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

PAULO HENRIQUE MENDONÇA BUENO

AVALIAÇÃO DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA:
UM ESTUDO SOBRE A DISTRIBUIÇÃO DE ARTIGOS PUBLICADOS

Brasília – DF
2021

PAULO HENRIQUE MENDONÇA BUENO

AVALIAÇÃO DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA:
UM ESTUDO SOBRE A DISTRIBUIÇÃO DE ARTIGOS PUBLICADOS

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

Professor Orientador:

Dr., Rafael Rabelo Nunes

Brasília – DF

2021

AVALIAÇÃO DAS ESTRUTURAS DE SEGURANÇA CIBERNÉTICA:

UM ESTUDO SOBRE A DISTRIBUIÇÃO DE ARTIGOS PUBLICADOS

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

Paulo Henrique Mendonça Bueno

Dr. Rafael Rabelo Nunes
Professor-Orientador

Dr. Aldery Silveira Júnior
Professor-Examinador

Dr. Carlos André de Melo Alves
Professor-Examinador

Brasília, 21 de maio de 2021

RESUMO

O objetivo geral deste estudo foi avaliar a distribuição de artigos publicados sobre o tema ‘segurança cibernética’ com a utilização de padrões para implementação de segurança cibernética. Para atender a esse objetivo, uma pesquisa descritiva de natureza bibliométrica foi realizada, com a avaliação de dados de 50 artigos que utilizaram o guia *Cybersecurity Framework* (CSF) do *National Institute of Standards and Technology* (NIST) ou padrões da série de padrões ISO/IEC 27000. Uma vez selecionados os artigos, metadados foram extraídos e foi realizado um tratamento de dados, agrupando-os por similaridade de aplicação, localidade e ano de publicação para compor a análise. Os resultados encontrados indicam que a distribuição da produção científica, de 2015 a 2021, utilizando-se de padrões das séries ISO/IEC 27000 e NIST CSF possuem um crescimento contínuo. Verificou-se também um interesse dos pesquisadores sobre segurança cibernética aplicada a pequenas e médias empresas. Espera-se que os resultados possam contribuir para a tomada de decisão de gestores, bem como para a compreensão da distribuição da utilização de padrões ISO e o guia de segurança cibernética da NIST.

Palavras-chave: Segurança Cibernética, Segurança da informação, *Frameworks*, Gerenciamento de Segurança da Informação, Revisão.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

O aumento da acessibilidade à tecnologia tem permitido que as organizações confiem cada vez mais suas atividades a sistemas, softwares e aplicações que recebem, transmitem e processam informações. Com isso, informações e sistemas, além de vantagens competitivas, tornam-se ativos a serem protegidos, uma vez que o número de ameaças e incidentes crescem à medida que a tecnologia se desenvolve.

Desse modo, as organizações, conforme surge a necessidade de se ter proteção adequada, buscam as formas que se ajustem as suas particularidades. Neste contexto, padrões como os da *International Organization for Standardization* (ISO) das séries 27000 bem como o guia de segurança cibernética do *National Institute for Standards and Technology* (NIST) auxiliam gestores e organizações na implementação de boas práticas de segurança cibernética.

Além das necessidades particulares de cada organização de proteger seus ativos, há também a obrigação de respeitar as novas legislações sobre proteção de dados pessoais, que se não respeitados podem gerar punições severas em alguns casos.

Assim, para a presente pesquisa, foi realizada uma avaliação das estruturas de segurança cibernética, analisando a distribuição de publicações com o uso de padrões das séries ISO/IEC 27000 e o *Cybersecurity Framework* (CSF) da NIST. Dessa forma, esse trabalho apresenta, em números, os temas abordados pelos artigos publicados bem como sua evolução no tempo e distribuição geográfica. Inicialmente, aborda a introdução do estudo, formulação do problema, objetivos geral, objetivos específicos e a justificativa.

A segunda parte, o referencial teórico, apresenta alguns conceitos importantes para a compreensão do tema, descrição dos padrões ISO e do guia NIST CSF, *frameworks* criados a partir do guia ou padrões utilizados nesse estudo, cultura de segurança cibernética e uma seção sobre regulamentação sobre o uso de dados no contexto brasileiro e no exterior.

A terceira parte apresenta a metodologia utilizada para este trabalho, destacando o tipo, a abordagem, a coleta de dados, a seleção e a análise dos dados.

A quarta parte apresenta os resultados divididos em seções, demonstrando em gráficos com os dados específicos da respectiva seção, e destaca pontos importantes percebidos. Por último, têm-se as conclusões do estudo e sugestões.

1.1. Contextualização

Nos anos de 1990 a 2000, a internet trouxe conectividade para todos os computadores que tivessem acesso a uma conexão ou linha telefônica, tendo alcance mundial. Foi nessa época que a internet ficou disponível para qualquer pessoa, o que antes era restrito ao governo, ao estudo acadêmico e a profissionais da área. Nesse início de expansão da internet, a segurança não era prioridade, e padrões de segurança para redes interconectadas não existiam ainda, pois, nesse período, todos os usuários de e-mail e internet até então eram cientistas de computação, ou seja, a necessidade de criptografia ou de algum tipo de autenticação não pareciam necessários.

Em 1993, houve a primeira conferência de *Defense Readiness Condition* (Defcon), que, em tradução literal, é "condição de prontidão de defesa". Essa conferência visou a reunir pessoas interessadas em segurança da informação, incluindo agentes de Estado. No fim dos anos 1990 e começo dos anos 2000, organizações grandes começaram a ter ferramentas de segurança da informação, momento em que os softwares de antivírus começaram a se popularizar (WHITMAN; MATTORD, 2015).

Também, em 1993, surge o BS7799 da British Standards, que iniciou como um código de prática, tornando-se um padrão de segurança da informação em 1995 (EZINGEARD; BIRCHALL, 2006). As exigências de se ter padrões de segurança e a globalização aumentaram a disseminação e o reconhecimento do BS7799, que posteriormente se tornou o padrão internacional ISO/IEC 17799 da *International Organization for Standardization* em 2000 (EZINGEARD; BIRCHALL, 2006).

Em 2002, uma segunda parte do BS7799 (BS7799-2) foi publicada trazendo significativas mudanças e permanecendo como padrão até ser internacionalizada na forma de ISO 27001 em 2005 (CALDER; WATKINS, 2008). Revisado em 2005 para assegurar que os controles fossem compatíveis, o ISO17799, em 2007, foi incorporado à sequência de numeração ISO/IEC de padrões de gerenciamento de segurança da informação e passou a ser identificado como ISO/IEC 27002:2005 (CALDER; WATKINS, 2008).

Nos anos mais recentes, a necessidade de segurança da informação vem sendo ainda mais percebida bem como a constatação de que é também uma questão de segurança nacional (WHITMAN; MATTORD, 2015). Sendo assim, em 2013, nos Estados Unidos, o presidente Barack Obama assinou a Ordem Executiva nº 13636, que visava à criação de uma estrutura de

segurança cibernética que melhorasse as capacidades básicas para infraestrutura crítica gerenciar o risco cibernético (THE WHITE HOUSE, 2013). Então, essa mesma ordem executiva deixou a encargo do *National Institute for Standards and Technology* (NIST) para dar seguimento às diretrizes, trabalhando em parceria com a iniciativa privada para encontrar pontos em comum sobre melhores práticas e padrões, para então construir sua estrutura de segurança cibernética (THE WHITE HOUSE, 2013).

Recentemente, países vêm adotando regulação sobre proteção de dados e reforçando a importância da segurança da informação. Apesar de apenas 20% dos executivos acreditarem na relevância da proteção de dados para seus negócios, empresas com clientes na Europa invariavelmente precisarão dar atenção a essas novas exigências, onde são bem severas, sob o risco de serem multadas (STASIAK, 2018). Além disso, há também os riscos de comprometimento de dados, tais como os ataques recentes de *ransomwares* – em que os dados são sequestrados.

Contudo, a situação mostra-se complexa mesmo para empresas que, aparentemente, gerenciam a segurança da informação. Entre março e junho de 2020, a *SolarWinds* foi atacada comprometendo aproximadamente 300 mil clientes em todo mundo, incluindo o Pentágono, o Exército, o Departamento de Estado, o Gabinete da Presidência, o Tesouro Nacional e o Departamento de Comércio dos Estados Unidos (US, 2020).

Em um contexto mais próximo do Brasil, um relatório do *Cybersecurity Observatory* levantou um dado alarmante: mais de 75% dos países da América Latina não possuem planos críticos de proteção da infraestrutura para responder a ciberataques. O documento também destaca que embora tenha ocorrido alguns avanços, os governos deveriam investir mais recursos para poder reduzir os impactos social e econômico desses incidentes cibernéticos, que, em 2019, já custaram mais de 90 bilhões de dólares. O relatório traz a maioria dos países dessa região também precisam monitorar e responder a ataques cibernéticos de uma forma mais sistemática e construir organizações centrais para coordenar as atividades de segurança cibernética (CYBER SECURITY OBSERVATORY, 2020).

As perdas no mundo por conta de crimes cibernéticos chegam à cifra aproximada de 1 trilhão de dólares, e a pandemia favoreceu a golpes aplicados por meio da internet, tendo em vista que uma quantidade significativa de empregados migrou para o trabalho remoto, criando um ambiente propício a esse tipo de crime (RILEY, 2020).

Embora nem todo ataque consiga extrair dinheiro diretamente de uma organização e que não tenha o resultado desejado dos criminosos, ainda pode gerar prejuízos inimagináveis, uma vez que um ataque de software malicioso (*ransomware*) interrompe as operações, em média, por 18 horas. Portanto, considerando a parada das atividades somada a um possível pagamento para os criminosos desbloquearem os sistemas, o prejuízo pode ser muito maior, podendo ainda haver impacto indireto em outras empresas em uma cadeia de suprimento (RILEY,2020).

1.2. Formulação do Problema

Na esfera pessoal, em um contexto em que há exposição, de várias formas, todos os dias, pode ocorrer de não se ter um pensamento sistemático sobre a crescente necessidade de se pensar em segurança de dados. No entanto, na esfera das organizações, que trabalham com muitos dados, o controle visando à segurança de dados é complexa e, para Castells (1999), existe somente uma única forma de controlar a rede de tecnologia da informação, não fazer parte da rede, porém o preço é elevado para quem optar por ficar fora da sociedade virtual, assim, consequentemente as organizações devem pensar sobre como lidar com essa realidade.

Organizações aplicam muitos recursos para manutenção de seus ativos de informação, recursos esses que poderiam ser usados exclusivamente para melhorar seus sistemas caso não houvesse ameaças (WHITMAN; MATTORD, 2015).

Com base nesse cenário, tem-se o interesse em investigar como as organizações, sejam públicas, sejam privadas, estão agindo para se enquadrarem nesse novo contexto, e também o que a comunidade acadêmica tem apresentado em suas investigações sobre segurança da informação e melhores práticas. Contudo a investigação foi direcionada às melhores práticas contidas no guia *Cybersecurity Framework* (CSF) da NIST e na série de padrões ISO/IEC 27000.

Desse modo, como pergunta de pesquisa, tem-se: “Como estão sendo aplicados os padrões de segurança cibernética no mundo?”.

1.3. Objetivo geral

O objetivo principal do estudo é avaliar os artigos publicados sobre segurança cibernética com foco no uso do guia *Cybersecurity Framework* (CSF) da NIST e da série de padrões ISO/IEC 27000 na produção de artigos.

1.4. Objetivos específicos

- Mapear artigos relacionados ao tema segurança cibernética com a utilização de padrões ISO/IEC 27000 ou o guia NIST CSF;
- Analisar conteúdo dos artigos, selecionar artigos que se adequem ao propósito deste estudo, extrair e agrupar dados para a análise;
- Traçar um panorama de como tem sido a distribuição desses padrões nos artigos segmentados por ano, tema e região geográfica;
- Identificar tendências dos artigos e aplicação;

1.5. Justificativa

Observa-se que, cada vez mais, há o uso de tecnologia no dia a dia das pessoas, e, com a inovação dessa área avançando, ocorre que em muitos casos as consequências geradas pelas novas tecnologias são difíceis de antecipar (KOHLER; SOM, 2014).

A *United Nations Economic Commission for Europe* (UNECE, 2019) afirma que ameaças cibernéticas são problemas que cruzam fronteiras nacionais, regionais e internacionais e, portanto, são fenômenos mundiais. Dessa forma, requer uma abordagem integrada em todos os níveis. Brechbuhl (2010) expõe que a responsabilidade pela segurança cibernética é algo compartilhado entre setores da economia, da sociedade, do governo, das organizações e dos indivíduos. Portanto, segurança cibernética não é mais uma matéria somente de tecnologia, ou seja, também é uma questão de gerenciamento de risco e que repercute por toda a organização (SAITO, 2016).

O trabalho de Suryotrisongko e Musashi (2019), *Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective*, busca encontrar artigos de revisões com algumas palavras-chave em seu título, não tendo como filtro nenhum tipo de tecnologia, metodologia ou *framework*. Sendo assim, eles focam em mapear tópicos de pesquisa e taxonomia, separando-os por teorias utilizadas, áreas e tópicos. Embora tenham um propósito diferente, trazem categorização relevante a mais de 100 artigos coletados e muitos deles, também revisões de literatura que, de alguma forma, condensam como estão distribuídos os tópicos. Entretanto não conseguem dar uma dimensão da evolução numérica das pesquisas em relação ao tempo, apresentando apenas números gerais e não focando em como esses temas se

desenvolvem no tempo. Dessa forma, falta uma perspectiva de quais problemas podem estar levantando o interesse da academia nos últimos anos.

No trabalho de Roy (2020), *A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard*, é realizado um comparativo dos *frameworks* NIST e ISO, visando a demonstrar as diferenças apresentadas entre os dois. Apesar de não ser uma revisão sistemática, é um trabalho que parcialmente coincide com o proposto aqui, a revisão sistemática proposta, porém com uma abordagem exclusivamente qualitativa, buscando apenas diferenciar as estruturas a um nível de debate. No entanto, apesar de trazer de forma simplificada as diferenças entre as estruturas, não aborda outras nuances do tema, ou seja, embora relevante, não demonstra como isso tem sido percebido no mundo real, ainda que fosse indiretamente.

Em *Review of National Cybersecurity Strategies*, de Mori e Goto (2018), procedeu-se a uma revisão em que foram observadas as estratégias de segurança cibernética em nível nacional, abordando como os países têm se portado nesse contexto, em especial o Japão. Sendo assim, Mori e Goto (2018) demonstram, por meio do *Global Cybersecurity Index* (GCI), em uma parte de seu trabalho, as pontuações dos 10 países com melhores pontuações e reúnem conhecimento ao longo do trabalho sobre segurança cibernética a um nível nacional. Mori e Goto (2018) também possuem um trabalho muito semelhante, *Review of National Cybersecurity Policies*, o qual eles trabalham outros países também, como o Reino Unido. Então os referidos autores possuem alguns trabalhos visando à defesa do espaço cibernético de uma forma nacional (institucional), e demonstram qualitativamente os esforços em países, mas ainda assim não é possível notar aspectos específicos, nem a utilização ou não de *frameworks*, tendo como foco um escopo mais amplo.

Este trabalho visa a mapear como têm sido os estudos na área de segurança cibernética com relação à aplicação de padrões, diferenciando-se por focar na distribuição por padrão e na distribuição temporal e geográfica. Com tema atual e cada vez mais relevante, este trabalho pode contribuir com dados que ilustram a realidade atual dos estudos ou a implementação de padrões ou guias, servindo de direcionamento para futuras investigações.

Neste contexto, este trabalho pode colaborar com gestores, estudantes e pesquisadores. Gestores podem se beneficiar dos resultados deste trabalho compreendendo quais padrões são mais aceitos e suas tendências, pois adotar um padrão ou guia mais utilizado significa aumentar a probabilidade de encontrar profissionais que auxiliem no atingimento de seu objetivo de

segurança. Estudantes e pesquisadores podem se beneficiar desse trabalho mediante à observação de que o panorama pode apresentar o estado atual do uso dos padrões ISO/IEC 27000 e o guia NIST CSF, indicando também tendências dos artigos que podem auxiliar no direcionamento do estudante ou pesquisador.

2. REFERENCIAL TEÓRICO

2.1. Segurança da informação

Assim como Von Solms e Van Niekerk (2013) afirmam que segurança cibernética em alguns casos é tratado como termo análogo a segurança da informação, esta seção trata de algumas definições que pertencem ao contexto e aos princípios da segurança da informação, pois são necessários para a compreensão da segurança cibernética.

2.1.1. Segurança da informação e segurança cibernética

A segurança da informação é a área que se dedica à proteção de ativos da informação, também podendo ser considerada uma prática de gestão de riscos que comprometam os conceitos de confidencialidade, integridade e disponibilidade da informação (SEMOLA, 2014).A segurança cibernética é a proteção não somente do espaço virtual em si, mas também daquilo que é trabalhado nesse bem como dos ativos que possam ser alcançados por meio do ciberespaço (VON SOLMS; VAN NIEKERK 2013). Embora segurança cibernética seja, em alguns casos, tratada como termo análogo à segurança da informação, esta protege a informação de possíveis danos que podem surgir de diversas formas de ameaças, tratando-a de maneira mais abrangente e considerando-a como ativo a ser protegido (VON SOLMS; VAN NIEKERK 2013).

De acordo com as definições da ISO/IEC 27000:2018, segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação. Nessa mesma definição, estão para serem inclusos a autenticidade, a responsabilidade, o não-repúdio e a confiabilidade. Normalmente o termo “segurança da informação” está atrelado à informação como ativo que requer algum tipo de proteção adequada.

Segundo a definição do glossário presente no site institucional da NIST em uma seção dedicada a pequenos negócios, *Small Business Security Corner*, segurança da informação é

descrita como uma abordagem que visa a garantir a confiabilidade, a integridade e a disponibilidade, protegendo e gerenciando o risco à informação e também ao sistema de informação; enquanto que, na mesma sessão do site NIST, *Small Business Security Corner*, define-se segurança cibernética como uma série de etapas para gerenciar riscos contra danos, acesso não autorizado, exploração de vulnerabilidades e restaurar, quando necessário os sistemas de informação e as informações neles contidas (NIST, 2019).

Para a finalidade deste trabalho, o termo segurança da informação terá o foco e será interpretado como segurança cibernética.

2.1.2. Princípios da segurança da informação

A segurança da informação é suportada por três princípios: a confidencialidade, que é não permitir que usuários, entidades ou processos não autorizados acessem a informação; a integridade, que é garantir que a informação esteja sempre completa e precisa; e a disponibilidade, que é, uma vez autorizado, garantir o acesso à informação demandada. A confidencialidade, integridade e disponibilidade são frequentemente citados como "Tríade C.I.A." ou "Triângulo C.I.A." (CHERDANTSEYA; HILTON, 2013; ISO, 2013).

Esse modelo, que é citado como a tríade da segurança da informação, é embasado nos estudos de Saltzer e Schroeder (1975), em que os termos confidencialidade, integridade e disponibilidade são citados como "liberação de informação não autorizada", "modificação de informação não autorizada" e "negação de uso não autorizada". Diante disso, desde o desenvolvimento do *mainframe*, o triângulo C.I.A. tem sido o padrão para segurança utilizado por organizações e governo (WHITMAN; MATTORD, 2015, p. 9).

Isso posto, um dos guias da NIST apresenta as definições de confidencialidade, integridade e disponibilidade como no Quadro 1:

Quadro 1 – Definições de confidencialidade, integridade e disponibilidade.

Palavra	Descrição/Significado
Confidencialidade	Preservar as restrições ao acesso de informações, com meios para proteção de privacidade pessoal e informações proprietárias.
Integridade	Proteção contra modificações, danos ou destruição indevida de informações, garantindo também a autenticidade e não repúdio das informações.
Disponibilidade	Garantir o acesso de forma confiável, para o uso da informação.

Fonte: NIST (2015).

2.1.3. Classificação da informação

Na classificação da informação no âmbito da segurança da informação, a ISO/IEC 27001:2013 e a NIST 800-60 possuem algumas diretrizes sobre o assunto, porém ambas afirmam que deve ser desenvolvida pela organização uma forma de classificar a importância e os seus tipos.

A norma NBR ABNT ISO 27001:2013 sugere que a classificação deve ser feita objetivando sua importância na organização para que a informação receba o nível de proteção adequado. Para se classificar a informação, consideram-se o valor, a criticalidade e a sensibilidade para modificação ou divulgação não autorizada. Desse modo, um rótulo deve ser criado e implementado de acordo com o esquema de classificação desenvolvido e adotado pela organização (ABNT, 2013).

O padrão NIST 800-60 preconiza que a informação e os sistemas de informação devem ser classificados de acordo com o impacto gerado por algum evento, ou seja, o quanto um fenômeno pode comprometer a capacidade da organização de continuar suas obrigações. As diretrizes FIPS 199 estabelecem que essa classificação deverá ser feita observando os três níveis de impacto (baixo, moderado, alto) e os três objetivos da segurança da informação (confidencialidade, integridade e disponibilidade). Nesse caso, a informação será categorizada pelo seu tipo (ex: financeira, médica, proprietária e outras), e isso será definido pela organização ou, em alguns casos, por força de lei, regulação e entes públicos no geral (NIST, 2008).

2.1.4. Principais componentes da segurança da informação

Para uma melhor compreensão dos componentes da segurança da informação, é necessária a compreensão de o que é um “sistema de informação” por definição. Segundo Laudon e Laudon (2013), sistema de informação é “um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações para apoiar a tomada de decisão e o controle em uma organização”. Nesse contexto, sistemas de informação possuem informação sobre pessoas, lugares e coisas importantes da organização, então além de ajudar na tomada de decisão, sistemas de informação também podem auxiliar os colaboradores a analisar problemas, criar novas soluções e ajudar na visualização de conteúdos complexos (LAUDON; LAUDON, 2013. p. 45).

Sistema de informação é todo o conjunto que viabiliza as organizações a usarem as informações, que são: pessoas, procedimentos e tecnologia, portanto sistema de informação não se delimita a hardware (WHITMAN; MATTORD, 2015. p. 19).

Sendo assim, para Whitman e Mattord (2015), os componentes principais de um sistema para que se possa entrar com informações e serem processadas, produzidas e armazenadas são: hardware, software, redes, pessoas, procedimentos e dados.

O Quadro 2 traz cada componente citado usando diretamente a definição da NIST. O quadro também inclui a definição de "procedimentos", realizada por Whitman e Mattord (2015. p. 21):

Quadro 2 – Componentes da Segurança da Informação.

	DESCRIÇÃO
Hardware	Os componentes físicos de um sistema de informação.
Software	Programas de computador (que são armazenados e executados por hardware de computador) e dados associados (que também são armazenados no hardware) que podem ser gravados ou modificados dinamicamente durante a execução.
Rede	Um meio de comunicação aberto, normalmente a internet, usado para transportar mensagens entre o requerente e outras partes. Salvo indicação em contrário, nenhuma suposição é feita sobre a segurança da rede; presume-se que seja aberto e sujeito a ataques ativos (por exemplo, personificação, *man-in-the-middle*, sequestro de sessão) e passivos (por exemplo, espionagem) em qualquer ponto entre as partes (por exemplo, requerente, verificador, CSP, RP).
Pessoas	Qualquer pessoa considerada um ativo pela gestão.
Procedimentos	Instruções escritas para realizar uma tarefa específica.
Dados	Uma representação das informações armazenadas ou transmitidas.

Fonte: NIST (2015); Whitman e Mattord (2015).

2.1.5. Ameaças, vulnerabilidades e riscos

Ameaças são "agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades", prejudicando os negócios de uma organização. As ameaças podem ser divididas em três classificações quanto à sua intencionalidade: naturais, que são ameaças da natureza (ex: terremoto); involuntárias, que são ameaças não intencionais, mas que são causadas por erros ou desconhecimento; e voluntárias, que são ameaças com intenção, que normalmente têm agente causadores como hackers, espiões e ladrões (SEMOLA, 2014).

Vulnerabilidades são fragilidades que facilitam a ocorrência de um incidente de segurança, afetando os princípios da segurança da informação. Elementos passivos não provocam incidentes por si só, necessitando de um agente ativo como uma ameaça para provocar um incidente (SEMOLA, 2014).

A NIST SP 800-53 possuí em seu vocabulário a definição para ameaças, vulnerabilidades e risco, como descrito no Quadro 3:

Quadro 3 – Definições: Ameaça, Vulnerabilidade e Risco.

Termo	Descrição
Ameaça	Qualquer circunstância ou evento com potencial de impactar adversamente as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais ou indivíduos por meio de um sistema de informações por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço. Além disso, o potencial de uma fonte de ameaça explorar com êxito uma vulnerabilidade específica do sistema de informações.
Vulnerabilidade	Uma falha, fraqueza ou deficiência em um sistema de informações, procedimentos de segurança do sistema, controles internos ou implementação que podem ser explorados ou acionados por uma fonte de ameaça. Fraquezas podem resultar em riscos de segurança e/ou privacidade.
Risco	Uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento potencial e, normalmente, em função de: (i) os impactos adversos que surgiriam se a circunstância ou evento ocorresse; ou (ii) a probabilidade de ocorrência.

Fonte: NIST (2015).

Risco é a probabilidade de ocorrer algum incidente; vulnerabilidade é uma abertura que algum sistema possa ter, facilitando a ocorrência de algum incidente; e ameaça são circunstâncias com potencial de gerar algum dano às operações (NIST, 2015).

O laboratório de tecnologia da informação da NIST mapeia, com banco de dados nacional de vulnerabilidades (NVD *Dashboard*), as vulnerabilidades e as exposições a ameaças mais comuns. Entre os dados apresentados, eles possuem hoje mais de 162 mil vulnerabilidades mapeadas. Dentro desse número, por meio do sistema de pontuação de vulnerabilidade comum (CVSS V3), que é um sistema que mede a gravidade das vulnerabilidades relativa às falhas de software, eles apontam como gravidade crítica: 12.067, gravidade alta: 34.418, gravidade média: 31.180 e gravidade baixa: 1.420 (NIST, 2021).

2.2. Padrões de segurança da informação

Padrão é uma prática convencionada que consiste em requisitos, especificações, diretrizes ou características para atividades ou para seus resultados. Em geral, são cumpridos para fazer um produto, entregar um serviço ou gerenciar um processo (GIUCA, 2018).

Frameworks são o núcleo de programas de gerenciamento de segurança cibernética, com seus facilitadores como: políticas, padrões, processos, procedimentos, metodologias, métodos e ferramentas. Também são a base da implementação e permitem que alcancem os resultados pretendidos de gerenciamento e mitigação de riscos de segurança cibernética (GIUCA, 2018).

2.3. NIST CYBERSECURITY FRAMEWORK (NIST CSF)

Com o nome oficial de *The Framework for Improving Critical Infrastructure Cybersecurity*, utiliza-se de uma linguagem comum para gerenciar e direcionar o risco de segurança cibernética, baseado nas necessidades das organizações com um custo-benefício sem colocar requisitos adicionais regulatórios (NIST, 2018).

Foi desenvolvido a partir de diretrizes da Casa Branca (*Executive Order* nº 13636) contando também com a participação de setores produtivos, acadêmicos e diversas categorias do governo (NIST, 2018).

Este *framework* tem uma abordagem baseada em risco para gerenciamento de segurança cibernética e é dividido em três componentes principais: núcleo ou estrutura básica (*core*), avaliação (*profile*) e níveis de implementação (*implementation tiers*) (NIST, 2018).

2.3.1. Estrutura básica do Cybersecurity Framework

A estrutura básica consiste em atividades orientadas a atingir resultados específicos de segurança cibernética, apresentados pelas partes interessadas, fornecendo um conjunto de atividades para alcançá-los. Contudo o *NIST CSF* não é uma lista de ações a serem feitas e deve ser aplicado conforme as necessidades e resultados esperados (NIST, 2018).

Ao todo, cinco funções de nível alto fazem parte da estrutura básica que são: identificar, proteger, detectar, responder e recuperar. As funções compõem o alto nível, enquanto cada função possui algumas categorias atreladas a ela, sendo ao todo 23 categorias distribuídas ao longo das funções (como na Figura 1).

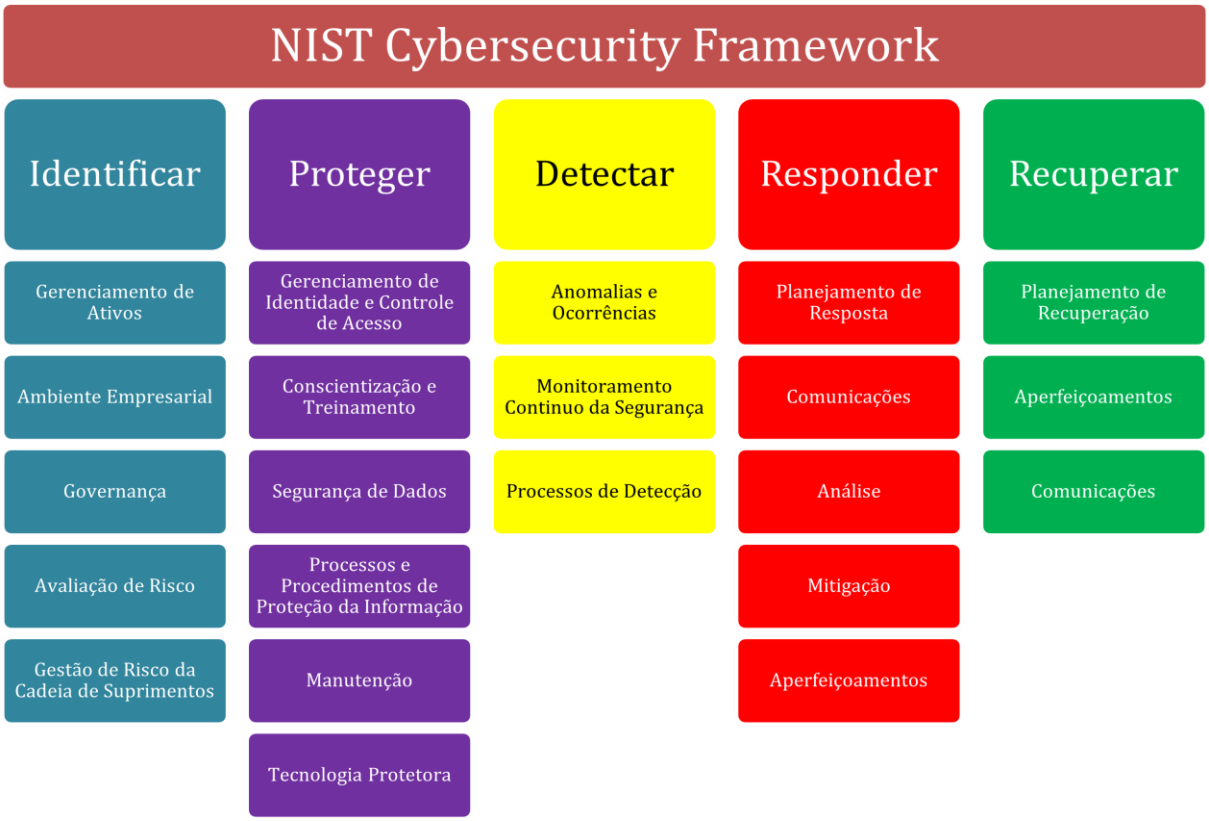


Figura 1- Funções principais e suas categorias. Fonte: NIST CSF (2018).

A estrutura básica também conta com subcategorias que se distribuem ao longo das categorias (ao todo são 108), que são declarações que trazem considerações para criação ou melhoria de um programa de segurança da informação (NIST, 2018).

Identificar: viabilizar a compreensão dos riscos de segurança cibernética para sistemas, pessoas, ativos, dados e recursos em um nível organizacional (NIST, 2018).

Proteger: descreve as prevenções adequadas visando a garantir o funcionamento dos serviços de infraestrutura crítica e limitar ou conter o impacto de potenciais eventos de segurança cibernética, empregando, muitas vezes, uma estratégia de defesa em camadas (NIST, 2018).

Detectar: define rotinas e ações de segurança adequadas visando à identificação de eventos de segurança cibernética a tempo de reagir a ameaça (NIST, 2018).

Responder: destaca as atividades adequadas a serem feitas quando um incidente de segurança ocorrer, para melhorar a resposta e reduzir o impacto do evento (NIST, 2018).

Recuperar: desenvolvimento de atividades apropriadas para melhorar o planejamento focado em aumento de resiliência e um plano de restauração de recursos ou serviços que foram prejudicados durante um ataque cibernético, melhorando a resposta a incidentes (NIST, 2018).

2.3.2. Avaliação da estrutura do Cybersecurity Framework

A avaliação viabiliza a criação de um esquema para implementação de segurança cibernética bem como é utilizada para identificar e priorizar demandas, podendo ser realizada de forma geral ou fazer várias análises de modo a avaliar componentes específicos e identificar necessidades específicas. Na avaliação de uma organização, analisam-se seus requisitos e objetivos organizacionais, propensão a risco e recursos em relação ao estado atual ou aos resultados desejados de acordo com a Estrutura Básica, tudo isso alinhado às funções, categorias e subcategorias (NIST, 2018).

Nesse sentido, a avaliação visa a melhorar os padrões de segurança e reduzir o risco em uma organização.

Para alcançar objetivos de gerenciamento de risco de segurança cibernética, uma comparação entre o estado atual e o estado desejado pode evidenciar as lacunas de segurança. Nesse cenário a organização pode direcionar melhor os recursos com uma abordagem guiada pelo risco e alcançar os objetivos de segurança da informação (NIST, 2018).

2.3.3. Níveis de implementação da estrutura do Cybersecurity Framework

Os níveis de implementação evidenciam a visão da organização sobre a postura atual quanto à segurança da informação e seus processos em relação a isso. O guia *NIST CSF* descreve quatro níveis de implementação (NIST, 2018).

A categorização de níveis leva em consideração o regime atual de gerenciamento de risco da organização como um todo, abrangendo requisitos legais e regulamentação, práticas de compartilhamento de informações, objetivos da organização e restrições (NIST, 2018).

Cada organização deve avaliar qual o nível requerido para que possa alcançar seus objetivos e suas metas como instituição, de forma que a implementação seja viável e que consiga reduzir o risco da segurança cibernética de ativos a níveis adequados (NIST, 2018).

Assim sendo, a NIST explicitamente afirma que esses níveis não são necessariamente uma representação de nível de maturidade, e sim uma forma de auxiliar a organização sobre risco cibernético na hora da tomada de decisão. A progressão para níveis de implementação mais altos é estimulada conforme uma análise de custo-benefício que aponte que a redução do risco de segurança cibernética seja viável e economicamente vantajosa (NIST, 2018).

São quatro os níveis de implementação, sendo assim, quanto maior o nível, mais sofisticadas são as práticas de gerenciamento de risco cibernético que estão nas definições do *framework* como no Quadro 4 *(*NIST, 2018*)*.

Quadro 4 – Níveis de Implementação.

Nível	**Item**	**Descrição**
Nível 1: Parcial	Processo de Gerenciamento de Risco	Com práticas não formalizadas, ou seja, são feitas caso a caso e na maioria das vezes de forma reativa. A maneira de lidar e o foco de risco da organização e ameaças não possuem uma priorização nas rotinas de segurança, não sendo diretamente direcionadas.
	Programa Integrado de Gerenciamento de Risco	Gerenciamento de risco irregular, uma vez que não há uma homogeneidade de experiências ou fontes de informação externas, com baixa consciência sobre o risco de segurança cibernética. Portanto não possui processos que permitam um compartilhamento de informações sobre segurança cibernética de forma adequada.
	Participação Externa	Possui pouca consciência do papel que exerce na cadeia de suprimentos em que está inserida em termos de risco cibernético, seja como fornecedor seja como usuário, isso é, não compreende seu papel dentro do sistema em que está inserida e, portanto, não troca informações com outras organizações
Nível 2: Risco Informado	Processo de Gerenciamento de Risco	Possui alguma diretriz de segurança cibernética, com foco em alguns objetivos de risco, ambiente de ameaças ou requisitos de negócio, entretanto, apesar de ter alguma política de segurança, em alguns casos, essas medidas não são instituídas pela organização inteira.
	Programa Integrado de Gerenciamento de Risco	Com uma abordagem que não abrange toda a organização, as informações são compartilhadas de modo informal dentro dela, ou seja, existe alguma consciência sobre o risco de segurança cibernética, portanto há práticas de segurança cibernética em alguns níveis da organização com avaliação de risco interna e externa, porém não sistemática ou reproduzível.
	Participação Externa	A organização possui consciência dos riscos da cadeia de suprimentos em que está inserida e troca informações com outras organizações, compreendendo seu papel dentro do sistema, entretanto não há uma formalização de como abordar os riscos.
Nível 3: Reproduzível	Processo de Gerenciamento de Risco	A organização já possui formalizada as práticas de gerenciamento de risco como uma política organizacional expressa, sendo elas atualizadas regularmente conforme há mudanças nos requisitos de negócio inseridos em um cenário dinâmico de ameaças e tecnologia.
	Programa Integrado de Gerenciamento de Risco	Conhecimento de riscos com políticas, processos e procedimentos definidos e implementados da forma como planejado, havendo uma abordagem para a organização como um todo de gerenciamento de risco cibernético. Portanto, os colaboradores possuem conhecimento e habilidade adequados para desempenho de suas funções, com métodos consistentes de resposta às mudanças nos paradigmas de risco. A comunicação do alto escalão é regular e há troca de informação sobre o risco de segurança cibernética de forma que a operação tenha sua análise de segurança cibernética analisada e assegurada.
	Participação Externa	Colabora e recebe informações de outras entidades, entendendo seu papel em um ecossistema maior e compreendendo os riscos de cadeia de suprimentos cibernéticos associados a sua atividade, complementando informações geradas internamente e ajudando outras entidades. Suas práticas são formalizadas e escritas, com estruturas de governança,

Nível	Item	Descrição
		explicitando requisitos e implementação e por fim monitoramento das práticas.
Nível 4: Adaptável	Processo de Gerenciamento de Risco	Com um processo de aperfeiçoamento contínuo, a organização adapta suas práticas de segurança cibernética com base em suas práticas atuais e anteriores, com expertise adquirida e indicadores, incorporando tecnologias e práticas mais avançadas de segurança cibernética. Em um cenário dinâmico de ameaças a organização tem uma postura ativa, adaptando-se e respondendo de forma eficaz as novas ameaças que surgem.
	Programa Integrado de Gerenciamento de Risco	Trata as possíveis ocorrências de segurança cibernética com uma abordagem que inclui toda a organização, com um gerenciamento de risco que se utiliza de políticas, processos e procedimentos sobre risco, com um orçamento que leva em consideração o ambiente de risco atual e previsto, pesando a tolerância a risco e a relação entre os objetivos da organização, e a segurança cibernética é abertamente compreendida e analisada no processo de tomada de decisão.
	Participação Externa	A organização compreende seu papel como um todo no ecossistema macro e contribui também para a comunidade sobre riscos, gerando e analisando informações com uma contínua avaliação de seus riscos conforme o cenário se altera. Com uma ação em tempo real, a organização busca agir de forma consistente sobre riscos da cadeia de suprimento cibernética que está inserida, usando muitas vezes acordos formais e informais para manutenção de um relacionamento de troca de informações com a cadeia de fornecimento.

Fonte: NIST (2018).

2.4. ISO 27000 SERIES

A *International Organization for Standardization* (ISO) é uma organização internacional de organismos de padronizações nacionais que desenvolve padrões tecnologia e comércio e possui vários comitês com grupos de interesse em cada matéria. Nesse contexto, os padrões ISO/IEC 27000 são os que detalham requisitos para um sistema de gerenciamento de segurança da informação. Outros *frameworks*, como o NIST CSF, indicam algumas recomendações ISO e são compatíveis com a série de padrões ISO 27000. Essa série tem como objetivo ajudar as organizações a implementarem um sistema de gerenciamento de segurança da informação (NIST, 2018; ISO, 2018).

Os padrões das séries ISO/IEC 27000 são separados da seguinte maneira:

- Terminologia/Vocabulário;
- Requisitos;
- Diretrizes gerais; e
- Diretrizes específicas de setores.

O padrão ISO/IEC 27000:2018, padrão de terminologia, descreve os fundamentos dos sistemas de gerenciamento de segurança da informação que compõem a série ISO 27000. Ele traz uma visão ampla dos padrões de sistema de gerenciamento de segurança da informação pertencentes à família de ISO 27000. Essa norma também traz os termos e as definições utilizadas em todos os padrões dessa série de padrões (ISO, 2018).

Padrões de requisitos se direcionam a fornecer os requisitos normativos para o desenvolvimento de sistemas de gerenciamento de segurança da informação, organizações de auditoria e emissores de certificação e também para aperfeiçoamento dos requerimentos já inclusos na ISO/IEC 27001:2013 (ISO, 2018). Os padrões de requisitos são três e estão descritos como no Quadro 5.

Quadro 5 – Padrões de requisitos

Padrões de Requisitos	**Descrição**
ISO/IEC 27001	Esse padrão detalha os requisitos para a organização implementar, melhorar, revisar ou manter um sistema de gerenciamento de segurança da informação, fornecendo também os requisitos para controles de segurança customizados para necessidades de uma organização ou parte dela, com finalidade de mitigar riscos associados aos ativos de informação que visam a proteger. Podendo ser usado por qualquer organização, grande ou pequena e de qualquer tipo (ISO, 2013).
ISO/IEC 27006	Direcionado para organizações vinculadas a certificação de sistema de gerenciamento de segurança da informação e de auditoria, ou seja, esse padrão é para a certificação de organizações que certificam a segurança pelos padrões ISO. Sendo assim, traz requisitos necessários para qualquer pessoa ou organização que forneça certificação de sistema de gerenciamento de segurança da informação (ISO, 2018).
ISO/IEC 27009	Detalha como inserir requisitos adicionais, melhorar e incluir controles além dos contidos no ISO/IEC 27001 para qualquer setor específico evitando conflito com os requisitos existentes, garantindo que os componentes inclusos possam ser incorporados (ISO, 2018).

Fonte: ISO(2013) e ISO(2018).

Padrões de diretrizes gerais e específicas são guias de implementação, enquanto os padrões de requisitos se focam mais normativamente, os de diretrizes focam em mecanismo para implementação, auditoria, avaliação e aperfeiçoamento (ISO, 2018). Os padrões de diretrizes gerais são dez e estão descritos no Quadro 6.

Quadro 6 – Padrões de diretrizes gerais

Padrões de Diretrizes Gerais	**Descrição**
ISO/IEC 27002	Traz referência a uma lista de práticas aceitas e boas práticas de controle, esta norma orienta no processo de implementação auxiliando a seleção de controles.

Padrões de Diretrizes Gerais	Descrição
	Nesse contexto, detalha sobre a implementação de controles de segurança da informação segundo as cláusulas de 5 a 18 da norma ISO/IEC 27001:2013 (ISO, 2018; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2013).
ISO/IEC 27003	Esse padrão fornece orientações e uma base para implementação de um sistema de gerenciamento de segurança da informação com êxito de acordo com a ISO/IEC 27001 (ISO, 2018).
ISO/IEC 27004	Esse padrão é destinado a ajudar organizações a avaliar o desempenho de seu sistema de gerenciamento de segurança da informação nos moldes dos requisitos da ISO/IEC 27001:2013. Portanto, traz uma estrutura para medição do desempenho e da eficácia da gestão da segurança da informação, dos processos e dos controles e por fim análise e avaliação de resultados do monitoramento e medição (ISO, 2018).
ISO/IEC 27005	Com uma abordagem de gestão de riscos orientada a processos, instrui e auxilia na implementação para satisfazer a ISO/IEC 27001 no que tange a requisitos de gerenciamento de risco de segurança da informação. Entretanto, para gestão de riscos de segurança da informação, essa norma não entrega um método específico, sendo responsabilidade da organização definir a sua abordagem no processo de gestão de riscos (ABNT, 2019)
ISO/IEC 27007	Fornece instrução para gerenciamento de um sistema de gerenciamento de segurança da informação. Detalha sobre auditorias internas ou externas de um sistema de gerenciamento de segurança da informação e avaliação dos profissionais do programa de auditoria de acordo com os requisitos da ISO/IEC 27001 (ISO, 2011).
ISO/IEC TR 27008	Sem finalidade de orientar sobre apuração de conformidade sobre à medição, avaliação de risco ou auditoria de um sistema de gestão de segurança da informação, especificado em outras orientações da ISO. Sendo assim, essa ISO dá foco nas revisões dos controles de segurança da informação, compreendido também a verificação da conformidade técnica, em relação a um padrão de implementação de segurança da informação, que é de competência da organização estabelecer (ISO, 2018).
ISO/IEC 27013	Trata sobre a ISO/IEC 27001 e ISO/IEC 20000-1, explicando características e pontos em comum, auxiliando empresas que tenham interesse em implementar esses dois padrões, ou que já tenha um e queira implementar o outro, ou para integrar os dois. Sendo assim, visa a proporcionar conhecimento para auxiliar organizações no planejamento de um sistema de gestão integrado com esses dois padrões (ISO, 2018).
ISO/IEC 27014	Este padrão visa a trazer orientação para uma governança de segurança da informação adequada, explicitando conceitos e princípios de governança de segurança da informação que permitam as organizações avaliarem, direcionarem, monitorarem e comunicarem sobre atividades relacionadas à segurança da informação de forma a dar suporte aos objetivos de negócios definidos (ABNT, 2013).
ISO/IEC TR 27016	Complementa outros padrões da família de sistemas de gerenciamento de segurança da informação, trazendo para a proteção de ativos de informação uma visão mais ampla no contexto em que a organização está inserida. Sendo assim, traz orientações de como avaliar seus ativos de informação e potenciais riscos dentro de uma visão também econômica, fornecendo assim uma noção de como

Padrões de Diretrizes Gerais	Descrição
	definir o montante de recursos que devem ser utilizados na proteção desses ativos por meio de modelos e exemplos (ISO, 2018).
ISO/IEC 27021	Estabelece as competências necessárias para os profissionais que atuam com sistemas de gerenciamento de segurança da informação para atuar em sistemas em conformidade com a ISO/IEC 27001:2013, ou seja, é direcionado a profissionais que almejam compreender e realizar o trabalho nesta área, empresas que buscam candidatos em potencial para atuarem com segurança da informação e organizações que desejam criar certificações e exames, ou treinamento para atuação em sistemas de gerenciamento de segurança da informação (ISO, 2018).

Fonte: ABNT (2013), ABNT (2019), ISO (2011) e ISO (2018).

Os padrões de diretrizes específicas são padrões que complementam e trazem processos adaptados a um setor ou particularidade específica, com um total de cinco padrões, estes estão descritos no Quadro 7.

Quadro 7 – Padrões de Diretrizes Específicas

Padrões de Diretrizes Específicas de Setor	Descrição
ISO/IEC 27010	Fornece informação sobre gerenciamento de informação entre organizações e/ou setores. Sendo assim traz orientações sobre como implementar segurança da informação em um ambiente de compartilhamento de informações com uma determinada comunidade, sendo destinado para iniciar, implementar, manter ou melhorar segurança da informação entre organizações e entre setores, podendo ser aplicado seja na esfera pública seja na privada, nacionalmente ou internacionalmente (ISO, 2018).
ISO/IEC 27017	Se trata de um código de conduta para controles de segurança da informação especificado na ISO/IEC 27002 para serviços em nuvem; sendo assim, traz orientações adicionais quanto a controles e implementação especificamente para serviços em nuvem, tanto para provedores desse serviço quanto para clientes (ISO, 2018).
ISO/IEC 27018	Para empresas públicas ou privadas, organizações não governamentais e instituições de governo que forneçam ou que atuem como controladores de informações de identificação pessoal em computação em nuvem, embora controladores possam estar sujeitos a outras regulamentações e obrigações adicionais. Então esse padrão indica quais são os objetivos de controle mais aceitos, controles e condutas para implementação para proteção de informações de identificação pessoal (ISO, 2018).
ISO/IEC 27019	Este padrão se refere a controles de segurança da informação para o setor de energia baseada na ISO 27002:2013, voltado para concessionárias de energia para controlar e monitorar a produção ou geração, transmissão, armazenamento e distribuição de energia elétrica, gás, óleo e calor. Portanto orienta sobre medidas e objetivos de segurança estabelecidos pela ISO 27002 e fornece

Padrões de Diretrizes Específicas de Setor	Descrição
	diretrizes para que seus controles atendam a requisitos especiais adicionais para sistemas usados por concessionárias, incluindo processos de avaliação e tratamento de risco que constam na ISO 27001:2013. Entretanto, esse padrão não inclui o controle de processo de instalações nucleares, essas são cobertas pela IEC 62645 (ISO, 2018).
ISO 27799	Fornece orientação sobre padrões de segurança da informação e gerenciamento de segurança da informação direcionado a instituições que gerenciam informações sobre saúde, ou seja, descreve os controles contidos nas ISO/IEC 27002 e suplementa alguns aspectos voltados a especificidade do setor (ISO, 2018).

Fonte: ISO (2018).

2.5. Outros Frameworks

Esta seção se dedica a destacar *frameworks* formulados a partir do guia NIST CSF ou dos padrões ISO/IEC 27000, que buscam solucionar ou simplificar algum problema específico.

2.5.1. Italian National Cyber Security Framework

Baseado no *framework* da NIST, a estrutura de segurança cibernética da Itália foi desenvolvida para abordar, de forma unificada, a segurança e a redução de riscos com foco em empresas pequenas, médias e grandes. A estrutura italiana pode se comunicar com outros padrões conhecidos devido à sua compatibilidade com a NIST. O *framework* cobre todo o ciclo de vida de um sistema de segurança desde a concepção ao desenvolvimento, operação e manutenção, fornecendo para pequenas empresas também uma série de práticas que são econômicas e simples (ARMENIA, 2019).

Trazendo para si os conceitos, de uma forma derivada, do núcleo, da avaliação e dos níveis de implementação da NIST, o *framework* italiano também cria dois novos conceitos: os níveis de prioridade, que ajudam a organização a identificar preliminarmente quais subcategorias se deve investir para redução de risco; e os níveis de maturidade, os quais permitem medir a maturidade de um procedimento ou tecnologia (ARMENIA,2019).

2.5.2. Avaliação de segurança cibernética para pequenas e médias empresas

Para pequenas e médias empresas (PME), a extensão e a complexidade e por não especificar níveis aceitáveis de segurança, ou base para comparação, a NIST, embora forneça uma base sólida, não permite que tenham medida a efetividade da implementação de práticas de segurança cibernética (BENZ; CHATTERJEE, 2020).

Pensando nisso, Benz e Chatterjee (2020) desenvolveram uma ferramenta de avaliação de segurança cibernética (CET) que especificamente se baseia em 35 dos 96 controles definidos pela NIST, sendo esses 35 os mais relevantes para medição do perfil de risco operacional de uma PME típica, levando em consideração a experiência dos autores e que uma PME pode não dispor do tempo necessário para trabalhar em cada um dos 96 controles, dada a sua própria limitação de recursos.

A metodologia da CET fornece recomendações para cada lacuna de segurança percebida, também fornecendo pontuações de custo-benefício para solução de algumas lacunas, levando em consideração o custo e o esforço de implementação. Esses mecanismos e essas formas de calcular e gerar recomendações foram criadas a partir de 10 anos de experiência, revisão da literatura e com opiniões de pessoas do setor de segurança cibernética e acadêmicos (BENZ; CHATTERJEE, 2020).

2.5.3. Cyber-Security Architecture Framework para países subdesenvolvidos

Focado em países subdesenvolvidos ou países em desenvolvimento, enquanto outras estruturas são consideradas mais robustas e completas, estas não são fáceis de implementar. Então construído com base no ITI-GAF que é uma estrutura de arquitetura desenvolvida pelo *Institute of Information Technology - Hanoi National University*, o *Cyber-Security Architecture Framework (CSAF)* vem com a proposta de avaliar o nível de segurança de uma organização de forma precisa, rápida e compreensível.

Assim, para criar o modelo de avaliação do CSAF, Viet et al. (2017) utilizaram os padrões ISO 27001 e ISO 27002 por sua cobertura ampla, com uma abordagem de gerenciamento de riscos focada no controle preventivo. Sendo assim, o CSAF pode ser aplicado a três níveis, que são o básico, o intermediário e o avançado, ou seja, conforme a necessidade pode-se optar por níveis mais complexos com uma maior cobertura.

Sendo assim, com o CSAF, cada organização pode identificar em que parte precisa de investimento e como isso interage com as outras partes, identificando pontos fortes e fracos de segurança cibernética, permitindo a curto e longo prazos desenvolver planos de ação e monitoramento. Então herda funcionalidades boas de arquiteturas maiores, porém simplificadas para se adequar à infraestrutura e à capacidade de países subdesenvolvidos ou em desenvolvimento (VIET et al., 2017).

2.6. Cultura de segurança cibernética

Alguns relatórios de empresas de tecnologia apontam que uma quantidade significativa de problemas da segurança da informação está diretamente relacionada a colaboradores que não estão seguindo as políticas de segurança da informação determinadas pela organização. Sendo assim, as empresas fornecem estruturas e possuem expectativas sobre isso, porém o risco acaba sempre ficando junto aos colaboradores, que nem sempre possuem um comportamento previsível (NTT *Security*, 2019; VEIGA, 2020).

Enquanto um conceito ideal de cultura de segurança da informação não é explicitamente bem definido, resultados negativos são normalmente direcionados a funcionários ou a falta de proatividade dos empregadores. Desse modo, visando à solução desses resultados negativos do contexto da organização importa definir uma cultura de segurança da informação com foco em proteger as informações, mediante políticas de segurança e procedimentos somados a uma cautelosa implementação de requisitos, tudo isso por meio de comunicação, iniciativas, formação e educação dos profissionais inseridos nesse contexto (VEIGA, 2020).

O próprio esforço sistemático, que tem de ser melhorar continuamente e alcançar esse patamar, segundo Veiga (2020), dada a própria natureza da noção de cultura de segurança da informação, é um obstáculo em si.

Nesse contexto, a ideia de mudança, de forma consciente ou inconsciente, pode gerar resistência nos colaboradores, ainda que seja percebida como algo positivo. Normalmente, os trabalhadores preferem continuar com o que são familiarizados, pois a mudança e a adaptação a novos métodos e procedimentos geram um estresse que pode favorecer para que mais erros aconteçam. Então entender que as organizações possuem sua própria cultura e que isso representa seu próprio clima e filosofia são os princípios básicos para mudança e é o que os responsáveis pela mudança devem seguir (WHITMAN; MATTORD, 2015. p. 525).

Portanto os obstáculos encontrados para melhorar a cultura de segurança cibernética estão relacionados a aspectos humanos como: treinamento, falta de treinamento ou treinamento insuficiente, conscientização, gestão fraca ou falta de gestão, compreensão, falta de conhecimento sobre o assunto, cultura em si, falta de confiança ou barreiras de mudança, sistemas complexos ou falta de um sistema direcionado à questão (VEIGA, 2020).

Então, para que seja desenvolvida uma cultura de segurança cibernética apropriada, o colaborador deve compreender as verdadeiras consequências de suas ações e passar a adotar procedimentos adequados para atingir o objetivo de segurança, mas isso deve ser feito de maneira coletiva com adesão total e compreensão de riscos; portanto, adoção de consequências para não conformidade e, em contrapartida também, ter reconhecimento de estar em conformidade devem ser considerados para gestão (VEIGA, 2020).

Sendo assim, no contexto de educar, aperfeiçoar e conscientizar os colaboradores para segurança da informação, também existem exercícios que podem ser feitos pela organização. Geralmente, em um exercício, são separados times em que as pessoas devem agir de acordo com um papel predeterminado, então esse trabalho em equipe permite desenvolver algumas funções da organização e integração em funções reais da organização (HAUTAMAKI, 2019).

O uso de jogos ou simulações já vem sendo investigado na educação de ensino superior para a preparação de futuros profissionais, e os resultados apontados até então são que, em boa parte dos casos, há um impacto positivo para alcançar um determinado objetivo (VLACHOPOULOS; MAKRI, 2017). No entanto, Hautamaki (2019) pondera que, devido à complexidade do tema, esse tipo de atuação ainda exige mais pesquisa sobre o assunto para que se compreenda melhor esse tipo de técnica.

2.7. Regulamentação sobre o uso de dados

No mundo atual, empresas coletam uma grande quantidade de informações pessoais de seus clientes, sejam dados como nome e endereço, seja rastreando o comportamento de navegação, mas esses dados normalmente são guardados com pouca segurança. Com várias notícias da mídia sobre incidentes de segurança e vazamento de dados, consumidores começam a ter ciência sobre o que acontece, levantando preocupações de como suas informações são tratadas (CONSUMERS INTERNATIONAL, 2018).

Nesse contexto, legisladores reconhecem a falta de proteção da legislação e passam a atualizar suas leis como no caso da *General Data Protection Regulation* (GDPR), lei sobre proteção de dados pessoais, que atualizou leis que datavam de 1995. Mais de 100 países possuem leis de proteção de dados e existe um crescente número dessas leis que tratam de proteção de dados (CONSUMERS INTERNATIONAL, 2018).

2.7.1. Lei Geral sobre Proteção de Dados Pessoais (LGPD)

A Lei Geral sobre Proteção de Dados Pessoais (LGPD) vem para preencher as lacunas de regulamentação do setor em uma sociedade cada vez mais orientada a dados, onde antes faltava segurança jurídica (MONTEIRO, 2018).

Nesse contexto, a Lei Geral sobre Proteção de Dados Pessoais é aplicada a organizações ou indivíduos, em território nacional, que se enquadrem nos perfis: tratamento de dados, oferta de bens ou serviços, tratamento de dados de indivíduos ou o objeto de tratamento de dados que tenham sidos coletados (BRASIL, 2018). Portanto, qualquer um que tenha relação com o uso de dados de pessoas localizadas no Brasil está sujeito a essa lei, ainda que a empresa não esteja localizada no País (BRASIL, 2018; IRAMINA, 2020).

De acordo com Iramina (2020), a LGPD possui sanções mais brandas quando comparada à regulação europeia, porém a estratégia dos legisladores é similar, com mecanismos de persuasão e punição que são aplicados de forma escalável e complementar.

Para Monteiro (2018), o País estava perdendo competitividade e, com a vinda desse marco, alguns pontos que eram conflituosos puderam ser preenchidos e substituídos. Dessa forma, o País se posiciona entre os países considerados com um nível de regulação adequado na proteção de dados pessoais e privacidade, que hoje são 120; e, segundo Farias (2019), a "LGPD no Brasil é mais uma das etapas no processo de mudança de regras em curso no mundo digital".

2.7.2. Regulamentações fora do Brasil

Com regulação semelhante, tem-se como exemplo mais conhecido a *General Data Protection Regulation* (GDPR), a qual a LGPD se inspirou. A GDPR tem seu conceito base, o direito à privacidade, criado em 1950, na Convenção Europeia dos Direitos Humanos. Segundo essa convenção, "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo

seu lar e pela sua correspondência". Desde então, a União Europeia tem procurado legislar em direção a alcançar esses ideais (WOLFORD, 2021; IRAMINA, 2020).

A extensão da GPDR vai além do próprio bloco, já que impõe obrigações a qualquer organização que vise ou colete dados de pessoas na União Europeia. Com multas que podem ultrapassar as dezenas de milhões de euros, isso faz a GPDR ser considerada uma legislação de privacidade mais rígida do que a LGPD, a exemplo de termos de sanções e punições. A regulamentação entrou em vigor no final de maio de 2018 (UNIAO EUROPEIA, 2016; FIELDING, 2019; IRAMINA, 2020).

O estado da Califórnia, nos Estados Unidos, criou o *California Consumer Privacy Act* (CCPA), que está em vigor desde 2020, e compartilha e replica vários mecanismos da GDPR, afetando apenas organizações locais e que possuam faturamento superior a US$ 25 milhões ou empresas cuja receita de venda de informações seja superior a 50% (FIELDING, 2019; STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, 2021).

No Japão, há o *The Act on the Protection of Personal Information* (APPI), que é bem alinhado com o GDPR, de tal forma que existe livre trânsito de dados entre Europa e Japão, pela semelhança entre as duas leis. Para tal, Japão concordou em implementar mais pontos de segurança para se alinhar as normas da União Europeia (NISHI, 2018).

2.7.3. Desafios na implantação da proteção de dados

Por outro lado, usando esse paralelo, a nossa regulação sobre o uso de dados na Europa, o GDPR, Gal e Aviv (2020) afirma que, com a nova regulação, o custo de estruturar os dados em conformidade com a lei pode ser alto, uma vez que é caracterizado por economia de escala e, assim, organizações menores podem não enxergar como lucrativo coletar dados.

A *European Comission (EC)* levanta preocupações que o GDPR coloque um peso desproporcional sobre pequenas e médias empresas, pois possuem menos recursos que as grandes empresas para se adaptar às mudanças que a legislação traz, ou seja, fortalece as grandes empresas e aumenta a concentração de poder de mercado (EUROPEAN COMISSION, 2020).

Nesse contexto, autoridades de proteção de dados trouxeram orientações, ferramentas, modelos e abertura para aconselhamento a pequenas e médias empresas. No entanto, a GDPR é muito nova como regramento e aborda um território ainda desconhecido na regulamentação,

sendo difícil que consiga levar em consideração todas as possibilidades e preocupações específicas de pequenas e médias empresas desde o início. Portanto, ainda há ações complementares que estão nas intenções da EC, que declarou que as medidas visando a apoiar as pequenas e médias empresas devem ser expandidas (EUROPEAN COMISSION, 2020).

Sendo assim, se uma legislação for capaz de reduzir os danos produzidos aos titulares dos dados, e com isso gerar um aumento de usuários com base no aumento da confiança ao ponto que compense os efeitos na perda de competitividade de alguns setores. Portanto, apesar da legislação afetar negativamente a competição, ela ainda pode gerar um aumento de bem-estar (GAL; AVIV, 2020).

3. METODOLOGIA

Essa Seção está dividida em 3 partes: tipo e descrição geral da pesquisa, população e amostra utilizada e procedimento de coleta e análise de dados. Portanto esta Seção tem como objetivo descrever as técnicas e os métodos utilizados para a execução dessa pesquisa.

3.1. Tipo e descrição geral da pesquisa

Pesquisas qualitativas são aquelas em que se destacam as particularidades de um caso, considerando se há uma relação indissociável entre o mundo e a subjetividade da coisa. Já em pesquisas quantitativas, observa-se a classificação de informações traduzidas em números, opiniões e informações (PRODANOV; FREITAS, 2013).

Nesse sentido, essa pesquisa tem abordagem qualitativa e quantitativa, pois os artigos coletados são avaliados e selecionados enquanto metadados são extraídos de forma qualitativa e, em seguida, os metadados são trabalhados e visualizados de forma quantitativa.

A pesquisa descritiva é feita quando o objetivo do pesquisador é descrever fenômenos, contextos ou eventos, ou seja, são trabalhos que procuram especificar propriedades, características e traços importantes de fenômenos analisados, descrevendo tendências de uma amostra (SAMPIERI et al., 2013, p. 99-102).

Revisão sistemática é definida por Fink (2014) como um método organizado e transparente, que possa ser replicado, que consiga avaliar trabalhos existentes registrados, sejam por pesquisadores, acadêmicos seja por profissionais. Para Higgins (2019), esse tipo de pesquisa foi desenvolvido para que as pessoas possam ser informadas por um entendimento atualizado de pesquisas relevantes a partir de uma necessidade de embasar decisões que afetam suas vidas, trazendo um resumo atualizado do estado atual do conhecimento da pesquisa.

Considerando as características apresentadas da pesquisa descritiva, essa se demonstra adequada para este trabalho, em que se procedeu a uma revisão bibliométrica que, segundo Vergara (2009), é sistematizada e se desenvolve na coleta de artigos publicados em periódicos em bases de dados on-line, posteriormente sendo analisados e selecionados.

3.2. População e amostra

A população deste trabalho é composta por artigos contidos nas bases de dados utilizando a palavra-chave *cybersecurity*, que retorna por base e quantidade de artigos respectivamente: *Google Scholar*, 254.000; *Semantic Scholar*, 14.800; *Scopus*, 10.281; *ScienceDirect* (Elsevier), 5.794 e *IEEExplore*, 5.693.

Com uma população total de 290.568 artigos, foram feitas novas formas de filtragem para viabilidade da pesquisa, então a amostra extraída para esse estudo é não probabilística, que segundo Sampieri et al. (2013) tem uma seleção informal em seu procedimento.

Para ter uma amostra mais direcionada ao tema, foram utilizadas mais combinações de palavras-chave/expressões-chave como: *action research*, *case study*, *critical infrastructure, cybersecurity, cyber, security, framework*, ISO, ISO/IEC 27000 *series,* NIST e *risk.* Não foi utilizado nenhum termo em português e foram selecionados os trabalhos que continham conteúdo adequado à pesquisa.

Para a seleção de artigos que compõem os resultados, o critério de inclusão adotado foi selecionar os artigos que continham a utilização total ou parcial do guia NIST CSF ou dos padrões das séries ISO/IEC 27000. Uma vez selecionados, os artigos tinham seus metadados extraídos, totalizando cinquenta artigos.

3.3. Procedimento de coleta e de análise de dados

Para a primeira etapa de desenvolvimento do trabalho, foi realizado mapeamento de artigos sobre a utilização de padrões ISO 27000 e o guia de segurança cibernética NIST CSF em revistas científicas e conferências. Com um critério amplo geográfico, a inclusão de artigos não se delimitou a nenhuma região, incluindo artigos de qualquer instituição em qualquer parte do globo.

A coleta de material foi realizada em um período de dois meses, entre fevereiro de 2021 e março de 2021, a busca foi feita utilizando bancos de dados para artigos científicos: *Google Scholar,* IEEExplore, *Scopus, ScienceDirect* e *SemanticScholar,* não se limitando a nenhuma revista científica específica, uma vez que existe uma vasta gama de revistas científicas que podem ter publicações relevantes ao tema. Portanto, a coleta foi realizada buscando publicações

relevantes especificamente ao tema, buscando artigos que tivessem o assunto direcionado à segurança cibernética e ao uso do guia NIST CSF ou as séries de padrões ISO/IEC 27000.

Por questões de viabilidade, a busca por artigos foi realizada exclusivamente pela internet, então alguns trabalhos importantes que possam não ter uma versão disponível on-line podem ter sido deixados de fora.

Assim, numa segunda etapa do desenvolvimento, foram selecionados, por meio de leitura e avaliação, artigos que utilizavam os padrões de segurança cibernética para aplicação em determinado setor/área de uma organização, seja ela pública e/ou seja privada, podendo fazer o uso integral ou parcial da estrutura escolhida ou até mesmo combinar com outras estruturas existentes, desde que utilizasse uma parte significativa de uma das estruturas escolhidas para esse trabalho.

Sendo assim, quando um artigo era selecionado, eram extraídos metadados para análise como:

- continente e país da universidade em que os autores do artigo eram filiados;
- temática aplicada, ou seja, contexto (exemplo: Setor Naval).
- de qual base de dados o trabalho foi coletado.
- ano de publicação.

Por fim, para a análise de dados, foram selecionados 50 artigos identificados como os que aplicavam o guia NIST CSF ou padrões ISO/IEC da série 27000. Após esse processo de análise de dados, foram extraídos os dados e metadados e inseridos em uma de planilha e posteriormente realizados a limpeza, o tratamento e o agrupamento para demonstração de resultados.

Uma vez agrupados os dados, foram gerados gráficos por base de dados, ano, geografia e tema. Contudo, quanto à distribuição por ano, gerou-se um gráfico suplementar utilizando regressão linear para averiguar a tendência do número de artigos por *framework*. Por fim, cada tipo de metadado conta com seção e discussão sobre os resultados em um capítulo que precede à conclusão, nele há a visualização dos metadado extraídos.

4. RESULTADOS E DISCUSSÃO

Esse capítulo apresenta os resultados a partir da análise dos metadados extraídos dos artigos selecionados, distribuídos em cinco subseções dedicadas a apresentar cada tipo de dado extraído e agrupado.

O número de artigos, ao todo cinquenta, foi selecionado para compor os resultados, porém existem artigos que utilizaram o NIST CSF combinado com padrões ISO/IEC 27000 no mesmo trabalho. Dessa forma, dos resultados, se feita uma soma das quantidades que aparecem, o número total será maior do que cinquenta em função de alguns artigos utilizaram ambas as estruturas de segurança.

4.1. Distribuição por base de dados

A Figura **Erro! Fonte de referência não encontrada.** mostra a quantidade de artigos utilizando uma das estruturas (ISO 27001 ou NIST) por base de dados. Como se pode verificar, a maior parte dos artigos selecionados foram extraídos da base *Scopus*. Também é possível notar que, dentro das bases procuradas, com exceção da *Scopus*, foram encontrados mais ISO do que NIST.

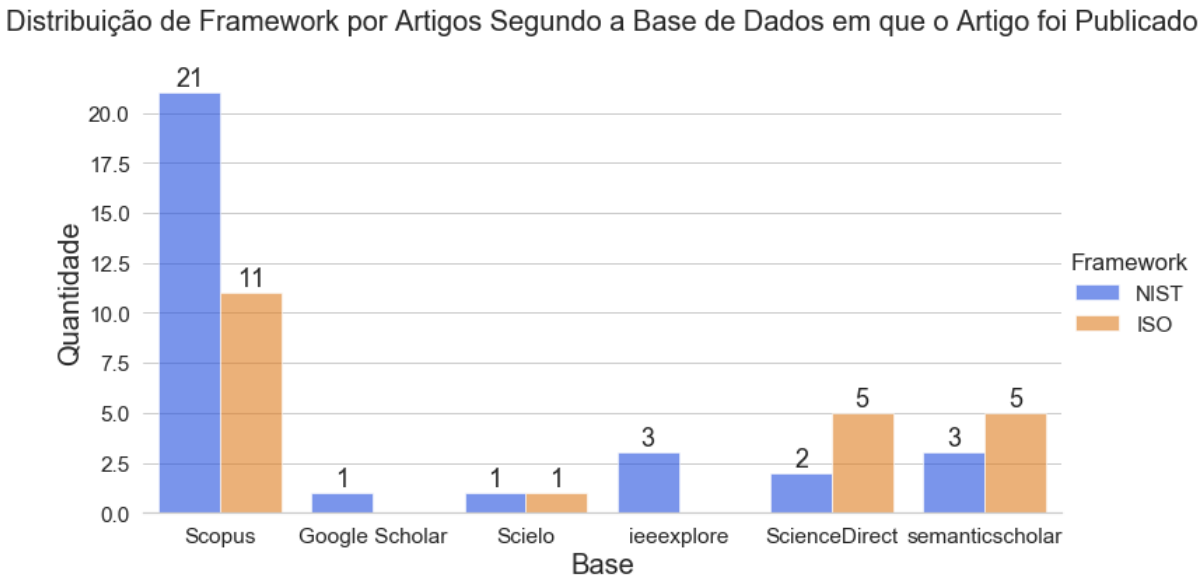


Figura 2 - Distribuição de framework por artigos segundo a base de dados em que o artigo foi publicado.

Quanto às bases de dados utilizadas e ao número de artigos selecionados, é possível deduzir que existem mais trabalhos para serem coletados, comparando as bases utilizadas em outros trabalhos, Suryotrisongko e Musashi (2019) utilizaram *Spinger Link*, *IEEE Xplore*, *ProQuest*, *Science Direct* e *ACM*, que, no caso, para este trabalho, dessas bases, foi

utilizado somente *ScienceDirect*, ou seja, ainda há mais território não explorado sobre os *frameworks* ISO, NIST, que, assim como essas bases citadas, podem haver outras menos conhecidas que possuam conteúdo relevante.

Dito isso, para uma amostragem maior, seria importante ampliar o escopo de bases de dados; e, para selecionar os artigos, validar qual base possui maior quantidade referente ao tema ou outras palavras-chave para obter uma filtragem mais eficiente.

4.2. Distribuição por ano de publicação do artigo

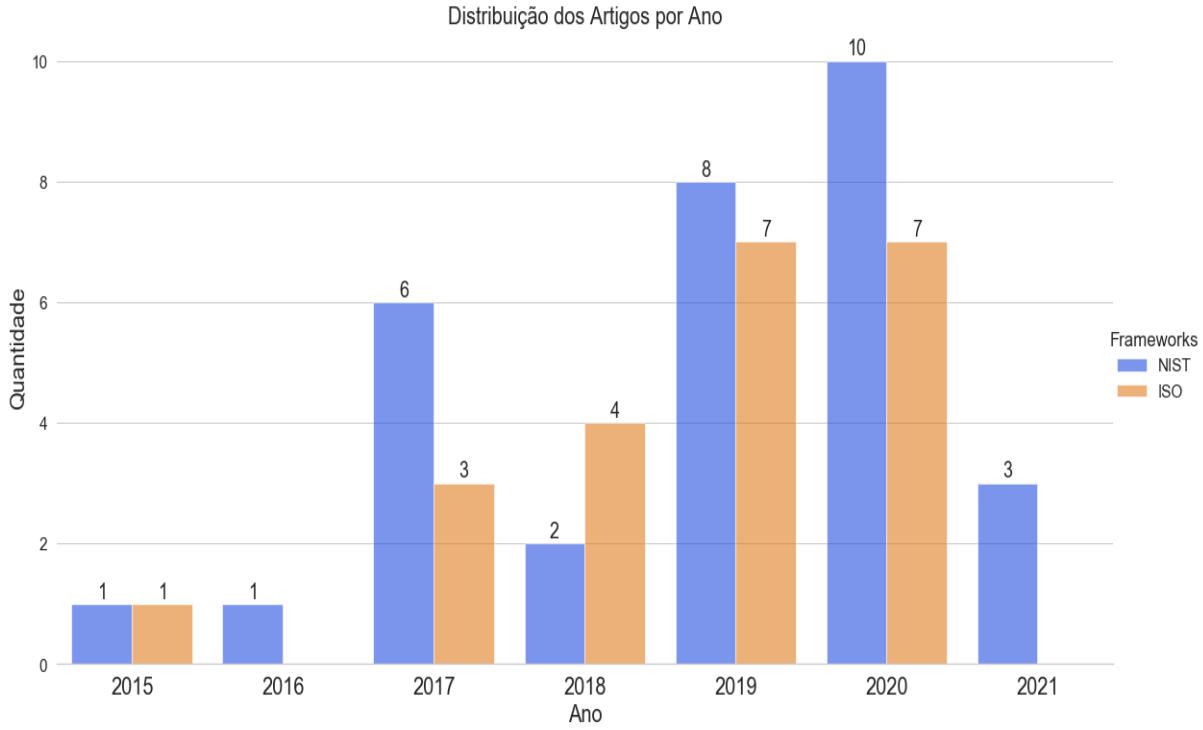


Figura 3 - Distribuição por ano

A Figura 3 mostra os artigos coletados distribuídos por ano e agrupados por uso de NIST. Também é possível notar um crescimento consistente de estudos na área de segurança cibernética.

Ao se observar a quantidade de artigos coletados agrupados por ano, observa-se que o ano de 2021 possui três artigos utilizando a estrutura da NIST exclusivamente, uma vez que não possuem nenhum ISO. Inicialmente parece algo pequeno ou de baixa relevância, mas o momento em que os artigos foram coletados era o fim do primeiro trimestre de 2021; esse fato demonstra que há potencialmente a tendência de crescimento. Para visualizar melhor essa

tendência, a Figura **Erro! Fonte de referência não encontrada.** desenha uma linha baseada em uma regressão linear que ilustra melhor o fenômeno.

Então, com a regressão linear, foi possível notar um crescimento no interesse e/ou na necessidade de se trabalhar o tema independente da escolha entre ISO ou NIST. Evidencia-se também que o guia NIST CSF tem crescido mais, mesmo as séries da família ISO/IEC 27000 existirem a mais tempo, não que uma exclua a outra, uma vez que a própria NIST herda alguns mecanismos de alguns padrões ISO.

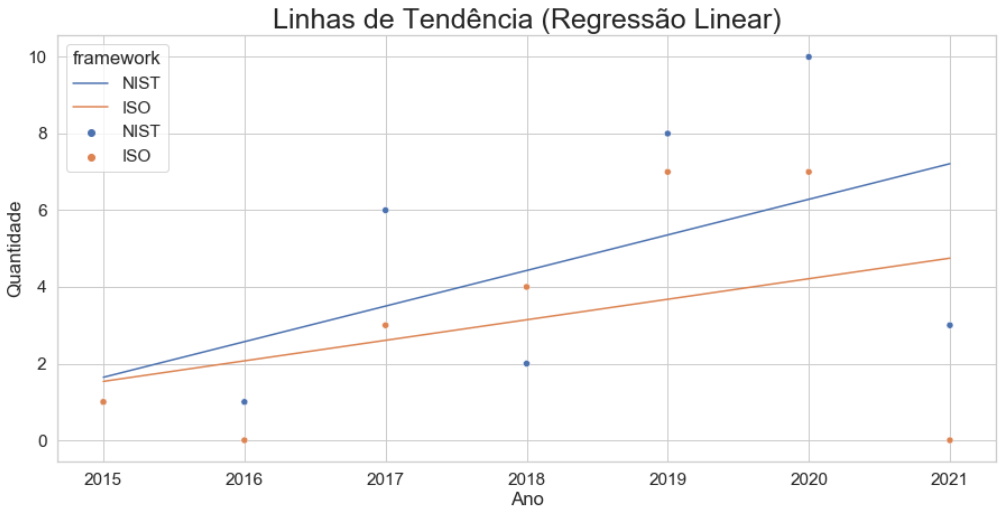


Figura 4 - Regressão/Linha de tendência

Observando os estudos que utilizaram NIST ou ISO, nota-se que, independentemente de qual está sendo mais utilizada, ambas demonstram uma tendência a crescer, ou seja, pode-se dizer que o tema tende a ser cada vez mais explorado a cada ano, tendo em vista que a sociedade caminha na direção de utilizar mais máquinas e automações. Desse modo, apesar de ambos os *frameworks* possuírem uma tendência a crescer, foi possível constatar que a NIST possui um crescimento mais acelerado em relação a ISO.

Entretanto, apesar da NIST possuir um crescimento maior no comparativo ano a ano, vale destacar que, se ignorado os artigos dos Estados Unidos (Figura **Erro! Fonte de referência não encontrada.**), é possível notar um equilíbrio entre a utilização dos *frameworks*. Então os Estados Unidos representam aproximadamente 30% dos artigos selecionados que utilizam o guia NIST CSF. Isso não exclui o fato de que a estrutura americana tem tido maior adesão e de que grandes organizações internacionais têm sua origem neste país, porém é importante se ater a esse destaque para compreender como a evolução tem acontecido.

4.3. Distribuição geográfica

A Figura **Erro! Fonte de referência não encontrada.** demonstra, de forma agrupada por *framework*, o continente das instituições às quais os autores dos artigos estão filiados. Portanto é possível notar, conforme ilustra a figura, que o interesse no uso de ferramentas NIST e ISO é relativamente balanceado na maioria das regiões, entretanto Oceania e América do Norte se destacam por terem interesse majoritariamente na estrutura de segurança cibernética americana.

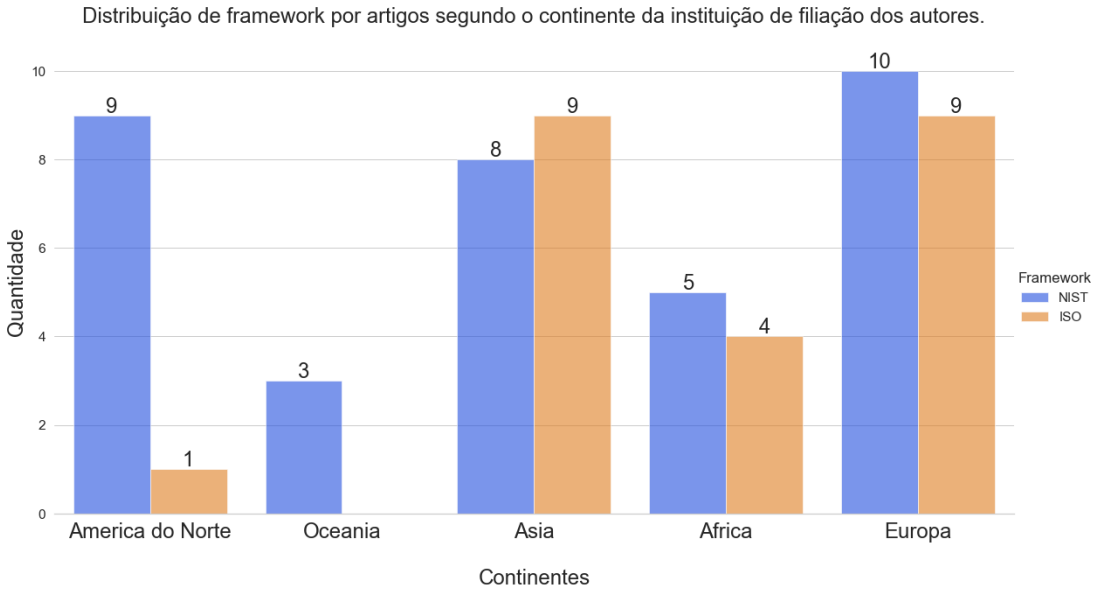
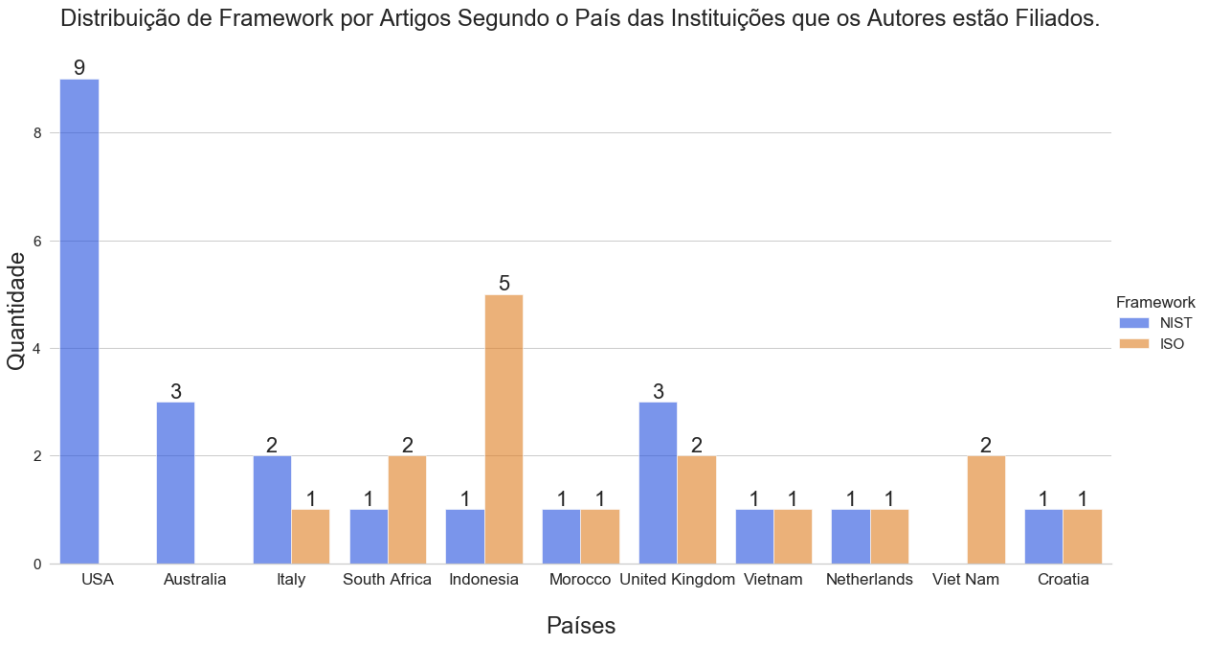


Figura 5 - Distribuição de framework por artigos segundo o continente da instituição de filiação dos autores.

Para ilustrar melhor, a Figura **Erro! Fonte de referência não encontrada.** mostra os países com instituições que publicaram mais que um artigo, utilizando NIST ou ISO, pois a contagem total de países envolvidos foram 32, destacando que há artigos com instituições de nacionalidades diferentes, ou seja, o que se propõe aqui é observar a nacionalidade das universidades interessadas em pesquisar o tema.

Quanto ao uso de NIST CSF ou ISO/IEC 27000, é possível notar que entre os continentes, a utilização é bem balanceada na Ásia, África e Europa. Contudo, quando se observa a América do Norte, há somente um artigo, estudo realizado no México, abordando ISO, enquanto que nos Estados Unidos há 9 artigos de NIST.



Sendo assim, os Estados Unidos provavelmente estão dando preferência para o *framework* nacional, enquanto outros países utilizam NIST e ISO de forma bem balanceada. WHITMAN e MATTORD (2015) reforçam esses dados afirmando que a maioria das empresas americanas podem ter resistência ao uso da ISO, com exceção de algumas poucas que possuem negócios na Europa (por conta de regulação específica), e ainda complementa que mesmo na origem do ISO 27002, vários países, incluindo Estados Unidos, Alemanha e Japão, afirmavam que haviam problemas básicos, por isso se recusaram a adotar esses padrões na época.

4.4. Distribuição de framework segundo o tema

Figura 6 - Distribuição de framework por artigos segundo o País das instituições que os autores estão filiados.

As nomenclaturas dos temas apresentados nessa seção foram elaboradas pelo próprio autor como uma forma de agrupar os dados por similaridade. Os artigos que foram classificados como “Não-Especificado” foram os que se propunham a implementação ou algum sistema, mas que não delimitavam ao tipo de organização a que se destinava. A Figura 7 apresenta os resultados distribuídos por tema, destaca-se que um artigo poderia ocupar mais do que um tema como por exemplo: Países Não-Desenvolvidos e Público/Governamental.

Observa-se que artigos que possuem temática de pequenas e médias empresas (PME) serem os de temas mais direcionados, superando artigos que focam em organizações de

tecnologia, algo que surpreende uma vez que segurança cibernética é diretamente relacionada a tecnologia.

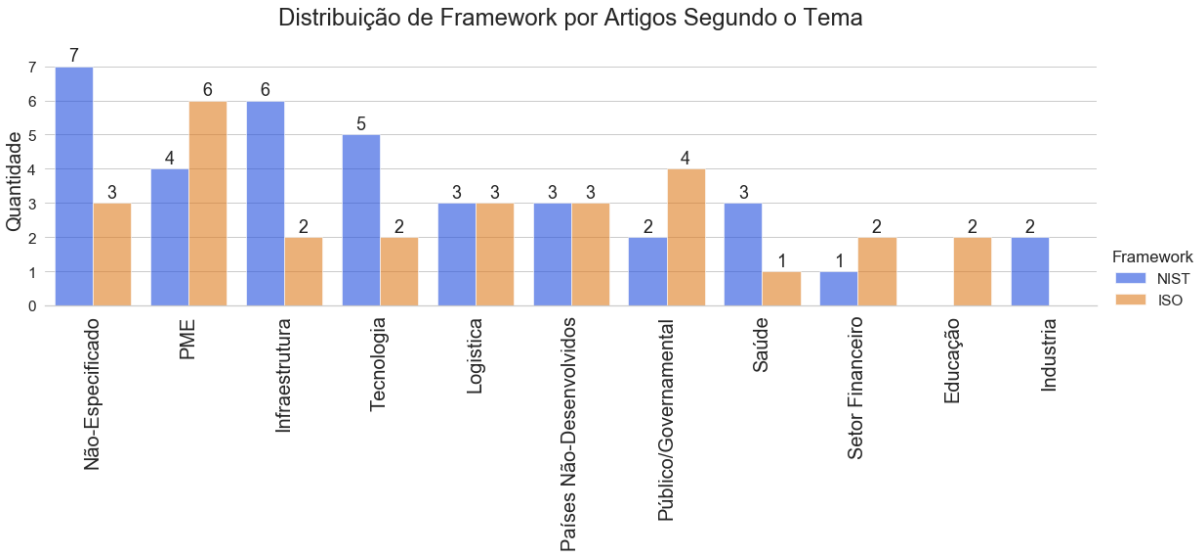


Figura 7 - Distribuição de framework por artigos segundo o tema

Assim, é possível que exista uma preocupação com pequenas empresas, uma vez que soluções de segurança não trazem novas funcionalidades. É mais difícil de ter ganho de popularidade, já que a segurança serve apenas aos interesses da organização, ou seja, não gera um impacto no objetivo principal do negócio (LE, 2017).

Desse modo, a realidade pode ser difícil para pequenas e médias empresas, tendo em vista que empresas maiores sofreram significativamente menos ataques e que empresas de porte médio correspondem a 50% dos incidentes registrados, ou seja, pessoas mal-intencionadas não estão atacando apenas os grandes, mas empresas menores podem estar em risco por ter uma estrutura mais defasada (STASIAK, 2018).

Dentro dos temas que foram agrupados, alguns possuem a possibilidade de serem decompostos, enquanto outras não, como PME, em sua maioria, não citam o setor específico, torna-se difícil segmentar. Dentro dos temas possíveis de serem decompostos, têm-se “Infraestrutura” e “Logística”.

.

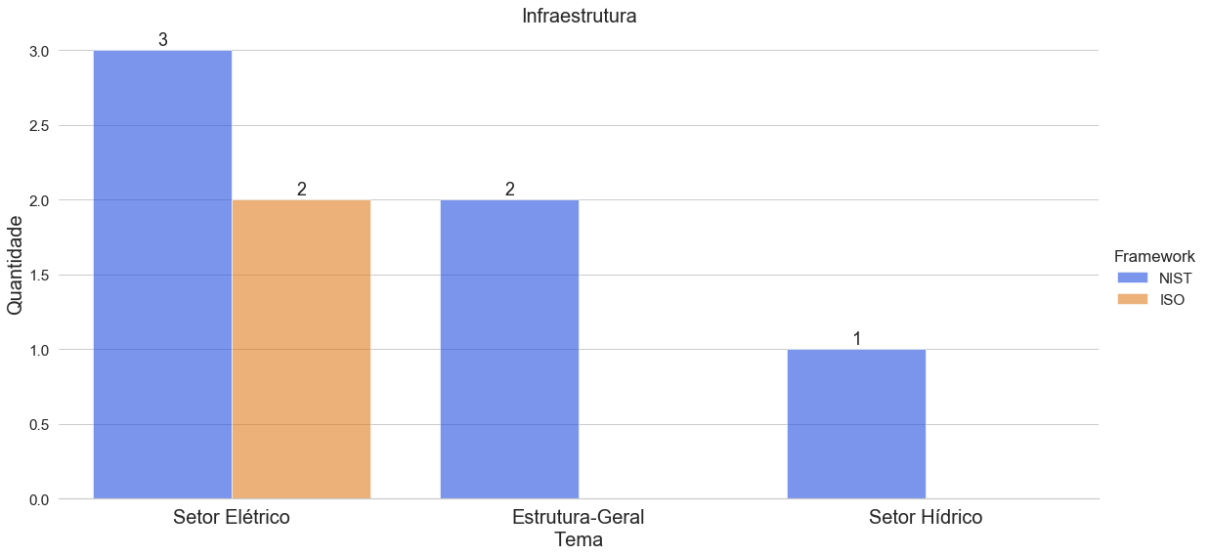


Figura 8 - Decomposição de tema - Infraestrutura

O tema de infraestrutura, representado pela Figura 8, tem em sua composição cinco artigos do setor elétrico e um do setor hídrico e dois de ‘Estrutura-Geral’. Estrutura-Geral são trabalhos dedicados à infraestrutura de forma “pura”, como prédios e instalações, podendo ser aplicado a estruturas críticas ou até mesmo um prédio residencial, por também se destinar a estruturas críticas, foi agrupado com “Infraestrutura”.

A Figura 9 decompõe os artigos do setor logístico, contabilizando os do setor naval (porto e navio), aviação civil e ferrovias.

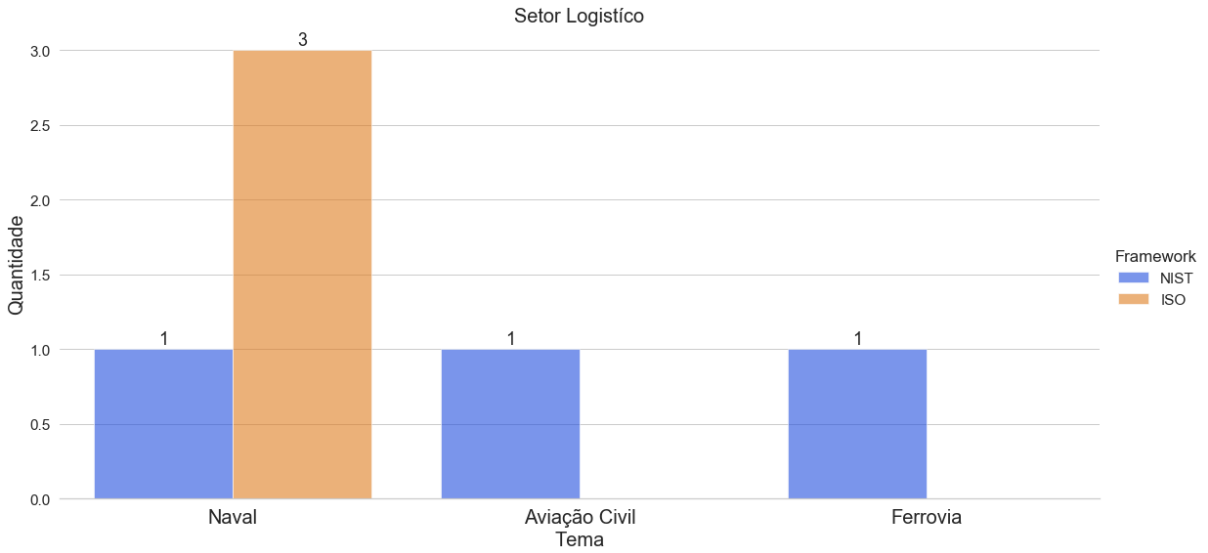


Figura 9 - Decomposição do tema - Setor Logístico

Dentro da decomposição do tema “Setor Logístico”, trabalhos direcionados ao setor naval foram destaques utilizando-se majoritariamente ISO, ou seja, embora quando agrupado como ‘Setor Logístico’ os *frameworks* empatem em quantidade, a Figura **Erro! Fonte de referência não encontrada.** demonstra que a utilização maior de ISO gera esse empate (quando agrupados).

4.5. Palavras-chave utilizadas nos artigos

Para trabalhar as palavras-chave dos artigos, foi feita uma nuvem de palavras para se obter uma visualização mais intuitiva de quais se destacam. Nessa nuvem de palavras, as que possuem maior frequência são maiores e a cor possui saturação maior.

Figura 10 - Nuvem de palavras dos artigos

A Figura 10 evidencia as palavras-chave mais frequentes nos artigos selecionados, em que os cinco mais frequentes são: *security*, *cyber*, *risk*, *information* e *system*. Os termos ISO e NIST estão em nono e décimo lugar na contagem de frequência de palavras-chave.

5. CONCLUSÃO

Este estudo teve como objetivo geral avaliar os artigos publicados sobre segurança cibernética com foco no uso de *frameworks* NIST CSF e as séries ISO 27000. Para atender ao objetivo geral, realizou-se um estudo descritivo, com abordagem quantitativa e qualitativa. Na composição dos resultados, 50 artigos foram selecionados para compor a amostra. A partir dos resultados desta pesquisa, foi possível atender ao objetivo geral e aos objetivos específicos.

O primeiro objetivo específico foi mapear artigos relacionados ao tema segurança cibernética com a utilização de padrões ISO/IEC 27000 ou o guia *Cybersecurity Framework* (CSF) da NIST. O segundo objetivo foi selecionar os artigos que trabalharam os padrões com viés de implementação. Esses objetivos foram alcançados por meio de análise qualitativa dos artigos e de seleção para compor os resultados, com a extração a agrupamento de metadados.

O terceiro objetivo específico foi traçar um panorama de como tem sido a distribuição desses padrões nos artigos, segmentados por ano, tema, região geográfica. O quarto objetivo foi identificar tendências dos artigos e aplicação. Estes objetivos (terceiro e quarto) foram atendidos: a Seção 4.2 atende aos objetivos de ano; a Seção 4.4 atende aos objetivos de tema; e a Seção 4.3 atende aos objetivos de distribuição geográfica.

A tendência de estudos sobre segurança cibernética e a utilização de padrões apresentam crescimento, como apresentado na Seção 4.2. Essa tendência de crescimento é notada para o uso tanto dos padrões ISO/IEC 27000 quanto para o guia *Cybersecurity Framework* (CSF) da NIST, entretanto o guia da NIST possui crescimento maior em relação ao uso dos padrões ISO, como percebido na regressão linear da Seção 4.2.

A tendência dos artigos em relação à distribuição geográfica está contida na Seção 4.3. A distribuição por continentes se mostrou equilibrada nos continentes asiático, africano e europeu. Porém Oceania e América do Norte apresentaram a utilização majoritária do guia da NIST, no caso da América do Norte.

A tendência dos artigos segundo o tema está relativamente bem representada em diversas formas de aplicação ou estudo, porém cabe destaque os estudos direcionados a pequenas e médias empresas (PME), tema de definição específica com maior número de artigos encontrados. Assim, existe um interesse em pesquisar sobre soluções para empresas pequenas ou médias, uma vez que essas são mais vulneráveis pela menor capacidade de investir em segurança cibernética.

Considerando o número significativo de trabalhos que também apresentaram como tema algo direcionado a países não-desenvolvidos, cabe ressaltar que é possível que exista um esforço dos pesquisadores em entender como estruturar a segurança cibernética para instituições com menos recursos disponíveis, tais como pequenas e médias empresas e países não-desenvolvidos.

Os objetivos específicos viabilizaram o objetivo geral desta pesquisa. Desse modo, por meio do estudo bibliométrico, foi possível descrever como e onde tem sido utilizados os padrões selecionados para este trabalho, observando quais temas e tendências têm sido abordados nas pesquisas disponíveis.

Este estudo pode colaborar com a comunidade acadêmica, pois traz um panorama do estado atual da produção de artigos envolvendo a utilização de padrões ISO da família de padrões ISO/IEC 27000 e o guia NIST CSF para segurança cibernética.

Após os resultados deste trabalho, há sugestões de investigações futuras, como investigar sobre estruturas de segurança cibernéticas desenhadas com um foco em pequenas empresas ou nações pobres, seja investigando como tem sido o desenvolvimento de estruturas menos complexas ou menos onerosas, seja criando e aplicando alguma versão simplificada de estrutura de segurança da informação de forma eficiente. Outra recomendação para pesquisas futuras é realizar novos estudos bibliométricos sobre o mesmo tema, mas com escopo maior de estruturas de segurança para comparar a evolução e também para observar se o campo de segurança cibernética como um todo está crescendo ou se há apenas uma troca (ex: diminui um de NIST e aumenta um de ISO, em vez de todos crescerem regularmente).

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:** Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014:** Tecnologia da informação – Técnicas de segurança – Governança de segurança da informação. Rio de Janeiro, 2013.

ARMENIA, S; FRANCO, E.; NONINO, F.; MEDAGLIA, C. Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks. **Systems Research and Behavioral Science**, v. 36, 21 set. 2018.

BENZ, M; CHATTERJEE, D. Calculated risk? A cybersecurity evaluation tool for SMEs. **Business Horizons**, v. 63, n. 4, p. 531-540, 2020.

BRASIL. **Lei nº 13.709/18, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 28 fev. 2021.

BRECHBUHL, H.; BRUCE, R.; DYNES, S.; JOHNSON, M.E. Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. **Information Technology for Development**, v. 16, p. 83-91, 2010.

CALDER, A.; WATKINS, S. **IT Governance**: A Manager's Guide to Data Security and ISO 27001 / ISO 27002. 4. ed. [*S. l.*]: Kogan Page, 2008.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999. v. 1.

CHERDANTSEVA, Y.; HILTON, J. A reference model of information assurance & security. In: **2013 International Conference on Availability, Reliability and Security**. IEEE, 2013. p. 546-555.

CONSUMERS INTERNATIONAL, Coming Together for Change. **The State of Data Protection Rules around the World: a briefing for consumer organisations.** Disponível em: <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>. Acesso em: 22 mai. 2021.

CYBER SECURITY OBSERVATORY. **CYBERSECURITY:** risks, progress, and the way forward in latin america and the caribbean. 2020. Disponível em: <www.cybersecurityobservatory.org>. Acesso em: 7 abr. 2021.

EUROPEAN COMMISSION (EC). **Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation.** European Commission COMM- EUR-Lex - 52020dc0264 -EN. 2020. Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264&qid=1618842473564>. Acesso em: 13 abr. 2021.

EZINGEARD, J.; BIRCHALL, D. Information Security Standards: Adoption Drivers (invited Paper). **International Federation for Information Processing Digital Library; Security Management, Integrity, and Internal Control in Information Systems**, v. 193, 2006.

FARIAS, E; RACHED, G. PRIVACY IN BRAZIL: analysis on the new law on data protection. In: INTERNATIONAL CONFERENCE ON WWW/INTERNET 2019, 18., 2019, Cagliari. **Proceedings of the 18th International Conference on WWW/Internet 2019.** Cagliari: Iadis Press, 2019. p. 177-180.

FIELDING, J. Four differences between the GDPR and the CCPA. **Help Net Security**, [*S. l.*], p. 1, 4 fev. 2019. Disponível em: <https://www.helpnetsecurity.com/2019/02/04/gdpr-ccpa-differences/>. Acesso em: 6 abr. 2021.

FINK, A. **Conducting Research Literature Reviews**: from the internet to Paper. 4. ed. Estados Unidos: SAGE Publications, 2014.

GAL, M.S.; AVIV, O. The competitive effects of the GDPR. **Journal of Competition Law & Economics**, v. 16, n. 3, p. 349-391, 2020.

GIUCA, O. et al. A Survey of Cybersecurity Risk Management Frameworks. In: **International Workshop Soft Computing Applications**. Springer, Cham, 2018. p. 240-272.

HAUTAMÄKI, J. et al. Cyber security exercise: Literature review to pedagogical methodology. In: **INTED Proceedings**. IATED Academy, 2019.

HIGGINS, J. **Cochrane Handbook for Systematic Reviews of Interventions.** 2. ed. Oxford: John Wiley & Sons, 2019. 704 p.

INTERNATIONAL ORGANIZATION FOR STANDARDZATION (ISO). **ISO/IEC 2382:2015:** Information technology – Vocabulary. 2015

INTERNATIONAL ORGANIZATION FOR STANDARDZATION. **ISO/IEC. 27000:2018:** Information technology – Security techniques – Information security management systems – Overview and vocabulary. Genebra, Suíça, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDZATION. **ISO/IEC 27001:2013:** Information technology – Security techniques – Information security management systems – Requirements. Genebra, Suíça, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDZATION. **ISO/IEC 27007:2011:** Information technology – Security techniques – Guidelines for information security management systems auditing. Genebra, Suíça, 2011.

ISO. **ISO STANDARDS ARE INTERNATIONALLY AGREED BY EXPERTS.** Disponível em: < https://www.iso.org/standards.html>. Acesso em: 2 mar. 2021.

IRAMINA, A. RGPD V. LGPD: ADOÇÃO ESTRATÉGICA DA ABORDAGEM RESPONSIVA NA ELABORAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL E DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA. **Revista de Direito, Estado e Telecomunicações**, v. 12, n. 2, 2020.

KÖHLER, A.R.; SOM, C. Risk preventative innovation strategies for emerging technologies the cases of nano-textiles and smart textiles. **Technovation**, v. 34, n. 8, p. 420-430, 2014.

KOSUTIC, D. Which one to go with – Cybersecurity Framework or ISO 27001? **27001 Academy**. 23 fev. 2014. Disponível em: <https://advisera.com/27001academy/blog/2014/02/24/which-one-to-go-with-cybersecurity-framework-or-iso-27001/>. Acesso em: 20 abr. 2021

LAUDON, K.C.; LAUDON, J.P. **Management Information Systems: Managing the Digital Firm.** 13 ed. Harlow: Pearson Education Limited, 2013.

LE, M. et al. An Assessment Model for Cyber Security of Vietnamese Organization. **VNU Journal of Science: Policy and Management Studies**, v. 33, n. 2, 2017.

LOVEJOY, K. **Organizations across the globe need to develop a ransomware payment policy, anticipating a potential future attack.** Junho 2020. Disponível em: <https://www.ey.com/en_gl/consulting/ransomware-to-pay-or-not-to-pay>. Acesso em: 2 abr. 2021.

MONTEIRO, R. L. **The new Brazilian General Data Protection Law - a detailed analysis.** 2018**.** Disponível em: <https://iapp*:*org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/>. Acesso em: 1º mar. 2021.

MORI, S.; GOTO, A. Reviewing National Cybersecurity Strategies. **Journal of Disaster Research**, v. 13, n. 5, p. 957-966, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST CSF:** Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, Estados Unidos. 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-53 Revision 4:** Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, Estados Unidos. 2015

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **SMALL BUSINESS CYBERSECURITY CORNER: Glossary.** 2019. Disponível em: <https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary>. Acesso em: 1º mar. 2021

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). About **Standards.gov**. 2019. Disponível em: https://www*:*nist*:*gov/standardsgov/about-standardsgov. Acesso em: 02/03/2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NATIONAL VULNERABILITY DATABASE: NVD Dashboard**. Disponível em: <https://nvd.nist.gov/general/nvd-dashboard>. Acesso em: 12 mai. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST SP 800-60**: Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg**,** Estados Unidos, 2008.

NTT SECURITY. **2019 Global Threat Intelligence Report**. 2019. Disponível em: <https://hello.global.ntt/en-us/newsroom/2019-global-threat-intelligence-report/> Acesso em: 26 abr. 2021.

NISHI, M. **Data Protection in Japan to Align With GDPR**. 24 set. 2018. Disponível em: <https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr>. Acesso em: 13 abr. 2021

PRODANOV,C.C.; DE FREITAS, E.C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição**. Editora Feevale, 2013.

RILEY, T. The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds**. Washington Post**, 7 Dez. 2020. Disponível em: <https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/>. Acesso em: 7 abr. 2021

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE. **California Consumer Privacy Act (CCPA).** Disponível em: <https://oag.ca.gov/privacy/ccpa>. Acesso em: 30 abr. 2021.

ROY, P.P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. In: **2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)**. IEEE, 2020. p. 1-3.

SAITO, W. H. It's Time To Think Of Cybersecurity As A Business Enabler. **Forbes**, [S. L.], 01 jul. 2016. Disponível em: <https://www.forbes.com/sites/williamsaito/2016/07/01/its-time-to-think-of-cybersecurity-as-a-business-enabler/?sh=73b067cc3cc8> Acesso em: 26 fev. 2021.

SALTZER, J.H.; SCHROEDER, M.D. The protection of information in computer systems. **Proceedings of the IEEE**, v. 63, n. 9, p. 1278 – 1308, Abril 1975.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, P. B. **Metodologia de Pesquisa**. 5a ed. São Paulo: McGraw-Hill, 2013.

SEMOLA, M. **Gestão da Segurança da Informação – Uma Visão Executiva.** 2. ed. Rio de Janeiro: Elsevier, 2014.

STASIAK, K. **Middle-market companies underestimate cybersecurity risks.** IndustryWeek. Julho 2018. Disponível em: <https://www.industryweek.com/leadership/article/22026028/middlemarket-companies-underestimatecybersecurity-risks>. Acesso em: 15 mar. 2021

SURYOTRISONGKO, H; MUSASHI, Y. Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. In: **2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)**. IEEE, 2019. p. 162-167.

THE WHITE HOUSE. Executive order nº 13636, de 12 de fevereiro de 2021. Improving critical infrastructure cybersecurity. **Improving Critical Infrastructure Cybersecurity**, Estados Unidos, 12 fev. 2013.

UNECE. This document contains a proposal for a common regulatory framework on cybersecurity and is hereby submitted for decision by the Working Party. **Report on the Sectoral Initiative on Cyber Security**. 11 set. 2019. Disponível em: <https://unece.org/DAM/trade/wp6/documents/2019/ECE_CTCS_WP.6_2019_9E.pdf/>. Acesso em: 12 mar. 2021.

UNIÃO EUROPEIA. (UE) 2016/679. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **REGULAMENTO (UE) 2016/679**, 26 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679/>. Acesso em: 12 mar. 2021.

US Treasury and commerce department targeted in cyber-attack. **BRITISH BROADCASTING CORPORATION**, 14 dez. 2020. Technology. Disponível em: <https://www.bbc.com/news/world-us-canada-55265442>. Acesso em: 2 abr. 2020.

VEIGA, A., et al. **Defining organizational information security culture – Perspectives from academia and industry,** Computers & Security, v. 92, 2020.

VERGARA, S. C. **Projetos e Relatórios de Pesquisa em Administração**. 10. ed. São Paulo: Atlas, 2009.

VIET, N.A. et al. Toward cyber-security architecture framework for developping countries: An assessment model. In: **International Conference on Advances in Information and Communication Technology**. Springer, Cham, 2016. p. 652-658.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97-102, 2013.

VLACHOPOULOS, D.; MAKRI, A. The effect of games and simulations on higher education: a systematic literature review. **International Journal of Educational Technology in Higher Education**, v. 14, n. 1, p. 1-33, 2017.

WHITMAN, M.; MATTORD, H. J. **Principles of Information Security.** 5 ed. Boston: Cengage Learning. 2015.

WOLFORD, B. **What is GDPR, the EU's new data protection law?.** Disponível em: <https://gdpr.eu/what-is-gdpr/>. Acesso em: 2 mar. 2021.