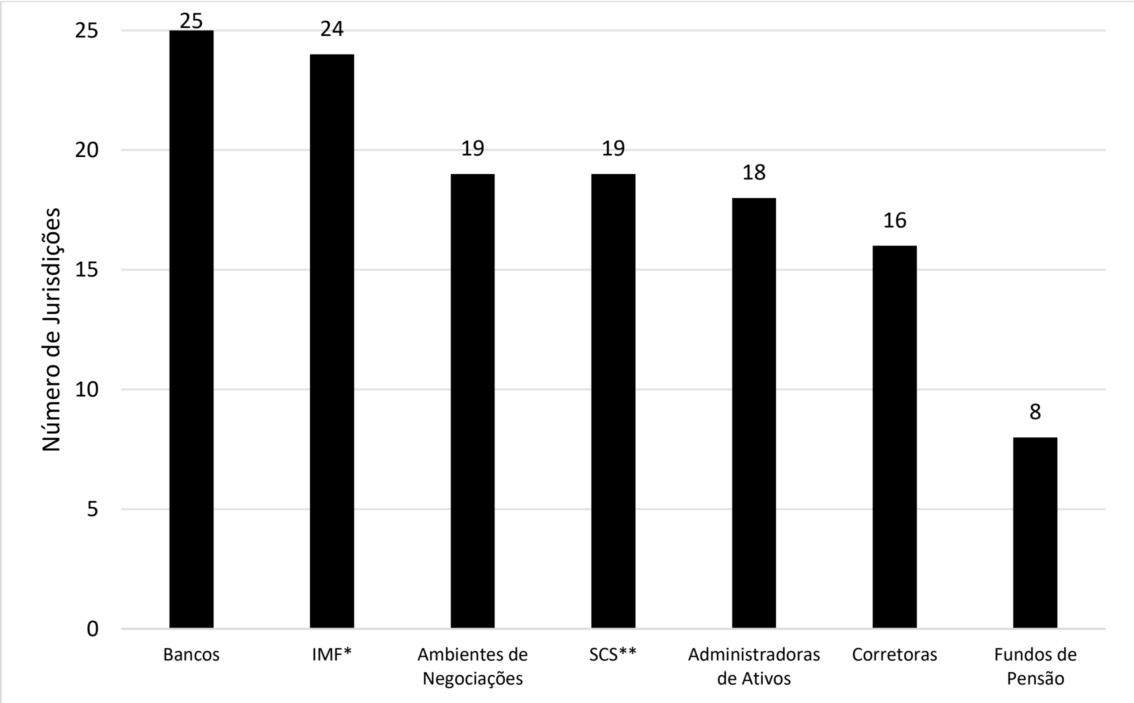

FIGURA 4 – Número de jurisdições que reportam esquemas de regulamentação ou de supervisão, por setor financeiro
Fonte: Adaptado de FSB, 2017.

Nota. *IFMF: Infraestrutura de Mercado Financeiro
Nota. **SCS: Setor de Companhias Seguradoras

Os membros do G20 sugeriram ao FSB, também, a criação de um léxico comum de termos importantes para a segurança cibernética no setor financeiro. Essa sugestão foi acatada e o FSB desenvolveu o *Cyber Lexicon* com termos relacionados à segurança cibernética e resiliência cibernética relativas ao setor financeiro (FSB, 2018). O objetivo deste léxico é apoiar o trabalho do FSB; dos órgãos normativos, incluindo o BCBS, o *Committee on Payments and Market Infrastructures* – CPMI[13], a *International Association of Insurance Supervisors* – IAIS[14] e o *International Organization of Securities Commissions* – IOSCO[15]; autoridades; e participantes do setor privado, como instituições financeiras e organizações de padrões internacionais, para tratar da segurança cibernética e da resiliência cibernética no setor financeiro. A ideia não é fazer do léxico uma norma legal, mas apoiar a atuação dos referidos autores (FSB, 2018).

Além do *Cyber Lexicon* do FSB, mais esforços também foram dedicados por outros organismos internacionais para melhor entender e reforçar a segurança cibernética no setor financeiro. O G7, por exemplo, elaborou um documento em que sugere oito elementos para a segurança cibernética no setor financeiro que devem ser seguidas pelas instituições que o compõe, podendo ser entendidos como etapas de um processo dinâmico e contínuo (ECB, 2016). O Quadro 4 apresenta um resumo destes elementos.

[13] O CPMI é um comitê do BIS, responsável por promover a segurança e a eficiência do pagamento, compensação, liquidação e acordos relacionados, apoiando a estabilidade financeira e a economia em geral (BIS, 2015).

[14] O IAIS é um organismo internacional de definição de padrões responsável por desenvolver e auxiliar na implementação de princípios, normas e outros materiais de apoio à supervisão do setor de seguros (IAIS, 2020).

[15] O IOSCO é um organismo internacional que reúne os reguladores mundiais de valores mobiliários e é reconhecido como o responsável pelo estabelecimento de padrões globais para o setor de valores mobiliários (IOSCO, 2020).

QUADRO 4
Elementos fundamentais de Segurança Cibernética no Setor Financeiro

Elemento	Recomendação
1 – Estratégia e Framework	Estabelecer e manter uma estratégia e uma estrutura de segurança cibernética adaptada aos riscos cibernéticos específicos e adequadamente informados por padrões e diretrizes internacionais, nacionais e do setor.
2 – Governança	Definir e facilitar o desempenho das funções e responsabilidades das pessoas que implementam, gerenciam e supervisionam a eficácia da estratégia e estrutura de segurança cibernética nas instituições para garantir a prestação de contas.
3 – Avaliação de Risco e Controle	Identificar funções, atividades, produtos e serviços, verificar sua importância e avaliar seus respectivos riscos cibernéticos; identificar e implementar controles para proteger e gerenciar esses riscos.
4 – Monitoramento	Estabelecer processos sistemáticos de monitoramento para detectar rapidamente incidentes cibernéticos e avaliar periodicamente a eficácia dos controles identificados, inclusive por meio de monitoramento, testes e auditoria.
5 – Resposta	(i) avaliar a natureza, escopo e impacto de um incidente cibernético; (ii) conter o incidente e diminuir seu impacto; (iii) notificar as partes interessadas; (iv) coordenar atividades de resposta conjunta, conforme necessário.
6 – Recuperação	Retomar as operações de maneira profissional, permitindo a correção contínua, inclusive (i) eliminar os restos nocivos do incidente; (ii) restaurar sistemas e dados ao estado normal; (iii) identificar e mitigar todas as vulnerabilidades que foram exploradas; (iv) remediar vulnerabilidades para evitar incidentes semelhantes; e (v) comunicar-se adequadamente interna e externamente
7 – Compartilhamento de Informações	Compartilhar informações confiáveis sobre segurança cibernética com as partes interessadas (incluindo entidades e autoridades públicas dentro e fora do setor financeiro) sobre ameaças, vulnerabilidades, incidentes e respostas para melhorar as defesas, limitar danos, aumentar a conscientização situacional e ampliar o aprendizado.
8 – Aprendizado Contínuo	Revisar a estratégia e estrutura de segurança cibernética regularmente e quando os eventos justificarem, para abordar mudanças nos riscos cibernéticos, alocar recursos, identificar e corrigir lacunas e incorporar o conhecimento adquirido.

Fonte: Adaptado de ECB, 2016.

Destaca-se que o termo ‘conscientização situacional’ é citado pelo G7, conforme Elemento 7 do Quadro 4. Para os fins deste estudo, este termo foi conceituado e mencionado na Seção 2.1.

O *Bank for International Settlements* – BIS[16] é outro organismo importante para o setor financeiro internacional, especialmente para o setor bancário, e também se preocupa com a segurança cibernética. Para o setor bancário, o BCBS, um dos comitês do BIS, tem especial importância. Este é formado por cinco grupos, que dão suporte ao trabalho técnico e forças-tarefa, que realizam tarefas específicas por um

[16] A missão do BIS é servir aos bancos centrais mundiais na busca pela estabilidade monetária e financeira, promover a cooperação internacional nessas áreas e atuar como um banco para os bancos centrais. Por meio de seus comitês, apoia os bancos centrais e outras autoridades jurisdicionais responsáveis pela estabilidade financeira, fornecendo análise de antecedentes e recomendações de políticas (BIS, 2020b).

tempo limitado (BIS, 2020b).

Um dos grupos do BCBS é o PDG, que desenvolve políticas que promovem um sistema bancário sólido e altos padrões de supervisão. Devido ao seu amplo escopo, o PDG criou vários grupos de trabalho e forças-tarefa especializados. Aqui, cabe o destaque para o ORG, pois este grupo, especificamente, é o reponsável por questões que envolvem a segurança cibernética no setor bancário ao fazer, no âmbito do referido Comitê, avaliações sobre o risco cibernético, entre outros (BIS, 2020ª).

Em novembro de 2018, o BCBS ressaltou que a frequência e o impacto das fraudes cibernéticas cresceram mais rapidamente do que a capacidade das empresas de impedi-las e se recuperar delas. O crime cibernético custava às empresas em 2018 perto de US$ 600 bilhões, contra US$ 445 bilhões em 2014, configurando-se como a terceira maior causa de prejuízos financeiros globais, perdendo apenas para a corrupção em governos e o tráfico de drogas (BIS, 2018).

Entre essas empresas, os bancos constituem o alvo favorito dos ataques cibernéticos. Uma pesquisa de 2017 estimou que uma instituição financeira típica enfrenta uma média de 87 (oitenta e sete) eventos cibernéticos por ano, sendo que um terço deles é bem sucedido (BIS, 2018). Este fato reforça a importância de se adotar medidas para segurança cibernética no âmbito do sistema bancário.

Nos EUA, o Departamento do Tesouro e os reguladores financeiros desenvolveram um processo para coordenar as atividades dos reguladores federais e estaduais de serviços financeiros, estabelecendo *o Financial and Banking Information Infrastructure Committee*, comitê encarregado de melhorar a resiliência do setor financeiro e bancário e promover parceria público-privada (ABEND *et al.*, 2008).

Em 2017, o Departamento de Serviços Financeiros de Nova Iorque expediu um documento contendo requerimentos de segurança cibernética para companhias de serviços financeiros. O documento reforça a preocupação com os crimes cibernéticos, destacando que podem causar perdas significativas para as entidades reguladas pelo departamento, bem como para as pessoas que podem ter suas informações pessoais reveladas e/ou roubadas para fins ilícitos. Para garantir a segurança, o departamento exige que as entidades reguladas mantenham um programa de segurança cibernética projetado para proteger a confidencialidade, integridade e disponibilidade dos sistemas de informação (DFS, 2017).

No Brasil, a preocupação com a segurança cibernética no setor financeiro e, especificamente, no setor bancário também existe. A este exemplo, o CMN expediu em 26 de abril de 2018 a Resolução nº 4.658, que 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 financeiras e demais instituições autorizadas a funcionar pelo BCB.” (CMN, 2018).

Por meio da Resolução nº 4.658, de 2018, o CMN, entre outras disposições, determina que instituições financeiras e demais instituições autorizadas, incluindo bancos, devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados (CMN, 2018).

Adicionalmente, em agosto de 2018, o BCB expediu a Circular nº 3.909, seguindo os mesmos moldes das diretrizes definidas pelo CMN, mas direcionando as regras especificamente para instituições de pagamento autorizadas a funcionar pela referida Autarquia (BCB, 2018).

Em 30 de janeiro de 2020, o BCB expediu a Circular nº 3.979, a qual dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil de informações relativas a eventos de risco operacional. No Art. 3º da Circular nº 3.979, de 2020, o BCB define como risco cibernético a possibilidade de ocorrência de perdas resultantes de incidentes cibernéticos. Por sua vez, o incidente cibernético é definido no Art. 4º da Circular no 3.979, de 2020, como sendo evento relacionado com o ambiente cibernético que:

> (i) produz efeito adverso ou representa ameaça aos sistemas de tecnologia da informação (TI) ou à informação que esses sistemas processam, armazenam ou transmitem; ou (ii) infringe políticas ou procedimentos de segurança referentes aos sistemas de TI (BCB, 2020).

Por fim, tanto o conceito de risco cibernético quanto de incidente cibernético dispostos na regulamentação brasileira guardam certo alinhamento aos conceitos previamente citados sobre esses termos presentes no *Cyber Lexicon*, documento editado pelo FSB e que foi discutido neste estudo anteriormente (FSB, 2018). Verifica-se, em complemento, que o CMN e o BCB, ao expedirem as resoluções e circulares que foram apresentadas nesta Seção, estão de acordo com as diretrizes e recomendações de órgãos internacionais de regulação financeira e bancária, a exemplo do FSB e do BCBS, já citados.

2.3. Análise Bibliomética e Segurança Cibernética

Pesquisadores e cientistas têm o compromisso de publicar os resultados de suas pesquisas e o conhecimento produzido por estes deve ser transformado em informação acessível para a comunidade científica. O foco das avaliações sobre ciência passou, com o decorrer dos anos, a ser os indicadores de resultados e de atividade científica. Sendo assim, os indicadores bibliométricos são essenciais para avaliar aquilo que se refere à ciência (MACIAS-CHAPULA, 1998).

Segundo Pritchard (1969), o termo 'bibliografia' seria a aplicação de métodos matemáticos e estatísticos em análises de livros e outros meios de comunicação.

Mais recentemente, Guedes e Borschiver (2005) definiram a bibliometria da seguinte forma:

> (...) uma ferramenta estatística que permite mapear e gerar diferentes indicadores de tratamento e gestão da informação e do conhecimento, especialmente em sistemas de informação e de comunicação científicos e tecnológicos, e de produtividade, necessários ao planejamento, avaliação e gestão da ciência e da tecnologia, de uma determinada comunidade científica ou país (GUEDES; BORSCHIVER, 2005).

Inicialmente, conforme Araujo (2006), a bibliometria voltava-se para a medida de livros, como quantidade de edições e exemplares, quantidade de palavras contidas nos livros etc., mas aos poucos foi-se voltando para o estudo de outros formatos, tais como artigos de periódicos e outros tipos de documentos. Depois, ocupou-se, também, da produtividade de autores e do estudo de citações.

Em relação aos pesquisadores, alguns estão preocupados com estudos bibliométricos puramente quantitativos (ARAÚJO, 2006). Outros, entretanto, colocam em questão a existência da bibliometria como disciplina científica e propõem que ela deveria ser somada a outras técnicas na realização de estudos (WHITE; WELLMAN; NAZER, 2004).

Sendo assim, muitos trabalhos têm utilizado técnicas bibliométricas aliadas a outros referenciais e métodos. Para Targino (1998), a título de exemplo, a região geográfica pode ser um fator interveniente na produção científica, ou seja, na análise bibliométrica é preciso levar em consideração também a região geográfica onde a produção científica é realizada, como país e/ou continente.

Quanto aos objetivos da bibliometria, uma contribuição importante foi dada por Mueller (2013). Em seu estudo bibliométrico para tentar entender o estado dos estudos métricos no Brasil sobre informação em ciência e tecnologia, a autora identificou quatro objetivos bibliométricos: (i) análise e mapeamento de autorias e coautorias, colaboração e redes; (ii) avaliação e descrição da literatura, impacto e indicadores; (iii) produção e produtividade, visibilidade de autores e instituições; e (iv) estudos de citação e cocitação (MULLER, 2013).

O estudo bibliométrico também pode contribuir para analisar publicações científicas pela perspectiva da abordagem empregada. Silva, Kimura e Sobreiro (2017), em seu artigo que trata sobre uma análise da literatura sobre risco sistêmico financeiro, classificaram sua amostra de artigos, entre outros pontos, pelo tipo de abordagem, classificando os artigos de acordo com as seguintes subcategorias: (i) quantitativo; (ii) qualitativo; (iii) quantitativo e qualitativo; (iv) revisão/pesquisa; e (v) não aplicável. A intenção do estudo, entre outros pontos, foi possibilitar a verificação da quantidade de artigos de uma amostra para cada tipo de abordagem. Verificou-se que a maioria dos artigos analisados possuía uma abordagem quantitativa, enquanto que uma reduzida quantidade enquadrarou-se como sendo de abordagem qualitativa. Uma minoria, ainda, foi classificada como qualitativa e quantitativa. Por fim, um pequeno número de artigos teve abordagem de revisão/pesquisa (SILVA; KIMURA; SOBREIRO, 2017).

A Bibliometria possui três leis clássicas que ajudam a entender as diferentes formas de análise. Essas Leis são conhecidas como: Lei de Lotka, que trata sobre a produtividade de autores; Lei de Bradford, que trata sobre a produtividade de periódicos; e Lei de Zipf, que analisa a frequência de palavras em determinado estudo estudo científico (GUEDES; BORSCHIVER, 2005).

A primeira lei, chamada de Lei de Lotka, afirma que “uma larga proporção da literatura científica é produzida por um pequeno número de autores, e um grande número de pequenos produtores se iguala, em proporção, ao reduzido número de grandes produtores” (ROMANI-DIAS, 2016, p. 29). É conhecida, também, como a Lei do Quadrado Inverso, justamente porque “aponta para a medição da produtividade dos autores, mediante um modelo de distribuição tamanho-frequência dos diversos autores em um conjunto de documentos” (VANTI, 2002, p. 153). A análise da produção de autores pode contemplar, ainda, o exame de coautoria, a qual serve para identificar os autores mais influentes em determinada área, com base no estudo de Fonseca e Jucá (2020).

A Lei de Bradford, ou Lei da Dispersão, possibilita estimar o grau de relevância de periódicos que atuam em áreas do conhecimento específicas. Assim, periódicos com mais publicações de artigos sobre determinado assunto tendem a estabelecer uma suposta superioridade em qualidade e maior relevância nesta área do conhecimento. Segundo esta lei, os primeiros artigos sobre um assunto são submetidos a um número restrito de periódicos. A publicação destes artigos incentiva outros autores a encaminhar seus artigos para esses mesmos periódicos. Ao mesmo tempo, outros periódicos, ao observar o crescimento do assunto, iniciam a publicação de artigos sobre a temática. Com todo esse interesse sobre o assunto, é possível estabelecer um núcleo de periódicos mais produtivos nesta área (MACHADO JUNIOR, 2016).

Por fim, a Lei de Zipf, também conhecida como a Lei do Mínimo Esforço, consiste em medir a frequência do aparecimento das palavras em vários textos. A partir daí, gera-se uma lista ordenada de termos de uma determinada disciplina ou assunto (VANTI, 2002). Zipf observou que em um texto suficientemente longo, existia uma relação

> (...) entre a freqüência que uma dada palavra ocorria e sua posição na lista de palavras ordenadas segundo sua freqüência de ocorrência. Essa lista era confeccionada levando-se em conta a freqüência decrescente de ocorrências. À posição nesta lista dá-se o nome de ordem de série (*rank*). Assim, a palavra de maior freqüência de ocorrência tem ordem de série 1, a de segunda maior freqüência de ocorrência, ordem de serie 2 e, assim, sucessivamente (GUEDES; BORSCHIVER, 2005, p.6).

Em análises bibliométricas também é relevante medir a frequência de palavras-chaves, que indicam o conteúdo de artigos e podem significar a tendência de pesquisa numa área (STROZZI *et al.*, 2017). O estudo das palavras-chaves pode, ainda, contemplar a análise de co-ocorrência delas, a qual pode ser feita com base no estudo de Fonseca e Jucá (2020). Por sua vez, estudar a co-ocorrência de palavras-chaves permite observar os temas mais endereçados pelos autores (Carvalho *et al.*, 2013).

Para avaliar a qualidade das publicações de determinados autores, e também dos periódicos de publicação científica, pode-se utilizar o *H Index*, ou Índice H, em português, e o Fator de Impacto*.* Conforme Thomaz, Assad e Moreira (2011), o Índice H de um pesquisador é o número de artigos publicados pelo pesquisador que tenham citações maiores ou iguais a esse número. Por exemplo, um pesquisador tem Índice H igual a dez caso ele tenha, pelo menos, dez artigos publicados, sendo que cada um deles tenha pelo menos dez citações. Portanto, quanto maior o número de artigos de grande interesse publicado pelo pesquisador, maior será o número de citações alcançadas, e maior será seu Índice H, o que reflete a qualidade acadêmico-científica do pesquisador e sua capacidade produtiva.

Já o Fator de Impacto é utilizado como instrumento de avaliação da qualidade das publicações desde os anos sessenta, sendo usado como critério de seleção dos periódicos a serem indexados pelo *Science Citation Index*[17]. O Fator de Impacto serve como meio de avaliação dos periódicos nas mais variadas instâncias. O valor do Fator de Impacto é considerado por autores para escolher o periódico que possa dar mais visibilidade aos seus trabalhos (THOMAZ; ASSAD; MOREIRA, 2011).

Percebe-se que a bibliometria é relevante para a ciência, pois por meio dela pode-se fazer análises importantes sobre a produção científica no mundo todo. No escopo da segurança cibernética, é possível encontrar análises bibliométricas sobre o assunto. Como o tema é de interesse de vários setores, como foi visto na Seção 2.1, identificam-se trabalhos com objetivos variados, mas que ajudam a exemplificar como a bibliometria pode ser aplicada no estudo da segurança cibernética.

Makawana e Jhaveri (2017), por exemplo, analisaram 149 trabalhos científicos entre 2015 e 2016. O objetivo do estudo foi esclarecer as tendências sobre o tema ‘aprendizado de máquina’ no contexto da segurança cibernética, e para isso verificaram: a quantidade de trabalhos publicado por país, com destaque para o Reino Unido; a quantidade de autores por trabalho, sendo que a maioria dos trabalhos foi publicada por 3 autores e a menor parte foi publicada por 8 autores ou mais; quantidade de artigos publicados por base de dados, destacando a base da IEEE como mais representativa; entre outros. O estudo conclui que o objetivo da maioria dos trabalhos analisados é detectar atividades maliciosas em sistemas de informação.

Outro estudo relevante é atribuído a Cojocaru e Cojocaru (2019). O artigo verifica o nível de pesquisa em segurança cibernética na República da Moldávia utilizando uma análise bibliométrica de trabalhos científicos disponibilizados em duas bases de dados internacionais. O objetivo é comparar o nível de pesquisa nacional com os países da Europa Oriental. A conclusão é que entre os países da Europa Oriental, a Moldávia tem uma contribuição pequena em termos de publicações internacionais sobre segurança cibernética.

Estay *et. al* (2020), também contribui com outro estudo, propondo uma revisão sistemática/bibliométrica sobre *frameworks* de avaliação de resiliência cibernética. O objetivo é identificar e analisar pesquisas sobre o tema, por meio da manipulação de

[17] Nota do autor: O *Science Citation Index* é um índice que informa a relevância dos periódicos dentro do contexto da produção científica.

dados de uma amostra que representa 36 setores diferentes e 25 diferentes áreas de pesquisa. Os autores analisaram 208 artigos publicados até o ano de 2019 e verificaram, entre outros: o número de publicações por ano, sendo que o ano de 2019 foi o ano com mais publicações; e o número de artigos publicados por periódico, com destaque para o jornal *IEEE Transactions on Smart Grid*. Entre as conclusões, destaca-se que há um interesse crescente em pesquisas sobre *frameworks* de avaliação de resiliência cibernética. No entanto, há uma alta dispersão na densidade de publicações em periódicos, o que é uma indicação de que ainda não há um foco claro de pesquisa sobre o tema.

Estes estudos, embora não tratem especificamente sobre o setor bancário, servem para ilustrar a existência de estudos bibliométricos científicos sobre segurança cibernética em diferentes setores, o que reforça a relevância do tema abordado neste trabalho. Além disso, os estudos ajudam a ilustrar possíveis caminhos para a pesquisa bibliométrica sobre segurança cibernética em geral.

3. MÉTODOS E TÉCNICAS DE PESQUISA

Este capítulo apresenta os métodos e as técnicas de pesquisa que foram empregadas na realização deste estudo e é dividido em quatro seções. A Seção 3.1 trata sobre a tipologia e descrição geral dos métodos de pesquisa. A Seção 3.2 traz a caracterização da área de estudo. A Seção 3.3 apresenta dados sobre a população e amostra observada. Por fim, a Seção 3.4 discorre sobre os procedimentos de coleta e análise dos dados.

3.1. Tipologia e descrição geral dos métodos de pesquisa

Esta pesquisa é descritiva por buscar especificar propriedades e características do objeto de estudo com o objetivo único de coletar e medir informações para análise, sem a intenção de relacionar conceitos ou variáveis. O recorte temporal empregado é o longitudinal, com dados coletados em diferentes pontos do tempo (SAMPIERI; COLLADO; LUCIO, 2013).

Quanto ao tipo de abordagem, esta pesquisa é definida como qualitativa, porque os dados coletados são secundários e a análise dos textos dos artigos é interpretativa, e também é quantitativa, no que se refere à análise bibliométrica do conjunto de artigos obtidos (AFONSO *et al.*, 2011). O conceito de análise bibliométrica adotado é aquele apresentado na Seção 2.3, atribuído a Guedes e Borschiver (2005).

3.2. Caracterização da área de estudo

A área de estudo desta pesquisa são artigos publicados em bases de dados de periódicos científicos. Entre o conjunto de possibilidades de pesquisas na área de segurança cibernética, optou-se neste estudo por direcionar a pesquisa para o setor bancário. O trabalho também encontra correlação com áreas de estudo como Administração, em especial o Gerenciamento de Riscos Operacionais, possibilitando pesquisas nas seguintes áreas: sistema financeiro e bancário internacional; tecnologia da informação; e segurança da informação.

3.3. População e amostra

A população compreendeu as publicações científicas disponíveis nas seguintes bases de dados acadêmicas, relacionadas no Portal de Periódicos da CAPES (CAPES, 2020): EBSCOhost, ProQuest, Scopus – Elsevier e *Web of Science* – WoS.

Para escolha das bases foram observados os seguintes critérios: (i) são indexadas pela CAPES e da área das Ciências Sociais Aplicadas; (ii) pertencem às subáreas de Administração de Empresas, Administração Pública e Contabilidade; (iii) possuem textos completos disponíveis; (iv) possuem abordagem internacional com publicações de qualidade, por serem revisadas por pares/especialistas; e (v) possuem ferramentas de busca que facilitam a identificação de artigos de acordo com os critérios de seleção definidos para este estudo.

A amostra é não probabilística, pois a escolha dos elementos não depende da probabilidade, mas de causas relacionadas com as características da pesquisa e aos objetivos do estudo (SAMPIERI; COLLADO; LUCIO, 2013). Para selecionar a amostra a partir da população, considerou-se os seguintes critérios:

Na 1ª etapa, para a pesquisa dos artigos nas bases de dados, foram utilizados os seguintes termos de busca em inglês: '*cyber security'*, '*cybersecurity'*, '*cyber crime*', '*cybercrime'* e '*cyber risk*', associadas às palavras '*banking'*, '*bank*' ou '*banks'*[18]. Os resultados foram os seguintes: 245 documentos na plataforma EBSCOhost; 2.591 documentos na ProQuest; 441 documentos na Scopus – Elsevier; e 189 documentos na WoS.

Na 2ª etapa, utilizou-se limitadores de pesquisa para refinar a busca. Os limitadores foram: revistas acadêmicas revisadas por especialistas/pares, documentos em idioma inglês e tipo de documento limitado a artigo científico. Os resultados foram os seguintes: 39 artigos na plataforma EBSCOhost; 121 artigos na ProQuest; 190 artigos na Scopus – Elsevier; e 84 artigos na WoS.

Na 3ª etapa foram excluídas as repetições de artigos que foram encontrados em mais de uma base de dados ao mesmo tempo. Adicionalmente, foi realizada a leitura dos resumos e introduções dos artigos remanescente para verificar se o assunto tem relação com o tema de interesse deste estudo. Com isso, foram

---

[18] Nota do autor: para maior objetividade da pesquisa, os indexadores de busca foram configurados para encontrar documentos com os termos de busca contidos no título, resumo e/ou palavras-chaves dos documentos.

aproveitados 72 artigos, sendo 14 artigos na EBSCOhost, 18 artigos na ProQuest, 35 artigos na Scopus – Elsevier e 5 artigos na WoS.

A Figura 5 é um modelo sintetizado das etapas para seleção dos artigos da amostra.

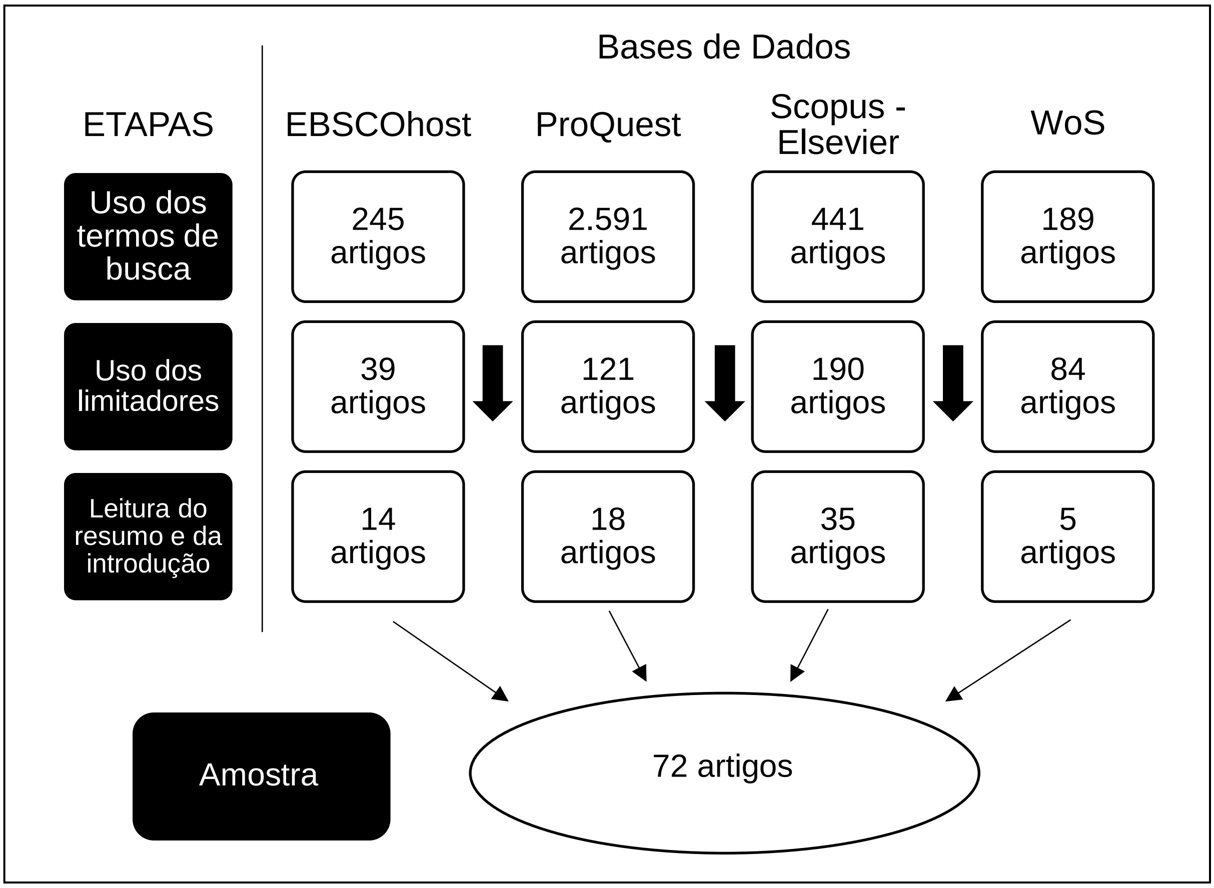

FIGURA 5 - Etapas para a seleção da amostra.
Fonte: Dados da pesquisa

3.4. Procedimentos de coleta e de análise de dados

A coleta dos dados compreendeu o intervalo entre o dia 28 de janeiro de 2020 e 08 de julho de 2020. Para a coleta dos dados, foram utilizadas quatro bases de dados: EBSCOhost, ProQuest, Scopus – Elsevier e WoS. Todas as bases de dados são indexadas pela Portal de Periódicos da CAPES, conforme citado na Seção 3.3 deste estudo.

Para a análise e tratamento dos dados foi empregada a estatística descritiva, a análise de conteúdo, a análise de coautoria, a técnica de elaboração de nuvens de palavras e a análise de co-ocorrência de palavras-chaves.

A estatística descritiva foi utilizada conforme Reis (2008), para levantamento dos dados, auxiliando a análise e interpretação de dados numéricos, utilizando de quadros, tabelas, gráficos e indicadores numéricos.

A análise de conteúdo foi utilizada para categorizar os artigos segundo à abordagem metodológica empregada, podendo ser ‘quantitativa’, ‘qualitativa’ ou ‘quantitativa e qualitativa’, com base em Silva, Kimura e Sobreiro (2017).

Também foi utilizada a análise de conteúdo para classificar os artigos em uma das três categorias sugeridas por Evesti, Kanstrén e Frantti (2017) e citadas na Seção 2.1: ‘Negócios’, ‘Legal’ ou ‘Técnico’. Para este objetivo, os artigos foram analisados em sua integralidade, respeitando-se a definição de análise de conteúdo sugerida por Bardin (1977):

> (...) um conjunto de técnicas de análise das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a interferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens.

A técnica de elaboração de nuvens de palavras foi utilizada para avaliar a frequência do aparecimento dos termos nas palavras-chave dos artigos e teve o objetivo de compreender quais temáticas científicas foram tratadas e identificadas nos elementos da amostra (REIS; DOMINGUES, 2014). As análises de coautoria e de co-ocorrência de palavras-chaves foram realizadas com base no estudo de Fonseca e Jucá (2020).

O Quadro 5 apresenta os itens utilizados para analisar os artigos de acordo com os objetivos específicos deste estudo.

QUADRO 5
Itens considerados para analisar os artigos

	Item	Forma de operacionalização do item
1	Quantidade de artigos por ano de publicação	1, 2, 3, 4 ou mais
2	Quantidade de artigos publicados por periódico	1, 2, 3, 4 ou mais
3	Classificação dos artigos conforme a quantidade de autores e análise de coautoria*	1, 2, 3, 4 ou mais
4	Quantidade de artigos por filiação acadêmica, indicando o continente da instituição à qual os autores estão vinculados	-Quantidade de artigos na África -Quantidade de artigos nas Américas -Quantidade de artigos na Ásia-Pacífico -Quantidade de artigos na Europa
5	Distribuição das palavras-chaves dos artigos e análise de co-ocorrências	Frequência de aparição das palavras-chaves e relações de co-ocorrência entre elas
6	Categorização dos artigos segundo à abordagem metodológica empregada	- Quantitativa; - Qualitativa; - Quantitativa / Qualitativa.
7	Classificação dos artigos de acordo com a ótica empregada	- Negócios; - Legal; - Técnico.

Fonte: Adaptado de Evesti, Kanstrén e Frantti, 2017; Silva, Kimura e Sobreiro, 2017; Rossi e Alves, 2020.

Nota. *A análise de coautoria foi realizada com base em Fonseca e Jucá (2020) e após a classificação dos artigos conforme a quantidade de autores. A forma de operacionalização da análise de coautoria é por meio da verificação de autoria compartilhada entre dois ou mais autores.

Por fim, para a confecção de tabelas, quadros e gráficos que são apresentados nos resultados foi utilizado o software Microsoft Excel e o LibreOffice Calc. Adicionalmente, o software VOSviewer foi utilizado para a confecção do mapa de coautoria, da nuvem de palavras e do mapa de co-ocorrência de palavras-chaves.

4. RESULTADOS E DISCUSSÕES

Este capítulo apresenta os resultados e discussões. A Seção 4.1 mostra a quantidade de artigos publicados por ano de publicação; a Seção 4.2 mostra a quantidade de artigos publicados por periódico; a Seção 4.3 apresenta a classificação dos artigos conforme a quantidade de autores e a análise de coautoria; a Seção 4.4 mostra a quantidade de artigos por filiação acadêmica ou instituição a que estão vinculados os autores; a Seção 4.5 apresenta a distribuição das palavras-chaves dos artigos e a análise de co-ocorrências; a Seção 4.6 apresenta a categorização dos artigos segundo à abordagem metodológica empregada; e, por fim, a Seção 4.7 apresenta a classificação dos artigos de acordo com a ótica empregada.

4.1. Quantidade de artigos publicados por ano de publicação

A Figura 6 mostra o gráfico da distribuição da publicação de artigos por ano. Pode-se perceber que o ano de 2019 possui a maior quantidade de publicações, com 21 artigos, representando 29,17% do total. Nos anos de 2004 e 2008 foram publicados 2 artigos, um em cada ano, sendo o período com menor produção. Entre os intervalos de 2004 a 2008 e o de 2008 a 2011 não houve publicações. Para o ano de 2020, considerou-se apenas o primeiro semestre, devido o período de coleta de dados.

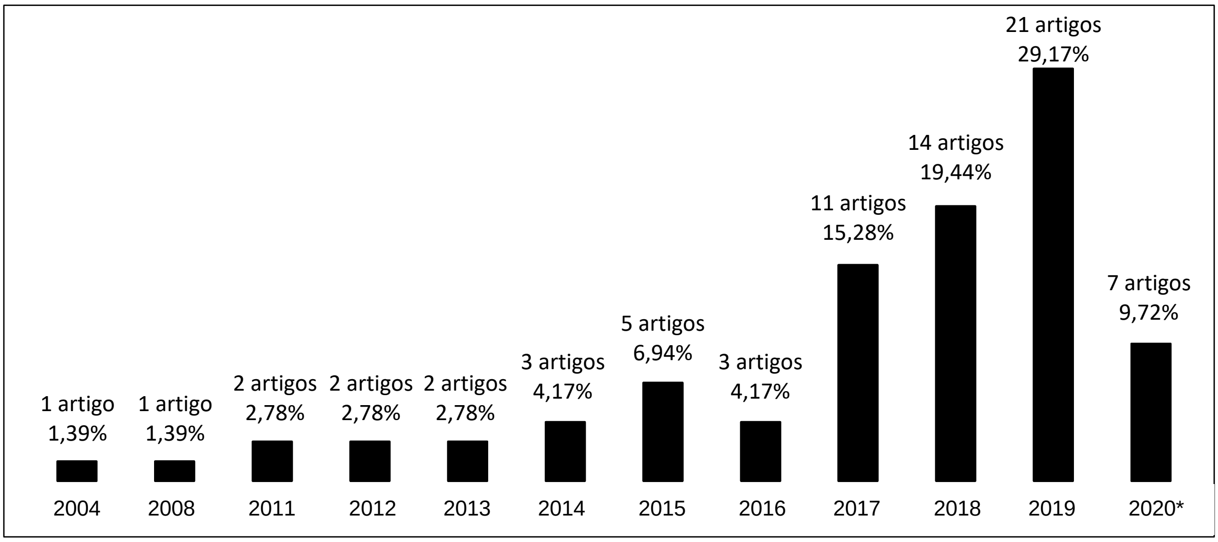

FIGURA 6 - Quantidade de artigos publicados por ano
Fonte: Dados da pesquisa.

Nota. *Para o ano de 2020 foram coletados artigos publicados até o mês de junho

Os resultados apresentados na Figura 6 mostram 29,17% de publicações acadêmicas no ano de 2019. Isto pode significar um maior interesse na publicação sobre o tema neste ano. Esses resultados são coerentes com o que foi exposto na Figura 1, na qual verificou-se que as buscas pelos termos ‘cyber security’ e ‘cybersecurity’ tiveram um aumento a partir de 2019 (GOOGLE, 2020). Cabe destacar, também, que apesar das buscas terem sido feitas até o mês de junho, o ano de 2020 aparece como o quarto ano com mais publicações de artigos.

4.2. Quantidade de artigos publicados por periódicos

A Tabela 1 apresenta a quantidade de artigos publicados por periódico. Os 72 artigos da amostra foram publicado em 56 periódicos. O periódico *Journal of Internet Banking and Commerce* tem destaque, com a publicação de 5 artigos, representando 6,94% da amostra. O periódico *Journal of Money Laundering Control* totalizou 4 artigos (5,56% da amostra). Três periódicos aparecem com 3 artigos publicados cada, totalizando 9 artigos (12,50% da amostra): *Crime, Law & Social Change*, *International Journal of Recent Technology and Engineering* e *Journal of Financial Crime*. Três periódicos aparecem com 2 publicações cada, totalizando 6 artigos (8,33% da amostra): *European Journal of Criminology*, *European Journal on Criminal Policy and Research* e *International Journal of Engineering and Advanced Technology*. Os demais 48 periódicos publicaram 1 artigo cada, totalizando 66,67% da amostra.

TABELA 1
Quantidade de artigos por periódico

Periódicos	**Quantidade de artigos por periódico**	**Quantidade total de artigos***	**Participação da amostra (%)**
Journal of Internet Banking and Commerce	5	5	6,94%
Journal of Money Laundering Control	4	4	5,56%
Crime, Law & Social Change / International Journal of Recent Technology and Engineering / Journal of Financial Crime	3	9	12,50%
European Journal of Criminology / European Journal on Criminal Policy and Research / International Journal of Engineering and Advanced Technology	2	6	8,33%
Demais 48 periódicos (1 artigo)	1	48	66,67%
Total		**72**	**100,00%**

Fonte: Dados da pesquisa

Nota. *A coluna ‘Quantidade total de artigos’ traz o resultado da multiplicação entre a quantidade de periódicos listados na coluna ‘Periódicos’ e os dados da coluina ‘Quantidade de artigos por periódico’.

Em relação à amostra, os periódicos *Journal of Internet Banking and Commerce* e *Journal of Money Laundering Control* figuram, respectivamente, como os mais produtivos sobre o tema ‘segurança cibernética no setor bancário’. O primeiro apresentou 5 artigos publicados, o que representa 6,94% do total da amostra, enquanto que o segundo apresentou 4 artigos publicados, representando 5,56% do total da amostra.

4.3. Classificação dos artigos conforme a quantidade de autores e análise de coautoria

O gráfico da Figura 7 apresenta a quantidade de autores por artigo publicado. Pode-se notar que a maioria dos artigos foi publicada por 2 autores, sendo 22 artigos da amostra, representando 30% do total. 20 artigos foram publicados por apenas um autor, representando 28% da amostra. Os artigos que foram publicados por 3 autores somam 17, o que representa 24% da amostra. 7 artigos foram publicados por 4 autores, representando 10% da amostra e apenas 6 artigos foram publicados por 5 autores ou mais, representando 8% do total.

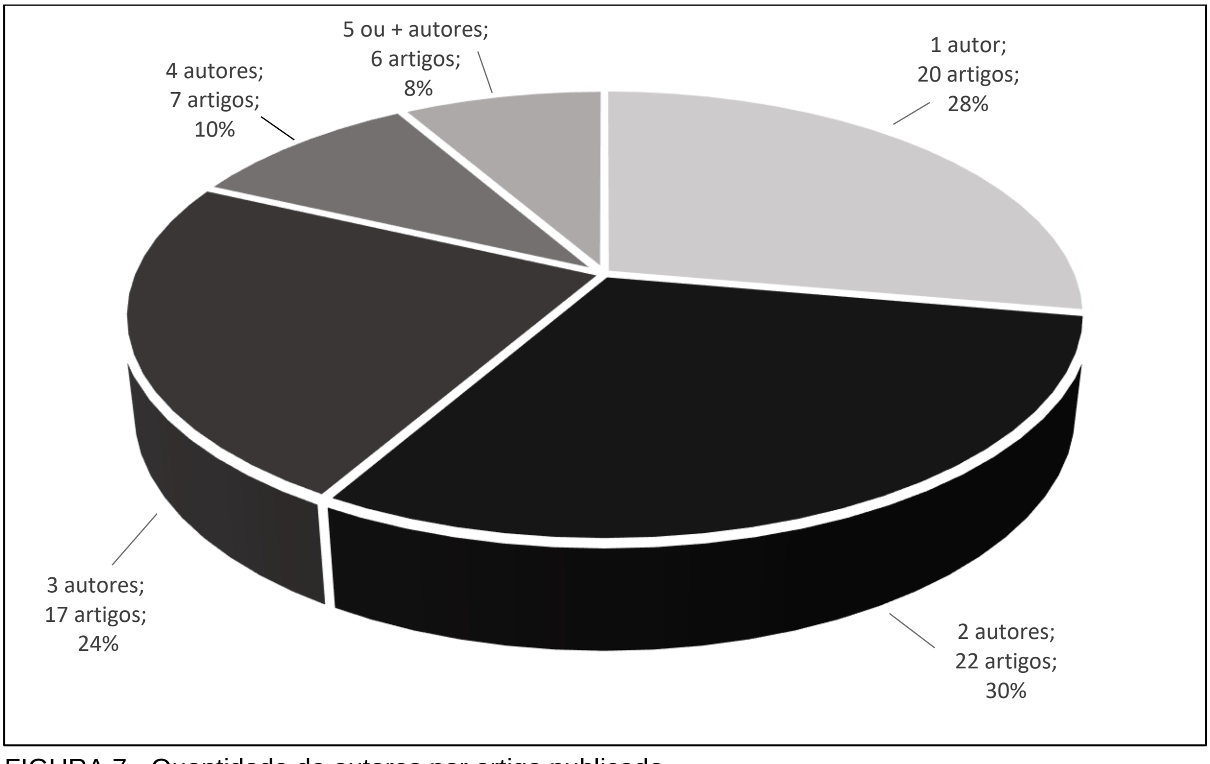

FIGURA 7 - Quantidade de autores por artigo publicado
Fonte: Dados da pesquisa

Diferente do estudo bibliométrico sobre segurnaça cibernética de Makawana e Jhaveri (2017), que teve como resultado a maioria de artigos tendo sido escritos por 3 autores, aqui verificou-se que a maioria foi publicada por 2 autores. Apesar do foco do citado estudo ter sido em pesquisas sobre aprendizado de máquina para segurança cibernética, a comparação dos seus resultados com os achados citados na Figura 7 pode ser útil para análise da produção acadêmica sobre segurança cibernética.

A Figura 8 apresenta o mapa de coautoria dos artigos da amostra. Os autores são representados pelos seus sobrenomes seguidos das iniciais dos primeiros nomes. A coautoria é representada pelas linhas que conectam os círculos. A espessura das linhas representa a frequência com que os autores publicaram artigos juntos e o tamanho dos círculos significa a relevância dos autores, isto é, quanto maior o círculo mais relevante para a amostra é o autor.

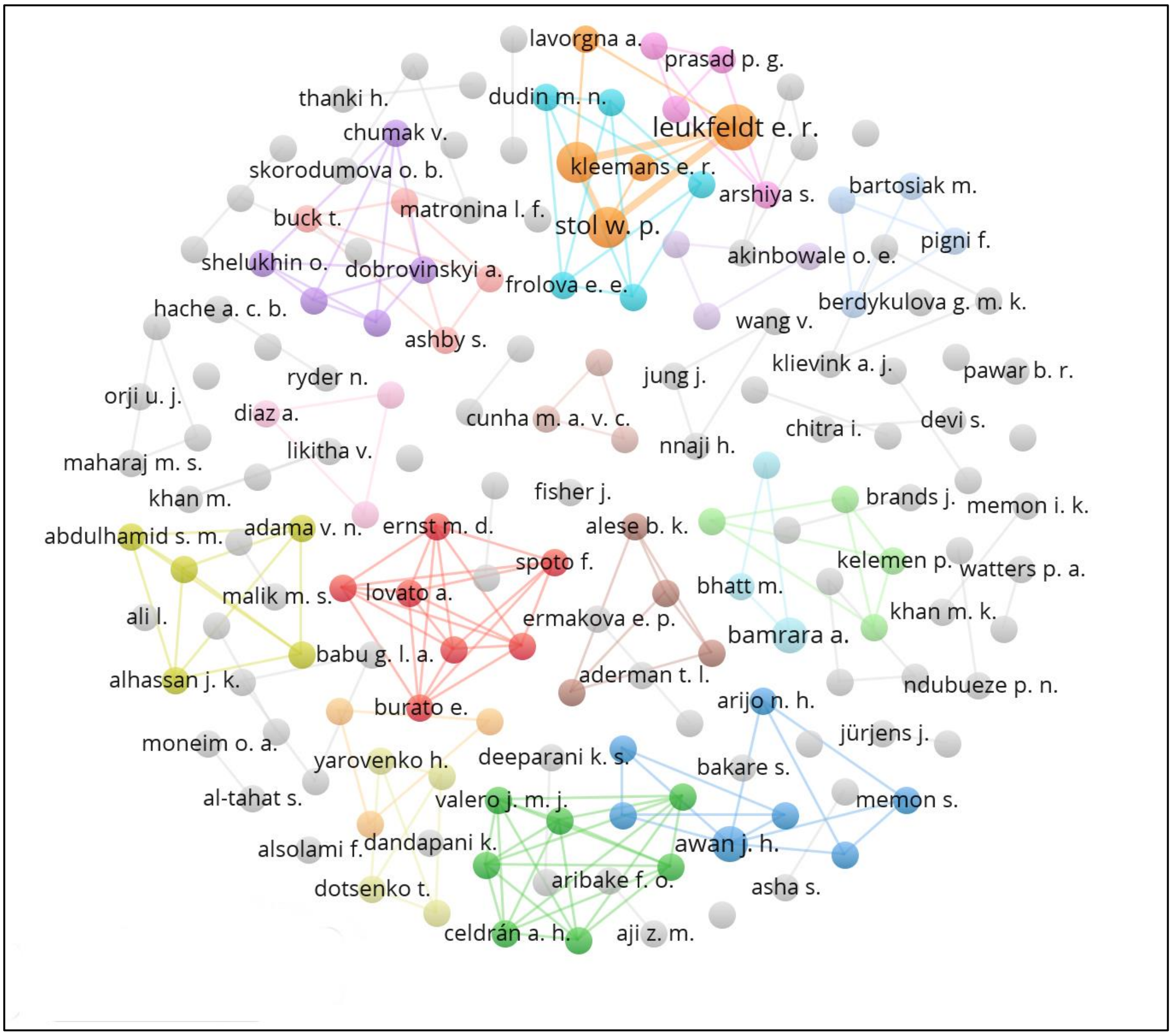

FIGURA 8 - Mapa de coautoria entre os autores da amostra
Fonte: Dados da pesquisa.

Verifica-se que os autores E. Rutger Leukfeldt, Edward R. Kleemans, Wouter P. Stol e Jawad Hussain Awan aparecem em evidência, o que significa que tiveram mais publicações de artigos individualmente. Destaca-se, ainda, que, os resultados mostraram que Rutger Leukfeldt e Edward R. Kleemans dividem a autoria de 4 artigos. Leukfeldt também é coautor junto com Wouter P. Stol em 3 artigos. Por terem maior relação de coautoria, as linhas que os conectam na Figura 8 têm maior espessura.

Verificou-se que há poucas conexões, e isto acontece porque há uma grande variedade de autores na amostra e a maior parte deles divide com outros a autoria de apenas um artigo. Adicionalmente, o presente estudo analisou a relação de coautoria sem relacionar os países da filiação acadêmica de todos os autores da amostra. No entanto, e com base nas análises de Fonseca e Jucá (2020), destaca-se que os autores Rutger Leukfeldt, Edward R. Kleemans e Wouter P. Stol, que têm destaque na relação de coautoria, possuem filiação acadêmica na Holanda.

4.4. Quantidade de artigos por filiação acadêmica ou instituição a que estão vinculados os autores

A Tabela 2 mostra a quantidade de artigos publicados por continente. Para isto, considerou-se o continente em que estão localizadas as universidades ou instituições a que estão vinculados os autores dos artigos. O total de instituições apuradas nos 72 artigos da amostra foi de 107. O continente europeu destaca-se por apresentar 44 instituições com publicações de artigos, equivalente a 41,12% do total. O continente americano aparece com 12 instituições, o que representa 11,21% do total, sendo o continente com menor número de instituições com artigos publicados. Pode-se perceber, com base nos resultados da análise, que os continentes africano e americano apresentaram a menor quantidade de instituições com artigos publicados, o que sugere uma oportunidade de pesquisa sobre o tema ‘segurança cibernética no setor bancário’ nesses dois continentes.

TABELA 2
Quantidade de artigos publicados por continente em que estão localizadas as instituições a que estão vinculados os autores

Continente	Quantidade de Instituições	Participação da amostra (%)
Europa	44	41,12%
Ásia-Pacífico	38	35,51%
África	13	12,15%
Américas*	12	11,21%
Total	**107**	**100,00%**

Fonte: Dados da pesquisa

Nota. *Somente uma instituição está localizada no Brasil, representando o continente americano.

Os resultados sugerem relação com o fato de que a região da Europa possui maior quantidade de países com métricas de segurança cibernética para avaliação de risco cibernético, conforme ITU (2018) e o exposto na Figura 2 deste estudo[19]. A relação também existe para as regiões da África e das Américas, pois as duas regiões possuem menos países com métricas de segurança cibernética para avaliação de risco cibernético.

Em complemento, o Quadro 6 apresenta as instituições que tiveram mais artigos publicados. Nota-se que as três instituições que mais publicaram artigos estão localizadas na Holanda, representando o continente Europeu. Além disso, outras duas instituições, que publicaram 2 artigos cada, também estão localizadas na Holanda.

[19] Ressalta-se que o estudo de ITU (2018) não é uma análise bibliométrica, além de não abranger todo o período de análise dos dados deste trabalho. No entanto, suas discussões são úteis como comparação e suas observações têm associação com os resultados aqui expostos.

QUADRO 6
Instituições com mais aparições na filiação acadêmica

Instituição	País	Continente	Número de aparições
Vrije Universiteit Amsterdam	Holanda	Europa	4
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)	Holanda	Europa	3
Open University of the Netherlands	Holanda	Europa	3
Bahauddin Zakariya University	Paquistão	Ásia-Pacífico	2
Leiden University	Holanda	Europa	2
Statistics Netherlands (CBS)	Holanda	Europa	2
Sumy State University	Ucrânia	Europa	2
Universität Koblenz	Alemanha	Europa	2
University of Bradford	Reino Unido	Europa	2
University of Nigeria	Nigéria	África	2
University of Sindh	Paquistão	Ásia-Pacífico	2

Fonte: Dados da pesquisa

4.5. Distribuição das palavras-chaves dos artigos e análise de co-ocorrências

Foram contabilizadas 245 palavras-chaves presentes nos 72 artigos da amostra. Para a análise, uma nuvem de palavras foi criada para visualização da distribuição das principais palavras-chaves e é apresentada na Figura 9. As palavras-chaves mais relevantes foram *'cyber crime'* (29 repetições), '*cyber security*' (14 repetições), '*phishing*' (13 repetições), '*security'* (7 repetições), '*internet banking*' (6 repetições), '*money laundering*' (5 repetições), '*cyber threat*' (4 repetições) e '*information security*' (4 repetições). Cabe destaque a ocorrência da palavra-chave '*covid-19*', com uma 1 aparição. Na nuvem de palavras, as palavras-chaves com mais relevância são apresentadas em tamanho maior, enquanto aquelas que possuem menos relevância aparecem em tamanho menor.

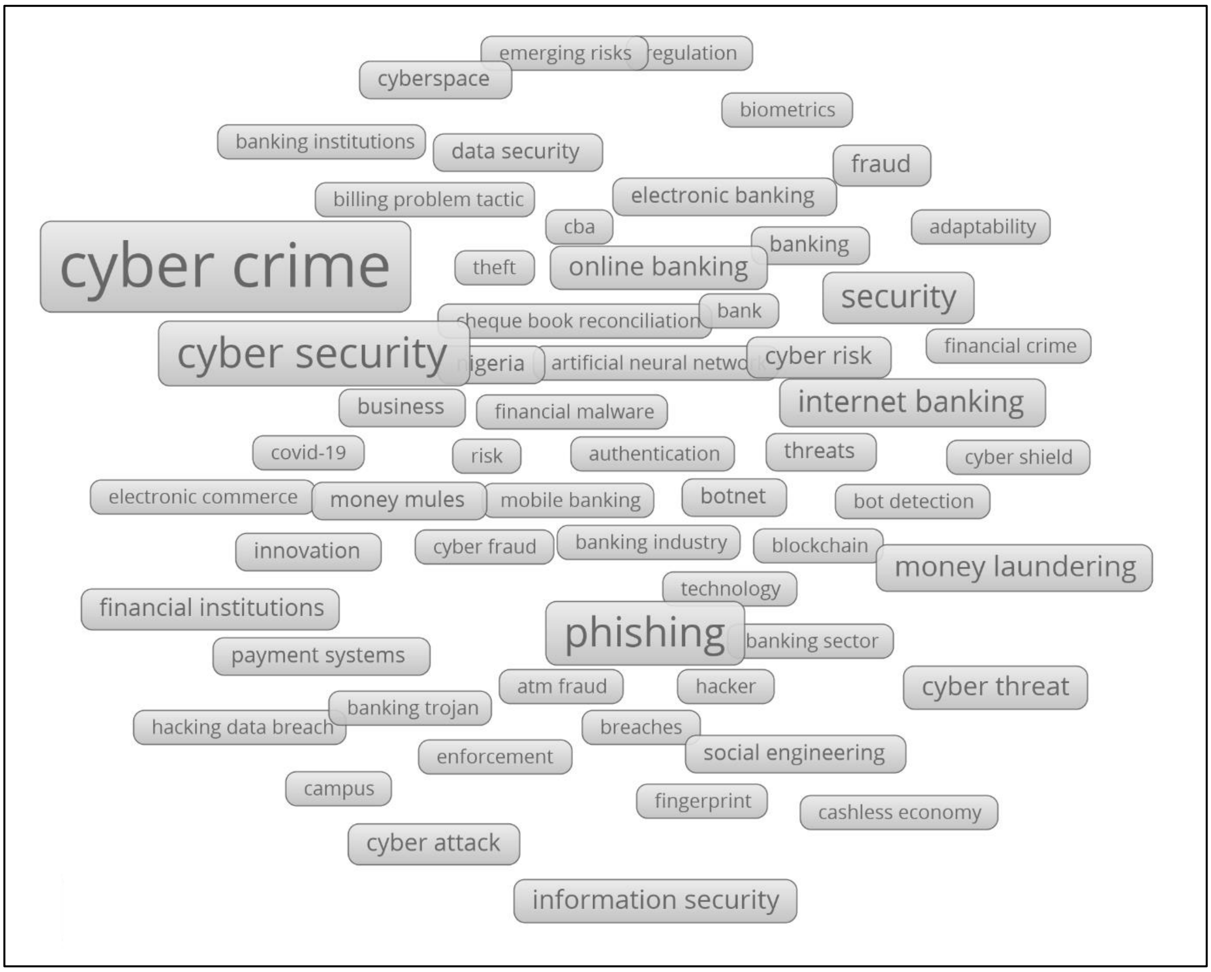

FIGURA 9 - Nuvem de palavras-chaves presentes nos artigos da amostra
Fonte: Dados da pesquisa (elaborado com o software VOSviewer).

Nota-se que as palavras-chaves '*cyber crime'*, '*cyber security'* e *'phishing'*, que aparecem com destaque na Figura 9, foram citadas no referencial teórico. As citações de *Cyber Crime*, ou crime cibernético, estão atribuídas a: Camillo (2017); Gordon e Ford (2006); e BIS (2018). As citações de *Cyber Security*, ou segurança cibernética, estão atribuídas a: Craigen, Diakun-Thibault e Purse (2014); DHS (2009); Ottis e Lorents (2010); ISO/IEC (2012); FSB (2018); Solms e Niekerk (2013); Mitnick e Simon (2003); Eswaran e Vinayagamoorthi (2019); Bagheri e Ridley (2017); CMN (2018); BCB (2018); entre outros. Já as citações de *Phishing,* um tipo de ataque relacionado à engenharia social, estão atribuídas a: Gordon e Ford (2006); e Hong (2012).

Adicionalmante, foi realizada uma análise das co-ocorrências das principais palavras-chaves presentes nos artigos. A Figura 10 apresenta o mapa destas co-ocorrências, o que permite observar os temas mais abordados pelos autores. As palavras-chaves que aparecem simultaneamente no mesmo artigo são aquelas que estão conectadas por linhas. A espessura das linhas representa a força da conexão entre as palavras-chaves, significando uma maior quantidade de aparições simultâneas em diferentes artigos. Destacam-se algumas conexões mais relevantes, representadas pelos pares de palavras-chaves '*cyber crime'* e '*phishing'*, '*cyber crime*' e *'money laundering'*, *'cyber crime'* e '*security'*, '*security'* e '*phishing'* e o par '*cyber security'* e '*cyber risk'*. Todos esses pares apareceram simultaneamente em mais de um artigo da amostra.

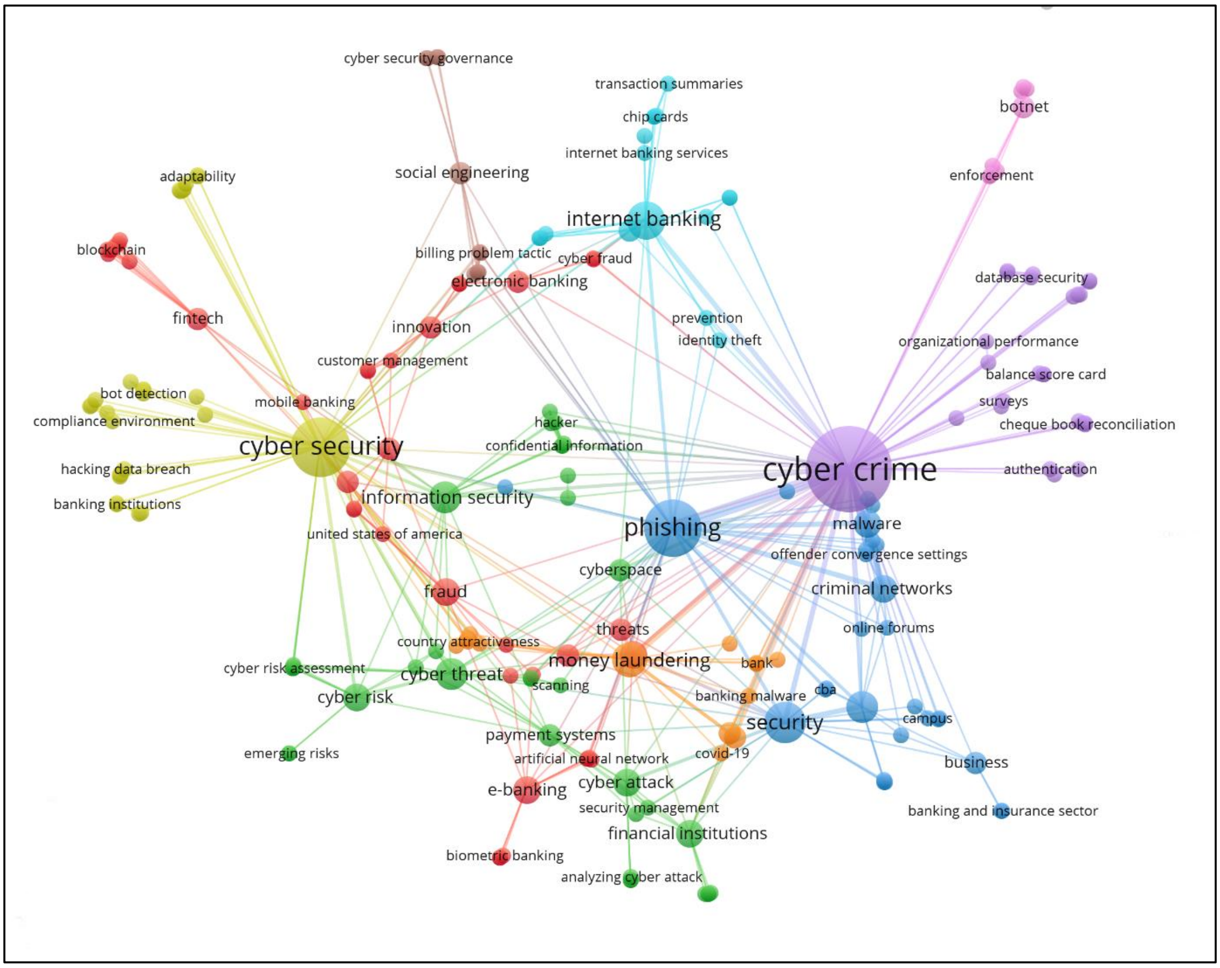

FIGURA 10 - Mapa de co-ocorrência de palavras-chaves presentes nos artigos da amostra
Fonte: Dados da pesquisa (elaborado com o software VOSviewer).

Nota-se, com base na Figura 10, por exemplo, que a palavra-chave '*cyber crime*', ou crime cibernético, apresenta vínculo com '*phishing'* que, por sua vez, apresenta co-ocorrência com a palavra-chave '*social engineering'*, ou engenharia social. Estes vínculos encontram relação com a definição sobre *phishing* atribuída a Hong (2012), citado na Seção 2.1 deste estudo.

Também com base na Figura 10 verifica-se co-ocorrência entre as palavras-chaves '*cyber crime'* e '*money laundering'*, ou lavagem de dinheiro. A vinculação entre essas duas palavras-chaves está em sintonia com o discurso de Tropina (2014) ao citar, na Seção 2.2, que a lavagem de dinheiro é um problema que pode ser relacionado aos crimes cibernéticos e ao sistema financeiro e bancário.

4.6. Categorização dos artigos segundo à abordagem metodológica empregada

A Figura 11 apresenta a categorização dos artigos quanto à metodologia empregada. Esta categorização foi baseada no estudo de Silva, Kimura e Sobreiro (2017) e está de acordo com o Quadro 5. A maioria dos artigos analisados possui abordagem qualitativa, com 44 artigos (61,11% do total da amostra). Em seguida, segue-se que 16 artigos são quantitativos (22,22% do total da amostra). Por fim, 12 artigos possuem abordagem quantitativa e qualitativa simultaneamente (16,67% do total da amostra).

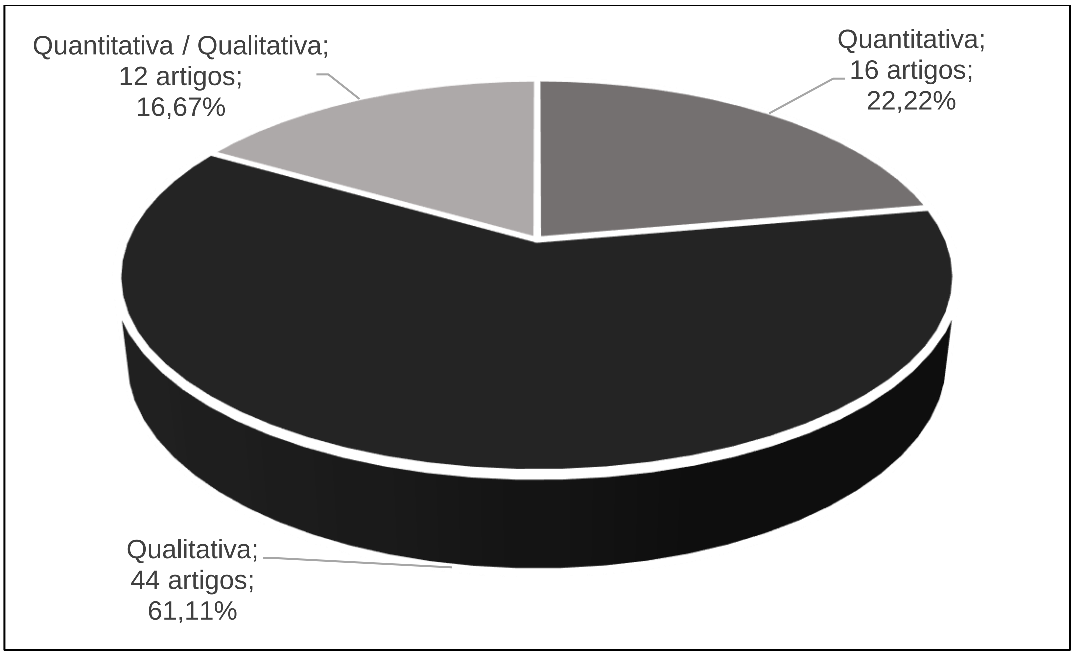

FIGURA 11 – Quantidade de artigos quanto à metodogolia empregada
Fonte: Dados da pesquisa

4.7. Classificação dos artigos de acordo com a ótica

A Figura 12 apresenta a classificação dos artigos de acordo com a ótica empregada. Para esta classificação foram adotadas as três óticas referentes à conscientização situacional em segurança cibernética propostas por Evesti, Kanstrén e Frantti (2017), apresentadas no Quadro 3 da Seção 2.1 deste estudo, sendo elas: ‘Negócios’, ‘Legal’ e ‘Técnico’.

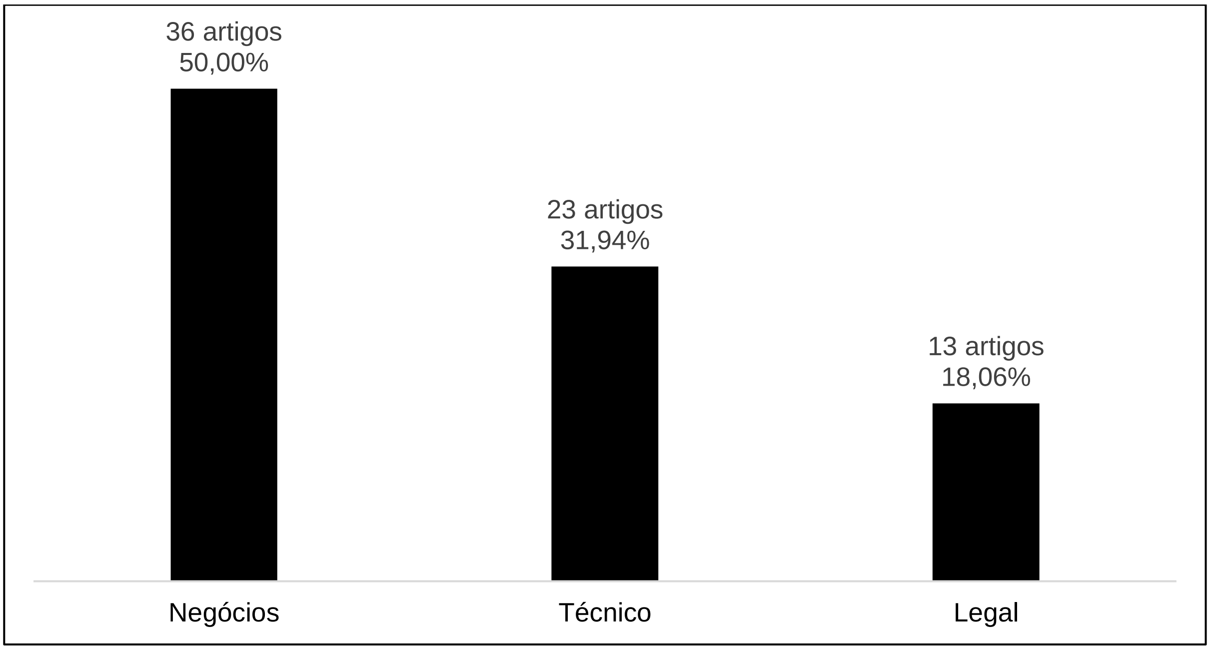

FIGURA 12 – Classificação dos artigos de acordo com a ótica
Fonte: Dados da pesquisa.

A ótica de ‘Negócios’ foi predominante, com 36 artigos, representando 50,00% da amostra. A ótica ‘Técnico’ apresentou 23 artigos, com representividade de 31,94% do total de artigos da amostra. A ótica ‘Legal’, por sua vez, apresentou 13 artigos, que representa 18,06% da amostra, sendo a ótica com menor predominância entre os artigos da amostra. Os resultados, com predominância da ótica de 'Negócios', estão em harmonia com o fato de os artigos terem sido coletados em bases de dados da área da Administração.

Evesti, Kanstrén e Frantti (2017) não definem se alguma das óticas tem maior importância para as organizações ou se todas são igualmente importantes. No entanto, os resultados deste estudo evidenciam que as pesquisas científicas estão mais direcionadas para a ótica de ’Negócio’, que aborda aspectos relacionados aos requisitos e preferências dos clientes e ameaças específicas do domínio comercial, conforme Quadro 3.

5. CONCLUSÕES E RECOMENDAÇÕES

Este capítulo apresenta as conclusões e recomendações do presente estudo, cujo objetivo geral foi investigar a produção internacional de artigos científicos sobre o tema ‘segurança cibernética no setor bancário’ constante em bases de dados da área de Administração. De modo a alcançar este objetivo, foi realzada uma pesquisa descritiva com abordagem qualitativa e quantitativa. A amostra foi composta de 72 artigos científicos extraídos de quatro bases de dados indexadas pelo Portal de Periódicos da CAPES, sendo elas: EBSCOhost, ProQuest, Scopus – Elsevier e WoS. Com base nos resultados encontrados a partir de análises descritivas e bibliométricas, que são sustentados pelo referencial teórico, foi possível atender ao objetivo geral e aos objetivos específicos descritos na Seção 1.4 do estudo.

O primeiro objetivo específico foi verificar a quantidade de artigos por ano de publicação. Este objetivo foi atendido na Seção 4.1 e o resultado foi representado pela Figura 6. Observou-se que não houve publicação de artigos nos anos 2005, 2006, 2007, 2009 e 2010. Os anos de 2017, 2018, 2019 e 2020 somam 73,61% de publicações do total da amostra, sendo que o ano de 2019 possui 29,17% de publicações no total. Cabe destaque ao ano de 2020, com 7 publicações, representando 9,72% da amostra, pois, apesar da coleta de dados contemplar artigos publicados somente até o mês de junho do referido ano, apresentou maior quantidade de artigos individualmente se comparado com os anos que contemplam o período entre 2004 e 2016.

O segundo objetivo específico foi mensurar a quantidade de artigos publicados por periódico, tendo sido atingido na Seção 4.2 e representado pela Tabela 1. Os 72 artigos da amostra foram publicados em 56 periódicos diferentes, sendo que o *Journal of Internet Banking and Commerce* foi o mais significativo, com 5 artigos publicados, representando 6,94% do total da amostra. O períodico *Journal of Money Laundering Control* também teve destaque, com 4 artigos publicados, representando 5,56% do total da amostra. Três periódicos tiveram 3 artigos publicados cada, totalizando 9 artigos (12,50% da amostra) e outros três periódicos aparecem com 2 publicações cada, totalizando 6 artigos (8,33% do total da amostra). Os demais 48 períodicos tiveram somente uma publicação cada, representando 66,67% do total da amostra.

O terceiro objetivo específico foi classificar os artigos conforme a quantidade de autores. Tal objetivo foi atingido na Seção 4.3 e representado pela Figura 7. Do total de artigos, 22 foram publicados por 2 autores (30% do total da amostra), 20 foram publicados por 1 autor (28% do total da amostra), 17 foram publicados por 3 autores (24% do total da amostra) e 7 foram publicados por 4 autores (10% do total da amostra) A menor parte dos artigos foi publicada por 5 ou mais autores (8% do total da amostra).

O quarto objetivo específico foi analisar os artigos conforme as relações de coautoria. Este objetivo foi atingido na Seção 4.3 e representado pela Figura 8. Verificou-se que há variedade de autores na amostra e a maior parte deles divide a autoria de apenas um artigo. Dos autores, Rutger Leukfeldt divide a autoria de 4 artigos com Edward R. Kleemans e de 3 artigos com Wouter P. Stol, tendo, todos eles, a filiação acadêmica em instituição localizada na Holanda.

O quinto objetivo específico foi verificar a quantidade de artigos segundo a filiação acadêmica dos autores. Este objetivo foi atingido na Seção 4.4 e representado pela Tabela 2. Das 107 instituições identificadas, 44 estão localizadas no continente europeu, representando 41,12% do total. Cabe destacar que as três instituições com maior número de aparições estão localizadas na Holanda, representando o continente europeu, sendo elas: *Vrije Universiteit Amsterdam*, *Netherlands Institute for the Study of Crime and Law Enforcement* e *Open University of the Netherlands*. Em contrapartida, somente 12 instituições estão localizadas nas Américas, representando 11,21% do total da amostra. Destaca-se que, na região das Américas, apenas uma instituição está localizada no Brasil.

O sexto objetivo específico foi analisar a distribuição e co-ocorrência de palavras-chaves dos artigos. Este objetivo foi atingido na Seção 4.5. A distribuição de palavras-chaves foi representada pela Figura 9 e o mapa de co-ocorrências foi representado pela Figura 10. Em relação à distribuição, destaca-se as palavras-chaves ‘*cyber crime’*, com 29 repetições, ‘*cyber security’*, com 14 repetições e ‘*phishing’*, com 13 repetições. Já em relação à análise de co-ocorrências, destacam-se os pares de palavras-chaves ‘*cyber crime*’ e ‘*phishing*’, ‘*cyber crime*’ e ‘*money laundering*’, ‘*cyber crime*’ e ‘*security*’, ‘*security*’ e ‘*phishing*’ e o par ‘*cyber security*’ e ‘*cyber risk*’.

O sétimo objetivo específico foi categorizar os artigos segundo à abordagem metodológica empregada. Este objetivo foi atingido na Seção 4.6 e foi representado pela Figura 11. A maioria dos artigos possui abordagem qualitativa, sendo 44 artigos representativos de 61,11% do total da amostra. Com abordagem quantitativa, 16 artigos foram categorizados, representando 22,22% do total da amostra. 12 artigos foram categorizados como sendo de abordagem quantitativa e qualitativa, representando 16,67% do total da amostra.

Por fim, o oitavo objetivo específico foi classificar os artigos de acordo com a ótica de ‘Negócios’, ‘Legal’ ou ‘Técnica’. Este objetivo foi atingido na Seção 4.7 e representado pela Figura 12. 36 artigos foram classificados na ótica de ‘Negócios’, representando 50% do total da amostra; 23 artigos foram classificados na ótica ‘Técnico’, representando 31,94% do total da amostra; e 13 artigos foram classificados na ótica ‘Legal’, representando 18,06% do total da amostra.

Com o atingimento de todos os objetivos específicos, foi possível atingir, como consequência, o objetivo geral, descrito na Seção 1.3. Por meio deste estudo, verificou-se que a distribuição da produção científtifica sobre o tema ‘segurança cibernética no setor bancário’ não foi uniforme ao longo dos anos. Verificou-se, também, que o periódico *Journal of Internet Banking and Commerce* teve 5 publicações de artigos. Destacou-se que 30% dos artigos foi escrito por 2 autores, sendo que há uma variedade de autores que dividem a autoria de apenas um artigo. Verificou-se, ainda, que a Europa apresentou 41,12% das publicações totais, sendo que a *Vrije Universiteit Amsterdam*, localizada na Holanda, teve 4 publicações. Sobre as palavras-chaves, predominou a aparição de ‘*cyber crime’*, que teve co-ocorrência, entre outras, com as palavras-chaves ‘*phishing’*, ‘*money laundering’* e ‘*security*’. A abordagem e a ótica predominantes foram, respectivamente, qualitativa e de ‘Negócios’.

As contribuições deste estudo no campo teórico permitem entender como tem se dada a produção de artigos científicos sobre o tema, evidenciando as características gerais dos estudos analisados, como a frequência de publicações durantes os anos, os periódicos mais relevantes, as abordagens metodológicas mais utilizadas pelos autores, as regiões onde os estudos estão mais concentrados, entre outros. Já como contribuição prática, a investigação da produção de artigos científicos sobre o tema deste trabalho mostrou-se relevante ao apresentar resultados que podem ser replicáveis em pesquisas futuras ou mesmo servir como comparação com estudos semelhantes.

Como recomendação para pesquisas futuras, sugere-se: (i) realizar novos estudos bibliométricos sobre o tema em períodos diferentes, com a finalidade de comparar resultados; (ii) realizar novos estudos considerando uma maior quantidade de bases de dados como população; (iii) realizar estudos que relacionem a segurança cibernética no setor bancário com crimes cibernéticos e a lavagem de dinheiro, pois foram dois temas que tiveram destaque na análise de palavras-chaves deste estudo, sinalizando que são preocupações importantes para o setor financeiro e bancário; (iv) realizar estudos sobre o tema ‘segurança cibernética no setor bancário’ que contemple a avaliação dos autores, a partir do Índice H, e dos periódicos, de acordo com seu Fator de Impacto, conforme citado na Seção 2.3; (v) realizar pesquisas sobre segurança cibernética no setor bancário brasileiro; (vi) realização de estudos com base nos resultado obtidos considerando análise de grafos e redes; (vii) realização estudos que identifiquem aspectos de segurança cibernética contidos nos artigos baseando-se na norma ISO/IEC 27032:2012 (ISO/IEC, 2012)

REFERÊNCIAS

ABEND, V. *Et al*. Cyber security for the banking and finance sector. *In*: VOELLER, J. **Wiley Handbook of Science and Technology for Homeland Security**. 1. Ed. Nova Iorque: John Wiley & Sons Inc, 2008.

AFONSO, M. H. F. *et al*. Como construir conhecimento sobre o tema de pesquisa? Aplicação do processo Proknow-c na busca de literatura sobre avaliação do desenvolvimento sustentável. **Revista de Gestão Social e Ambiental – RGSA**, São Paulo, v. 5, n. 2, p. 47–62, maio/ago. 2011. DOI: 10.5773/rgsa.v5i2.424. Disponível em: https://rgsa.emnuvens.com.br/rgsa/article/view/424/pdf_13. Acesso em: 02 jun. 2020.

AGRAFIOTIS, I. *Et al*. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. **Journal of Cybersecurity**, *[s. l]*, v. 4, n. 1, p. 1-15, out. 2018. DOI: https://doi.org/10.1093/cybsec/tyy006. Disponível em: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288. Acesso em: 3 maio 2020.

BAGHERI, S; RIDLEY, G. Organizational Cyber Resilience: research opportunities. *In*: AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS, 28., 2017, Hobart, Australia. **ACIS 2017 Proceedings**. Hobart: University of Tasmania, 2017.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 1977. ISBN: 972-44-0898-1.

BCB. Banco Central do Brasil, [2020?]. **Recomendações de Basileia. Disponível** em: https://www.bcb.gov.br/estabilidadefinanceira/recomendacoes basileia. Acesso em: 14 abr. 2020.

BCB. Banco Central do Brasil. Diretoria Colegiada. Circular nº 3.909, de 16 de agosto de 2018. 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 de pagamento autorizadas a funcionar pelo Banco Central do Brasil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 22, 20 ago. 2018.

BCB. Banco Central do Brasil. Diretoria Colegiada. Circular nº 3.979, de 30 de janeiro de 2020. Dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil de informações relativas a eventos de risco operacional. **Diário Oficial da União**: seção 1, Brasília, DF, p. 90-91, 31 jan. 2020.

BCBS. Basel Committee on Banking Supervision. 2003. **Sound Practices for the Management and Supervision of Operational Risk**. Disponível em: https://www.bis.org/publ/bcbs183.pdf. Acesso em: 27 maio 2020.

BIENER, C.; ELING, M.; WIRFS, J. H. Insurability of Cyber Rick: an empirical analysis. **Geneva Papers on Risk and Insurance: Issues and Practice**, Basingstoke, Inglaterra, v. 40. N. 1, p. 131-158, jan. 2015. Disponível em:

https://www.alexandria.unisg.ch/238242/1/Insurability%20of%20Cyber%20Risk%20An%20Empirical%20Analysis.pdf. Acesso em: 28 abr. 2020.

BIS. Bank for International Settlements**.** 2015. **Committee on Payments and Market Infrastructures (CPMI) – overview**. Disponível em: https://www.bis.org/cpmi/. Acesso em: 14 maio 2020.

BIS. Bank for International Settlements. 2020ª. **Committees & associations**. Disponível em: https://www.bis.org/bcbs/mesc.htm?m=3%7C14% 7C573%7C74. Acesso em: 28 mar. 2020.

BIS. Bank for International Settlements. 2020b. **About BIS – overview**. Disponível em: https://www.bis.org/about/index.htm. Acesso em: 14 maio 2020.

BIS. Bank for International Settlements. 2020c. **About BIS – overview**. Disponível em: https://www.bis.org/fsi/index.htm. Acesso em: 08 jun. 2020.

BIS. Bank for International Settlements. Cyber-security and operational resilience. *In*: INTERNATIONAL CONFERENCE OF BANKING SUPERVISORS, 20., nov. 2018, Abu Dhabi, United Arab Emirates. **Workshop 6 [...]**. Abu Dhabi: BCBS, 2018.

BIS. Bank for International Settlements. Operational and cyber risks in the financial sector. **BIS Working Papers**, *[s. l.]*, n. 840, fev. 2020d. Disponível em: https://www.bis.org/publ/work840.pdf. Acesso em: 14 maio 2020.

BJORCK, F. *et al*. Cyber Resilience – Fundamentals for a Definition. *In*: ROCHA, A. *Et al*. **New Contributions in Information Systems and Technologies**, 1. Ed. *[s. l]*: Springer-AISC, 2015.

BURGER, Erick W. *Et al*. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. *In*: 2014 ACM WORKSHOP ON INFORMATION SHARING & COLLABORATIVE SECURITY, 1., 2014, Nova Iorque. **WISCS '14: Proceedings [...]**. Nova Iorque: Association for Computing Machinery, 2014. P. 51-60.

CAMILLO, Mark. Cybersecurity: Risks and management of risks for global banks and financial institutions. **Journal of Risk Management in Financial Institutions**, *[s. l]*, v. 10, n. 2, p. 196-200, dez. 2017. Disponível em: https://www-409.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf. Acesso em: 3 maio 2020.

CANONGIA, C; MANDARINO, R. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, dez. 2009. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/view/349. Acesso em: 25 fev. 2020.

CAPES. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. **Portal de Periódicos CAPES/MEC**. 2020. Disponível em: http://www.periodicos.capes.gov.br/. Acesso em: 03 jun. 2020.

CARLSSON-SZLEZAK, P.; REEVES, M.; SWARTZ, P. What Coronavirus Could Mean for the Global Economy. **Harvard Business Review**, p. 01-10, March, 2020. Disponível em: https://hbr.org/2020/03/what-coronavirus-could-mean-for-the-global-economy. Acesso em: 24 maio 2020.

CARVALHO, M. M. *Et al*. An overview of the literature on technology roadmapping (TRM): Contributions and trends. **Technological Forecasting and Social Change**, *[s. l]*, v. 80, n. 7, set. 2013. DOI: https://doi.org/10.1016/j.techfore.2012.11.008.

CATOTA, F. *et al*. Cybersecurity 61nterdisc response capabilities in the Ecuadorian financial sector. **Journal of Cybersecurity**, *[s. l]*, v. 4, n. 1, abr. 2018. DOI: https://doi.org/10.1093/cybsec/tyy002. Disponível em: https://academic.oup.com/cybersecurity/article/4/1/tyy002/4990518. Acesso em: 14 maio 2020.

CEBULA, J. J.; YOUNG, L. R. Software Engineering Institute. Technical Note CMU/SEI-2010-TN-028. **A Taxonomy of Operational Cyber Security Risks**, Pittsburgh, 2010. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a537111.pdf. Acesso em: 02 maio 2020.

CMN. Conselho Monetário Nacional. Resolução Nº 4.568, de 26 de abril de 2018. 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 financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.. **Diário Oficial da União**: seção 1, Brasília, DF, p. 26-28, 30 abr. 2018.

CMU. Carnegie Mellon University: Software Engineering Institute, nov. 2016. **Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response**. Disponível em: https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html. Acesso em: 27 maio 2020.

COJOCARU, Irina; COJOCARU, Igor. A bibliometric analysis of cybersecurity research papers in Eastern Europe: case study from the Republic of Moldova. *In*: CENTRAL AND EASTERN EUROPEAN EDEM AND EGOV DAYS, 2019, Budapeste, Hungria**. A bibliometric analysis [...]**. Viena, Austria: Facultas Verlags- und Buchhandels, 2019, p. 151-162.

CRAIGEN, D; DIAKUN-THIBAULT, N; PURSE, R. Defining Cybersecurity. **Technology Innovation Management Review**, Ottawa, v. 4, n. 10, p. 13-22, out. 2014. Disponível em: https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_October2014.pdf. Acesso em: 15 abr. 2020.

CRISANTO, J. C; PRENIO, J. Financial crime in times of Covid-19 – AML and cyber resilience measures. **FSI Briefs**, [*s. l.*], n. 7, maio 2020. Disponível em: https://www.bis.org/fsi/fsibriefs7.pdf. Acesso em: 08 jun. 2020.

DFS. New York Department of Financial Services. **Cybersecurity Requirements for Financial Services Companies**. 2017. Disponível em:

http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf. Acesso em: 14 maio 2020.

DHS. Department of Homeland Security. 2020. **About DHS**. Disponível em: https://www.dhs.gov/about-dhs. Acesso em: 27 maio 2020.

DHS. Department of Homeland Security. **National Infrastructure Protection Plan 2009**: Partnering to Enhance Protection and Resiliency. 2009. Disponível em: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf. Acesso em: 22 abr. 2020.

ECB. European Central Bank. **G7 Fundamental Elements of Cybersecurity for the Financial Sector**. 2016. Disponível em: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf. Acesso em: 14 maio 2020.

ELNAGDY, S. A. *Et al*. Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing. *In*: INTERNATIONAL CONFERENCE ON CYBER SECURITY AND CLOUD COMPUTING, 2016, Beijing, China. **Proceedings [...]**. Beijing, IEEE, 2016. P. 295-300.

ESTAY, D. A. S. et. al. A systematic review of cyber-resilience assessment frameworks. **Computers & Security,** *[s. l.],* v. 97, out. 2020.

ESWARAN, R; VINAYAGAMOORTHI, G. Cyber Security and Information Security. **International Journal of Recent Technology and Engineering**, Bhopal, Índia, v. 8, n.3, edição especial, p. 372-374, out. 2019. Disponível em: https://www.ijrte.org/download/volume-8-issue-3S/. Acesso em: 25 fev. 2020.

EVESTI, A.; KANSTRÉN, T.; FRANTTI, T. Cybersecurity Situational Awareness Taxonomy. *In*: INTERNATIONAL CONFERENCE ON CYBER SITUATIONAL AWARENESS, DATA ANALYTICS AND ASSESSME, 3., 2017, Londres. **Proceedings [...]**. Londres: IEEE, 2017. P. 1-8.

FONSECA, P. V; JUCÁ, M. N. The Influence of Taxes on Foreign Direct Investment: Systematic Literature Review and Bibliometric Analysis. **European Research Studies Journal**, *[s. i.]*, v. 23, n. 2, p. 55-77, abr. 2020.

FSB. Financial Stability Board. **Cyber Lexicon**. 2018. Disponível em: https://www.fsb.org/2018/11/cyber-lexicon/. Acesso em: 14 maio 2020.

FSB. Financial Stability Board. **Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices**. 2017. Disponível em: https://www.fsb.org/wp-content/uploads/P131017-2.pdf. Acesso em: 15 maio 2020.

GOOGLE. **Google Trends**, 2020. Disponível em: https://trends.google.com.br/trends/?geo=BR. Acesso em: 22 maio 2020.

GORDON, S; FORD, R. On the definition and classification of cybercrime. **Journal in Computer Virology**, *[s. l.]*, v. 2, p. 13-20, jul. 2006. DOI:

https://doi.org/10.1007/s11416-006-0015-z. Disponível em: https://link.springer.com/article/10.1007/s11416-006-0015-z. Acesso em: 2 maio 2020.

GUAMAN, A. M. *Et al*. Systematic Review: Cybersecurity Risk Taxonom. *In*: INTERNATIONAL CONFERENCE ON SOFTWARE PROCESS IMPROVEMENT, 6., 2017, Zacatecas, Mexico. **Proceedings [...]**. Zacatecas: AISC, 2017. P. 137-146.

GUEDES, V. L. S.; BORSCHIVER, S. Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *In*: Encontro Nacional de Ensino e Pesquisa em Informação, 2005, Salvador, Bahia. **Anais [...]**. Salvador: Universidade Federal da Bahia, 2005. Disponível em: http://www.cinform-anteriores.ufba.br/vi_anais/docs/VaniaLSGuedes.pdf. Acesso em: 20 maio 2020.

HONG, J. The state of phishing attacks. **Communications of the ACM**, *[s. l.],* v. 50, n.1, jan. 2012. DOI: https://doi.org/10.1145/2063176.2063197.

IAIS. International Association of Insurance Supervisors**.** 2020. **Welcome to the website of the International Association of Insurance Supervisors (IAIS)**. Disponível em: https://www.iaisweb.org/home. Acesso em: 15 maio 2020.

IBRAHIM, S. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. **International Journal of Law, Crime and Justice**, *[s. l.]*, v. 47, p. 44-57, dez. 2016. DOI: https://doi.org/10.1016/j.ijlcj.2016.07.002. Disponível em: https://www.sciencedirect.com/science/article/pii/S1756061616300787?via%3Dihub. Acesso em: 03 maio 2020.

IOSCO. International Organization of Securities Commissions. 2020. **About IOSCO**. Disponível em: https://www.iosco.org/about/?subsection=about_iosco. Acesso em: 15 maio 2020.

ISO/IEC. The International Organization for Standardization / The International Electrotechnical Commission. **ISO/IEC 27002:2013:** Information technology — Security techniques — Code of practice for information security controls. [*s. l.*]: ISO/IEC, 2013.

ISO/IEC. The International Organization for Standardization / The International Electrotechnical Commission. **ISO/IEC 27032:2012:** Information technology — Security techniques — Guidelines for cybersecurity. [*s. l.*]: ISO/IEC, 2012.

ITU. International Telecommunication Union, 2018. **Global Cybersecurity Index (GCI)**. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Acesso em: 25 out. 2020.

KLAPER, D; HOVY, E. A Taxonomy and a Knowledge Portal for Cybersecurit. *In*: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 15., 2014, Nova Iorque. **Proceedings [...]**. Nova Iorque: Association for Computing Machinery, 2014. P. 79-85.

LEI, Yongdeng *et al*. Rethinking the relationships of vulnerability, resilience, and adaptation from a disaster risk perspective. **Natural Hazards**, *[s. l.]*, v. 70, p. 609-627, set. 2013. DOI: https://doi.org/10.1007/s11069-013-0831-7. Disponível em: https://link.springer.com/article/10.1007/s11069-013-0831-7. Acesso em: 2 maio 2020.

MACHADO JUNIOR, C. *Et al*. As Leis da Bibliometria em Diferentes Bases de Dados Científicos. **Revista de Ciências da Administração**, Florianópolis, v. 18, n. 44, p. 111-123, abr. 2016. DOI: https://doi.org/10.5007/2175-8077.2016v18n44p111. Disponível em: https://periodicos.ufsc.br/index.php/adm/article/view/2175-8077.2016 v18n44p111. Acesso em: 17 maio 2020.

MACIAS-CHAPULA, Cesar A. O papel da informetria e da cienciometria e sua perspectiva nacional e internacional. **Ciência da Informação**. Brasília, v. 27, n. 2, maio/ago. 1998. Disponível em <http://www.scielo.br/scielo.php?script=sci_ arttext&pid=S0100-19651998000200005&lng=en&nrm=iso>. Acesso em: 20 maio 2020.

MAKAWANA, P. R; JHAVERI, R. H. A Bibliometric Analysis of Recent Research on Machine Learning for Cyber Security. **Intelligent Communication and Computational Technologies**, Singapura, v. 19, p. 213-226, out. 2017. DOI: https://doi.org/10.1007/978-981-10-5523-2_20. Disponível em: https://link.springer. com/chapter/10.1007/978-981-10-5523-2_20. Acesso em: 22 maio 2020.

MIRANDA, A. N.; ALVES, C. A. M. Análise do nível de divulgação do risco operacional: estudo em bancos com carteira comercial com base na regulamentação brasileira. **Revista de Administração e Contabilidade da Unisinos**, Brasília, v. 16, n. 3, jul/set. 2019. DOI: 10.4013/base.2019.163.01. Disponível em: http://revistas.unisinos.br/ index.php/base/article/view/base.2019.163.01/60747339. Acesso em: 27 maio 2020.

MITNICK, K. D; SIMON, W. L. **The art of deception: controlling the human 64nterdis of security**. 1. Ed., Nova Jersey: John Wiley & Sons, 2003. ISBN: 978-0764542800.

MUELLER, S. P. M. Estudos métricos da informação em ciência e tecnologia no Brasil realizados sobre a unidade de análise artigos de periódicos. **Liinc em Revista**, Rio de Janeiro, v. 9, n. 1, p. 6-27, maio 2013. DOI: https://doi.org/10.18617/liinc.v9i1.558. Disponível em: http://revista.ibict.br/liinc/article/view/3429/2999. Acesso em: 21 maio 2020.

OTTIS, R; LORENTS, P. Cyberspace: Definition and Implications. *In*: PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 5., 2010, Ohio, EUA. **Proceedings [...].** Ohio: Academic Conferences International Limited, 2010. P. 267-270.

PRITCHARD, A. Statistical bibliography or bibliometrics? **Journal of Documentation**, Londres, v. 25, n. 4, p. 348-349, dez. 1969.

PUSCHMANN, T. Fintech. **Business & Information Systems Engineering**, *[s. l.]*, v. 59, n. 1, p. 69-76, fev. 2017. DOI: https://doi.org/10.1007/s12599-017-0464-6.

Disponível em: https://link.springer.com/article/10.1007/s12599-017-0464-6. Acesso em: 13 maio 2020.

ROMANI-DIAS, M. **Negócios sociais: estudo bibliométrico e análise sistemática da literatura nacional e internacional**. Tese (Programa de Pós-Graduação de Mestrado e Doutorado em Administração) – Centro Universitário FEI, São Paulo, 2016. DOI: https://doi.org/10.31414/ADM.2016.D.127991. Disponível em: https://repositorio. Fei.edu.br/bitstream/FEI/163/1/fulltext.pdf. Acesso em: 17 maio 2020.

ROSSI, M; ALVES, C. A. M. Crowdfunding: uma análise da produção científica em bases de dados de 2013 a 2017. **Revista Brasileira de Gestão e Inovação**, Brasília, v. 7, n. 3, p. 83-99, maio/ago. 2020. DOI: 10.18226/23190639.v7n3.04. Disponível em: http://ucs.br/etc/revistas/index.php/RBGI/article/view/6809/pdf. Acesso em: 05 jun. 2020.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B. **Metodologia de Pesquisa**. 5. Ed., Porto Alegre: Penso, 2013. ISBN: 978-85-65848-36-7.

SCHATZ, D; BASHROUSH, R; WALL, J. Towards a More Representative Definition of Cyber Security. **Journal of Digital Forensics, Security and Law**, Florida, v. 12, n. 2, artigo 9, jun. 2017. DOI: https://doi.org/10.15394/jdfsl.2017.1476. Disponível em: https://commons.erau.edu/jdfsl/vol12/iss2/8/. Acesso em: 05 abr. 2020.

SILVA, W; KIMURA, H; SOBREIRO, V. A. An analysis of the literature on systemic financial risk: a survey. **Journal of Financial Stability**, *[s. l]*, v. 28, p. 91-114, fev. 2017.

SOLMS, R. V; NIEKERK, J. V. From information security to cyber security. **Computers & Security**, *[s. l.]*, v. 38, p. 97-102, out. 2013. DOI: https://doi.org/10.1016/j.cose.2013.04.004. Disponível em: https://www.sciencedirect. com/65nterdi/article/pii/S0167404813000801. Acesso em: 3 maio 2020.

STROZZI, F. *et al*. Literature review on the “Smart Factory” concept using bibliometric tools. **International Journal of Production Research**, *[s. l.]*, v. 55, n. 22, maio 2017. DOI: https://doi.org/10.1080/00207543.2017.1326643.

TARGINO, Maria das Graças. **Comunicação científica: o artigo de periódico nas atividades de ensino e pesquisa do docente universitário brasileiro na pós-graduação**. 1998. Tese (Doutorado em Ciência da Informação) – Curso de Pós-Graduação em Ciência da Informação, Universidade de Brasília, Brasília, 1998.

TROPINA, T. Fighting 65nter laundering in the age of online banking, virtual currencies and internet gambling. **ERA Forum**, *[s. l.]*, v. 15, p. 69-84, fev. 2014. DOI: https://doi.org/10.1007/s12027-014-0335-2.

VANTI, N. A. P. Da bibliometria à webometria: uma exploração conceitual dos mecanismos utilizados para medir o registro da informação e a difusão do conhecimento. **Ciência da Informação**, Brasília , v. 31, n. 2, p. 369-379, ago. 2002. DOI: https://doi.org/10.1590/S0100-19652002000200016. Disponível em: http://www.

Scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652002000200016&lng=en&nrm=iso. Acesso em: 17 maio 2020.

WHITE, H. D.; WELLMAN, B.; NAZER, N. Does citation reflect social structure?: Longitudinal evidence from the “Globenet” 66nterdisciplinar research group. **Journal of the American Society for Information Science and Technology**, *[s. l]*, v. 55, n. 2, p. 111-126, nov. 2003.

WHO. World Health Organization. **Who caracterizes COVID-19 as a pandemic**. 2020. Disponível em: <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen>. Acesso em: 10 maio 2020.

APÊNDICES

APÊNDICE A – Relação dos artigos coletados

Nr	Título	Autor(es)	Periódico	ISSN	Ano
1	Cyber Crime Influencing Businesses in South Africa	1-Marlien Herselman / 2-Matt Warren	Issues in Informing Science & Information Technology	1547-5840	2004
2	’Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas:1 a critical analysis of the United Kingdom’s legislative provisions and policies to tackle online fraud	1-Ana Carolina Blanco Hache / 2-Nicholas Ryder	Information & Communications Technology Law	1360-0834	2011
3	Multilevel authentication system for stemming crime in online banking	1-Boniface Kayode Alese / 2-Aderonke F. Thompson / 3-Olufunso D. Alowolodu / 4-Blessing Oladele	Interdisciplinary Journal of Information, Knowledge & Management	1555-1229	2018
4	Banking malware and the laundering of its profits	1-Bart HM Custers / 2-Ronald LD Pool / 3-Remon Cornelisse	European Journal of Criminology	1477-3708	2019
5	A formally verified digital signature device for smartphones	Peter Trommler	International Journal on Computer Science and Information Systems (JADIS)	1646-3692	2015
6	Online Banking Operating Pattern and Risk of Cyber Fraud - Findings from Empirical Research	1-Heena Thanki / 2-Shankrrao Junare	Pacific Business Review International	0974-438X	2019
7	An Explorative Study of Satisfaction Level of Cyber-crime Victims with Respect to E-services of Banks	1-Atul Bamrara / 2-Gajendra Singh / 3-Mamta Bhatt	Journal of Internet Banking and Commerce	1204-5357	2012
8	Varying Impacts of Electronic Banking on the Banking Industry	Sali Bakare	Journal of Internet Banking and Commerce	1204-5357	2015
9	Cyber crimes: a threat to the banking industry	Padmaavathy PA	International Journal of Management Research and Reviews	2249-7196	2019
10	Cyber crimes-a constant threat for the business sectors and its growth (a study of the online banking sectors in gcc)	Liaqat Ali	The Journal of Developing Areas	0022-037X	2019
11	Discerning Novel Value Chains in Financial Malware	1-R. S. van Wegberg / 2-A. J. Klievink / 3-M. J. G. van Eeten	European Journal on Criminal Policy and Research	0928-1371	2017
12	ATM Security: A case study of Emerging Threats	1-Ella Nsonta Kasanda / 2-Jackson Phiri	International Journal of Advanced Studies in Computers, Science and Engineering	2278 7917	2018

continua

continuação

Nr	Título	Autor(es)	Periódico	ISSN	Ano
13	Fishing as a cybercrime in the internet banking system: Economic and legal aspects	1-Oleksandr Ilchenko / 2-Volodymyr Chumak / 3-Serhii Kuzmenko / 4-Oleksandr Shelukhin / 5-Artem Dobrovinskyi	Journal of Legal, Ethical and Regulatory Issues	1544-0036	2019
14	Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime	1-E. Rutger Leukfeldt / 2-Anita Lavorgna / 3-Edward R. Kleemans	European Journal on Criminal Policy and Research	0928-1371	2017
15	A soft computing approach to detect e-banking phishing websites using artificial neural network	1-Shafi'i Muhammad Abdulhamid / 2-Mubaraq Olamide Usman / 3-Oluwaseun A. Ojerinde / 4-Victor Ndako Adama / 5-John K. Alhassan	i-Manager's Journal on Computer Science	2347-2227	2018
16	Internet banking: identity theft and solutions - the nigerian perspective	1-Deborah Uzoamaka Ebem / 2-Joseph Chinonye Onyeagba / 3-Geraldine Egondu Ugwuonah	Journal of Internet Banking and Commerce	1204-5357	2017
17	Compliance landscape in central and eastern europe – the case of hungary	1-Levente Kovács / 2-Sandor David	Journal of Money Laundering Control	1368-5201	2017
18	Evaluation and analysis of cyber attacks in nigeria	1-Adejoro Cornelius Onimisi / 2- Ogwueleka Francisca Nonyelum	IUP Journal of Information Technology	0973-2896	2018
19	Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis	1-E. Rutger Leukfeldt / 2-Edward R. Kleemans / 3-Wouter P. Stol	Crime, Law & Social Change	0925-4994	2017
20	A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists	1-E. Rutger Leukfeldt / 2-& Edward R. Kleemans / 3-Wouter P. Stol	Crime, Law & Social Change	0925-4994	2017
21	Capacity building in cyber security to make India secure to go cashless	1-I. Chitra / 2-Sumangala Devi	International Journal of Recent Technology and Engineering	2277-3878	2019
22	The innovative approach to increasing cybersecurity of transactions through counteraction to money laundering	1-Serhiy Lyeonov / 2-Olha Kuzmenko / 3-Hanna Yarovenko / 4-Tatiana Dotsenko	Marketing and Management of Innovations	2227-6718	2019
23	Data security and consumer trust in FinTech innovation in Germany	1-Harrison Stewart / 2-Jan Jürjens	Information and Computer Security	2056-4961	2018
24	Electronic finance – recent developments	Krishnan Dandapani	Managerial Finance	0307-4358	2017
25	Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe	Shewangu Dzomira	Risk Governance and Control: Financial Markets and Institutions	2077-429X	2014

continua

continuação

Nr	Título	Autor(es)	Periódico	ISSN	Ano
26	An introduction to quantum computers and their effect on banking institutions	Tae L. Aderman	International Journal of Financial Research	1923-4023	2019
27	Big Data and Service Operations	Maxime C. Cohen	Production and Operations Management	1059-1478	2018
28	Phishing in an academic community: A study of user susceptibility and behavior	1-Alejandra Diaz, / 2-Alan T. Sherman / 3-Anupam Joshi	Cryptologia	0161-1194	2019
29	Legal regulation of digital banking in russia and foreign countries (european union, usa, prc)	1-E. P. Ermakova / 2-E. E. Frolova	Vestnik Permskogo Universiteta - Juridicheskie Nauki	1995-4190	2019
30	Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance	1-Marco Alexandre Terlizzi / 2-Fernando de Souza Meirelles / 3-Maria Alexandra Viegas Cortez da Cunha	Journal of Applied Security Research	1936-1610	2017
31	Piercing the veil of national security: Does China’s banking it security regulation violate the TBT agreement?	Nan-xiang Sun	Asian Journal of WTO and International Health Law and Policy	1819-5164	2016
32	Methods of laundering money resulted from cyber-crime	1-Mircea Constantin Scheau / 2-Stefan Pop Zaharie	Economic Computation and Economic Cybernetics Studies and Research	0424-267X	2017
33	Digital financial services: Role of cyber security for digital india	1-K. S. Deeparani / 2-B. Jeya Prabha	International Journal of Mechanical and Production Engineering Research and Development	2249-6890	2018
34	Revolution of Technological Innovation in Indian Banking Sector: Problems and Prospects	Bhakti Ranjit Pawar	International Journal of Economic Research	0972-9380	2017
35	Botnet Detection on the Analysis of Zeus Panda Financial Botnet	1-S Sarojini / 2-S Asha	International Journal of Engineering and Advanced Technology (IJEAT)	2249–8958	2019
36	Awareness of security risks associated with payment systems analysed by the methods of multidimensional statistics	1-Antonín Koraus / 2-Miroslav Gombár / 3-Pavel Kelemen / 4-Stanislav Backa	Journal of Security and Sustainability Issues	2029-7025	2019
37	A secured way to enhance online banking transaction	1-Maleeha Khan / 2-Vinjam Likitha / 3-G. Vijay Kumar	International Journal of Innovative Technology and Exploring Engineering (IJITEE)	2278-3075	2019
38	Cybercrime: an emerging threat to the banking sector of Pakistan	1-Muhammad Shoukat Malik / 2-Urooj Islam	Journal of Financial Crime	1359-0790	2019

continua

continuação

Nr	Título	Autor(es)	Periódico	ISSN	Ano
39	Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship	1-Jelle Brands / 2-Johan van Wilsem	European Journal of Criminology	1477-3708	2019
40	Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks	1-Adedayo Solomon Williams / 2- Manoj S. Maharaj / 3-Adebowale I. Ojo	International Journal of Computing and Digital Systems	2210-142X	2019
41	Victims of cybercrime in Europe: a review of victim surveys	1-Carin M. M. Reep-van den Bergh1 / 2-Marianne Junger	Crime Science	2193-7680	2018
42	Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria	Uchenna Jerome Orji	Tilburg Law Review	2211-0046	2018
43	Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance	1-Markus Riek / 2-Rainer Beohme / 3-Tyler Moore	IEEE Transactions on Dependable and Secure Computing	1545-5971	2016
44	Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks	1-E. Rutger Leukfeldt / 2-Edward R. Kleemans / 3-Wouter P. Stol	British Journal of Criminology	0007-0955	2016
45	The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters	Jonathan Fisher	Journal of Financial Crime	1359-0790	2008
46	Fear of On-line Victimization Among Undergraduate Students: A Comparative Study of Two Selected Urban Universities	1-Sadiq Isa Radda / 2-Philip Nnameziri Ndubueze	African Journal of Criminology & Justice Studies	1554-3897	2013
47	Cybersecurity Compliance in the Financial Sector	Derek Mohammed	Journal of Internet Banking and Commerce	1204-5357	2015
48	Emerging IT Risks: Insights from German Banking	1-Simon Ashby / 2-Trevor Buck / 3-Stephanie No¨th-Zahn / 4-Thomas Peisl	Geneva Papers on Risk & Insurance	1018-5895	2018
49	Anti Phishing for Mid-Range Mobile Phones	1-Imran Khan Memon / 2-Muhammad Khalid Khan	International Journal of Computer and Communication Engineering	2010-3743	2013
50	A Conceptual Perspective for Identifying and Preventing Phishing Attacks	1-B. Ravi Raju / 2-B. Namratha / 3-G. L. Anand Babu	International Journal of Recent Technology and Engineering	2277-3878	2019
51	Cyber risk management in digital environment: Case of Kazakhstani bank	Galiya Mertai Kyzy Berdykulova	International Journal of Engineering and Advanced Technology (IJEAT)	2249-8958	2019
52	BioPay: Your Fingerprint is Your Credit Card	Fahad Alsolami	International Journal of Advanced Computer Science and Applications	2158-107X	2019

continua

continuação

Nr	Título	Autor(es)	Periódico	ISSN	Ano
53	Improving the Security and QoE in Mobile Devices through an Intelligent and Adaptive Continuous Authentication System	1-José María Jorquera Valero / 2-Pedro Miguel Sánchez Sánchez / 3-Lorenzo Fernández Maimó / 4-Alberto Huertas Celdrán / 5-Marcos Arjona Fernández / 6-Sergio De Los Santos Vílchez / 7-Gregorio Martínez Pérez	Sensors	1424-8220	2018
54	Targeting Target with a 100 million dollar data breach	1-Federico Pigni / 2-Marcin Bartosiak / 3-Gabriele Piccoli / 4-Blake Ives	Journal of Information Technology Teaching Cases	2043-8869	2018
55	Evaluating Database Security and Cyber Attacks: A Relational Approach	Bamrara A	Journal of Internet Banking and Commerce	1204-5357	2015
56	Research of Human Factors in Information Security	1-Boris Ivanovich Skorodumov / 2-Olga Borisovna Skorodumova / 3-Liliya Fedorovna Matronina	Modern Applied Science	1913-1844	2015
57	E-banking: Online Transactions and Security Measures	Hameed Ullah Khan	Research Journal of Applied Sciences, Engineering and Technology	2040-7459	2014
58	Fighting money laundering in the age of online banking, virtual currencies and internet gambling	Tatiana Tropina	ERA Forum	1612-3093	2014
59	Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities	1-Jawad Hussain Awan / 2-Shahzad Memon / 3-Sheeraz Memon / 4-Kamran Taj Pathan / 5-Niaz Hussain Arijo	Mehran University Research Journal of Engineering and Technology	2413-7219	2018
60	Evaluating biometrics for online banking: The case for usability	1-Rana Tassabehji / 2-Mumtaz A. Kamala	International Journal of Information Management	0268-4012	2012
61	Static Identification of Injection Attacks in Java	1-Fausto Spoto / 2-Elisa Burato / 3-Michael D. Ernst / 4-Pietro Ferrara / 5-Alberto Lovato / 6-Damiano Macedonio / 7- Ciprian Spiridon	ACM Transactions on Programming Languages & Systems	0164-0925	2019
62	Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime	Benoit Dupont	Crime, Law & Social Change	0925-4994	2017

continua

continuação

Nr	Título	Autor(es)	Periódico	ISSN	Ano
63	Mitigation of Cyber Risks in the Field of Electronic Payments: Organizational and Legal Measures	1-Mihail Nikolaevich Dudin / 2- Vadim Nikolaevich Zasko / 3- Evgeniya Evgenevna Frolova / 4- Natalya Georgievna Pavlova / 5- Ekaterina Petrovna Rusakova	Journal of Advanced Research in Law and Economics	2068-696X	2018
64	A methodology for analyzing the credential marketplace	1-Paul A. Watters / 2- Stephen McCombie	Journal of Money Laundering Control	1368-5201	2011
65	The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks	1-Saqer Al-Tahat / 2- Osama Abdel Moneim	International Journal of Scientific and Technology Research	2277-8616	2020
66	Internet banking in Nigeria: Cyber security breaches, practices and capability	1-Victoria Wang / 2- Harrison Nnaji / 3- Jeyong Jung	International Journal of Law, Crime and Justice	1756-0616	2020
67	Analysis of cyber-crime effects on the banking sector using balance score card: a survey of literature	1-Oluwatoyin Esther Akinbowale / 2-Heinz Eckart Klingelhöfer / 3- Mulatu Fikadu Zerihun	Journal of Financial Crime	13590790	2020
68	Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system	1-Norman Mugarura / 2-Emma Ssali	Journal of Money Laundering Control	1368-5201	2020
69	Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money rules	Ehi Eric Esoimeme	Journal of Money Laundering Control	1368-5201	2020
70	The Mediating Role Of Perceived Security On The Relationship Between Internet Banking Users And Their Determinants	1-Fadare Olusolade Aribake / 2-Zahurin Mat Aji	International Journal of Advanced Research in Engineering and Technology	0976-6480	2020
71	Steganography Security On Bank System	1-Shaik Arshiya / 2-B. Aruna / 3-P. Guru Prasad / 4-Ravi Kumar Tenali	International Journal of Recent Technology and Engineering	2277-3878	2019
72	Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions	1-Tanvir Fatima Naik Bukht / 2-Muhammad Ahsan Raza / 3-Jawad Hussain Awan / 4- Rizwan Ahmad	International Journal Of Computer Science And Network Security	1738-7906	2020