Universidade de Brasília

Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas

Departamento de Administração

Lucca Seabra Cruz

SECURITY BY DESIGN: uma análise da produção de artigos acadêmicos em bases de dados de 2018 a 2022

Brasília – DF

2023

LUCCA SEABRA CRUZ

SECURITY BY DESIGN: uma análise da produção de artigos acadêmicos em bases de dados de 2018 a 2022.

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

2023

LUCCA SEABRA CRUZ

SECURITY BY DESIGN: uma análise da produção de artigos acadêmicos em bases de dados de 2018 a 2022.

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

Lucca Seabra Cruz

Dr. Carlos André de Melo Alves

Professor-Orientador

Dr. Rafael Rabelo Nunes

Professor-Examinador

Dra. Fabiana Freitas Mendes

Professora-Examinadora

Brasília, 28 de novembro de 2023

AGRADECIMENTOS

Gostaria de agradecer a Deus que meu deu a vida e a todos os amigos e familiares que torcem pelo meu sucesso. Agradeço especialmente aos meus pais, Jefferson e Maria José, que sempre me apoiaram, me amaram e nunca mediram esforços para que eu pudesse encontrar o caminho do crescimento, da felicidade e da realização. Agradeço aos meus irmãos Rafael e Letícia pela compreensão, carinho e companheirismo durante toda a trajetória. Por último, quero agradecer ao Prof. Dr. Carlos André de Melo Alves por todo seu apoio, paciência e dedicação durante o desenvolvimento deste trabalho.

RESUMO

O objetivo geral deste estudo é descrever a produção de artigos científicos com o tema *security by design* presente em bases de dados acadêmicas no período de 2018 a 2022. Foi desenvolvida uma análise bibliométrica por meio de pesquisa descritiva, abordagem quali-quantitativa e amostra não probabilística de 76 artigos provenientes das bases de dados *Scopus*, *Web of Science* e *ProQuest*. O tratamento dos dados se deu por estatística descritiva, elaboração de nuvem de palavras e análise de conteúdo. A análise de conteúdo consistiu no mapeamento da presença ou ausência dos dez princípios de *security by design* da OWASP (2016) no texto da amostra de artigos. Como principais resultados, identificou-se que o ano de 2022 obteve 27,63% da amostra. 69,44% das instituições as quais os autores são filiados se encontram na Europa. Os periódicos *IEEE Access* e o *Sensors* publicaram 9,21% dos artigos e o *IEEE Transactions on Industrial Informatics* e *Future Generation Computer Systems publicaram* 2,63% cada. As instituições *Florida Atlantic University*, a *University of Haifa* e a *University of Campania Luigi Vanvitelli* participaram da produção de 3 artigos cada. Houve 81,58% dos artigos escritos por três ou mais autores. A abordagem quali-quantitativa esteve presente em 47,37% dos artigos e a qualitativa em 44,74% deles. Os princípios de *security by design* mais encontrados nos artigos da amostra foram "Minimize a área de superfície de ataque", presente em 80,26% da amostra, "Estabeleça padrões seguros", presente em 68,42%, e "Aplique a defesa em profundidade", presente em 55,26%. Na distribuição de palavras-chave, 'IoT' obteve 36 aparições, seguida por '*security*' com 14 aparições e '*cybersecurity*' com 10 aparições. O estudo busca trazer reflexões para administradores, desenvolvedores de *software*, gestores de segurança da informação e estudiosos que busquem entender a aplicação dos conhecimentos sobre o tema almejando o aprimoramento da gestão de segurança cibernética nas organizações.

Palavras-chave: *security by design*, análise bibliométrica, segurança cibernética, análise de conteúdo.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CISA - *Cybersecurity and Infrastructure Security Agency*

CSA - *Cyber Security Agency*

DOI - *Diffusion of Innovation*

EU - *European Union*

IEC - *International Electrotechnical Commission*

IoT - *Internet of Things*

ISO - *International Organization for Standardization*

ISSN - *International Standard Serial Number*

IT - *Information Technology*

NIST - *National Institute of Standards and Technology*

OWASP - *Open Web Application Security Project*

SDL - *Security Development Lifecycle*

SDLC - *Software Development Life Cycle*

SSDF - *Secure Software Development Framework*

TIC - Tecnologia da Informação e Comunicação

UAV - *Unmanned Aerial Vehicle*

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

A evolução das tecnologias da informação trouxe mudanças profundas no mundo e impactou a humanidade em diversas dimensões, tornando a tecnologia um pilar essencial para o funcionamento social e econômico da sociedade. Apesar de todos seus benefícios, esse desenvolvimento acabou por trazer novas vulnerabilidades em roupagens anteriormente desconhecidas, preocupando os especialistas e responsáveis por políticas públicas no que tange a proteção das tecnologias da informação e comunicação (TICs) por preverem um aumento da frequência de ataques cibernéticos a cada ano (FISCHER, 2016).

No cenário atual, a segurança cibernética vem se tornando um assunto estratégico para as organizações pelo fato de os dados terem um protagonismo cada vez maior, tanto por gerar vantagens competitivas ao transformá-los em informação quanto por seu imenso potencial destrutivo em caso de eventuais ataques cibernéticos não neutralizados.

Conforme o *National Institute of Standards and Technology* - NIST (2015, p.48),

> a segurança cibernética é definida como a prevenção de danos, uso não autorizado, exploração e, se necessário, a restauração dos sistemas eletrônicos de informação e comunicação e das informações contidas por eles a fim de reforçar a confidencialidade, integridade e disponibilidade desses sistemas.

Os ataques cibernéticos nos negócios podem ocasionar danos categorizados em cinco grandes temas, sendo eles físicos, digitais, econômicos, psicológicos, danos à reputação e, por fim, sociais (AGRAFIOTES; NURSE; UPTON, 2018). Os danos físicos ou digitais representam um risco à vida e à infraestrutura. Possíveis consequências relacionadas aos danos econômicos são a queda no preço das ações, penas judiciais e redução dos lucros. Os impactos psicológicos recaem sobre os indivíduos da organização, podendo gerar neles vergonha, depressão e constrangimento. Os danos à reputação são considerados por muitos os de maior impacto, resultando em uma desconfiança por parte dos clientes, gerando a perda destes e de potenciais novos consumidores, situação que pode perdurar por muito

tempo. Por último, conforme o estudo citado previamente neste parágrafo, os danos sociais desaguam em crises que afetam as relações internas, prejudicando processos e o bom funcionamento da organização.

As estratégias de implantação da segurança cibernética nas organizações costumam implementar a proteção ao redor de uma estrutura previamente desenvolvida, aplicando a segurança ao final de todo processo. Ao optar por esse caminho, acaba-se por ignorar falhas e vulnerabilidades que poderiam ter sido sanadas caso a segurança fosse pensada desde o princípio do desenvolvimento de produtos e processos. O conceito de *security by design*[1], também conhecido por *secure by design*, aparece como um conceito que busca elevar o nível de segurança ao seu máximo potencial.

A abordagem *security by design* "visa tornar os sistemas tão livres de vulnerabilidades quanto possível, tendo em conta a segurança desde as fases iniciais do processo de *design*" (CASOLA et al., 2016). O termo *security by design* pode ser definido como

> uma abordagem de desenvolvimento de software e hardware que busca minimizar as vulnerabilidades do sistema e reduzir a superfície de ataque por meio do projeto e construção da segurança em todas as fases do SDLC." (CSA, 2017).

Mesmo sendo reconhecida como uma boa prática, a aplicação dessa abordagem ainda não alcançou um nível de adesão ideal pelo fato de poucas metodologias e ferramentas terem sido desenvolvidas e testadas, por poucas possuírem um nível considerável de maturidade, por serem bastante complexas, por possuírem um alto custo de implementação e alta especificidade de aplicação (CASOLA et al., 2020, p.2).

1.2. Formulação do Problema

A evolução da segurança no processo de desenvolvimento de *software* se mostra uma necessidade para que as organizações possam lidar com novos tipos de riscos e vulnerabilidades, sendo o conceito de s*ecurity by design* importante no contexto de melhores práticas de segurança cibernética. O conceito inspirou a criação

[1] Existem definições semelhantes para o termo na literatura em português como segurança por escopo. Porém, o estudo optou por manter a utilização do termo em inglês.

de conjuntos de princípios que transmitem práticas essenciais e pontos importantes a serem considerados durante a fase de desenvolvimento como os princípios de *security by design* da *Open Web Application Security Project* - OWASP (2016).

Apesar de haver um consenso cada vez maior a respeito de sua relevância, ainda existem muitas barreiras que impedem que o conceito 'Security by Design' seja amplamente compreendido, divulgado e implementado nas organizações. Uma dessas barreiras é a dificuldade em implementar uma mudança de consciência por parte das lideranças para que a segurança seja tratada de maneira proativa e como uma questão estratégica, modificando a cultura organizacional com o intuito de integrar e direcionar esforços de diversas áreas para alcançar um nível mais elevado de segurança para seus produtos (CAVOUKIAN; DIXON, 2013).

Nesse sentido, o desenvolvimento de uma análise bibliométrica da produção científica a respeito do assunto mostra-se útil, podendo servir como subsídio a essa tomada de consciência por parte dos gestores, desenvolvedores de *software* e pesquisadores, reunindo os principais artigos, autores e instituições que buscam evoluir o debate a respeito do tema *security by design*, trazendo luz às suas vantagens em relação às abordagens reativas amplamente utilizadas como estratégia de segurança cibernética.

Tendo em vista o exposto, o presente trabalho busca responder o seguinte problema de pesquisa: **Qual é a produção de artigos científicos sobre o tema *'security by design'* presente em bases de dados acadêmicas no período de 2018 a 2022?**

1.3. Objetivo Geral

O presente estudo possui como objetivo geral descrever a produção de artigos científicos com o tema "*security by design"* presente em bases de dados acadêmicas no período de 2018 a 2022.

1.4. Objetivos Específicos

Os objetivos específicos do trabalho são:

- Objetivo Específico 1 (OE1): identificar a produção de artigos científicos por ano de publicação;
- Objetivo Específico 2 (OE2): verificar a distribuição de instituições às quais os autores estão filiados, segmentadas por continente;
- Objetivo Específico 3 (OE3): verificar a distribuição de artigos produzidos conforme o periódico em que foram publicados;
- Objetivo Específico 4 (OE4): averiguar a quantidade de artigos produzidos conforme a filiação acadêmica;
- Objetivo Específico 5 (OE5): segmentar os artigos conforme a quantidade de autores;
- Objetivo Específico 6 (OE6): categorizar os artigos conforme a abordagem metodológica utilizada;
- Objetivo Específico 7 (OE7): mapear a presença de princípios relacionados à *security by design* nos artigos da amostra;
- Objetivo Específico 8 (OE8): identificar a distribuição de palavras-chave nos artigos da amostra.

1.5. Justificativa

O estudo sobre *security by design* é de interesse não só da área da computação, mas atrai também outras áreas (Kang e Kim, 2022). Isso mostra a amplitude do tema e sua relevância em diversas aplicações, inclusive a gestão de riscos cibernéticos nas organizações.

O *Cyber Resilience Act* (EU, 2022) enfatiza a relevância do tema trazendo argumentos a respeito do impacto que produtos inseguros podem causar para os consumidores e propondo como um de seus objetivos certificar que os manufatores de produtos que possuem elementos digitais, *hardware* quanto de *software*, melhorem a segurança de seus produtos desde a fase de projeto e desenvolvimento e durante todo o ciclo de vida.

A contribuição teórica do presente trabalho se justifica em proporcionar um estudo bibliométrico da produção científica recente de periódicos acadêmicos, podendo ser de utilidade para estudiosos da área de Administração no que tange aos assuntos de gestão de riscos, gestão de processos e estratégia organizacional.

O estudo também contribui para acadêmicos que buscam o conhecer e se inteirar sobre os trabalhos mais recentes e de como se encaminhou a discussão a respeito do tema nos últimos cinco anos. Mostra também a interdisciplinaridade das pesquisas da área de Administração com metodologias utilizadas de forma estratégicas nas áreas de Biblioteconomia, Documentação e Ciência da Informação.

O estudo possui como contribuição prática possibilitar aos gestores e profissionais da área um panorama da produção científica a respeito do tema, mapeando os autores e instituições de maior relevância para que possam se aprofundar no assunto e ampliar dados e informações no que se refere ao impacto e importância da abordagem e às diversas possibilidades de aplicação por meio de modelos e *frameworks* de *security by design*. O trabalho auxilia, portanto, o entendimento de referências para implementação de processos de desenvolvimento de *software* seguros.

Por fim, existem *softwares* comerciais que podem apresentar falhas de *design* e implementação, as quais poderiam ser evitadas, carecendo do investimento de gestores para o assunto (ANDERSON e MOORE, 2006). Isso evidencia um potencial cenário para investimento no estudo do tema *security by design*, buscando-se sanear vulnerabilidades e aprimorar a gestão nas organizações.

2. REFERENCIAL TEÓRICO

O referencial teórico é subdividido em três assuntos que representam os pilares do presente trabalho: 2.1) Segurança Cibernética; 2.2) *Security by Design; 2.3)* Análise Bibliométrica.

2.1. Segurança Cibernética

O termo segurança cibernética é reconhecido por muitos como de difícil delimitação pela sua abrangência e variedade de definições, das quais muitas são dependentes de um contexto específico, subjetivas e algumas acabam por confundir mais que esclarecer (CRAIGEN; DIAKUN-THIBAULT; PURSE, 2014). Muitos pesquisadores concordam que falta uma definição comum para o termo em diferentes âmbitos, como empresariais, governamentais e acadêmicos (FISCHER, 2016; BAYLON, 2014; CRAIGEN; DIAKUN-THIBAULT; PURSE, 2014).

De acordo com Craigen, Diakun-Thibault e Purse (2014), a carência de uma definição concisa e abrangente que abarque o aspecto multidisciplinar da segurança cibernética impede o desenvolvimento tecnológico e científico da área de atuação ao reforçar definições puramente técnicas, dividindo áreas que deveriam estar trabalhando juntas para resolver desafios complexos de segurança cibernética.

É possível identificar que a maior parte das definições de segurança cibernética são provenientes de instituições governamentais (SHARTZ; BASHROUSH; WALL, 2017). Maurer e Morgus (2014) compilaram em seu trabalho uma grande variedade de definições de segurança cibernética originadas dessas instituições, sendo uma delas, citada por Shartz, Bashroush e Wall (2017) como uma das mais representativas, a definição do governo sul-africano, o qual afirma que

> Segurança cibernética é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de risco, ações, treinamento, melhores práticas, asseguramento e tecnologias que podem ser utilizadas para proteger o ambiente cibernético e a organização e os recursos do usuário. Recursos da organização e do usuário incluem aparelhos computacionais conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicação e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético (SOUTH AFRICA, 2010, p.12 apud Maurer; Morgus, 2014, p.30).

O NIST (2018a, p.45) define a segurança cibernética como "O processo de proteger a informação ao prevenir, detectar e responder ataques", sendo também definida como "A habilidade de proteger ou defender o uso do espaço cibernético de ataques cibernéticos" (NIST, 2012, p.B-3), sendo o espaço cibernético definido da seguinte forma:

> Um domínio global dentro do ambiente de informações que consiste em uma rede interdependente de infraestrutura de sistemas de informação incluindo a internet, redes de telecomunicação, sistemas computacionais e processadores e controladores incorporados (NIST, 2012, p.B-3).

Para fins deste estudo, a definição de segurança cibernética adotada é a proposta pela ISO/IEC 27032:2012, definindo-a como a preservação da confidencialidade, integridade e disponibilidade da informação no espaço cibernético. O espaço cibernético, por sua vez, é um ambiente complexo resultante da interação entre pessoas, *software* e serviços na internet por meio de dispositivos tecnológicos e redes conectadas a eles, as quais não existem em nenhuma forma física (ISO/IEC, 2012).

Para Ottis e Lorents (2010), não existe um consenso para a definição do termo espaço cibernético, apenas a ideia compartilhada pela maioria das definições de que o termo faz referência a redes de conexão global entre *hardware*, *software* e dados. Em seu trabalho, buscaram adicionar um fator geralmente desconsiderado, o tempo, propondo que o "espaço cibernético é um conjunto dependente do tempo de sistemas de informação e usuários humanos que interagem com esses sistemas" (OTTIS; LORENTS, 2010, p.2).

Essas definições evidenciam a predominância de definições técnicas para o termo assim como foi citado anteriormente. Em busca de construir uma definição que abrangesse o aspecto multidisciplinar da segurança cibernética, Craigen, Diakun-Thibault e Purse (2014, p.17) chegaram a seguinte proposta:

> A segurança cibernética é a organização e o conjunto de recursos, processos e estruturas usados para proteger o espaço cibernético e os sistemas habilitados para o ciberespaço contra ocorrências que desalinhem os direitos de propriedade *de jure* dos *de facto*.

A definição proposta traz as diversas dimensões da cibersegurança e a considera como fruto da interação entre humanos e sistemas. Amplia-se a noção da proteção, sendo está voltada não somente à informação, mas ao espaço cibernético

e sistemas que tradicionalmente não são vistos como parte desse espaço. O uso da palavra "ocorrências" abrange eventos intencionais, acidentais e naturais, ampliando a ideia de proteger apenas de ataques cibernéticos intencionais. A descrição das ocorrências que "desalinhem os direitos de propriedade *de jure* dos *de facto*" descreve um dos resultados do ataque cibernético bem-sucedido, as informações em posse de indivíduos não autorizados, abarcando o objetivo de proteção das informações e privacidade de dados (CRAIGEN; DIAKUN-THIBAULT; PURSE, 2014).

Outros pesquisadores que buscaram propor uma melhor definição do termo segurança cibernética foram Shartz, Bashroush e Wall (2017). Os autores utilizaram a abordagem de uma revisão semi-sistemática da literatura (MÄNTYLÄ et al., 2014, p.66), chegando a seguinte definição de segurança cibernética:

> A abordagem e ações associadas aos processos de gerenciamento de riscos de segurança seguidos por organizações e estados para proteger a confidencialidade, integridade e disponibilidade dos dados e recursos usados no espaço cibernético. O conceito inclui diretrizes, políticas e um conjunto de salvaguardas, tecnologias, ferramentas e treinamento para proporcionar a melhor proteção para o estado do ambiente cibernético e seus usuários (SHARTZ; BASHROUSH; WALL, 2017, p.66).

Os autores afirmam que a definição é de grande valor por reunir por meio de métodos científicos os conceitos chave que envolvem a segurança cibernética, analisando vinte e oito diferentes definições que atenderam aos critérios de inclusão, pontuando-as e usando-as como matéria-prima para a construção de uma definição com maior representatividade.

Há autores na literatura que diferenciam o conceito de segurança cibernética do conceito de segurança da informação. A segurança da informação, de acordo com ISO/IEC (2009), é a "preservação da integridade, confidencialidade e disponibilidade da informação". A definição se apresenta como a proteção dos três pilares ou características da segurança da informação. Esses pilares são descritos por Pinheiro (2020, p. 44) da seguinte forma:

> A confidencialidade consiste na garantia de que a informação será restrita e seguramente guardada; já a integridade busca garantir que a informação será preservada em sua exatidão por meio de métodos de processamento específicos; por fim, a disponibilidade garante que os usuários autorizados tenham acesso às informações sempre que necessário.

De acordo com Solms e Niekerk (2013), a segurança da informação se limita à proteção da informação contra possíveis danos provenientes de ameaças e

vulnerabilidades enquanto a segurança cibernética envolve a proteção não só do espaço cibernético, mas de todos que operam nesse espaço, incluindo seus recursos que se conectam ao espaço cibernético.

O impacto causado pela maior parte dos ataques cibernéticos é limitado, porém, ataques bem-sucedidos a infraestruturas críticas podem causar danos consideráveis à segurança nacional, economia, vida e segurança dos indivíduos (FISCHER, 2016). O dano cibernético pode impactar as organizações de diversas maneiras, podendo ser definido como

> o dano originado como resultado direto de um ataque conduzido totalmente ou parcialmente por meio de infraestruturas digitais e das informações, dispositivos e aplicações de software das quais essas infraestruturas são compostas (AGRAFIOTIS et al., 2018).

Agrafiotis et al. (2018), em seu estudo sobre a taxonomia dos danos cibernéticos nas organizações, classifica esses danos em cinco diferentes categorias: dano físico ou digital; dano econômico; dano psicológico; dano de reputação; dano social e societal. Cada um dos tipos de dano cibernético pode ser dividido em subtipos menores, sendo essa relação explicitada no Quadro 1.

QUADRO 1 - Tipos e subtipos de danos cibernéticos

Tipo de dano cibernético	Subtipos de dano cibernético
Dano físico ou digital	Dano ou indisponibilidade; Destruição; Roubo; Comprometimento; Contaminação física ou digital; Exposição ou Vazamento; Corrupção da integridade; Redução de performance; Dano no corpo físico humano; Dor humana; Perda de vida humana; Processo judicial; Abuso (má utilização de ativos); Maus-tratos (brutalização de ativos); Roubo de informações pessoais.
Dano econômico	Interrupção das operações; Interrupção de vendas ou do faturamento; Redução de clientes; Redução de lucros; Redução do crescimento; Redução de investimentos; Queda de valor das ações Roubo financeiro; Perda financeira ou de capital; Penas regulatórias; Custos de investigação; Custos de relações públicas; Pagamentos de compensações; Pagamentos por extorsão; Perda de empregos; Vítimas de golpes.
Dano psicológico	Confusão; Desconforto; Frustração; Preocupação e ansiedade; Entristecimento; Depressão; Constrangimento; Vergonha; Sentimento de culpa; Perda de autoconfiança; Baixa satisfação; Mudanças negativas na percepção.
Dano de reputação	Dano na percepção pública; Redução da boa vontade corporativa; Dano no relacionamento com os consumidores; Dano no relacionamento com fornecedores; Redução de oportunidades de negócio; Dificuldade no recrutamento de novos funcionários; Escrutínio da mídia; Perda de funcionários chave; Perda ou suspensão de credenciamentos ou certificações; Redução do *escore* de crédito.
Dano social e societal	Mudanças negativas na percepção do público; Interrupção de atividades do dia a dia; Impacto negativo na nação; Queda moral interna da organização.

Fonte: Adaptado de Agrafiotis et al. (2018, p.9-10).

A fim de lidar melhor com o número crescente de ameaças advindas dos contínuos avanços tecnológicos e levando em consideração a amplitude da área, foi construída uma relação de cooperação entre o setor privado e as instituições governamentais para se resolver problemas complexos de cibersegurança (PINHEIRO, 2020), inclusive. Foram desenvolvidos diversos *frameworks* e normas para padronizar boas práticas em segurança cibernética. Entre os *frameworks* mais reconhecidos estão o da família de normas ISO/IEC 27000 e o framework de cibersegurança NIST.

A família de normas ISO 27000 surgiu em 2006 como um conjunto de diretrizes de proteção e prevenção de segurança da informação para criação, manutenção, análise, melhoria, revisão e funcionalidade do sistema de gestão de segurança da informação, sendo este definido como "sistemas corporativos que abrangem todos os processos organizacionais ou parte deles e buscam proteger as informações da empresa [...]" (PINHEIRO, 2020, p.41).

As empresas que implementam e praticam a manutenção das normas recebem a certificação ISO após se submeterem a um processo de auditoria, demonstrando o seu compromisso com essas boas práticas. De acordo com Pinheiro (2020), as vantagens proporcionadas pelo uso das normas técnicas são propor diretrizes para a identificação dos riscos em relação à segurança da informação; definição de mecanismos de controle para gerenciar ou eliminar os riscos; possibilidade de adaptação de controles de acordo com as áreas específicas ou conforme a necessidade; proteção da reputação da empresa; redução de custos em relação à segurança ao prevenir riscos.

Outra instituição que é referência mundial em segurança cibernética é o NIST (*National Institute of Standards and Technology*), a qual fornece o *Framework* para Melhoramento de Cibersegurança de Infraestrutura Crítica. O *framework* consiste em atividades para guiar a cibersegurança, entendendo-a como parte integrante da gestão de riscos da organização (NIST, 2018a).

O *framework* NIST pode ser subdividido em três: *framework core*; *framework implementation tiers*; *framework profile*. O *framework core* fornece um conjunto de atividades e referências para se alcançar a segurança cibernética, sendo dividido em cinco funções, cada com uma ordem hierárquica de categorias, subcategorias e referências normativas, sendo as cinco funções identificar, proteger, detectar, responder e recuperar (PINHEIRO, 2020). O *framework implementation tiers* proporciona contextos de como a organização enxerga a segurança cibernética, analisando em que grau suas políticas de gestão de risco de cibersegurança estão alinhadas às atividades apresentadas no framework (NIST, 2018a). Por fim, a terceira parte, o framework *profile* busca alinhar as atividades do negócio com as funções, categorias e subcategorias conforme sua necessidade específica, auxiliando a organização na definição de suas metas tendo em vista seus recursos e tolerância ao risco (PINHEIRO, 2020).

2.2. Security by Design

A integração das tecnologias da informação com os mais diversos aspectos da vida social pode ser considerado como um processo inevitável, conectando pessoas

sistemas, processos e dados. Os riscos advindos desse processo, como demonstrado anteriormente, fizeram com que fosse essencial buscar o desenvolvimento de processos e produtos pensados para serem seguros desde sua origem (CISA, 2023), ou seja, produtos desenvolvidos através de uma metodologia que implemente a segurança de maneira proativa e não reativa, metodologia pela qual pode ser exemplificada pela abordagem *security by design*.

De acordo com a *Cybersecurity and Infrastructure Security Agency* - CISA, o termo *secure by design* traz a ideia de produtos construídos de forma a proteger de agentes cibernéticos mal-intencionados que obtém acesso aos dispositivos, dados e infraestrutura conectada (CISA, 2023). O termo também pode ser definido, quando relacionado ao conceito de *Internet of Things* - IoT, como "Foco no estágio de *design* para garantir que a segurança seja incorporada aos produtos de IoT para o consumidor e aos serviços conectados" (DDCMS, 2018, p.33).

De acordo com Cavoukian e Dixon (2013, p.8), o termo se refere a "uma abordagem para a segurança da informação que, assim como *Privacy by Design*, é ao mesmo tempo holística, criativa, antecipatória, interdisciplinar, robusta, responsável e incorporada nos sistemas". Para fins deste estudo, a definição de *security by design* usada como referência é a da *Cyber Security Agency of Singapore* - CSA, conforme segue:

> *Security-by-Design* é uma abordagem de desenvolvimento de *software* e *hardware* que busca minimizar as vulnerabilidades do sistema e reduzir a superfície de ataque por meio do projeto e construção da segurança em todas as fases do SDLC. Isso inclui incorporar especificações de segurança dentro do projeto, contínua avaliação da segurança em cada fase e adesão às boas práticas (CSA, 2017, p.4)[2].

A incorporação da segurança no escopo de sistemas seguros pode-se dar de duas formas: por meio do software e por meio do hardware (CAVOUKIAN; DIXON, 2013). Por sua vez, o *software development lifecycle* - SDLC é um conceito relacionado ao *security by design* e definido como um processo que considera a segurança antes mesmo do processo de desenvolvimento, considerando-a em todas

[2] Tradução do original: *Security-by-Design is an approach to software and hardware development that seeks to minimise systems vulnerabilities and reduce the attack surface through designing and building security in every phase of the SDLC. This includes incorporating security specifications in the design, continuous security evaluation at each phase and adherence to best practices.*

as suas fases ao incorporar tecnologias de segurança capazes de se adaptar a cada fase do processo de desenvolvimento (LEE; PARK, 2016).

É possível que haja confusão entre os conceitos correlatos, porém não análogos, *security by design*, *privacy by design* e *secure by default*. O termo *secure by default*, apesar de ser similar a *security by design*, se refere a produtos que apresentam usabilidade segura por padrão por nenhuma ou quase nenhuma mudança em suas configurações ou custos adicionais (CISA, 2023; CAVOUKIAN; DIXON, 2013) e, juntamente com a abordagem *security by design*, ajuda a aliviar o peso dos riscos cibernéticos sob os consumidores.

O conceito de *privacy by design* é uma abordagem que, assim como o conceito de *security by design*, busca implementar conceitos de privacidade de dados desde as primeiras fases de desenvolvimento, sendo que "privacidade é sobre controle, permitir que os indivíduos mantenham o controle pessoal sobre suas informações de identificação pessoal com relação à sua coleta, uso e divulgação" (CAVOUKIAN; DIXON, 2013, p.5).

Cavoukian e Dixon (2013) esclarecem as divergências entre os conceitos de *security by design* e *privacy by design* expondo que enquanto *privacy by design* busca respeitar e proteger informações pessoais ao dar o poder de controle aos indivíduos sobre sua própria coleção de dados, *security by design* busca habilitar e proteger atividades e bens tanto das pessoas quanto das organizações.

Existem muitas propostas de conjunto de princípios de *design* de *software* seguro (OWASP, 2016; NIST, 2018b; NCSC, 2019), sendo que nenhuma delas é definida como oficial, havendo divergências em relação às prioridades segundo o viés e opinião de cada autor a respeito do processo de desenvolvimento de *software*. De maneira geral, esses princípios são diretrizes para guiar gestores e desenvolvedores que buscam construir sistemas seguros, tendo em vista a proteção dos três pilares da segurança da informação, a confidencialidade, integridade e disponibilidade.

Um dos conjuntos de princípios mais citados são os da *Open Web Application Security Project* (OWASP, 2016), o qual sugere um conjunto de 10 princípios: (1) Minimize a área de superfície de ataque; (2) estabeleça padrões seguros; (3) conceda privilégio mínimo; (4) Aplique a defesa em profundidade; (5) falhe seguramente; (6) não confie nos serviços; (7) separação de tarefas; (8) evite a segurança por obscuridade; (9) mantenha a segurança simples; (10) corrija problemas de segurança

corretamente. Cada um dos dez princípios são descritos e exemplificados por meio do Apêndice A do presente trabalho.

Cavoukian e Dixon (2013) também desenvolveram sete princípios de *security by design* baseados nos sete princípios de *privacy by design* propostos por eles, os quais demonstram a forte correlação entre os dois conceitos, sendo que a privacidade é parte integral da segurança, a qual é essencial para que a privacidade seja contemplada.

Existem muitos *frameworks* e conjunto de diretrizes de desenvolvimento de *software* que abordam a ideia de incorporação da segurança desde os primeiros estágios do ciclo de desenvolvimento além de diversos *frameworks* específicos de *security by design*. A série de publicações NIST SP 800 contém documentos que abordam o assunto. O NIST SP 800-160 trata da engenharia de segurança de sistemas, trazendo princípios conceitos e atividades relacionados ao tema, tendo como um de seus propósitos "Promover uma mentalidade comum para fornecer segurança a qualquer sistema, independentemente de seu escopo, tamanho, complexidade ou estágio do ciclo de vida do sistema" (NIST, 2018b, p.3).

O NIST também demonstra como os princípios citados no parágrafo anterior, conceitos e atividades podem ser efetivamente aplicados a atividades de engenharia de sistemas. O NIST SP 800-218, intitulado como *Secure Software Development Framework* (SSDF), é um conjunto de práticas de desenvolvimento de *software* seguro de alto nível que podem ser integradas em cada um dos estágios do SDLC (NIST, 2022). O NIST SP 800-53 proporciona um catálogo de controles de privacidade e segurança para sistemas de informação e organizações para proteger as operações, bens, indivíduos e outras organizações de riscos cibernéticos (NIST, 2020). Apesar de não tratar especificamente da incorporação da segurança no SDLC, o documento fornece uma gama de controles que podem ser implementados durante as etapas de seu desenvolvimento.

A Microsoft desenvolveu um processo de desenvolvimento de *software* seguro que pode ser usado para inspirar empresas com o mesmo objetivo, o Microsoft SDL. O Microsoft SDL tem como objetivo reduzir os defeitos de código e *design* de seus produtos e reduzir a severidade dos impactos causados por esses defeitos. A empresa estima que o uso da metodologia chegou a reduzir em 87% o número de boletins de segurança (GOERTZEL et al., 2007, p. 122). O Microsoft SDL prossegue ao longo de seis fases (requerimentos, *design*, implementação/desenvolvimento, verificação,

lançamento e suporte e manutenção) mapeando as tarefas de segurança relevantes a cada etapa de desenvolvimento dentro do SLDC. A norma ISO/IEC 27034-1 apresenta um conjunto de diretrizes de gestão da segurança durante o SDLC, com o propósito de assistir as empresas na integração contínua da segurança em todo o ciclo de vida da aplicação (ISO, 2011).

A implementação da abordagem *security by design* demanda grandes esforços por partes das lideranças organizacionais para tratar a segurança como uma prioridade de negócio e não apenas mais um recurso técnico (CISA, 2023), o que exige uma mudança cultural dentro do contexto organizacional partindo do nível estratégico e posteriormente para a organização como um todo. As instituições governamentais e a sociedade já demandam que as empresas tomem para si uma maior responsabilidade perante as consequências geradas da vulnerabilidade de seus produtos, tirando parte do peso das costas dos consumidores (CISA, 2023; EU, 2023; NCSC, 2019). Apesar de ser uma necessidade urgente, existem muitos desafios e barreiras que dificultam a implementação da abordagem e da segurança cibernética como um todo.

Muitos dos desafios envolvendo a implementação de uma abordagem *security by design* são comuns à área de segurança cibernética de modo geral. De acordo com Dupont (2013), um grande problema para a implementação da abordagem é o fato dela ser incompatível com os ciclos de inovação cada vez mais velozes, onde há uma necessidade de se lançar produtos novos o mais cedo possível para que não se perca espaço no mercado para os competidores. Isso se materializa como um grande desincentivo econômico que enfraquece a busca por implementação de padrões de segurança.

Fischer (2016) também denuncia outros desafios, argumentando que os desenvolvedores possuem um foco maior em funcionalidades em detrimento da incorporação da segurança nos primeiros estágios de desenvolvimento por razões econômicas, sendo que os benefícios da segurança são difíceis de se mensurar e naturalmente incertos, e o contraste entre os incentivos para o crime cibernético e segurança cibernética, onde o crime é consideravelmente barato, lucrativo e seguro de ser praticado.

A falta de transparência do mercado também é um grande impedimento para que as pessoas escolham produtos mais seguros, pois são impedidas de conhecer o nível de segurança do produto para que façam a melhor escolha e premiar as

empresas que mais valorizam sua segurança, sendo a falta de transparência e o uso de segurança por obscuridade, prática contrária ao *security by design* (OWASP, 2016; CAVOUKIAN; DIXON, 2013). Essa falta de transparência pode promover táticas para a construção de monopólios no meio da tecnologia por meio da assimetria de informação em relação às especificações e configurações de segurança presentes em produtos (ANDERSON, 2001).

A visão dos desenvolvedores a respeito da necessidade da abordagem *security by design* é um fator de relevância para entender o nível em que se encontra a discussão e prática do tema no cotidiano das organizações pelo ponto de vista de quem pensa, cria e mantém esses sistemas em funcionamento. Conforme o estudo de Spiekerman, Korunovska e Langheinrich (2019), a maior parte deles, sendo um total de 124 participantes, concorda que se deve procurar a implementação das abordagens de *privacy by design* e *security by design* e poucos consideram os temas inúteis entre seus pares, cerca de 10% deles. Mesmo assim, 40% dos participantes não se sentem responsáveis pela integração das abordagens e 40% deles não sentem prazer em trabalhar com elas. Isso pode se originar do fato deles não possuírem tempo, autonomia e controle para se engajar em relação ao tema. A organização possui parcela da responsabilidade de sustentar essas crenças, sendo que 31% delas possuía fracas diretrizes de segurança. O estudo conclui que

> o design de sistemas seguros sofre significativamente com a interação entre normas organizacionais fracas (crenças normativas), baixo controle de engenharia (tempo, autonomia, conhecimento) e limitada percepção de responsabilidade (SPIEKERMAN; KORUNOVSKA; LANGHEINRICH, 2019, p.612).

Ainda existe uma grande resistência por parte dos gestores para adoção de princípios de segurança ocasionados pela crença de que esses princípios limitam as atividades do negócio ou funcionalidades de seus produtos, enxergando nesses *tradeoffs* um jogo de "soma-zero". Alguns dos conflitos advindos desse dilema foram listados por Cavoukian e Dixon (2013), entre eles o fácil acesso *versus* acesso seguro, a conveniência versus segurança e simplicidade de implementação *versus* uso seguro, sendo necessário entender e reconhecer o conflito, entender os métodos e tecnologias dentro do cenário e alternativas potenciais que possam mitigá-lo, buscando "acomodar todos os interesses e objetivos legítimos de uma forma positiva 'ganha-ganha', não por meio de abordagem de soma-zero" (CAVOUKIAN; DIXON,

2013, p.9). Mesmo com a existência dessas trocas, a adoção de medidas de segurança deve sempre contemplar todos os objetivos de um sistema e não os inibir sem que haja uma real necessidade para isso e tendo em vista o princípio de se manter a segurança simples (OWASP, 2016), considerando inclusive princípios descritos no Apêndice A. Dessa maneira, a implementação de medidas de segurança tenderá ao sucesso na medida em que considera os interesses dos diversos *stakeholders* envolvidos e gerando benefícios mútuos a todas as partes envolvidas.

A utilização de princípios de *security by design* não só fortalecem a postura de segurança da organização para com seus clientes e a reputação da marca para desenvolvedores, mas também diminui os custos de manutenção e correção para os fabricantes no longo prazo (CISA, 2023). Partindo do pressuposto de que produtos desenvolvidos com a abordagem de *security by design* são aqueles em que a segurança do consumidor é um dos objetivos principais do negócio e não só um recurso técnico, pensando nesse objetivo antes do processo de desenvolvimento, a CISA (2023) faz algumas propostas aos fabricantes de *software* sugerindo que estes sigam três princípios básicos: o fardo da segurança não deve cair somente nos consumidores; adotar a transparência e responsabilidade (prestação de contas) de maneira radical; criar uma estrutura organizacional e liderança para atingir essas metas. Seguindo esses princípios por meio da abordagem de *security by design*, pode-se evitar a probabilidade de sofrer as consequências dos diversos tipos de danos cibernéticos como aqueles classificados por Agrafiotis et al. (2018), descritos no Quadro 1 do presente trabalho.

2.3. Análise bibliométrica

A bibliometria é um campo de pesquisa interdisciplinar, com origens nos estudos de documentação e biblioteconomia, que se estende a quase todos os campos de pesquisa, abrangendo conteúdos da matemática, ciências sociais, ciências naturais, engenharias e ciências da vida (GLÄNZEL, 2003).

> Inicialmente voltada para a medida de livro (quantidade de edições e exemplares, quantidade de palavras contidas nos livros, espaço ocupado pelos livros nas bibliotecas, estatísticas relativas à indústria do livro), aos poucos foi se voltando para o estudo de outros formatos de produção bibliográfica, tais como artigos de periódicos e outros tipos de documentos,

> para depois ocupar-se também, da produtividade de autores e do estudo de citações (ARAÚJO, 2006, p.12-13).

Segundo Donthu et al. (2021), a análise bibliométrica pode ser de grande valia para decifrar e mapear o conhecimento científico acumulado e a evolução de campos científicos, permitindo uma compreensão acerca de um grande volume de dados não estruturados, ajudando a construir bases para o avanço de áreas da ciência, proporcionar aos acadêmicos uma visão geral em um único lugar, identificar lacunas no conhecimento, derivar novas ideias de investigação e posicionar suas pretendidas contribuições ao campo.

Desde seu princípio a bibliometria possui duas principais preocupações: a análise da produção científica e a busca de benefícios práticos para bibliotecas (ARAÚJO, 2006). Atualmente suas técnicas podem ser divididas em duas categorias: análise de performance para medir a contribuição de autores e instituições; mapeamento da ciência para analisar relacionamentos entre os agentes envolvidos no meio científico (DONTHU et al., 2021).

Muitos autores consideram que o termo bibliometria foi cunhado pela primeira vez por Pritchard (1969) em seu trabalho *Statistical Bibliography or Bibliometrics?* (BROADUS, 1987a; GLÄNZEL, 2003) no qual o autor buscava uma denominação mais satisfatória para a área, havendo um consenso a respeito dessa necessidade entre os estudiosos do assunto, substituindo o termo estatística bibliográfica cunhado por E. Wyndham Hulme em 1922 (PRITCHARD, 1969; GUEDES E BORSCHIVER, 2005). Pritchard (1969, p.2) definiu a bibliometria como "a aplicação de métodos matemáticos e estatísticos a livros e outras mídias de comunicação".

De acordo com Broadus (1987b), a definição ainda possui falhas por ser demasiadamente abrangente, característica presente em muitas definições posteriores, e imprecisa no uso da palavra "mídia", deixando sua delimitação vaga. Para sanar esse problema, Broadus (1987b, p. 376) propõe a seguinte denominação: "A bibliometria é o estudo quantitativo de unidades físicas publicadas, ou de unidades bibliográficas, ou dos substitutos de qualquer uma delas". Conforme o próprio autor, pode ser que a definição seja considerada muito restrita por excluir a Lei de Kipf, a qual é tratada como uma distribuição bibliométrica.

Apesar de Pritchard (1969) ser considerado por muitos o primeiro usuário do termo, havendo uma afirmação em seu próprio trabalho que o mesmo fez uma intensiva busca a qual falhou em encontrar usos anteriores do termo, foi demonstrado

que o primeiro autor a utilizar o termo bibliometria (no francês "*bibliométrie*") foi Paul Otlet (2018) em 1934 em sua obra Tratado de Documentação (ARAÚJO, 2006; ROUSSEAU, 2014; VANTI, 2002), afirmando que, naquele momento, outras áreas do conhecimento estavam destinando esforços no sentido de realizar descrições quantitativas e mais minuciosas de suas medições.

É possível diferenciar bibliologia de bibliometria. A bibliologia é "a arte de escrever, de publicar e difundir os dados da ciência" (OTLET, 2018, p.11) ou "uma ciência e uma técnica gerais do documento" (OTLET, 2018, p.11). Por sua vez, a bibliometria seria "a parte definida da bibliologia que se ocupa da medida ou quantidade aplicada aos livros (aritmética ou matemática bibliológica)" (OTLET, 2018, p.18).

De acordo com Guedes e Borschiver (2005, p.2), a bibliometria é "um conjunto de leis e princípios empíricos que contribuem para estabelecer os fundamentos teóricos da Ciência da Informação". As mesmas autoras resumem a bibliometria como

> 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 E BORSCHIVER, 2005, p.15).

Glänzel (2013) identificou que a bibliometria contemporânea pode ser dividida em três principais componentes ou objetivos: bibliometria para praticantes da bibliometria (metodologia); bibliometria para disciplinas científicas; bibliometria para a gestão em ciência e tecnologia (políticas científicas). De acordo com Glänzel (2013), a bibliometria para praticantes da bibliometria se refere ao domínio básico da pesquisa bibliométrica pelo qual são conduzidas as pesquisas metodológicas.

A bibliometria para disciplinas científicas é o grupo de interesse mais vasto e diverso entre os três, onde a bibliometria é usada como instrumento de serviço a alguma especialidade e vista como uma extensão da ciência da informação. Por fim, a bibliometria para gestão em ciência e tecnologia é, de acordo com o autor, o tópico mais relevante para o campo na atualidade, sendo o domínio da avaliação de pesquisa onde "as estruturas nacionais, regionais e institucionais da ciência e sua apresentação comparativa estão em primeiro plano" (GLÄNZEL, 2003, p.10).

Ao desenvolver um levantamento de estudos métricos realizados com dados extraídos de artigos, Mueller (2013) identificou quatro objetivos bibliométricos: análise

e mapeamento de autorias e coautorias, colaboração e redes; avaliação e descrição da literatura, impacto e indicadores; produção e proatividade, visibilidade de autores e instituições; estudos de citação e co-citação. É importante ressaltar que um mesmo estudo pode ter não apenas um, mas vários objetivos de maneira simultânea (MUELLER, 2013).

É de relevância contextualizar o posicionamento da bibliometria e diferenciá-la de suas subáreas relacionadas subordinadas como a ciência da informação, a infometria, a cienciometria e um conceito mais recente, a webometria. De acordo com Tague-Sutcliffe (1992, p.1) bibliometria é "o estudo dos aspectos quantitativos da produção, disseminação e uso de informações registadas". Segundo o autor, a cienciometria seria o estudo dos aspectos quantitativos da ciência como disciplina ou atividade econômica, sendo parte da sociologia da ciência por ser um instrumento que auxilia na formação de suas políticas e a infometria pode ser descrita como

> o estudo dos aspectos quantitativos da ciência enquanto uma disciplina ou atividade econômica. A cienciometria é um segmento da sociologia da ciência, sendo aplicada no desenvolvimento de políticas científicas. Envolve estudos quantitativos das atividades científicas, incluindo a publicação e, portanto, sobrepondo-se à bibliometria (TAGUE-SUTCLIFFE, 1992, p.1, traduzido por MACIAS-CHAPULA, 1998).

De acordo com Almind e Ingwersen (1997), a webometria pode ser denominada com a aplicação de métodos infométricos e outras medidas quantitativas à *World Wide Web*, abarcando a pesquisa de todas as comunicações baseadas na internet.

A análise estatística da literatura científica começou bem antes do termo ser cunhado (GLÄNZEL, 2003; BROADUS, 1987b), seja por Pritchard (1969) ou por Otlet (2018). Guedes e Borschiver (2005) identificaram diversas leis de importância para o campo da bibliometria, as quais são apresentadas e descritas por meio do Quadro 2.

QUADRO 2 - Leis e princípios bibliométricos

Ciência da informação		
Bibliometria		
Leis e Princípios	**Focos de Estudo**	**Principais Aplicações**
Lei de Bradford	periódicos	estimar o grau de relevância de periódicos, em dada área do conhecimento
Lei de Lotka	autores	estimar o grau de relevância de autores, em dada área do conhecimento
Leis de Zipf	palavras	indexação automática de artigos científicos e tecnológicos
Ponto de Transição (T) de Goffman	palavras	indexação automática de artigos científicos e tecnológicos
Colégios Invisíveis	citações	identificação da elite de pesquisadores, em dada área do conhecimento
Fator de Imediatismo ou de Impacto	citações	estimar o grau de relevância de artigos, cientistas e periódicos científicos, em determinada área do conhecimento
Acoplamento Bibliográfico	citações	estimar o grau de ligação de dois ou mais artigos
Co-citação	citações	estimar o grau de ligação de dois ou mais artigos
Obsolescência da Literatura	citações	estimar o declínio da literatura de determinada área do conhecimento
Vida-média	citações	estimar a vida-média de uma unidade da literatura de dada área do conhecimento
Teoria Epidêmica de Goffman	citações	estimar a razão de crescimento e declínio de determinada área do conhecimento
Lei do Elitismo	citações	estimar a o tamanho da elite de determinada população de autores
Frente de Pesquisa	citações	identificação de um padrão de relação múltipla entre autores que se citam
Lei dos 80/20	demanda de informação	composição, ampliação e redução de acervos

Fonte: Adaptado de Guedes e Borschiver (2005, p.14).

Os responsáveis pela elaboração das três leis bibliométricas mais conhecidas são Lotka, Zipf e Bradford (GUEDES; BORSCHIVER, 2005; VANTI, 2002). A Lei de Lotka, conhecida como lei do quadrado inverso, foi formulada em 1926 e tem como objeto a medição da produtividade científica dos autores, na qual conclui que poucos autores são responsáveis por uma larga proporção da produção científica enquanto a produção de uma larga parcela de autores se iguala à de poucos dos principais autores (SANTOS E KOBASHI, 2009), sendo "a relação entre o número de autores e o número de artigos publicados por esses, em qualquer área científica, segue a Lei do Inverso do Quadrado $1/n^2$" (GUEDES; BORSCHIVER, 2005, p. 5).

A Lei de Zipf está relacionada à frequência de ocorrência de palavras em um texto longo ou vários textos e foi elaborada em 1935 (SANTOS; KOBASHI, 2009; VANTI, 2002). De acordo com Santos e Kobashi (2009),

> Zipf extraiu sua lei de um princípio geral do “esforço mínimo”: palavra cujo custo de utilização seja pequeno ou cuja transmissão demande esforço mínimo são frequentemente usadas em texto grande (SANTOS E KOBASHI, 2009, p.157).

Zipf desenvolveu a equação "*r * f = c"*, na qual *r* (*rank*) é a ordem de série de uma palavra (posição na lista de palavras mais frequentes em ordem decrescente) e f a frequência de ocorrência da palavra sendo o produto dessas duas variáveis gerando um valor aproximado à constante *c*.

> Ele descobriu que a palavra mais utilizada aparecia 2653 vezes, a centésima palavra mais utilizada ocorria 256 vezes e a duocentésima palavra ocorria 133 vezes. Zipf viu então que a posição de uma palavra multiplicada pela sua frequência era igual a uma constante de aproximadamente 26500 (ARAÙJO, 2006).

Por fim, uma terceira Lei muito conhecida no campo da bibliometria é a Lei de Bradford desenvolvida em 1934, conhecida também como lei de dispersão do conhecimento, a qual tem como objeto de estudo os periódicos, estimando seu grau de relevância em uma área específica do conhecimento (GUEDES; BORSCHIVER, 2005). A Lei de Bradford busca segmentar os periódicos de acordo com sua produtividade ao diferenciá-los em três zonas para identificar os periódicos mais relevantes e que mais contribuíram para uma determinada coleção ou tema (ARAÚJO, 2006).

3. MÉTODOS E TÉCNICAS DE PESQUISA

O presente capítulo tem como objetivo apresentar a metodologia utilizada no desenvolvimento do trabalho, sendo dividido em quatro seções: 3.1) Tipologia e descrição geral dos métodos de pesquisa; 3.2) Caracterização da área de estudo; 3.3) População e Amostra; 3.4) Procedimentos de coleta e análise de dados.

3.1. Tipologia e descrição geral dos métodos de pesquisa

O presente trabalho é caracterizado como uma pesquisa descritiva, buscando especificar características de uma amostra e descrever suas tendências, possui um recorte temporal longitudinal pelo fato de coletar dados de diferentes períodos para realizar inferências em relação à evolução da área estudada (SAMPIERI; COLLADO; LUCIO, 2013).

O estudo possui abordagem quantitativa no que tange à coleta de dados secundários, medição numérica e análise estatística da amostra, sendo também qualitativa em relação à análise de conteúdo empregada para tratar textos dos artigos nesta pesquisa (BARDIN, 1977). A definição de análise bibliométrica adotada como referência para fins deste estudo é a de Guedes e Borschiver (2005, p.15) apresentada na Seção 2.3 deste trabalho.

3.2. Caracterização da área de estudo

A amostra escolhida como representativa desse estudo é compreendida por artigos publicados em bases de dados de periódicos acadêmicos revisados por pares, e que tratam a respeito de segurança cibernética, mais especificamente do tema *security by design*, área que está diretamente correlacionada à gestão de riscos nas organizações. As bases de dados selecionadas são bases internacionais que abrangem a área de administração e com acesso disponibilizado através do Portal de Periódicos da CAPES.

3.3. População e amostra

A população do estudo compreende artigos científicos provenientes de três diferentes bases de dados: *Scopus - Elsevier*, *Web of Science* e *ProQuest*. As bases de dados foram escolhidas por possuírem acesso disponibilizado pelo Portal de Periódicos da CAPES por meio do acesso CAFe (Comunidade Acadêmica Federada), serem de qualidade internacionalmente reconhecida e baseadas em mecanismos de revisão por pares e por serem bases multidisciplinares que abrangem a área de Administração.

A amostra presente no estudo possui caráter não probabilístico pois "a escolha dos elementos não depende da probabilidade, mas das características da pesquisa" (SAMPIERI; COLLADO; LUCIO, 2013, p. 195). A amostra foi selecionada a partir de um processo de quatro etapas, seguindo a ordem descrita a seguir.

A primeira etapa consistiu em localizar nas bases de dados publicações que possuíssem os termos '*security by design*' ou *'secure by design'* em seu título, resumo ou palavras-chave. Com essa busca, foram obtidos os seguintes resultados: 537 artigos na *Scopus*, 365 artigos na *Web of Science* e 501 artigos na *ProQuest*, totalizando 1403 artigos.

Na segunda etapa foram aplicados os limitadores de pesquisa, excluindo as publicações fora do período entre 2018 e 2022 e limitando em apenas publicações do tipo artigo acadêmico. A escolha desse período contemplou os cinco anos mais recentes e que estavam concluídos antes da publicação deste estudo. Também foram excluídos artigos com acesso negado pelo periódico. Foi obtido o seguinte resultado após a filtragem: 71 artigos na *Scopus*, 90 artigos na *Web of Science* e 56 artigos na *ProQuest*, totalizando 217 artigos.

Na terceira etapa foram removidos os artigos repetidos presentes em mais de uma base de dados, conservando-os onde foram encontrados pela primeira vez, resultando em: 71 artigos na *Scopus*, 21 artigos na *Web of Science* e 5 artigos na *ProQuest*, totalizando 97 artigos.

Na quarta etapa foi feita uma breve leitura do corpo completo de cada artigo a fim de retirar da amostra artigos que não possuíam uma estrutura de artigo completa

(introdução, desenvolvimento, conclusão, resumo e palavras-chave) e artigos onde o uso do termo não foi usado de acordo com a definição de *security by design* proposta pela CSA (2017), citada na seção 2.2, ou onde o termo foi citado brevemente e não foi desenvolvido no texto. Após essa última etapa, chegou ao resultado final de 56 artigos na *Scopus*, 18 artigos na *Web of Science* e 2 artigos na *ProQuest*, totalizando 76 artigos. A Figura 1 ilustra o processo e os resultados provenientes de cada etapa, chegando ao resultado final de 76 artigos. A relação final dos artigos se encontra no Apêndice B ao final do estudo.

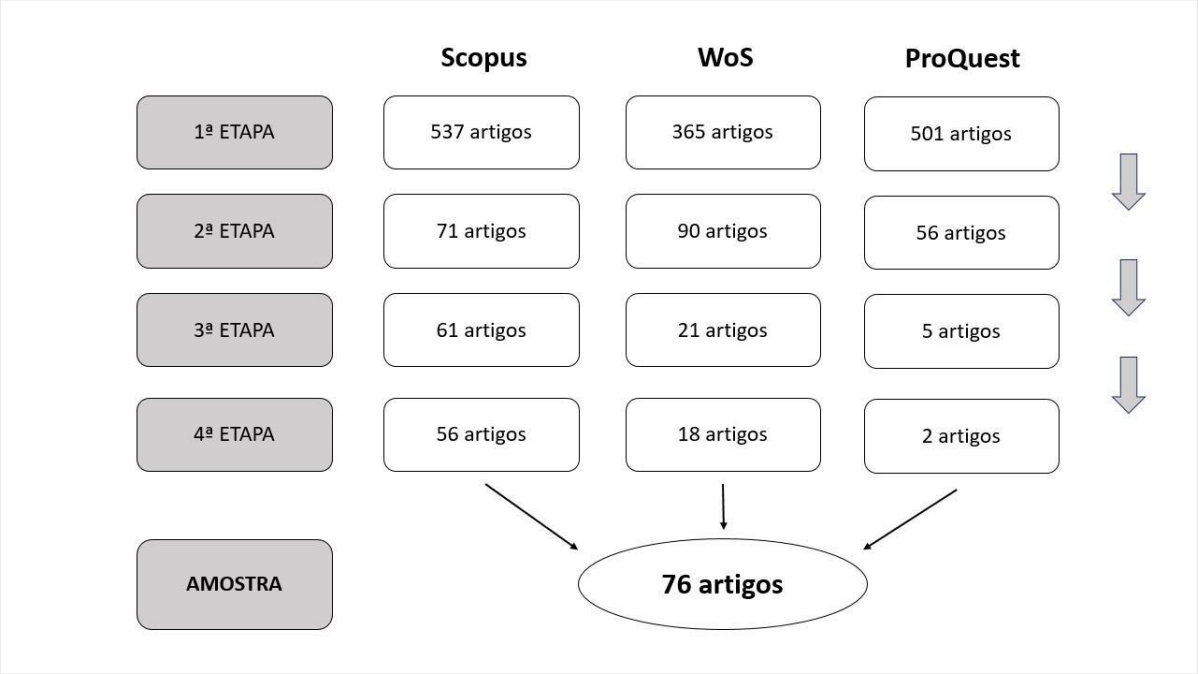

FIGURA 1 - Etapas para seleção da amostra
Fonte: Elaborada pelo autor e inspirado em ROSSI JUNIOR (2018).
Legenda: WoS significa '*Web of Science*'.

3.4. Procedimentos de coleta e de análise de dados

A amostra de artigos do presente trabalho foi coletada ao longo do período entre as datas de 23 de fevereiro de 2023 e 29 de abril de 2023, na cidade de Brasília-DF. A coleta de dados se deu pelo uso de três diferentes bases de dados relacionadas ao Portal de Periódicos da Capes, como foi citado na seção 3.3, sendo elas as seguintes bases: Scopus - Elsevier, Web of Science e ProQuest.

Para realizar a análise de dados da amostra, foram utilizadas a técnica de estatística descritiva, a técnica de elaboração de nuvem de palavras e a implementação da análise de conteúdo com o intuito de verificar a presença e ausência de princípios de sec*urity by design* em cada um dos textos que compõem a amostra. A sequência detalha cada uma das técnicas utilizadas para análise de dados neste estudo.

A estatística descritiva foi utilizada seguindo a definição de Akamine e Yamamoto (2013, p.2), descrevendo-a como "a parte da estatística que trabalha com organização e apresentação de dados". Nesse sentido, foram utilizados gráficos, tabelas, quadros e indicadores baseados na contagem de frequência e exibição de percentuais para realização da análise de dados.

A elaboração de nuvem de palavras tem como objetivo representar visualmente a frequência em que são mencionadas as palavras-chave nos textos da amostra, sendo um indicador dos principais assuntos e conceitos abordados nesses textos de maneira geral (ATENSTAEDT, 2012).

A análise de conteúdo empregada no estudo segue a metodologia proposta por Bardin (1977), analisando cada artigo e utilizando como regra de enumeração a presença ou ausência dos princípios de *security by design* usados como referência para o trabalho presentes no Apêndice A e baseados no OWASP (2016), como foi citado na Seção 2.2. Como o Apêndice B possui 10 categorias e a amostra é composta *por 76 ar*tigos, desta maneira foram feitas 760 verificações de princípios no total.

É importante frisar que um artigo pode ter a presença de mais de um ou mesmo nenhum dos dez princípios. A verificação foi feita por meio da leitura de todo o corpo do artigo. A classificação foi feita a partir de duas estratégias. A primeira delas foi verificar a quantidade de artigos que abordam cada princípio, identificando os princípios mais abordados pelos autores em um *ranking*. A segunda estratégia foi a segmentação da amostra de acordo com a quantidade de princípios abordados em cada artigo, permitindo identificar o volume total de princípios utilizados por cada autor em sua pesquisa, separadamente.

Por fim, foi utilizado o Microsoft Excel para realizar a confecção de gráficos e tabelas para demonstração visual dos resultados originados das análises estatísticas da amostra e para construção dos quadros com os resultados da análise de conteúdo.

O sofware WordClouds.com[3], também, foi utilizado com o intuito de construir a nuvem de palavras-chave. Para construção da nuvem de palavras-chave foram consideradas todas as palavras-chave presentes nos artigos.

[3] Disponível em https://www.wordclouds.com.

4. RESULTADOS E DISCUSSÃO

O presente capítulo trata a respeito dos resultados e discussões do trabalho. A Seção 4.1 mostra a quantidade de artigos publicados por ano de publicação. A Seção 4.2 mostra a quantidade de instituições às quais os autores dos artigos estão afiliados, segmentada por continente. A Seção 4.3 mostra a quantidade de artigos publicados por periódico. A Seção 4.4 mostra a quantidade de artigos publicados por filiação acadêmica ou instituição pela qual os autores são filiados. A Seção 4.5 mostra a segmentação de artigos por seu número de autores. A Seção 4.6 mostra a segmentação dos artigos por abordagem metodológica. A Seção 4.7 mostra a análise de conteúdo mapeando a presença de princípios relacionados à *security by design* nos artigos da amostra. A Seção 4.8 mostra a análise da distribuição de palavras-chave da amostra.

4.1. Quantidade de artigos por ano de publicação

Esta subseção busca apresentar os resultados para subsidiar o atendimento do Objetivo Específico 1 (OE1): identificar a produção de artigos científicos por ano de publicação. Inicialmente, a Figura 2 mostra a quantidade de artigos por ano de publicação. É possível perceber uma variação entre os anos. Enquanto o ano de 2019 apresentou 10 artigos (13,16% da amostra), em 2022 houve a presença de 21 artigos (27,63% da amostra). A partir dos dados da Figura 2, é possível afirmar, também, que houve uma diferença entre a quantidade de artigos produzidos entre o ano de 2018 (13 artigos) e a quantidade de artigos produzida no ano final de 2022 (21 artigos). Considerando os anos de 2020 a 2022, verificam-se 53 artigos publicados, totalizando 69,74% dos artigos da amostra.

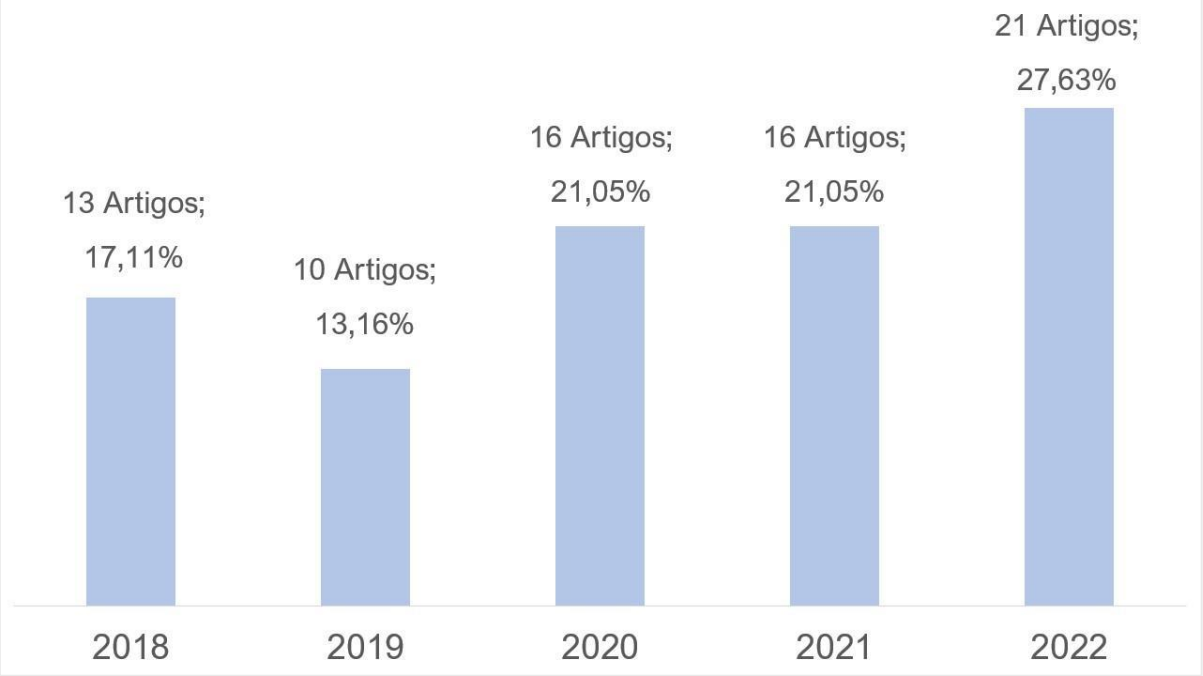

FIGURA 2 - Produção de artigos por ano no período entre 2018 e 2022
Fonte: Elaborada pelo autor, a partir dos dados da pesquisa.
Legenda: o valor de 100% representa todos os 76 artigos da amostra.

4.2. Quantidade de instituições às quais os autores dos artigos estão afiliados, segmentada por continente

Esta subseção tem como objetivo apresentar os resultados para atender o Objetivo Específico 2 (OE2): verificar a distribuição de instituições às quais os autores estão filiados, segmentadas por continente. A Figura 3 mostra a quantidade de instituições por continente no qual estão localizadas geograficamente com o intuito de analisar onde estão concentradas as pesquisas relacionadas ao tema. Foram contabilizadas 144 instituições as quais os autores dos artigos da amostra estão vinculados. O continente isolado com a maior número de instituições é a Europa, onde estão localizadas 100 das 144 instituições, representando 69,44% do total, seguida pela Ásia e Oceania com um total de 28 instituições, representando 19,44% do total. Os continentes com menos instituições são a África e a América do Sul, com 4 (2,78% do total) e 3 (2,08% do total) instituições respectivamente, o que pode indicar a oportunidade de se avançar estudos sobre o tema em instituições nos países africanos e sul-americanos.

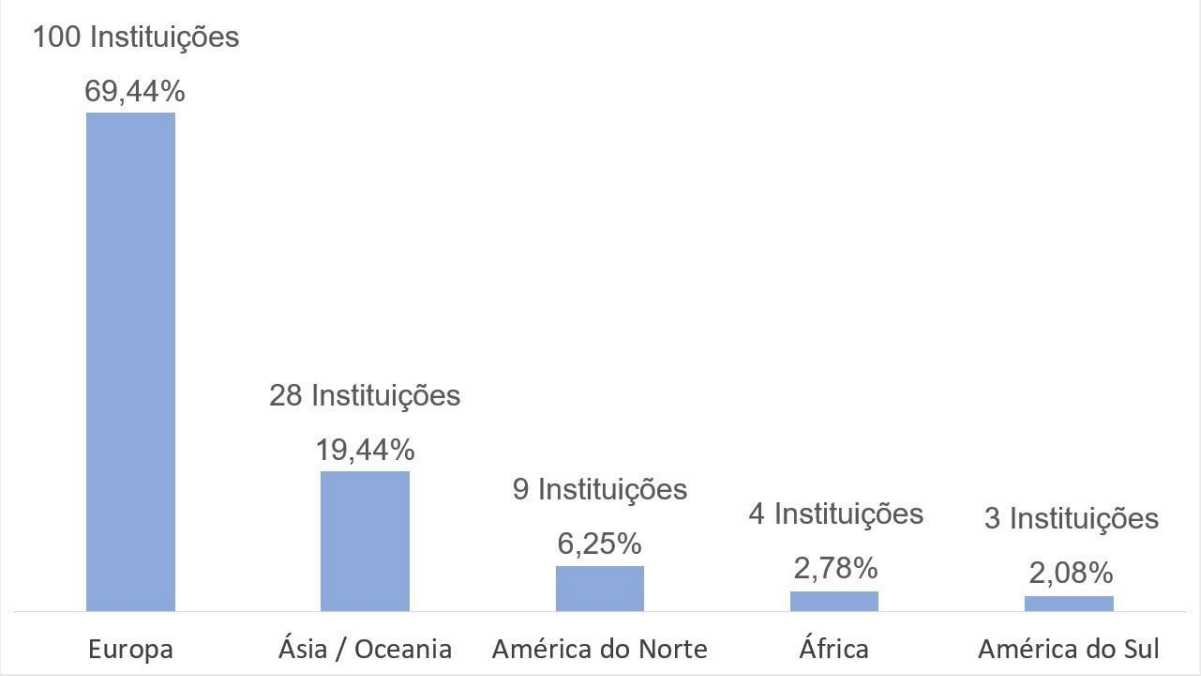

FIGURA 3 - Quantidade de instituições por continente
Fonte: Elaborada pelo autor, a partir dos dados da pesquisa.
Legenda: o valor de 100% representa todas as 144 instituições.

Em relação ao continente norte americano, não foram encontradas muitas instituições estadunidenses, apesar de o país ser sede de instituições de grande renome no assunto e que desenvolvem padrões de segurança cibernética reconhecidos como referência e implementados em diversos países. Mesmo possuindo uma das instituições de maior produção, a *Florida Atlantic University* situada em Boca Raton na Flórida, a quantidade final de instituições do continente norte-americano no levantamento chega ao total de 9 instituições (6,25% do total).

4.3. Quantidade de artigos publicados por periódico

Esta subseção tem o intuito de, por meio de seus resultados, atender o Objetivo Específico 3 (OE3): verificar a distribuição de artigos produzidos conforme o periódico em que foram publicados. A Tabela 1 mostra a quantidade de artigos publicados por cada periódico acadêmico e sua percentagem de participação na amostra. Os 76 artigos que compõem a amostra foram publicados em 56 periódicos diferentes. Dois periódicos possuem um número de publicações de 7 artigos: o *IEEE Access* e o *Sensors*, sendo responsáveis individualmente pela publicação de 9,21% dos artigos,

totalizando juntos 18,42% de participação na amostra. Outros dois periódicos apresentaram um número de publicações de 3 artigos cada, o *IEEE Transactions on Industrial Informatics* e o *Future Generation Computer Systems*, com 3,95% de participação individual da amostra, possuindo juntos 7,89% de participação na amostra total.

TABELA 1 - Quantidade de artigos por periódico

Periódico	Quantidade de artigos publicados	Percentagem de participação na amostra
IEEE Access	7	9,21%
Sensors	7	9,21%
IEEE Transactions on Industrial Informatics	3	3,95%
Future Generation Computer Systems	3	3,95%
Software Quality Journal	2	2,63%
Cybersecurity	2	2,63%
Journal of Systems and Software	2	2,63%
Computers and Security	2	2,63%
Demais 48 periódicos (1 artigo cada)	48	63,16%
Total	76	100,00%

Fonte: Dados da pesquisa.

Quatro periódicos apresentaram um número de publicações de 2 artigos cada, o *Software Quality Journal*, o *Cybersecurity*, o *Journal of Systems and Software* e o *Computers and Security*, com 3,95% de participação individual na amostra, possuindo juntos 7,89% de participação na amostra. Os demais periódicos, 48 de 56 deles, possuem um número de publicações de apenas 1 artigo cada com 1,32% de participação individual na amostra, possuindo juntos 63,16% de participação na amostra.

4.4. Quantidade de artigos publicados por filiação acadêmica

A subseção 4.4 visa apresentar os resultados a fim de atender o Objetivo Específico 4 (OE4): averiguar a quantidade de artigos produzidos conforme a filiação acadêmica. Os 76 artigos que compõem a amostra foram produzidos por autores filiados a 144 diferentes instituições. A Tabela 2 descreve a quantidade de aparições dessas instituições nos artigos. Existem 3 instituições que possuem participação em três artigos, representando 2,08% do total de instituições: Florida Atlantic University, University of Campania Luigi Vanvitelli e a University of Haifa. As instituições com participação em dois artigos totalizam 18, representando 12,50% do total de instituições. Verifica-se que 123 de 144 instituições, possui participação em apenas um artigo, representando 85,42% do total de instituições.

TABELA 2 - Quantidade de participações por instituição

Instituições	Quantidade de participações	percentagem das instituições
Florida Atlantic University / University of Campania Luigi Vanvitelli / University of Haifa	3 participações	2,08%
Aristotle University of Thessaloniki / Athens University of Economics & Business / Centre for Research & Technology Hellas / CNR-IIT / Cranfield University / ITMO University / Menofia University / Radboud University Nijmegen / SPC RAS / Universidade de Santiago de Compostela / University College London / University of Brighton / University of Castilla-La Mancha / University of Charles Darwin / University of Naples Federico II / University of Sannio / University of the Aegean / Uppsala University	2 participações	12,50%
Demais 123 instituições	1 participação	85,42%

Fonte: Dados da pesquisa.
Legenda: o valor de 100% representa todas as 144 instituições.

4.5. Segmentação de artigos conforme a quantidade de autores

O propósito desta subseção é fornecer os resultados para auxiliar o atendimento do Objetivo Específico 5 (OE5): segmentar os artigos conforme a quantidade de

autores. A Tabela 3 expõe a segmentação dos artigos da amostra de acordo com a quantidade de autores que o produziram. É possível observar 3 artigos produzidos por um autor, representando 3,95% da amostra. Os artigos que possuem dois autores totalizaram 11, representando 14,47% da amostra. Os artigos que possuem 3 autores totalizaram 22, representando 28,95% da amostra e sendo a categoria com o maior número de artigos. Os artigos que possuem quatro autores, a segunda maior categoria em número de artigos, totalizaram 21, representando 27,63% da amostra. Os artigos que possuem cinco ou mais autores totalizaram 19, representando 25,00% da amostra. Assim, artigos com 3 ou mais autores totalizam 81,58% da amostra.

TABELA 3 - Segmentação de artigos por quantidade de autores

Quantidade de autores	Quantidade de artigos	Percentagem da amostra
5 ou mais autores	19	25,00%
4 autores	21	27,63%
3 autores	22	28,95%
2 autores	11	14,47%
1 autor	3	3,95%
Total	76	100,00%

Fonte: Dados da pesquisa.

4.6. Segmentação por abordagem metodológica

O enfoque desta subseção é apresentar os resultados para apoiar o alcance do Objetivo Específico 6 (OE6): categorizar os artigos conforme a abordagem metodológica utilizada. A Figura 6 expõe a segmentação dos artigos da amostra conforme a abordagem metodológica utilizada. A categorização foi feita por meio dos critérios propostos por Sampieri, Collado e Lucio (2013). A abordagem quantitativa totalizou o número de 6 artigos, representando 7,89% do total da amostra. A abordagem qualitativa totalizou o número de 34 artigos, representando 44,74% do total da amostra. A abordagem mista, ou quali-quantitativa, totalizou o número de 36 artigos, representando 47,37% do total da amostra e sendo a categoria com a maior quantidade de artigos.

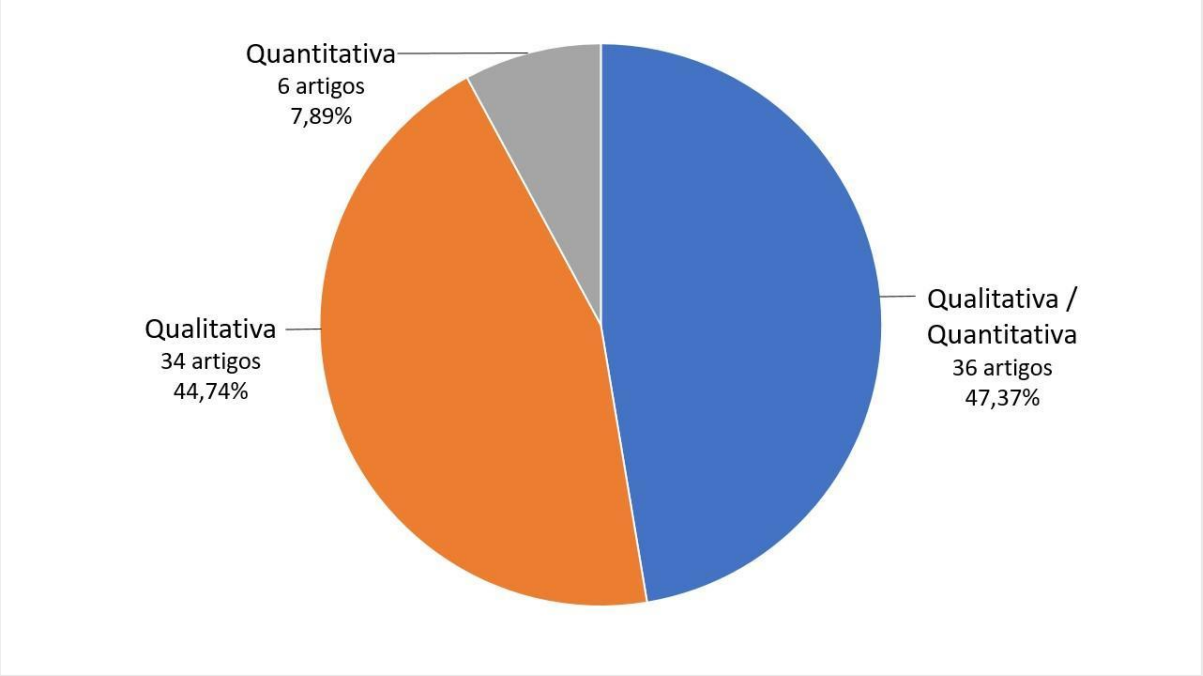

FIGURA 4 - Quantidade de artigos por abordagem metodológica
Fonte: Elaborada pelo autor, a partir dos dados da pesquisa.

Legenda: o valor de 100% representa todos os 76 artigos da amostra.

4.7. Mapeamento da presença de princípios de *security by design* nos artigos da amostra

O propósito desta subseção é oferecer resultados que contemplem o alcance do Objetivo Específico 7 (OE7): mapear a presença de princípios relacionados à *security by design* nos artigos da amostra. A Tabela 4 apresenta o número de artigos que abordam cada princípio de *security by design* propostos pela OWASP (2016) a percentagem de presença desses princípios no total de artigos da amostra. A identificação da presença e ausência dos princípios foi feita por meio da análise de conteúdo explicada na Seção 3.4 do presente estudo, e os resultados detalhados dessa análise constam do Apêndice C.

TABELA 4 - Quantidade de artigos com presença e ausência de cada princípio

Princípio	Número de presença em artigos	Percentagem de presença na amostra	Número de ausência em artigos	Percentagem de ausência na amostra
Minimize a área de superfície de ataque	61	80,26%	15	19,74%
Estabeleça padrões seguros	52	68,42%	24	31,58%
Aplique a defesa em profundidade	42	55,26%	34	44,74%
Conceda privilégio mínimo	35	46,05%	41	53,95%
Separação de tarefas	22	28,95%	54	71,05%
Falhe seguramente	18	23,68%	58	76,32%
Mantenha a segurança simples	18	23,68%	58	76,32%
Não confie nos serviços	15	19,74%	61	80,26%
Evite a segurança por obscuridade	10	13,16%	66	86,84%
Corrija problemas de segurança corretamente	8	10,53%	68	89,47%

Fonte: Dados da pesquisa.
Legenda: a soma das percentagens de cada linha representa 100% dos princípios em cada artigo.

A Tabela 4 apresenta todos os princípios de maneira ordenada, partindo do princípio com presença na maior quantidade artigos para os princípios com presença em uma menor quantidade. O princípio “Minimize a área de superfície de ataque” esteve presente em 61 dos 76 artigos (80,26% da amostra), o princípio “Estabeleça padrões seguros” esteve presente em 52 artigos (68,42% da amostra) e o princípio “Aplique a defesa em profundidade” esteve presente em 42 artigos (55,26% da amostra). O princípio “Corrija problemas de segurança corretamente” esteve presente em 8 artigos (10,53% da amostra).

O princípio “Minimize a área de superfície de ataque”, citado na Tabela 4, transmite a ideia de que que cada recurso adicionado a uma aplicação traz consigo um risco adicional e consequentemente uma expansão da área de superfície de ataque, sendo o objetivo do desenvolvimento seguro diminuir o risco geral ao diminuir a área de superfície de ataque (OWASP, 2016). O princípio se encontra na própria definição da abordagem *security by design* utilizada como referência para este trabalho a qual afirma que a abordagem “busca minimizar as vulnerabilidades do sistema ao reduzir a superfície de ataque [...]” (CSA, 2017, p.4).

O princípio “Estabeleça padrões seguros”, citado, também, na Tabela 4, transmite a ideia de que a experiência do usuário deve ser segura por padrão, cabendo ao usuário abrir mão da segurança, caso seja permitido, e o princípio "Aplique a defesa em profundidade" transmite a ideia da importância de usar múltiplos controles que abordem o risco de maneiras diferentes (OWASP, 2016). Esses princípios foram previamente citados no referencial teórico e constam, também, do Apêndice A.

A Tabela 5 apresenta a segmentação dos artigos por quantidade de princípios presentes e princípios ausentes. Os artigos com a presença de até 2 princípios totalizaram 20, representando 26,32% da amostra. Os artigos que com a presença de 3 a 4 princípios totalizaram 29, representando 38,16% da amostra. Os artigos com a presença de 5 a 6 princípios totalizaram 21, representando 27,63% da amostra. Os artigos que com a presença de 7 a 10 princípios totalizaram 6, representando 7,89% da amostra.

TABELA 5 - Quantidade de artigos considerando o número de princípios

quantidade de princípios presentes	quantidade de artigos	Percentagem da amostra
Até 2 princípios	20	26,32%
De 3 a 4 princípios	29	38,16%
De 5 a 6 princípios	21	27,63%
De 7 a 10 princípios	6	7,89%
Total	76	100,00%

Fonte: Dados da pesquisa.

Em complemento, o Apêndice C, presente no final deste estudo, ilustra de forma detalhada a presença e ausência dos dez princípios citados por OWASP (2016) em cada um dos artigos que compõem a amostra.

4.8. Distribuição de palavras-chave dos artigos

Em última análise, a subseção 4.8 tem como objetivo apresentar os resultados que subsidiem o atendimento do Objetivo Específico 8 (OE8): identificar a distribuição de palavras-chave nos artigos da amostra. Foram identificadas 340 palavras-chave

diferentes nos artigos da amostra antes de serem tratadas. As palavras-chave *'security by design*', *'secure by design'* e sinônimos, bem como palavras-chave que os incluem foram posteriormente retiradas pelo fato dos termos terem sido utilizadas para a busca nas bases de dados. Após o processo de retirada, chegou-se a quantidade de 333 palavras-chave diferentes.

Para melhor analisar a representatividade dos termos, foram identificadas as palavras-chave sinônimas, unificando-as para que seus pesos fossem contabilizados de forma conjunta. O mesmo foi feito com as siglas e suas formas por extenso. Ao final, chegou-se ao número final de 254 palavras-chave diferentes, constatando-se que 198 palavras-chave obtiveram apenas uma aparição.

A Figura 8 apresenta a nuvem de palavras construída a partir das palavras-chave provenientes dos 76 artigos que compõem a amostra, onde o tamanho de cada palavra é proporcional à sua frequência de aparições. Foram consideradas na nuvem de palavras apenas as palavras-chave com duas ou mais aparições, sendo composta por um total de 56 palavras.

Por fim, a palavra-chave que obteve maior frequência foi 'IoT' (*Internet of Things*) com 36 aparições, seguida por '*security*' com 14 e '*cybersecurity*' com 10 aparições. A palavra-chave '*cyber-physical systems*' obteve 8 aparições e '*privacy*' obteve 7 aparições. Duas palavras-chave obtiveram 6 aparições, '*cloud computing*' e '*data protection*'. A palavra-chave '*energy*' obteve 5 aparições. Seis palavras-chave obtiveram 4 aparições, dentre elas '*privacy by design*', reforçando a ideia de uma relação entre os termos *security by design* e *privacy by design* mencionado por Cavoukian e Dixon (2013). Quatorze palavras-chave obtiveram 3 aparições, vinte e oito obtiveram 2 aparições.

FIGURA 5 - Nuvem de palavras-chave dos artigos da amostra
Fonte: Elaborada pelo autor por meio do software WordClouds.com, a partir dos dados da pesquisa.
Legenda de siglas selecionadas: IEC - *International Electrotechnical Commission*; IoT - *Internet of Things*; IT - *Information Technology;* SDLC - *Software Development Life Cycle;* UAV - *Unmanned Aerial Vehicle.*

5. CONCLUSÕES E RECOMENDAÇÕES

O presente capítulo apresenta as conclusões e recomendações do trabalho, o qual possui o objetivo geral de descrever a produção de artigos científicos com o tema *security by design* presente em bases de dados acadêmicas no período de 2018 a 2022. Para este fim, foi realizada uma pesquisa descritiva, utilizando-se da abordagem qualitativa e quantitativa para análise dos dados. A amostra possui caráter não probabilístico e é formada por 76 artigos provenientes das bases de dados *Scopus*, *Web of Science* e *ProQuest* por meio de acesso disponibilizado pelo Portal de Periódicos da CAPES. A análise dos dados foi feita por meio de estatística descritiva, análise de conteúdo e análise de nuvem de palavras. Os resultados do estudo possibilitaram o alcance do objetivo geral presente na Seção 1.3 e de todos os objetivos específicos estabelecidos na Seção 1.4 do presente estudo.

O primeiro objetivo específico (OE1) foi identificar a produção de artigos científicos por ano de publicação, sendo alcançado na Seção 4.1 do presente estudo. No ano de 2018, foram produzidos 13 artigos (17,11% da amostra), seguido de 10 artigos (13,16% da amostra) no ano de 2019. Os anos de 2020 e 2021 obtiveram, cada um deles, a produção de 16 artigos (21,05% da amostra). Por último, o ano de 2022 obteve o maior número de artigos com 21 produzidos (27,63% da amostra). Verificam-se 53 artigos (69,74% da amostra) publicados nos anos de 2020 a 2022.

O segundo objetivo específico (OE2) foi verificar a distribuição de instituições às quais os autores estão filiados, segmentadas por continente, sendo alcançado na Seção 4.2 do presente estudo. 100 das 144 instituições (69,44% do total) se encontram no continente europeu. A Ásia e Oceania obtiveram o número de 28 instituições (19,44% do total de instituições). A América do Norte obteve 9 instituições (6,25% das instituições), a África obteve 4 (2,78% do total de instituições) e a América do Sul, obteve 3 (2,08% do total de instituições).

O terceiro objetivo específico (OE3) foi verificar a distribuição de artigos produzidos conforme o periódico em que foram publicados, sendo alcançado na Seção 4.3 do presente estudo. Os artigos da amostra foram publicados em 56 periódicos diferentes. O *IEEE Access* e o *Sensors* publicaram 7 artigos (9,21% da amostra) cada. Outros dois periódicos publicaram 3 artigos (3,95% da amostra) cada, o *IEEE Transactions on Industrial Informatics* e o *Future Generation Computer*

Systems. Quatro periódicos publicaram 2 artigos (2,63% da amostra) cada e os demais 48 periódicos publicaram apenas 1 artigo (1,32% da amostra) cada.

O quarto objetivo específico (OE4) foi averiguar a quantidade de artigos produzidos conforme a filiação acadêmica, sendo alcançado na Seção 4.4 do presente estudo. Das 144 instituições, 3 possuem participação em três artigos, representando 2,08% do total de instituições: Florida Atlantic University, University of Campania Luigi Vanvitelli e a University of Haifa. As instituições com participação em dois artigos totalizam 18 (12,50% do total) e 123 instituições (85,42% do total) possuem participação em apenas um artigo.

O quinto objetivo específico (OE5) foi segmentar os artigos conforme a quantidade de autores, sendo alcançado na Seção 4.5 do presente estudo. Poucos artigos foram produzidos por apenas um único autor, totalizando 3 artigos (3,95% da amostra). Os artigos com dois autores totalizaram 11 (14,47% da amostra). Os artigos com três autores totalizaram 22 (28,95% da amostra). A categoria de artigos com 4 autores totalizou 21 artigos (27,63% da amostra). Os artigos com 5 ou mais autores totalizaram 19 (25,00% da amostra). Artigos com 3 ou mais autores totalizam 81,58% da amostra.

O sexto objetivo (OE6) específico foi categorizar os artigos conforme a abordagem metodológica utilizada, sendo alcançado na Seção 4.6 do presente estudo. A abordagem quantitativa totalizou o número de 6 artigos (7,89% da amostra), sendo a menos expressiva em número de artigos. A abordagem qualitativa totalizou o número de 34 artigos (44,74% da amostra). A abordagem metodológica com a maior quantidade de artigos foi a quali-quantitativa com 36 artigos (47,37% da amostra).

O sétimo objetivo específico (OE7) foi mapear a presença de princípios relacionados à *security by design* nos artigos da amostra, sendo alcançado na Seção 4.7 do presente estudo. O princípio “Minimize a área de superfície de ataque” esteve presente em 61 artigos (80,26% da amostra), “Estabeleça padrões seguros” esteve presente em 52 artigos (68,42% da amostra) e o princípio “Aplique a defesa em profundidade” esteve presente em 42 artigos (55,26% da amostra). O princípio “Corrija problemas de segurança corretamente” esteve presente em 8 artigos (10,53% da amostra).

Em relação a quantidade de princípios encontrados por artigo, 20 artigos (26,32% da amostra) abordaram até 2 princípios, 29 artigos (38,16% da amostra)

abordaram de 3 a 4 princípios, 21 artigos abordaram de 5 a 6 princípios (27,63% da amostra), 6 artigos abordaram de 7 a 10 princípios (7,89% da amostra).

Por fim, o oitavo objetivo específico (OE8) foi identificar a distribuição de palavras-chave nos artigos da amostra, sendo alcançado na Seção 4.8 do presente estudo. Ao final, foram contabilizadas 254 palavras-chave diferentes. A palavra-chave que obteve a maior frequência foi a 'IoT' com 36 aparições, seguida por '*security*' com 14, '*cybersecurity*' com 10, '*cyber-physical systems*' com 8 e '*privacy*' com 7 aparições. Duas palavras-chave obtiveram 6 aparições, '*cloud computing*' e '*data protection*' e a palavra '*energy'* obteve 5 aparições.

Ao contemplar todos os objetivos específicos, foi possível alcançar o objetivo geral do estudo descrito na Seção 1.3. Por meio do presente trabalho, foi possível descrever a produção de artigos científicos com o tema *security by design* presente em bases de dados acadêmicas no período de 2018 a 2022 através de um estudo descritivo, análise de conteúdo e análise bibliométrica. O estudo identificou que a produção de artigos acadêmicos não foi uniforme, apurando-se 69,74% da amostra publicada de 2020 a 2022. O continente europeu foi a sede de 69,44% das instituições as quais os autores estão filiados. Os periódicos com mais publicações foram o *IEEE Access* e o *Sensors* com 7 artigos cada. Houve 81,58% dos artigos escritos por três ou mais autores. A abordagem metodológica mais utilizada foi a quali-quantitativa e a palavra-chave com o maior número de aparições foi 'IoT' (*Internet of Things*).

Em adição, três princípios OWASP apareceram em mais de 50,00% dos artigos da amostra: “Minimize a área de superfície de ataque” (80,26% da amostra), “Estabeleça padrões seguros” (68,42% da amostra) e “Aplique a defesa em profundidade” (55,26% da amostra). A distribuição de palavras-chave indicou 'IoT' com 36 aparições, 'security' com 14 aparições, 'cybersecurity' com 10 aparições.

O presente trabalho contribui para o campo acadêmico ao proporcionar informações bibliométricas referentes a produção de artigos acadêmicos que tratam do tema dentro do período estudado. Analisa a distribuição da produção ao longo dos anos, principais periódicos de publicação e instituições, continentes com maior número instituições as quais os autores estão filiados, qual abordagem metodológica mais comum e análise da distribuição de palavras-chave identificando temas correlatos. O presente trabalho também contribui ao identificar os princípios de *security by design* da OWASP (2016) mais abordados na amostra por meio da análise de conteúdo.

O estudo também proporciona aos gestores um panorama de como se encaminha a discussão no meio acadêmico, servindo como base para conhecimento dos principais autores e instituições que tratam do assunto para que estejam aptos a aplicar o conhecimento proveniente dos mais atuais estudos e serem capazes de direcionar e liderar processos de desenvolvimento de *softwares* cada vez mais seguros.

As recomendações para futuros trabalhos são as seguintes:

- desenvolver estudos semelhantes a fim de comparação para uma análise mais rica da produção por meio de um horizonte temporal mais extenso;
- realizar estudo semelhante utilizando-se de diferentes bases de dados;
- realizar um estudo que aborde a relação do tema com o conceito de *IoT*, o qual obteve destaque na análise da distribuição de palavras-chave;
- realizar estudo bibliométrico abordando conceitos correlatos como *privacy by design* e *Secure Software Development Lifecycle*;
- realizar um estudo que identifique a utilização do termo *security by design* traduzido para outras línguas além do inglês, como para o português e espanhol, assim como analisar a produção científica de trabalhos acadêmicos que abordem os conceitos encontrados;
- Analisar a produção científica sobre *security by design* comparando os estudos publicados no Brasil com aqueles que são publicados no exterior; e
- realizar um estudo que analise como a interação entre variáveis, como crenças normativas, baixo controle de engenharia e limitada percepção de responsabilidade podem afetar o desenho de sistemas seguros.

REFERÊNCIAS

AGRAFIOTES, I.; NURSE, J.R. C.; UPTON, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 2018, 1–15 Oxford University Press, Oxford, 2018. Disponível em: https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288. Acesso em: 29 mar 2023.

AKANIME, C. T.; YAMAMOTO, R. K. Estudo Dirigido de Estatística Descritiva. São Paulo: Editora Saraiva, 2013. ISBN 9788536517780. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536517780/. Acesso em: 12 jun. 2023.

ALMIND, T. C.; INGWERSEN, P. Informetric analyses on the world wide web: methodological approaches to “webometrics”. Journal of Documentation, v. 53, n. 4, p. 404–426, 1997.

ANDERSON, R. Why Information Security is Hard - An Economic Perspective. In: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC '01). IEEE Computer Society, 2001.

ANDERSON, R.; MOORE, T. The Economics of Information Security. Science, v. 314, n. 5799, p. 610–613, 2006.

ARAÚJO, C. A. Bibliometria: evolução histórica e questões atuais. Em Questão, Porto Alegre, v. 12, n. 1, p. 11–32, 2006.

ATENSTAEDT, R. Word cloud analysis of the BJGP. British Journal of General Practice, v. 62, n. 596, p. 148–148, mar. 2012. DOI: https://doi.org/10.3399/bjgp12X630142

BARDIN, L. Análise de conteúdo. Tradução de Luís Antero Reto e Augusto Pinheiro. Lisboa: Edições 70, 1977.

BROADUS, R. N. Early approaches to bibliometrics. v. 38, n. 2, p. 127–129, 1 mar. 1987a.

BROADUS, R. N. Toward a definition of “bibliometrics”. Scientometrics, v. 12, n. 5, p. 373–379, 1 nov. 1987b.

CASOLA, V.; BENEDICTIS, A.D.; RAK, M.; VILLANO, U. A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. Journal of Systems and Software, Volume 163, 2020. Elsevier Inc, 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0164121220300042?via%3Dihub. Acesso em: 29 mar 2023.

CASOLA, V.; BENEDICTIS, A.D.; RAK, M.; VILLANO, U. Security-by-design in clouds: a Security-SLA driven methodology to build secure cloud applications. Procedia Computer Science. 97. 53-62. Madrid, Spain, 2016.

CAVOUKIAN, A.; DIXON, M. Privacy and Security by Design: An Enterprise Architecture Approach. Information and Privacy Commissioner. Toronto, Ontario, Canadá, 2013. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf. Acesso em: 29 mar 2023.

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/article/835.

CYBER SECURITY AGENCY OF SINGAPORE (CSA). Security-by-Design Framework. Singapore, 09 November 2017. Disponível em: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf?sfvrsn=560b9ff3_0>. Acesso em: 09 abr. 2021.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default. Arlington, Virginia: CISA, 2023. Disponível em: https://www.cyber.gov.au/about-us/view-all-content/publications/principles-and-approaches-for-security-by-design-and-default. Acesso em: 2 mai. 2023.

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT. Secure by Design: Improving the cyber security of consumer Internet of Things Report. United Kingdom, 2018. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973926/Secure_by_Design_Report__V2.pdf.

DONTHU, N.; KUMAR, S.; MUKHERJEE, D.; PANDEY, N.; LIM, W. M. How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, v. 133, p. 285–296, set. 2021. DOI: 10.1016/j.jbusres.2021.04.070.

DUPONT, B. Cybersecurity Futures: How Can We Regulate Emergent Risks? Technology Innovation Management Review, v. 3, n. 7, p. 6–11, 2013. Disponível em: https://timreview.ca/article/700. Acesso em 10 abr 2023.

EUROPEAN UNION. Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Brussels, Belgium: European Commission, 2022. Disponível em: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. Acesso em: 06 maio 2023.

FISCHER, E. A. Cybersecurity Issues and Challenges: In Brief. Congressional Research Service, Washington, D.C., U.S., 2016. Disponível em: https://sgp.fas.org/crs/misc/R43831.pdf. Acesso em: 19 abr 2023.

GLÄNZEL, W. Bibliometrics as a research field: A course on theory and application of bibliometric indicators. Course Handouts, 2003.

GOERTZEL, K. M.; WINOGRAD, T.; MCKINLEY, H. L.; OH, L.; COLON, M.; MCGIBBON, T.; FEDCHAK, E.; VIENNEAU, R. Software Security Assurance: A State-of-the-Art Report (SOAR). Herndon, Virginia, United States of America: IATAC, 2007.

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.

ISO/IEC. ISO/IEC 27032:2012 - Information technology — Security techniques — Guidelines for cybersecurity. 1st ed. Geneva: ISO, 2012. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. Acesso em: 19 abr 2023.

ISO/IEC. ISO/IEC 27034-1:2011 - Tecnologia da informação - Técnicas de segurança - Gestão de segurança de aplicações. Genebra: ISO, 2011. Disponível em: https://www.iso.org/standard/44378.html.

ISO/IEC. ISO/IEC 27000:2009 - Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO/IEC, 2009. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-1:v1:en. Acesso em: 25 abr 2023.

KANG, S.; KIM, S. CIA-level driven secure SDLC framework for integrating security into SDLC process. Journal of Ambient Intelligence and Humanized Computing 13, 4601–4624, 2022. DOI: 10.1007/s12652-021-03450-z.

LEE, K.-H.; PARK, Y. B. Adaption of Integrated Secure Guide for Secure Software Development Lifecycle. International Journal of Security and Its Applications, v. 10, n. 6, p. 145–154, 2016.

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.

MÄNTYLÄ, M. V.; ADAMS, B.; KHOMH, F.; ENGSTRÖM, E.; PETERSEN, K. On rapid releases and software testing: a case study and a semi-systematic literature review. Empirical Software Engineering, v. 20, n. 5, p. 1384–1425, 29 out. 2014.

MAURER, T.; MORGUS, R. Compilation of Existing Cybersecurity and Information Security Related Definitions. New America, 2014. Disponível em: http://www.jstor.org/stable/resrep10487. Acesso em: 19 abr 2023.

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, 2013. DOI: https://doi.org/10.18617/liinc.v9i1.558.

NATIONAL CYBER SECURITY CENTER (NCSC). Cyber security design principles. London, United Kingdom, 2019. Disponível em: https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1. U.S. Department of Commerce, 2018a. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em: 19 abr 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NISTIR 8074, Volume 2. U.S. Department of Commerce, 2015. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf. Acesso em: 29 mar 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for

Mitigating the Risk of Software Vulnerabilities. NIST SP 800-218. U.S. Department of Commerce, 2022.

NATIONAL INSTITUITE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. NIST 800-53. U.S Department of Commerce, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST SP 800-160 Volume 1. U.S. Department of Commerce, 2018b.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP). Security by Design Principles. Los Angeles, California, United States of América, 2016. Disponível em: https://wiki.owasp.org/index.php/Security_by_Design_Principles. Acesso em: 09 abr 2023.

OTLET, Paul. Tratado de documentação: o livro sobre o livro: teoria e prática. Tradução de Taiguara Villela Aldabalde et al. Brasília: Briquet de Lemos / Livros, 2018. 742 p. Disponível em: https://repositorio.unb.br/bitstream/10482/32627/1/LIVRO_TratadoDeDocumenta%c3%a7%c3%a3o.pdf.

OTTIS, R.; LORENTS, P. Cyberspace: Definition and Implications. International Conference on Information Warfare and Security, Reading, p. 267-XII, 04 2010.

PINHEIRO, P. P. Segurança Digital - Proteção de Dados nas Empresas. Barueri, São Paulo: Grupo GEN, 2020. E-book. ISBN 9788597026405. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 18 abr. 2023.

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

ROSSI JÚNIOR, Márcio. Crowdfunding: uma análise da produção científica em bases de dados de 2013 a 2017. 2018. 54 f. Trabalho de Conclusão de Curso (Bacharelado em Administração)—Universidade de Brasília, Brasília, 2018.

ROUSSEAU, R. Forgotten founder of bibliometrics. Nature, v. 510, n. 7504, p. 218, jun. 2014.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. D. P B. Metodologia de pesquisa. Porto Alegre: Grupo A, 2013. E-book. ISBN 9788565848367. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788565848367/. Acesso em: 03 jun. 2023.

SANTOS, R. N. M. D.; KOBASHI, N. Y. Bibliometria, cientometria, infometria: conceitos e aplicações. Revista P2P e INOVAÇÃO, v. 2, n. 1, 2009. Disponível em: http://hdl.handle.net/20.500.11959/brapci/119278. Acesso em: 18 maio 2023.

SCHARTZ, D.; BASHROUSH, R.; WALL, J. Towards a More Representative Definition of Cyber Security. Jornal of Digital Forensics, Security and Law. Vol. 12: No. 2, Article 8. DOI:https://doi.org/10.15394/jdfsl.2017.1476. Disponível em: at:https://commons.erau.edu/jdfsl/vol12/iss2/8. Acesso em: 19 abr 2023.

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.

SOUTH AFRICA. Notice of Intention to make South African National Cybersecurity Policy, p.12. Pretoria, South Africa, 2010 apud MAURER e MORGUS (2014).

SPIEKERMANN, S.; KORUNOVSKA, J.; LANGHEINRICH, M. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. Proceedings of the IEEE, v. 107, n. 3, p. 600–615, 2018.

TAGUE-SUTCLIFFE, J. An introduction to informetrics. Information Processing & Management, v. 28, n. 1, p. 1–3, jan. 1992. DOI: https://doi.org/10.1016/0306-4573(92)90087-G..

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, v. 31, n. 2, p. 369–379, ago. 2002.

APÊNDICES

Apêndice A – Princípios de Security By Design da OWASP

Princípio	Descrição	Exemplo
Minimize a área de superfície de ataque	Todo recurso adicionado a um aplicativo adiciona uma certa quantidade de risco ao aplicativo geral. O objetivo do desenvolvimento seguro é reduzir o risco geral, reduzindo a área da superfície de ataque.	Se um aplicativo da web implementa ajuda on-line com uma função de pesquisa suscetível a ataques de injeção de SQL, a probabilidade de ataque é menor se o acesso for restrito a usuários autorizados e pode ser praticamente eliminada se a função de pesquisa for deletada na reescrita do recurso de ajuda.
Estabeleça padrões seguros	Existem muitas maneiras de oferecer uma experiência "fora da caixa" para os usuários. No entanto, por padrão, a experiência deve ser segura e cabe ao usuário reduzir sua segurança – se for permitido.	Por padrão, o envelhecimento e a complexidade da senha devem ser ativados. Os usuários podem desativar esses dois recursos para simplificar o uso do aplicativo e aumentar o risco.
Conceda privilégio mínimo	O princípio recomenda que as contas tenham o menor privilégio necessário para executar seus processos de negócios. Isso abrange direitos do usuário, permissões de recursos, como limites da CPU, memória, rede e permissões do sistema de arquivos.	Se um servidor de *middleware* exigir apenas acesso à rede, leia o acesso a uma tabela de banco de dados e a capacidade de gravar em um *log*, isso descreve todas as permissões que devem ser concedidas. Sob nenhuma circunstância o *middleware* deve receber privilégios administrativos.
Aplique a defesa em profundidade	Onde um controle seria razoável, mais controles que abordam riscos de diferentes maneiras são melhores. Os controles, quando usados em profundidade, podem tornar vulnerabilidades graves extraordinariamente difíceis de explorar.	É improvável que uma interface administrativa defeituosa seja vulnerável a ataques anônimos se ela ocultar corretamente o acesso às redes de gerenciamento de produção, verificar a autorização administrativa do usuário e registrar todo o acesso.
Falhe seguramente	Os aplicativos falham regularmente em processar transações por vários motivos. Como eles falham pode determinar se um aplicativo é seguro ou não.	Imagine um cenário em que um aplicativo atribui automaticamente a um usuário o status de administrador quando ocorre um erro durante uma operação. Isso é um risco à segurança, pois qualquer erro acidental pode dar a um usuário privilégios de administrador.
Não confie nos serviços	Muitas organizações utilizam os recursos de processamento de terceiros, que provavelmente têm políticas e postura de segurança	Um provedor de programas de fidelidade compartilha informações com o Internet Banking, incluindo a quantidade de pontos de recompensa

	diferentes das suas. É improvável que você possa influenciar ou controlar terceiros externos. Portanto, a confiança implícita dos sistemas executados externamente não é garantida.	e uma lista de itens resgatáveis. Antes de exibir esses dados aos usuários, é necessário verificar a segurança, garantir que os pontos de recompensa sejam positivos e não improvavelmente grandes.
Separação de tarefas	Um controle chave de fraude é a separação de tarefas. Certas funções têm níveis de confiança diferentes dos usuários normais. Em particular, os administradores são diferentes dos usuários normais. Em geral, os administradores não devem ser usuários do aplicativo.	Um administrador deve poder ativar ou desativar o sistema, definir a política de senha, mas não deve poder logar na loja como um usuário super privilegiado, com o poder "comprar" mercadorias em nome de outros usuários.
Evite a segurança por obscuridade	A segurança através da obscuridade é um controle de segurança fraco e quase sempre falha quando é o único controle. Isso não quer dizer que guardar segredos seja uma má ideia, significa simplesmente que a segurança dos principais sistemas não deve depender de manter os detalhes ocultos.	A segurança de um aplicativo não deve depender do conhecimento do código fonte que está sendo mantido em segredo. Deve-se contar com muitos outros fatores, incluindo políticas razoáveis de senha, defesa em profundidade, arquitetura de rede sólida e controles de fraude e auditoria.
Mantenha a segurança simples	A área da superfície do ataque e a simplicidade andam de mãos dadas. Certos modismos de engenharia de software preferem abordagens excessivamente complexas ao que de outra forma seria um código relativamente direto e simples. Os desenvolvedores devem evitar soluções complexas quando uma abordagem mais simples for mais rápida e resumida.	Embora possa estar na moda ter uma série de *beans* de entidade *singleton* em execução em um servidor de *middleware* separado, é mais seguro e rápido simplesmente usar variáveis globais com um mecanismo *mutex* apropriado para proteger contra as condições da corrida.
Corrija problemas de segurança corretamente	Depois que um problema de segurança for identificado, é importante desenvolver um teste para ele e entender a causa raiz do problema. Quando os padrões de design são usados, é provável que o problema de segurança seja generalizado entre todas as bases de código, portanto, é essencial desenvolver a correção certa sem introduzir regressões.	Um usuário descobriu que pode ver o saldo de outro usuário ajustando seu cookie. Como o código de manuseio de cookies é compartilhado entre todos os aplicativos, uma alteração em apenas um aplicativo será direcionada para todos os outros aplicativos. A correção deve ser testada em todas as aplicações afetadas.

Fonte: adaptado de OWASP (2016)

Apêndice B – Relação dos artigos pesquisados

Nr	Título	Autor(es)	ISSN	DOI	Ano
1	'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home	Jiahong Chen; Lachlan Urquhart.	1360-0834	10.1080/13600834.2021.1957193	2022
2	A comprehensive side-channel information leakage analysis of an in-order RISC CPU microarchitecture	Davide Zoni; Alessandro Barenghi; Gerardo Pelosi; William Fornaciari.	1084-4309	10.1145/3212719	2018
3	A joint safety and security analysis of message protection for CAN bus protocol	Luca Dariz; Gianpiero Costantino;Massimiliano Ruggeri; Fabio Martinelli.	2415-6698	10.25046/aj030147	2018
4	A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach	Casola, Valentina; De Benedictis, Alessandra; Rak, Massimiliano; Villano, Umberto.	0164-1212	10.1016/j.jss.2020.110537	2020
5	A Security Analysis Method for Industrial Internet of Things	Mouratidis, Haralambos; Diamantopoulou, Vasiliki.	1551-3203	10.1109/TII.2018.2832853	2018
6	A security-aware framework for designing industrial engineering processes	Dedousis, Panagiotis; Stergiopoulos, George; Arampatzis, George; Gritzalis, Dimitris.	2169-3536	10.1109/ACCESS.2021.3134759	2021
7	A Security-by-Design Decision-Making Model for Risk Management in Autonomous Vehicles	Abdel-Basset, Mohamed; Gamal, Abduallah; Moustafa, Nour; Abdel-Monem, Ahmed; El-Saber, Nissreen.	2169-3536	10.1109/ACCESS.2021.3098675	2021
8	A Survey on Industrial Control System Testbeds and Datasets for Security Research	Mauro Conti; Denis Donadel; Federico Turrin.	1553-877X	10.1109/COMST.2021.3094360	2021
9	A tour of secure software engineering solutions for connected vehicles	Bertolino, Antonia; Calabro', Antonello; Di Giandomenico, Felicita; Lami, Giuseppe; Lonetti, Francesca; Marchetti, Eda; Martinelli, Fabio; Matteucci, Ilaria; Mori, Paolo.	0963-9314	10.1007/s11219-017-9393-3	2018
10	A design approach to IoT endpoint security for production machinery monitoring	Tedeschi, Stefano; Emmanouilidis, Christos; Mehnen, Jörn; Roy, Rajkumar.	1424-8220	10.3390/s19102355	2019
11	Abstract security patterns and the design of secure systems	Fernandez, Eduardo B.; Yoshioka, Nobukazu; Washizaki, Hironori; Yoder, Joseph.	2096-4862	10.1186/s42400-022-00109-w	2022
12	Achieving security-by-design through ontology-driven	Veloudis, Simeon; Paraskakis, Iraklis; Petsos, Christos;	0167-739X	10.1016/j.future.2018.08.042	2019

	attribute-based access control in cloud environments	Verginadis, Yannis; Patiniotakis, Ioannis; Gouvas, Panagiotis; Mentzas, Gregoris.			
13	An improved forensic-by-design framework for cloud computing with systems engineering standard compliance	Akilal, Abdellah; Kechadi, M-Tahar.	2666-2825	10.1016/j.fsidi.2021.301315	2022
14	Analysis of Security Vulnerability Levels of In-Vehicle Network Topologies Applying Graph Representations	Petho, Zsombor; Khan, Intiyaz. ; Torok, Árpád	0923-8174	10.1007/s10836-021-05973-x	2021
15	Analysis on Security and Privacy Guidelines: RFID-Based IoT Applications	Hezam Akram Abdulghani; Nijdam, Niels Alexander; Konstantas, Dimitri.	2169-3536	10.1109/ACCESS.2022.3227449	2022
16	Analytical Review of Cybersecurity for Embedded Systems	ABDULMOHSAN ALOSEEL; HONGMEI HE; CARL SHAW; MUHAMMAD ALI KHAN.	2169-3536	10.1109/ACCESS.2020.3045972	2021
17	ARMET: Behavior-Based Secure and Resilient Industrial Control Systems	Muhammad Taimoor Khan; Dimitrios Serpanos; Howard Shrobe.	0018-9219	10.1109/JPROC.2017.2725642	2018
18	Artificial Intelligence-Based Surveillance System for Railway Crossing Traffic	Pavel Sikora ; Lukas Malina; Martin Kiac; Zdenek Martinasek; Kamil Riha; Jiri Prinosil ; Leos Jirik; Gautam Srivastava.	1530-437X	10.1109/JSEN.2020.3031861	2021
19	Assistive Multimodal Robotic System (AMRSys): Security and Privacy Issues, Challenges, and Possible Solutions	Marchang, Jims; Di Nuovo, Alessandro.	2076-3417	10.3390/app12042174	2022
20	Autonomous Vehicle: Security by Design	Chattopadhyay, Anupam; Lam, Kwok-Yan; Tavva, Yaswanth.	1524-9050	10.1109/TITS.2020.3000797	2021
21	Blockchain and IoT Integration: A Systematic Survey	Alfonso Panarello; Nachiket Tapas; Giovanni Merlino; Francesco Longo; Antonio Puliafito.	1424-8220	10.3390/s18082575	2018
22	Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey	Bellini, Emanuele; Iraqi, Youssef; Damiani, Ernesto.	2169-3536	10.1109/ACCESS.2020.2969820	2020
23	Checking security compliance between models and code	Katja Tuma; Sven Peldszus; Daniel Strüber; Riccardo Scandariato; Jan Jürjens.	1619-1366	10.1007/s10270-022-00991-5	2022
24	CIA-level driven secure SDLC framework for integrating security into SDLC process	Kang, S., Kim, S.	1868-5137	10.1007/s12652-021-03450-z	2022
25	Continuous deployment of trustworthy smart IoT systems	Ferry, Nicolas; Nguyen, Phu H.; Song, Hui; Rios, Erkuden; Iturbe, Eider; Martinez, Satur; Rego, Angel.	1660-1769	10.5381/jot.2020.19.2.a16	2020

26	CYBERSECURITY STRATEGIES IN INDUSTRY 4.0	Raicu, Gabriel; Raicu, Alexandra.	2067-3604	10.54684/ijmmt.2022.14.3.233	2022
27	Design and verification of a mobile robot based on the integrated model of cyber-Physical systems	Levshun, Dmitry; Chevalier, Yannick; Kotenko, Igor; Chechulin, Andrey.	1569-190X	10.1016/j.simpat.2020.102151	2020
28	Design of secure microcontroller-based systems: Application to mobile robots for perimeter monitoring	Levshun, Dmitry; Chechulin, Andrey; Kotenko, Igor.	1424-8220	10.3390/s21248451	2021
29	DLT Based Authentication Framework for Industrial IoT Devices	Lupascu, Cristian; Lupascu, Alexandru; Bica, Ion.	1424-8220	10.3390/s20092621	2020
30	Efficient quantum-based security protocols for information sharing and data protection in 5G networks	Ahmed A. Abd EL-Latif; Bassem Abd-El-Atty; Salvador E. Venegas-Andraca; Wojciech Mazurczyk.	0167-739X	10.1016/j.future.2019.05.053	2019
31	Enabling data-driven anomaly detection by design in cyber-physical production systems	Rui Pinto; Gil Gonçalves; Jerker Delsing; Eduardo Tovar.	2096-4862	10.1186/s42400-022-00114-z	2022
32	EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme	Khurshid, Anum; Alsaaidi, Reem; Aslam, Mudassar; Raza, Shahid.	2169-3536	10.1109/ACCESS.2022.3225973	2022
33	Framework-based security measures for Internet of Thing: A literature review	Rueda-Rueda, Johan Smith; Portocarrero, Jesus M. T.	2299-1093	10.1515/comp-2020-0220	2021
34	Homomorphic-encrypted volume rendering	Mazza, Sebastian; Patel, Daniel; Viola, Ivan.	1077-2626	10.1109/TVCG.2020.3030436	2021
35	Integrating security and privacy in software development	Baldassarre, Maria Teresa; Barletta, Vita Santa; Caivano, Danilo; Scalera, Michele.	0963-9314	10.1007/s11219-020-09501-6	2020
36	Internet of Things Forensics: A Review	Hany F. Atlam; Ezz El-Din Hemdan; Ahmed Alenezi; Madini O. Alassaf; Gary B. Wills.	2542-6605	10.1016/j.iot.2020.100220	2020
37	Internet of Things: Evolution and technologies from a security perspective	Ande, Ruth; Adebisi, Bamidele; Hammoudeh, Mohammad; Saleem, Jibran.	2210-6707	10.1016/j.scs.2019.101728	2020
38	IoT Based information and communication system for enhancing underground mines safety and productivity: Genesis, taxonomy and open issues	Ankit Singh; Dheeraj Kumar; Jürgen Hötzel.	1570-8705	10.1016/j.adhoc.2018.06.008	2018
39	IoT Platforms and Security: An Analysis of the Leading Industrial/Commercial Solutions	Fortino, Giancarlo; Guerrieri, Antonio; Pace, Pasquale; Savaglio, Claudio; Spezzano, Giandomenico.	1424-8220	10.3390/s22062196	2022
40	iRECOVer: Patch your IoT on-the-fly	Maroof, Uzma; Shaghaghi, Arash; Michelin, Regio; Jha, Sanjay.	0167-739X	10.1016/j.future.2022.02.014	2022

41	On using contextual correlation to detect multi-stage cyber attacks in smart grids	Ömer Sen; Dennis van der Velde; Katharina A. Wehrmeister; Immanuel Hacker; Martin Henze; Michael Andres.	2352-4677	10.1016/j.segan.2022.100821	2022
42	PDGuard: an architecture for the control and secure processing of personal data	Mitropoulos, Dimitris; Sotiropoulos, Thodoris; Koutsovasilis, Nikos; Spinellis, Diomidis.	1615-5262	10.1007/s10207-019-00468-5	2020
43	PLUG-N-HARVEST Architecture for secure and intelligent management of near-zero energy buildings	Marin-Perez, Rafael; Michailidis, Iakovos T.; Garcia-Carrillo, Dan; Korkas, Christos D.; Kosmatopoulos, Elias B.; Skarmeta, Antonio.	1424-8220	10.3390/s19040843	2019
44	Practical evaluation of a reference architecture for the management of privacy level agreements	Vasiliki Diamantopoulou; Haralambos Mouratidis.	2056-4961	10.1108/ICS-04-2019-0052	2019
45	Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security	Haber, Eldar; Tamò-Larrieux, Aurelia.	0267-3649	10.1016/j.clsr.2020.105409	2020
46	Privacy intrusiveness in financial-banking fraud detection	Gabudeanu, Larisa; Brici, Iulia; Mare, Codrutta; Mihai, Ioan Cosmin; Scheau, Mircea Constantin.	2227-9091	10.3390/risks9060104	2021
47	Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process	D. Polverini; F. Ardente; I. Sanchez; F. Mathieux; P. Tecchio; L. Beslay.	0167-4048	10.1016/j.cose.2017.12.001	2018
48	RESTsec: a low-code platform for generating secure by design enterprise services	Christoforos Zolotas; Kyriakos C. Chatzidimitriou; Andreas L. Symeonidis.	1751-7575	10.1080/17517575.2018.1462403	2018
49	Secure Consensus via Objective Coding: Robustness Analysis to Channel Tampering	Marco Fabris; Daniel Zelazo.	2168-2216	10.1109/TSMC.2022.3177756	2022
50	Secure Development of Big Data Ecosystems	Moreno, Julio; Fernandez, Eduardo B.; Serrano, Manuel A.; Fernandez-Medina, Eduardo.	2169-3536	10.1109/ACCESS.2019.2929330	2019
51	Secure Links: Secure-by-Design Communications in IEC 61499 Industrial Control Applications	Tanveer, Awais; Sinha, Roopak; Kuo, Matthew M. Y.	1551-3203	10.1109/TII.2020.3009133	2021
52	Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0	Mosteiro-Sanchez, Aintzane; Barcelo, Marc; Astorga, Jasone; Urbieta, Aitor.	0278-6125	10.1016/j.jmsy.2020.10.011	2020
53	Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking	Restuccia, Francesco; D'Oro, Salvatore; Melodia, Tommaso.	2327-4662	10.1109/JIOT.2018.2846040	2018

54	Security aspects in modern service component-oriented application logic for social e-commerce systems	Faisal Nabi; Xiaohui Tao; Jianming Yong.	1869-5450	10.1007/s13278-020-00717-9	2021
55	Security by Design for Big Data Frameworks Over Cloud Computing	F. M. Awaysheh; M. N. Aladwan; M. Alazab; S. Alawadi; J. C. Cabaleiro; T. F. Pena.	0018-9391	10.1109/TEM.2020.3045661	2022
56	Security by Design: Aspirations and Realities in a Regulatory Context	BYGRAVE, Lee A.	2387-3299	10.18261/olr.8.3.2	2022
57	Security in centralized data store-based home automation platforms: A systematic analysis of nESt and hue	Kafle, Kaushal; Moran, Kevin; Manandhar, Sunil; Nadkarni, Adwait; Poshyvanyk, Denys.	2378-962X	10.1145/3418286	2020
58	Security policies by design in NoSQL document databases	Blanco, Carlos; García-Saiz, Diego; Rosado, David G.; Santos-Olmo, Antonio; Peral, Jesús; Maté, Alejandro; Trujillo, Juan; Fernández-Medina, Eduardo.	2214-2134	10.1016/j.jisa.2022.103120	2022
59	Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Sec	Guggenmos, Florian; Häckel, Björn; Ollig, Philipp; Stahl, Bastian.	0167-4048	10.1016/j.cose.2022.102747	2022
60	Security-by-design in multi-cloud applications: An optimization approach	Casola, Valentina; De Benedictis, Alessandra; Rak, Massimiliano; Villano, Umberto.	0020-0255	10.1016/j.ins.2018.04.081	2018
61	Sensei: Enforcing secure coding guidelines in the integrated development environment	De Cremer, Pieter; Desmet, Nathan; Madou, Matias; De Sutter, Bjorn.	0038-0644	10.1002/spe.2844	2020
62	Smart Interconnected Infrastructures for Security and Protection: The DESMOS Project	Michail Feidakis; Christos Chatzigeorgiou; Christina Karamperi; Lazaros Giannakos; Vasileios-Rafail Xefteris; Dimos Ntioudis; Athina Tsanousa; Dimitrios G. Kogias; Charalampos Patrikakis; Georgios Meditskos; Georgios Gorgogetas; Stefanos Vrochidis; Ioannis Kompatsiaris.	2073-431X	10.3390/computers10090116	2021
63	System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats	Choi, Seul-Ki; Yang, Chung-Huang; Kwak, Jin.	1976-7277	10.3837/tiis.2018.02.022	2018
64	The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention	Rob Kitchin; Martin Dodge.	1063-0732	10.1080/10630732.2017.1408002	2019
65	The application of the methodology for secure cyber–physical systems design to improve the semi-natural model of the railway infrastructure	Levshun, Dmitry; Chechulin, Andrey; Kotenko, Igor.	0141-9331	10.1016/j.micpro.2020.103482	2021

66	The Importance of Security Is in the Eye of the Beholder: Cultural, Organizational, and Personal Factors Affecting the Implementation of Security by Design	Renana Arizon-Peretz; Irit Hadar; Gil Luria.	0098-5589	10.1109/TSE.2021.3119721	2022
67	The Personalized Parkinson Project: Examining disease progression through broad biomarkers in early Parkinson's disease	Bloem B.R. ; Marks W.J., Jr. ; Silva De Lima A.L.; Kuijf M.L.; Van Laar T. ; Jacobs B.P.F.; Verbeek M.M.; Helmich R.C. ; Van De Warrenburg B.P. ; Evers L.J.W.; Inthout J.; Van De Zande T.	1471-2377	10.1186/s12883-019-1394-3	2019
68	Threat analysis of software systems: A systematic literature review	Tuma K.; Calikli G.; Scandariato R.	0164-1212	10.1016/j.jss.2018.06.073	2018
69	Threat modeling of a multi-UAV system	Almulhem, Ahmad.	0965-8564	10.1016/j.tra.2020.11.004	2020
70	Towards a Security Reference Architecture for NFV	Alnaim, Abdulrahman Khalid; Alwakeel, Ahmed Mahmoud; Fernandez, Eduardo B.	1424-8220	10.3390/s22103750	2022
71	TrustE-VC: Trustworthy Evaluation Framework for Industrial Connected Vehicles in the Cloud	Aladwan, Mohammad N.; Awaysheh, Feras M.; Alawadi, Sadi; Alazab, Mamoun; Pena, Tomas F.; Cabaleiro, Jose C.	1551-3203	10.1109/TII.2020.2966288	2020
72	Understanding developers' privacy and security mindsets via climate theory	Arizon-Peretz, Renana; Hadar, Irit; Luria, Gil; Sherman, Sofia.	1382-3256	10.1007/s10664-021-09995-z	2021
73	What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices	Blythe, John M.; Johnson, Shane D.; Manning, Matthew.	2193-7680	10.1186/s40163-019-0110-3	2020
74	What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?	Blythe, John M; Sombatruang, Nissy; Johnson, Shane D.	2057-2085	10.1093/cybsec/tyz005	2019
75	What topics should or should not be included in software security education-Qualitative content analysis	Shouki A. Ebad.	1061-3773	10.1002/cae.22554	2022
76	When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities	Wattana Viriyasitavat; Tharwon Anuphaptrirong; Danupol Hoonsopon.	2452-414X	10.1016/j.jii.2019.05.002	2019

Fonte: Dados da pesquisa.
Legenda: NR - número; ISSN - *International Standard Serial Number*; DOI - *Digital Object Identifier*;

Apêndice C – Resultado da Análise de Conteúdo

Resultado da análise de conteúdo																																								
Princípios	**Artigos**																																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
P1	P	P	P	P	A	A	A	P	P	P	P	P	A	P	P	P	A	P	P	P	P	P	A	P	P	P	A	P	P	P	P	P	A	P	P	A	P	P
P2	P	A	A	A	A	A	A	A	P	P	P	A	A	A	P	P	A	P	P	P	P	P	P	P	P	P	P	P	A	P	P	A	P	P	P	P	P	P
P3	A	A	A	P	A	A	A	A	P	A	P	A	A	A	P	A	A	P	P	A	A	P	A	A	P	A	P	A	P	A	A	A	A	P	P	P	P	A
P4	P	P	P	P	P	A	A	A	A	P	A	A	A	P	P	A	A	P	P	P	P	A	A	A	P	P	A	P	A	P	A	A	P	A	P	P	P	P
P5	P	A	A	A	A	A	A	A	P	A	A	A	A	P	P	P	P	A	P	P	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
P6	A	A	A	A	A	A	A	A	A	A	A	A	A	A	P	A	A	A	A	P	A	P	A	A	A	P	A	A	P	A	A	A	A	P	P	A	P	A
P7	A	A	A	A	P	A	A	P	A	A	P	A	A	A	P	A	A	P	P	A	P	P	A	P	A	A	A	A	P	A	A	A	A	P	A	A	A	A
P8	A	A	A	A	A	A	A	A	A	A	A	A	A	A	P	A	A	A	A	A	A	A	A	A	A	A	A	A	A	P	A	A	A	P	A	A	A	A
P9	P	A	A	A	A	A	A	A	A	A	P	A	A	A	P	A	A	A	P	A	A	P	A	P	A	A	A	A	A	P	P	A	P	A	P	A	A	A
P10	A	A	A	A	A	A	A	P	P	A	A	A	A	A	P	A	A	A	P	A	A	A	A	A	P	A	A	A	A	A	A	A	A	A	A	A	A	A

Apêndice C – Resultado da Análise de Conteúdo (continuação)

Resultado da análise de conteúdo																			
Princípios	**Artigos**																		
	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
P1	P	P	P	P	P	A	P	P	P	P	A	P	P	P	P	P	P	P	P
P2	P	P	P	P	P	P	P	P	A	A	A	P	P	P	P	A	P	P	P
P3	P	A	A	P	P	P	A	P	A	P	A	P	A	P	P	A	P	P	P
P4	P	P	P	P	P	A	P	A	A	A	A	P	P	P	P	A	P	A	P
P5	A	P	A	P	P	A	A	A	A	A	A	A	A	P	A	P	P	A	A
P6	A	A	A	P	A	A	A	P	A	A	A	A	A	P	A	A	A	A	P
P7	P	P	A	P	P	P	A	A	A	A	A	A	A	A	A	A	P	A	A
P8	A	A	P	A	A	A	A	A	A	P	A	A	A	A	P	A	P	A	P
P9	A	P	A	A	A	A	A	A	P	A	A	A	P	A	P	A	A	A	A
P10	A	A	A	A	A	A	A	A	P	A	A	A	A	P	A	A	A	A	A

Princípios	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
P1	A	P	A	P	P	P	P	P	A	P	P	P	P	P	P	A	P	P	P
P2	A	P	P	P	P	P	P	P	A	P	A	A	P	P	A	A	P	A	P
P3	P	A	A	A	P	A	A	P	A	P	A	A	P	P	A	A	P	P	P
P4	P	A	P	A	P	P	P	P	A	A	A	A	P	P	A	A	P	A	A
P5	A	A	A	A	A	A	P	A	A	A	A	A	A	P	A	A	A	P	P
P6	A	A	A	A	A	A	A	P	A	A	A	A	A	A	P	A	A	A	P
P7	P	A	A	A	P	A	A	P	A	A	A	A	P	A	A	A	A	A	P
P8	P	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	P	A
P9	A	A	A	P	P	A	A	P	A	A	A	A	A	A	A	A	A	P	A
P10	A	A	A	P	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A

Fonte: Dados da pesquisa.

Legenda: P1 - Minimize a área de superfície de ataque; P2 - Estabeleça padrões seguros; P3 - Conceda privilégio mínimo; P4 - Aplique a defesa em profundidade; P5 - Falhe seguramente; P6 - Não confie nos serviços; P7 - Separação de tarefas; P8 - Evite a segurança por obscuridade; P9 - Mantenha a segurança simples; P10 - Corrija problemas de segurança corretamente; P - Presente; A - Ausente. Os artigos foram numerados de 1 a 76 em correspondência com o Apêndice B. Os 38 primeiros artigos são apresentados nesta parte do apêndice e os demais são apresentados em sua continuação.