ÁREA TEMÁTICA
AI – ADMINISTRAÇÃO DA INFORMAÇÃO

A UTILIZAÇÃO DOS FRAMEWORKS NIST CSF E DA SÉRIE NBR ABNT ISO 27.000 NO CONTEXTO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

RESUMO

O índice de ataques cibernéticos a organizações e instituições ao redor do mundo tem crescido muito e, como consequência, esse tema tem sido cada vez mais discutido e analisado no contexto organizacional. A adoção de *frameworks* de gestão de segurança da informação por uma organização é um dos fatores de sucesso para a mitigação de riscos de ocorrência de incidentes de segurança. Esse trabalho teve como objetivo avaliar como têm sido utilizados os *frameworks* de segurança da informação "*The Framework for Improving Critical Infrastructure Cybersecurity*" do *National Institute of Standards and Technology* (NIST) e a série de padrões NBR ABNT ISO 27000 da *International Organization for Standardization* (ISO), traduzidos no Brasil, pela ABNT. Para isso, realizou-se uma pesquisa descritiva de natureza bibliométria. Examinaram-se 50 trabalhos disponíveis em repositórios nacionais e internacionais. O tratamento dos dados empregou estatística descritiva, a técnica de nuvem de palavras e a análise de conteúdos. Verificou-se uma tendência de alta na adoção dos dois Frameworks, assim como o nível de utilização e aplicação em locais específicos. Esse trabalho pode contribuir para que as empresas, organizações, instituições e pesquisadores possam obter insumos, subsídios e conhecimento, visando auxiliar a tomada de decisão na escolha de qual *framework* a ser adotado para realização da Gestão do processo de Segurança da Informação.

Palavras-chave: cybersecurity, NIST, ISO 27000.

ABSTRACT

The rate of cyber-attacks on organizations and institutions around the world has grown a lot and, as a consequence, this has been an increasingly discussed and analyzed topic in the institutional and organizational context of companies in general. The adoption of Frameworks to perform the information security management of a company is one of the most relevant success factors for the mitigation of financial and image losses as a result of these attacks. This work evaluated how the National Institute of Standards and Technology (NIST) cybersecurity Frameworks "The Framework for Improving Critical Infrastructure Cybersecurity" and the International Organization for Standardization (ISO) series of standards have been used to carry out information security management. This work researched and evaluated qualitatively the works published in several databases. More than 50 papers were selected and the data from these studies were extracted, analyzed and consolidated, generating information and identifying trends. There was an upward trend in the adoption of the two Frameworks, as well as the level of use and application in specific locations. The objective of this work was, therefore, to provide means for companies, organizations, institutions and researchers to obtain inputs, subsidies and knowledge, aiming to assist decision making in the choice of the Framework to be adopted to perform the Management of the Information Security process, reducing the risk success of cyber-attacks, avoiding financial losses and compromising the image of institutions in general.

Keywords: cybersecurity; NIST, ISO 27000.

1 INTRODUÇÃO

As organizações em todo o mundo têm enfrentado cada vez mais desafios no que tange aos riscos cibernéticos. Com a pandemia da COVID-19 e a necessidade do distanciamento social, houve uma potencialização desses riscos já que as organizações passaram a operar pelo uso de tecnologias por meio do trabalho remoto. Esta modalidade criou um ambiente propicio para o aumento desses riscos, expondo ainda mais as organizações e os seus colaboradores. Há registros de prejuízos na ordem de um trilhão de dólares, devido à materialização de riscos cibernéticos em corporações (THE WASHINGTON POST, 2020).

Um exemplo de ataque cibernético de grandes proporções aconteceu entre março e junho de 2020 quando houve um ataque a SolarWinds, empresa proprietária do software Orion que é utilizado comercialmente para o monitoramento de redes e de aplicativos. Esse ataque afetou aproximadamente 300 mil pessoas em todo mundo, incluindo organizações dos Estados Unidos da América que têm bom histórico de gerenciamento de riscos cibernéticos, tais como: Pentágono, o Exército Americano, Departamento de Comércio, Tesouro Nacional, Gabinete da Presidência (BRITISH BROADCASTING CORPORATION [BBC], 2020).

Observa-se uma dependência cada vez maior dos resultados estratégicos organizacionais atrelados às tecnologias, podendo-se citar como exemplo, a Internet das Coisas (IoT) e a Inteligência Artificial, as quais são implantadas no contexto da indústria 4.0. Riscos de vírus do tipo malware, enviando instruções para hardware e modificando operações críticas nos processos empresariais, surgem com uma frequência cada vez maior. Com isso, ataques aos ativos físicos como, redes elétricas, satélites, instalações nucleares, entre outras, são identificados nos planos de riscos empresariais e, como consequência, os ataques passam a utilizar métodos cada vez mais evoluídos e sofisticados. A necessidade da gestão da segurança da informação tem crescido muito à medida que existe um aumento e sofisticação dos ataques a estes ativos (WHITMAN e MATTORD, 2015, p. 47).

A segurança cibernética, também conhecida como segurança digital, é a prática de proteger as informações, dispositivos e ativos digitais. Ela se baseia em três pilares: confidencialidade, integridade e acesso (MICROSOFT, 2021).

No entanto, a segurança deve ser entendida como um processo e não como um produto. Nesse sentido, ela requer também a implantação de cuidadosos processos e práticas, como: backups de dados, bons hábitos cibernéticos, atualização de softwares, senhas fortes e únicas, autenticação multi-fator, bloqueio de dispositivos, dentre outros (MICROSOFT, 2021).

Um framework de segurança cibernética se traduz por uma sequência de processos para estabelecer um controle de segurança completo em sistemas empresariais. Eles criam modelos de construção de programas de segurança da informação, gerenciando riscos e combatendo fragilidades. Para tanto, eles devem oferecer: certificados de segurança, redução de riscos de invasão, normas de segurança, políticas de segurança, dentre outras funcionalidades (IT-EAM, 2020).

Este trabalho tem por objetivo mostrar quais frameworks vêm sendo utilizados prioritariamente no mundo para a realização da gestão da segurança da informação, assim como apresentar um entendimento sobre os aspectos bibliométricos e práticos que norteiam as suas utilizações.

O trabalho está estruturado em sessões, as quais abordam aspectos teóricos associados aos frameworks de segurança da informação mais conhecidos, o método bibliométrico utilizado para a realização da pesquisa sistemática, e o levantamento de informações qualitativas e quantitativas, sobre as quais foram realizadas

avaliações estatísticas, elaboradas para a identificação de aspectos comparativos. Por fim, os resultados encontrados foram apresentados em forma gráfica com as respectivas discussões.

2 REFERENCIAL TEÓRICO

A segurança da informação tem como objetivo preservar a informação por meio de três princípios: a integridade, a disponibilidade e a confidencialidade (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO], 2018). O primeiro princípio está relacionado com a completude ou a acurácia da informação, em que ela só pode ser manipulada ou alterada por quem tem autorização; o segundo princípio está relacionado com a propriedade de que a informação esteja acessível e utilizável no momento necessário para o seu uso; e o último princípio está relacionado com que a informação não seja disponibilizada ou liberada para indivíduos, entidades ou processos não autorizados (SEMOLA, 2014; CHERDANTSEYA e HILTON, 2013; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS [ABNT], 2013; ISO, 2018).

A informação pode residir não só dentro do ambiente tecnológico, podendo ser materializada fisicamente. Nesse sentido, há o de Segurança Cibernética, mais restrito, que se trata da proteção do ciberespaço e tudo que trabalha nele (SOLMS e NIEKERK 2013). Embora existam alguns casos em que esses conceitos de segurança da informação e segurança cibernética possam ser tratados como análogos, o que pode diferenciar a segurança da informação é o fato de proteger a informação de diversas ameaças que possam surgir (SOLMS e NIEKERK 2013).

A adoção de um sistema de gestão da segurança da informação é uma decisão estratégica para uma organização, e é operacionalizado por meio da aplicação de um processo de gestão de riscos que permite trazer confiança às partes interessadas de que os riscos estão gerenciados adequadamente (ABNT, 2013). Há alguns padrões que são úteis para a implantação desse sistema de gestão de segurança da informação. Em geral, eles são cumpridos para fazer um produto, realizar um serviço ou para o gerenciamento de processos, e os (GIUCA, 2018).

Frameworks de segurança de informação são considerados como o núcleo de uma gestão da segurança da informação. Estes são responsáveis por conter políticas, padrões, processos, procedimentos, metodologias, métodos e ferramentas que são considerados básicos para a implantação do processo de gestão da segurança da informação. Com a sua adoção, as organizações podem ser direcionadas para atingir resultados pretendidos nesta área (GIUCA, 2018). No presente trabalho foram utilizados os padrões da série ISO/IEC 27000 e o Framework NIST CSF por questões de viabilidade.

O primeiro *Framework* possui o nome de "*The Framework for Improving Critical Infrastructure Cybersecurity*" - Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica. Este Guia tem como objetivo direcionar gestores no sentido de realizarem a gestão de riscos de segurança cibernética baseado nas necessidades das instituições.

O Guia em questão teve sua origem e desenvolvimento a partir das diretrizes da Casa Branca (*executive order* nº 13636). Também contou com a participação de diversos setores entre eles, acadêmico, produtivo e outras categorias do governo (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [NIST], 2018).

Este Framework possui uma divisão que se baseia em riscos voltados para a segurança cibernética e contém 3 componentes principais:

- Núcleo ou estrutura básica (*core*),
- Avaliação (*profile*),
- Níveis de implantação (*implementation tiers*) (NIST, 2018).

O outro *Framework International Organization for Standardization* é uma organização responsável por desenvolver diversos padrões com vários grupos de interesse em cada área. Neste sentido, um destes padrões é que foi definido pela ISO/IEC 27000, nos quais são detalhados os requisitos para auxiliar as organizações a realizar seu gerenciamento de segurança da informação (ABNT, 2013).

Alguns outros *Frameworks* utilizam desta norma para criar seus próprios controles de segurança e, entre eles, pode-se citar o NIST CSF (NIST, 2018). A série ISO 27000 contém padrões de requisitos que direcionam sua linha de atuação em: desenvolver um sistema de gerenciamento de segurança da informação, auxiliar organizações de auditoria e entidades emissoras de certificação, e, também, auxiliar a atingir os requisitos para aperfeiçoamento já inclusos na ISO/IEC 27001:2013 (ABNT, 2013).

A série ISO/IEC 27000 tem como objetivo auxiliar as corporações a implementar um sistema de gerenciamento de segurança da informação (NIST, 2018; ABNT, 2013).

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

- Terminologia/Vocabulário,
- Requisitos,
- Diretrizes gerais
- Diretrizes específicas de setores

3. METODOLOGIA

O presente trabalho trata -se de uma pesquisa bibliométrica (Santos & Kobashi, 2009), que tem como característica ser descritivo focando nas características do objeto (Sampieri et al., 2006). Esta pesquisa foi sistematizada e teve seu desenvolvimento baseado na coleta de artigos publicados em periódicos de acesso público através de bases online (Vergara, 2009).

O material coletado refere -se a diferentes momentos do tempo, apresentando assim um recorte temporal longitudinal. Foram utilizadas abordagens quantitativas e qualitativas para análise de informações (Sampieri et al., 2006).

A população utilizada neste trabalho trata -se das publicações disponíveis em base de dados como Google Scholar, Semantic Scholar, Scopus, ScienceDirect (Elsevier), IEEExplore.

Referente a amostra, trata -se de não-probabilística intencional (Sampieri et al., 2006). Os seguintes critérios foram utilizados para selecionar a amostra da população:

a) Foram utilizadas palavras e expressões-chave em inglês com relação ao tema para realizar a busca dos artigos em cada uma das bases de dados. Foram utilizados termos como *action research, case study, critical infrastructure, cybersecurity, cyber, security, framework, ISO, ISO/IEC 27000 series, NIST* e *risk*

b) Em seguida foram selecionados artigos com relação ao publicados de 2015 até 2021 que possuíam resumo e palavras chaves correspondentes ao interesse da pesquisa.
c) Ao final foram selecionados 50 artigos depois de uma análise em relação ao tema abordado em cada um dos artigos coletados

A coleta de artigos foi realizada durante fevereiro de 2021 e março de 2021. Os procedimentos de análise de dados se basearam no emprego de estatística descritiva (Reis, 1996).

O conceito de nuvem de palavras foi utilizado para elaborar de forma gráfica a frequência das palavras-chaves e termos utilizados nos artigos coletados (Ribeiro & Domingues, 2014). Para gerar estas nuvens de palavras foram mantidos termos em conjunto como por exemplo "*case study*", "*ISO/IEC 27000* series" entre outros. Conectores e preposições foram excluídas da nuvem de palavras.

Com o intuito de analisar os dados, foi utilizado a análise de conteúdo, estendida com um conjunto de técnicas e análises de comunicações (Bardin, 1979). Os artigos foram examinados e verificados o quanto este foi relevante ao tema da pesquisa. Os artigos tiveram seus dados coletados, tratados e trabalhados sendo agrupados por base de dados, ano, continente, país, setor e transformados em informações.

Métodos estatísticos foram utilizados para auxiliar na identificação de tendências, dentre estes métodos pode ser citado a regressão linear, e o índice de correlação (Cohen, 1998).

Através das planilhas eletrônicas os dados foram transformados em informações, gráficos foram construídos para a exibição destes resultados.

4. DISCUSSÃO DOS RESULTADOS

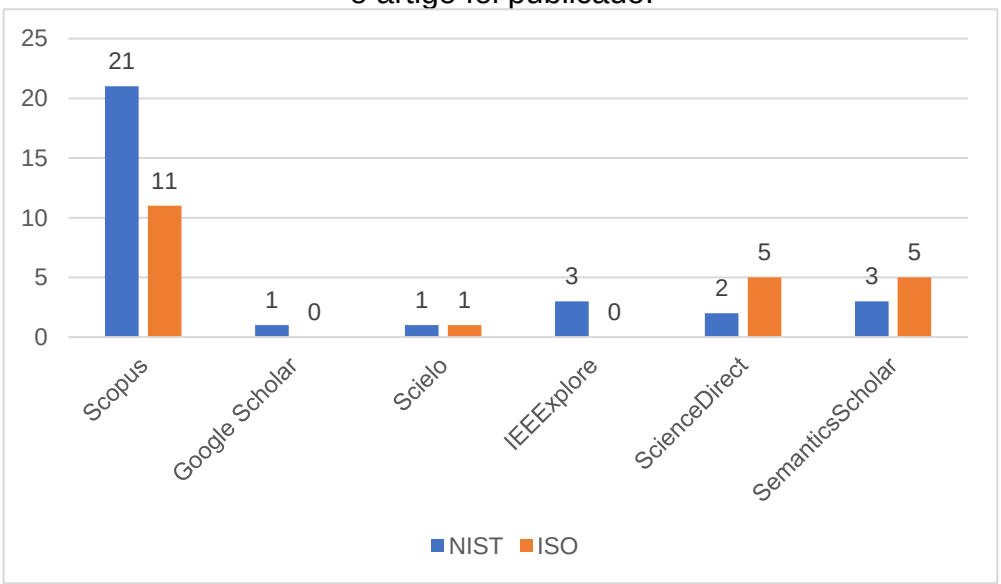
Para a realização dessa revisão sistemática envolvendo os *Frameworks* da NIST e da ISO foi necessário se valer de palavras chaves para a realização das buscas por artigos e publicações nas bases de dados identificadas. As palavras chaves mais utilizadas nas buscas que apresentaram resultados significativos foram: *cybersecurity, cyber, security, risk* e *system*. Outras palavras também obtiveram relevância como, por exemplo, *information*, NIST e *Framework*. A nuvem de palavras apresentada na Figura 1 possibilita ilustrar bem as palavras em destaque por tamanho.

Figura 1 – Nuvem de palavras chaves utilizadas para coletar os artigos

Fonte: Elaborado pelos autores (2021)

O Gráfico 1 mostra a quantidade de artigos coletados por base de dados, agregando-os por *Framework* NIST e ISO. O Gráfico 1 também consegue ilustrar que a maior parte dos artigos coletados foram da base de dados “Scopus”. Ao se analisar as bases de dados que não são Scopus verifica-se um destaque maior para o modelo ISO.

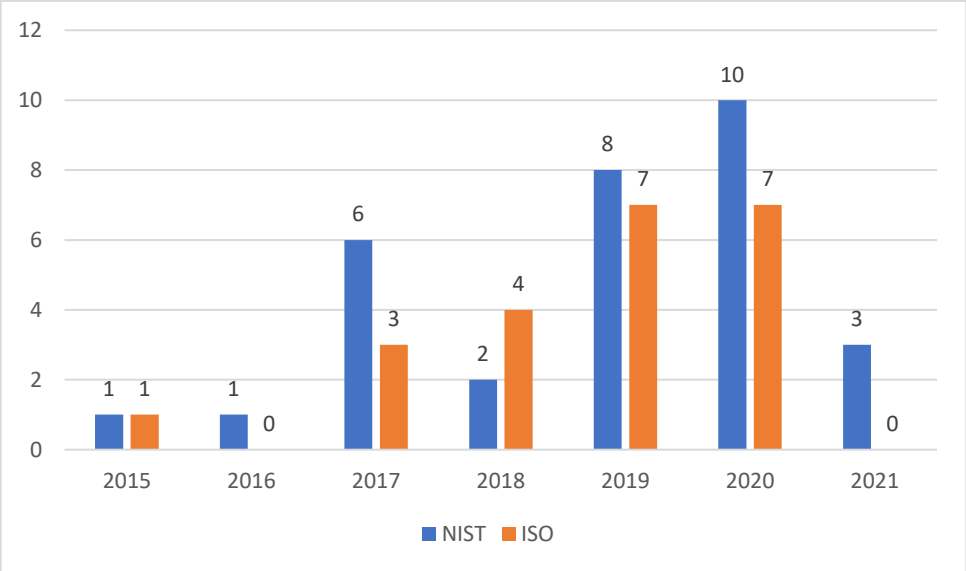
Gráfico 1 – Distribuição de *Framework* por artigos segundo a base de dados em que o artigo foi publicado.



Fonte: Elaborado pelos autores (2021)

Já o Gráfico 2 ilustra uma série temporal de publicações, este mostra a quantidade de artigos publicados ao longo dos anos segregados por *Framework* ISO e NIST. Por meio desse gráfico é possível notar ainda um crescimento consistente de estudos na área de segurança cibernética.

Gráfico 2 – Distribuição por ano de publicação do artigo



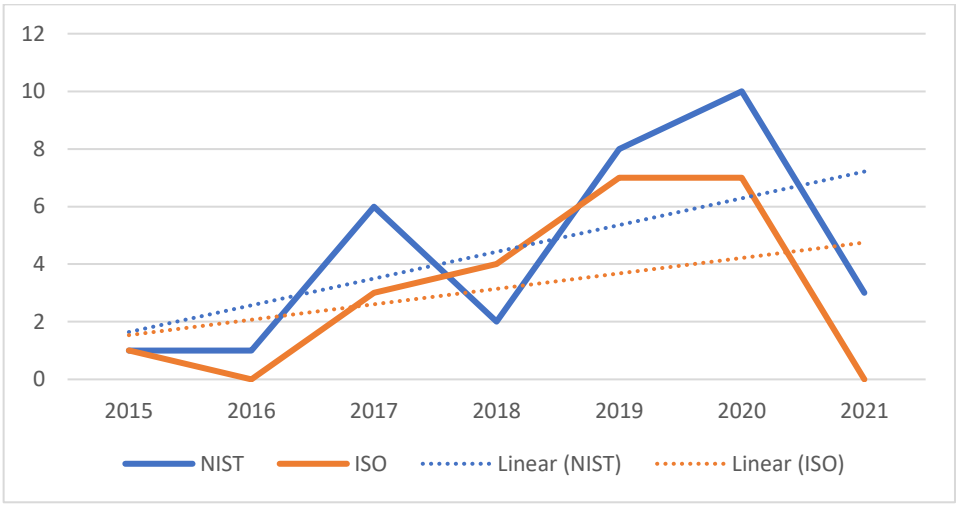
Fonte: Elaborado pelos autores (2021)

Ao se avaliar a quantidade de artigos coletados e agrupados por ano, é possível verificar que no primeiro bimestre de 2021 já se pode verificar a existência de três artigos publicados que utilizam o CSF da NIST.

Ao realizar uma correlação dos anos com a quantidade de trabalhos publicados, desprezando-se o ano de 2021 que ainda não foi concluído, verifica-se um coeficiente R = 0,85 para NIST e R = 0,94 para ISO. Esses números, segundo Cohen (1998), mostram a existência de uma forte correlação no aumento da utilização desses dois *Frameworks* ao longo dos anos.

Ao realizar uma regressão linear esta apresenta como resultado uma tendência de alta. O Gráfico 3 mostra o resultado da aplicação dessa regressão em linhas tracejadas ilustrando melhor esse fenômeno.

Gráfico 3 – Regressão linear mostrando tendência de alta na adoção de *Frameworks*



Fonte: Elaborado pelos autores (2021)

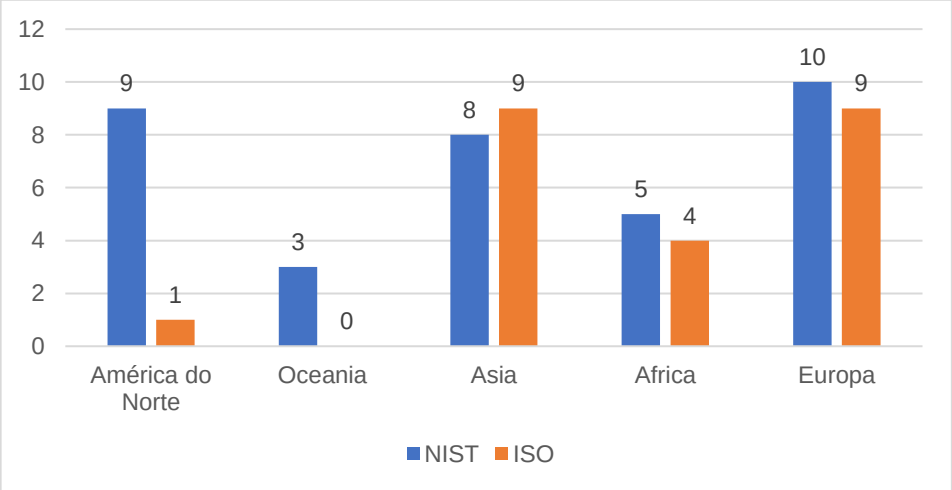
Também é possível identificar que a curva de regressão do CSF NIST tem crescido mais em relação a da ISO. Entretanto é bom ressaltar que o próprio CSF da NIST herda controles e mecanismos da ISO.

Este mesmo fenômeno pode ser visto no relatório "*The Life and Times of Cybersecurity Professionals*" elaborado pela ESG - *The Enterprise Strategy Group* de 2017 que entrevistou membros da ISSA - *International Social Security Association* em todo o mundo. Ao questionar as empresas se elas tomaram alguma ação em relação à segurança da informação nos últimos anos, pelo menos 52% das grandes organizações responderam que adotaram alguma parte do CSF (OLTSIK, 2017). Este fato foi publicado pela própria NIST em seu site. Esses dados são importantes e justificam a maior ascendência da curva de regressão relativas aos estudos e artigos identificados com base na NIST, quando comparados com aqueles baseados na ISO 27000 series.

Cabe ainda destacar que por mais que a NIST possua uma curva de crescimento maior, o maior número de artigos publicados foi desenvolvido nos Estados Unidos. Verifica-se que os Estados Unidos detêm aproximadamente 30% dos artigos que utilizam o NIST como base de pesquisa. Se esse fato for excluído, percebe-se um equilíbrio entre os dois padrões. Este fato será discutido mais adiante.

O Gráfico 4 apresenta a distribuição da quantidade de artigos publicados e coletados, por continente. A imagem consegue mostrar um equilíbrio de publicações nos continentes, à exceção do continente Norte Americano e da Oceania, onde se pode perceber o predomínio de trabalhos elaborados com o CSF da NIST.

Gráfico 4 – Distribuição de *Framework* por artigos segundo o continente da instituição de filiação dos autores.



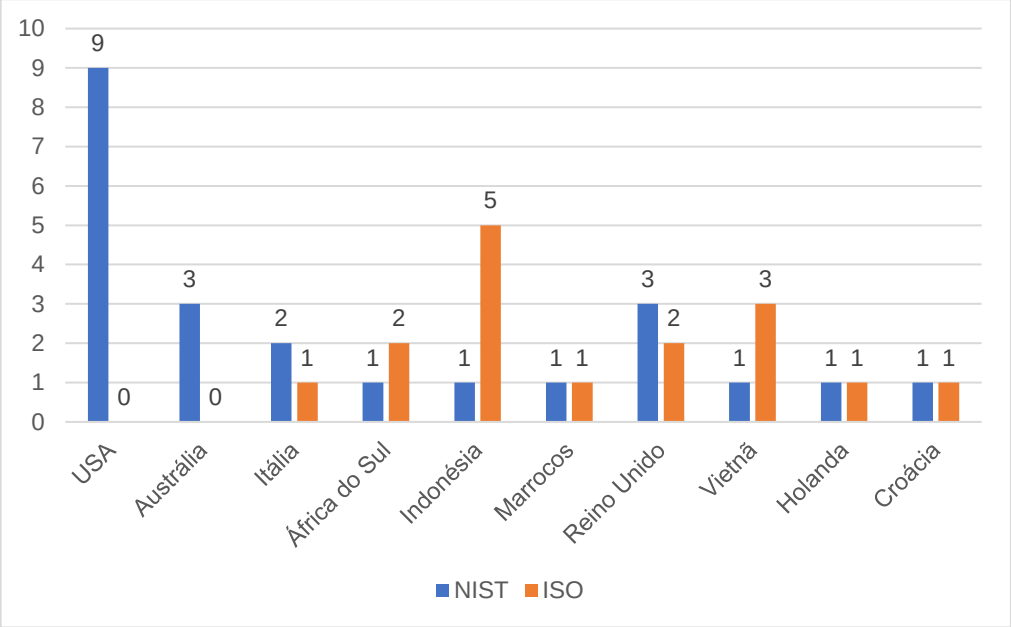
Fonte: Elaborado pelos autores (2021)

Ao olharmos para o equilíbrio na Europa, é importante ressaltar o papel da ISO 27000 Serie no cumprimento de questões legais. Esta tem sido utilizada amplamente neste continente para auxiliar no cumprimento da GDPR - *General Data Protection Regulation*, a Lei Geral de Proteção de dados da Europa. Empresas europeias fizeram estudos e constataram que ela cumpre entre 75% a 80% dos requisitos legais da lei (NAKAMURA; FORMIGONI FILHO; IDE, 2019).

Também há um incentivo da própria GDPR para que as empresas se certifiquem na ISO 27001 para que se aproximem da conformidade com a lei (LOPES; GUARDA; OLIVEIRA, 2019). Cerca de 73% das empresas que utilizam a ISO 27001 concordam que a norma auxilia no atingimento dos objetivos exigidos pela GDPR. Estes fatos e dados justificam o equilíbrio muito grande identificado neste trabalho em relação aos artigos publicados com uso do Guia ISO e do *Framework* NIST no nos países da Europa.

O Gráfico 5 mostra a distribuição dos artigos publicados, por país. Verifica-se que os Estados Unidos têm dado preferência aos estudos com o CSF. Considerando os demais países com estudos publicados, é possível identificar um equilíbrio entre NIST e ISO, apresentando resultados de forma bem balanceada.

Gráfico 5 – Distribuição de framework por artigos segundo o País das instituições que os autores estão filiados



Fonte: Elaborado pelos autores (2021)

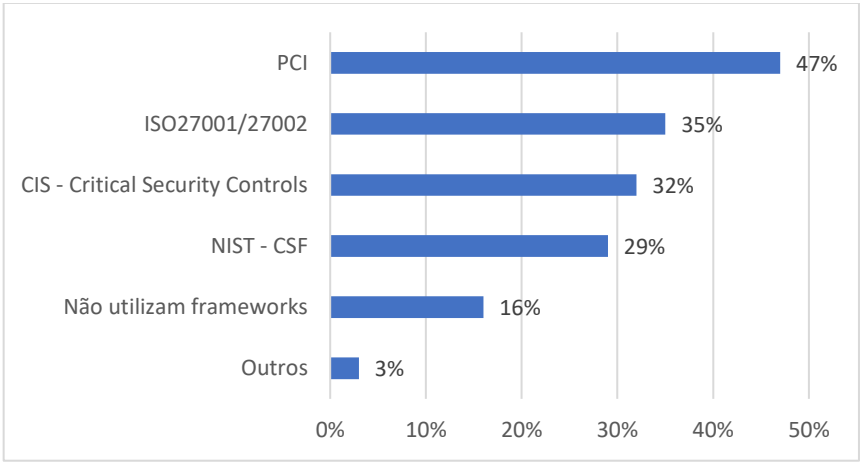
Ao compararmos esses dados com outro relatório também divulgado no próprio site da NIST "*Trends In Security Framework Adoption*" elaborado em 2016 somente nos Estados Unidos, temos as seguintes informações: Cerca de 70% das empresas que adotaram o NIST alegaram considerar este uma melhor prática de segurança da informação; 29% adotaram o CSF porque um parceiro de negócios exigia; 28% adotaram o CSF porque um contrato federal o exigia (DIMENSIONAL RESEARCH, 2016).

Estes números justificam o alto número da adoção do CSF da NIST nos Estados Unidos identificado neste estudo. Este fenômeno de alta da adoção do CSF neste país quando comparado a outros países pode ser explicado até mesmo pelos aspectos legais exigidos pelos Órgãos e Agências americanas.

Ainda comparando os dados do presente trabalho com o relatório *Trends In Security Framework Adoption* é possível ver que em 2016 o CSF da NIST estava apenas em quarto lugar em preferência nos Estados Unidos (DIMENSIONAL RESEARCH, 2016). O Gráfico 6 mostra, a seguir, a preferência por *Frameworks* de segurança da informação nos Estados Unidos, no ano de 2016.

Cabe destacar nesse ponto, que as empresas podem adotar mais de um *Framework*.

Gráfico 6 – Preferência de *Frameworks* de segurança de informação até 2016 nos Estados Unidos



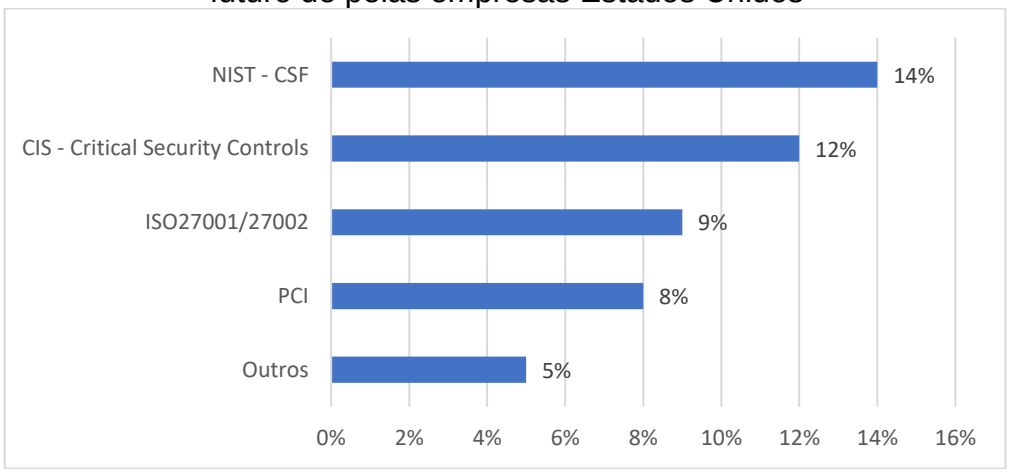
Fonte: Adaptado de *Dimensional Research* (2016)

A principal justificativa para o NIST não estar em primeiro lugar no ano de 2016 é o fato de o PCI ser um *Framework* voltado para o varejo (DIMENSIONAL RESEARCH, 2016). Outra justificativa é que aproximadamente mais da metade das empresas que adotaram o CSF da NIST relataram a necessidade de um alto investimento para cumprir todas as funcionalidades do Guia (DIMENSIONAL RESEARCH, 2016).

Outra justificativa apresentada para a supremacia do uso da Norma ISO no ano de 2016 em relação ao CSF da NIST apresentada neste mesmo relatório, é o fato da ISO até então ser mais conhecida e famosa do que o CSF mundialmente (DIMENSIONAL RESEARCH, 2016).

É importante ressaltar que o relatório citado se atém ao ano de 2016, entretanto este divulgou projeções que apontam uma adesão maior do CFS da NIST nos Estados Unidos no futuro. Essas projeções vão de encontro ao que o presente estudo mostrou, um aumento significativo do uso do CSF do NIST pelos artigos publicados nos últimos dois anos. (DIMENSIONAL RESEARCH, 2016). O Gráfico 7 ilustra esse cenário.

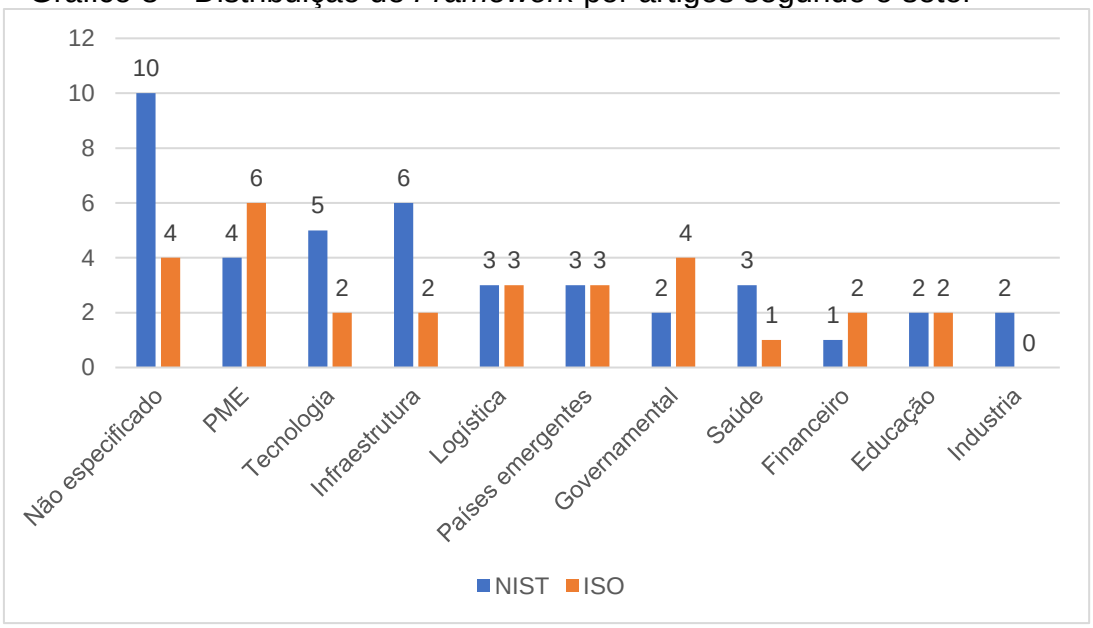
Gráfico 7– Pretensões em adoção de *Frameworks* de segurança da informação no futuro de pelas empresas Estados Unidos



Fonte: Adaptado de *Dimensional Research* (2016)

O Gráfico 8 mostra a distribuição de trabalhos publicados, por setor da economia. É importante ressaltar que um trabalho pode se apresentar em mais de um setor económico. Os trabalhos que estão como “Não-Especificado” representam projetos de implantações ou sistemas de informação, sem, no entanto, definir especificamente a qual setor se destinava.

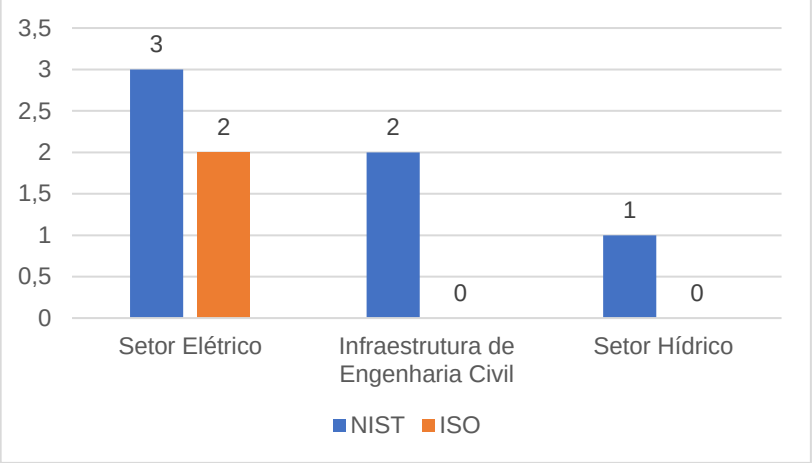
Gráfico 8 – Distribuição de *Framework* por artigos segundo o setor



Fonte: Elaborado pelos autores (2021)

Ao se decompor o setor de infraestrutura, pode-se observar que 5 artigos são do Setor Elétrico, 1 do Setor Hídrico e 2 do Setor de Engenharia Civil. O Gráfico 9 mostra claramente a predominância de artigos do NIST para esse segmento da economia.

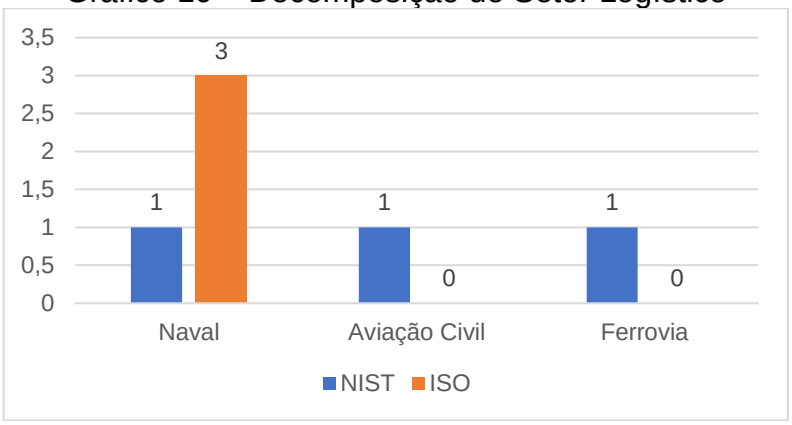
Gráfico 9 – Decomposição do setor Infraestrutura



Fonte: Elaborado pelos autores (2021)

Aprofundando as análises no setor de logística, constata-se a existência de trabalhos para o Setor Naval, Aviação Civil e Ferrovias. Desta forma, é possível se verificar um equilíbrio entre ISO e NIST, mas se as atenções forem direcionadas para Setor Naval, o qual se destaca entre os demais, observa-se um maior direcionamento de estudos voltados ao uso do Guia da ISO. Já os demais utilizam predominantemente o *Framework* da NIST. O Gráfico 10 mostra essas informações.

Gráfico 10 – Decomposição do Setor Logístico



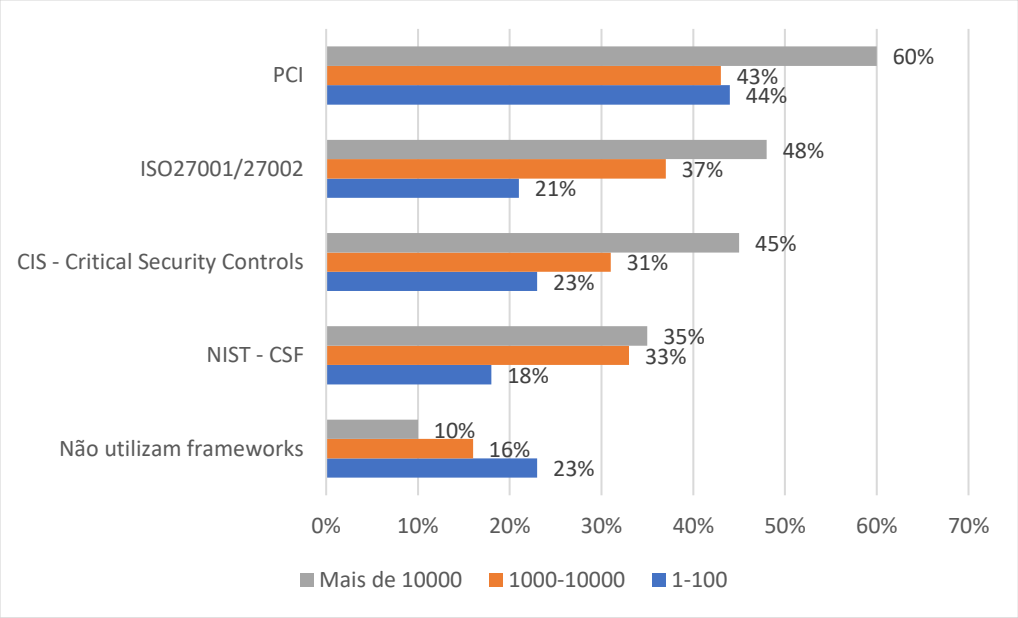
Fonte: Elaborado pelos autores (2021)

Um aspecto que chama atenção ao analisarmos os setores é o fato de que alguns artigos se apresentaram como PME - Pequenas e Médias Empresas não especificarem a quais setores da economia essas categorias empresariais pertenciam. Entretanto é de fundamental importância destacar esse fato, uma vez que esse setor é um dos que mais sofre ataques cibernéticos, quando comparados com as grandes empresas e sua preferência pelo ISO. Ele corresponde a mais de 50% dos incidentes de segurança da informação registrados, uma vez que apresentam infraestruturas tecnológicas mais defasadas (STASIAK,2018).

O mesmo ainda pode ser visto no relatório "*Trends In Security Framework Adoption*". Devido ao alto custo para a implantação das diretrizes da NIST é possível observar que o Guia da ISO tinha maior preferência de uso no ano de 2016, não somente pelas maiores empresas, mas também pelas médias e pequenas empresas. Esse aspecto corrobora com o que foi identificado no presente trabalho,

onde de percebeu uma preferência das pequenas e médias empresas pelo uso do Guia da ISO. Este Fato que vai de encontro a justificativa da necessidade de alto investimento para cumprir todas as funcionalidades do CSF (DIMENSIONAL RESEARCH, 2016). O Gráfico 11 ilustra esse cenário.

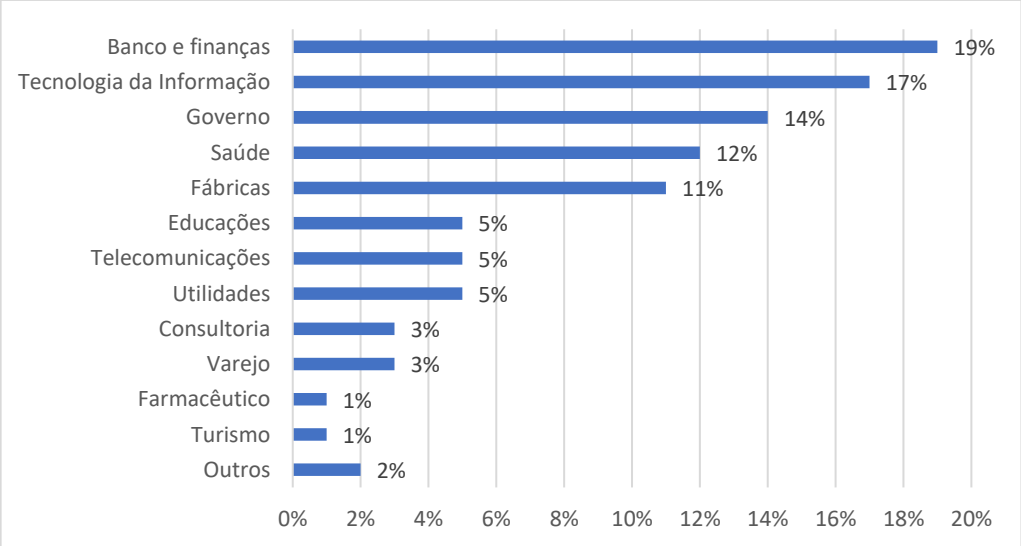
Gráfico 11– Preferência de *Frameworks* de segurança de informação por tamanho de empresas em funcionários até 2016 nos Estados Unidos



Fonte*:* Adaptado de *Dimensional Research* (2016)

Este mesmo mostra ainda a presença do uso do Guia da NIST nos Estados Unidos em diversos setores, como o presente trabalho mostrou a nível global. É possível verificar um destaque das aplicações do Guia NIST em setores como Tecnologia da Informação, Governamental e o setor Bancário. O Gráfico 12 mostra como tem sido adotado o modelo NIST nos Estados Unidos.

Gráfico 12– Preferência de adoção de *Frameworks* de segurança da informação por setor de empresas Estados Unidos



Fonte: Adaptado de *Dimensional Research* (2016)

Assim, este trabalho conseguiu relatar um equilíbrio entre os dois *Frameworks* e suas aplicabilidades no geral. Também mostrou quais países e setores onde cada um se destaca. Também um debate com dados de estudos técnicos divulgados pela NIST foi feito com os dados e informações encontradas no presente trabalho.

5. CONCLUSÃO

Este trabalho procurou fazer uma avaliação das publicações que se utilizaram dos Frameworks de Segurança Cibernética do NIST CSF e da série ISO 27000 como base de suas pesquisas ao redor do mundo.

Para tanto, foi realizada uma revisão bibliométrica, na qual mais de 50 artigos foram selecionados, onde 29 utilizaram o *Framework* da NIST e 21 utilizaram o Guia da ISO 21000 Series, e outros dois utilizaram ambos. Como pôde ser verificado, a aplicação de ambos os padrões está relativamente equilibrada, conforme foi constatado no presente trabalho. Entretanto, cabe ressaltar que parte desse equilíbrio vem do alto índice de adoção do NIST CSF pelos Estados Unidos nos últimos anos, uma vez que até o ano de 2016 o uso do Guia da ISO se mostrava superior.

Importante destacar ainda que nos outros continentes, em especial na Europa, também foi verificado um equilíbrio, sendo que nesse continente há um incentivo governamental para que as empresas optem pela certificação ISO 27001, visando se adequarem às exigências da Lei que regula a privacidade dos dados, a GDPR.

O presente estudo também mostrou, por meio de correlação estatística, que com o passar dos anos tem aumentado a preocupação das empresas e organizações em com a segurança cibernética. Utilizando-se de regressão linear foi possível verificar um aumento do uso da NIST CSF e do Guia ISO 27000 ao longo dos últimos anos.

O trabalho demonstrou ainda que os *Frameworks* NIST CSF e ISO 27000 estão sendo adotados por diversos setores, destacando-se os setores de Tecnologia da Informação, Governo, Bancários e Finanças. Também demonstrou ainda a preocupação das pequenas e médias empresas em adotarem essas estruturas de segurança da informação para si, uma vez que as pequenas e médias empresas são alvo de mais de 50% dos ataques cibernéticos, uma vez que possuem infraestruturas tecnológicas defasadas e dificuldades financeiras para implantar os frameworks, cujo custo é elevado.

Por fim, foram disponibilizadas informações importantes sobre as tendências de uso dos *Frameworks* da NIST CSF e da ISO 27000 *series* no âmbito da segurança cibernética, a partir de análises de trabalhos publicados nesse segmento de pesquisa, visando colaborar com as empresas e com a comunidade acadêmica em geral.

Este trabalho teve como limitações o exame dos artigos da amostra coletada no período específico relatado anteriormente e a análise dos *Frameworks* CSF da NIST e ISO27000 Series. Entretanto sugere-se como iniciativa futura e de aprimoramento, replicar este mesmo trabalho em outros períodos, ampliando o escopo do trabalho a outros *Frameworks e suas respectivas* aplicabilidades.

6. REFERÊNCIAS

Associação Brasileira de Normas Técnicas. NBR 27002: Tecnologia da Informação: Técnicas de Segurança: Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

Bardin, L. Análise de Conteúdo. (L. A. Reto & A. Pinheiro, Trad)**.** São Paulo: Edições 70, Livraria Martins Fontes. (Obra Original Publicada em 1977). 1979

British Broadcasting Corpooration. US Treasury and commerce department targeted in cyber-attack. Dezembro 2020. Disponível em: https://www.bbc.com/news/world-us-canada-55265442 Acesso em: 02/04/2020

Cohen, J. Statistical Power Analysis for the Behavioral Sciences, Second Edition. Mahwah, NJ: Lawrence Erlbaum Associates, 1998

Dimensional Research Trends in Security Framework Adoption**:** a survey of it and security professionals. Dimensional Research, 2016. Disponível em: https://static.tenable.com/marketing/tenable-csf-report.pdf. Acesso em: 17 maio 2021.

Ezingeard, J. Birch, D. Information Security Standards: Adoption Drivers. International Federation for Information Processing Digital Library; Security Management, Integrity, and Internal Control in Information Systems. 2006.

Giuca O., et al. A Survey of Cybersecurity Risk Management Frameworks. In: Soft Computing Applications, Proceedings of the 8th International Workshop Soft, Romênia. Springer. 2018. v. 1, pp 264-296.

IT-EAM. Ntenda a importância dos frameworks de segurança da informação. Disponível em: https://it-eam.com/framework-de-seguranca-da-informacao/. 2020. Acesso em: 29 maio 2021.

Lopes, Isabem M.; Guarda, T; Oliveira, P. How ISO 27001 Can Help Achieve GDPR Compliance. In: 2019 14TH Iberian Conference on Information Systems and Technologies (CISTI), 14., 2019, Coimbra. 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). [S.L.]: Ieee, 2019. p. 1-6.

Makamura, E.; Formigoni Filho, J. R.; IDE, M. C., Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais. *In*: Workshop de Regulação, Avaliação da Conformidade e Certificação da Segurança, 5., 2019, São Paulo. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 11-16. DOI: https://doi.org/10.5753/wrac.2019.14032.

MICROSOFT. **O que é segurança cibernética?** Disponível em: https://support.microsoft.com/pt-br/topic/o-que-%C3%A9-seguran%C3%A7a-cibern%C3%A9tica-8b6efd59-41ff-4743-87c8-0850a352a390. 2021 Acesso em: 29 maio 2021

National Institute of Standards and Technologies. NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, Estados Unidos. 2018

National Institute of Standards and Technologies. Small Busines Cybersecurity Corner: Glossary**.** 2019. Disponível em: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary. Acesso em: 01 mar. 2021

Oltsik, J. The Life and Times of Cybersecurity Professionals**:** a cooperative research project by esg and issa. The Enterprise Strategy Group, 2017. Disponível em: https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf. Acesso em: 17 maio 2021.

Reis, E. Estatística descritiva. Lisboa: Edições Sílabo. 1996

Ribeiro, H. C. M., & DOMINGUES, L. M. A. Produção acadêmica em governança corporativa sob a ótica comparativa dos congressos Anpad e AOM Meeting 2008 a 2011. Revista de Governança Corporativa, 1(1), 57-83, 2014

Sampieri, R. H., COLLADO, C. F., & LUCIO, P. B. Metodologia de pesquisa. 3a ed. São Paulo: McGraw-Hill, 2006

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

Santos, R. N. M., & KOBASHI, N. Y. Bibliometria, Cientometria, Infometria: conceitos e aplicações. Tendências da Pesquisa Brasileira em Ciência da Informação, 2(1), 155-172, 2009.

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

Solms, R.V., NIEKERK, J.V.; From information security to cyber security. *Computers & Security*, 38, pp. 97–102*.* 2013.

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: 15/03/2021

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

The Washington Post. 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: 07/04/2021

Whitman, M.; Mattord, H. J. Principles of Information Security. 5 ed. Boston: Cengage Learning. 2015.