DISSERTAÇÃO DE MESTRADO PROFISSIONAL

UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO

Fernando Rocha Moreira

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELETRICA

UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO

A PROPOSAL FOR PRIORITIZATION OF CYBERSECURITY CONTROLS USING A MULTI-CRITERIA METHOD

FERNANDO ROCHA MOREIRA

ORIENTADOR: RAFAEL RABELO NUNES

COORIENTADOR:DEMETRIO ANTONIO DA SILVA FILHO

PUBLICAÇÃO: PPEE.MP.013
BRASÍLIA -DF: ABRIL - 2022

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO

Fernando Rocha Moreira

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Rafael Rabelo Nunes, Ph.D, FT/UnB _____
Orientador

Prof. Edna Dias Canedo, Ph.D, FT/UnB _____
Examinador Interno

Prof. Laerte Peotta de Melo, Ph.D _____
Examinador Externo

FICHA CATALOGRÁFICA

MOREIRA, F.R.
UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO [Distrito Federal] 2022.
xvi, 60 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Riscos	2. Segurança da informação
3. Métodos Multicritério	4. MCDA
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

MOREIRA, F. R. (2022). *UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 60 p.

CESSÃO DE DIREITOS

AUTOR: Fernando Rocha Moreira
TÍTULO: UMA PROPOSTA PARA PRIORIZAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA COM O USO DE UM MÉTODO MULTICRITÉRIO .
GRAU: Mestre em Engenharia Elétrica ANO: 2022

Fernando Rocha Moreira
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho à minha avó Lourdinha, meu anjo da guarda.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e por me fortalecer ajudando a ultrapassar todos os desafios encontrados ao longo da realização deste trabalho. Agradeço minha esposa Éryka por me apoiar e me dar forças sempre que precisei. A toda minha família, em especial meus pais, Maria do Carmo e Fernando, irmãs, Andréia e Letícia, e todos os meus avós por serem minha base. Ao professor, amigo e parceiro de trabalho, Rafael Rabelo, essencial no meu processo de formação intelectual e profissional, pela dedicação e por tudo o que aprendi ao longo dos anos no mestrado. Agradeço ao professor Demétrio pelas correções, conselhos, apontamentos e pelo ensinamento da metodologia científica. À UnB e a todos os professores por terem me concedido a chance de aprender e desenvolver intelectualmente. Agradeço a meus amigos e colegas de mestrado, Eduardo, Marcus e Fábio, pessoas com quem tenho aprendido muito com suas experiências e conhecimentos. Aos meus amigos, Mário Lúcio, Marcela, Petterson, Ana Clara, Guilherme e Amanda, amigos com quem sempre posso contar. Agradeço aos meus Senseis de Karatê, Paulo e Valter, essenciais no meu processo de formação disciplinar. A todos os meus colegas de trabalho. A todas as pessoas que, diretamente ou indiretamente, participaram do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado.

RESUMO

A quantidade de crimes cibernéticos, a perda em volume financeiro e a demanda por transparência exigida pelo mercado e órgãos regulamentadores têm desafiado os gestores a realizar uma gestão de riscos de segurança da informação. Realizar uma gestão de riscos de segurança baseada em controles não é trivial, uma vez que a quantidade de boas práticas contidas nos frameworks é grande, e os gestores se veem diante de um desafio de escolha e priorização destes. Utilizando de metodologias multicritério, os decisores conseguem realizar a modelagem do problema, bem como realizar a priorização dos controles de segurança, conforme recomendado pela ISO 31010. Entretanto, os métodos multicritérios mais utilizados na literatura apresentam como objetivo somente a precisão dos cálculos de priorização das alternativas, não têm foco na construção do conhecimento e, muitas vezes, não conseguem envolver todas as partes interessadas, dificultando o processo de compreensão do problema. O MCDA-C é um método multicritério com abordagem mista, qualitativa e quantitativa, com foco na construção do conhecimento, ouvindo todas as partes interessadas em diversos níveis organizacionais. Esse método traz como resultado os pontos de desempenho, maximização e minimização dos controles de segurança da informação. Neste trabalho, propõe-se a utilização do MCDA-C como um método que auxilia os gestores de segurança da informação a priorizar os controles. O CSF NIST foi utilizado como framework de boas práticas para esse trabalho. Por fim, o trabalho demonstra que o MCDA-C é capaz de compreender o problema em todos os níveis organizacionais e construir o conhecimento de forma que os gestores consigam utilizá-lo onde os recursos devem ser aplicados e priorizados.

ABSTRACT

The amount of cybercrime, the loss in financial volume and the demand for transparency required by the market and regulatory bodies have challenged managers to perform information security risk management. Performing a security risk management based on controls is not trivial, since the amount of good practices contained in the frameworks is large, and managers are faced with the challenge of choosing and prioritizing them. Using multi-criteria methodologies, decision makers are able to model the problem and prioritize the security controls as recommended by ISO 31010. However, the most commonly used multi-criteria methods in the literature have as their objective only the precision of the calculations for prioritizing alternatives, they do not focus on knowledge construction and often fail to involve all interested parties, making the process of understanding the problem and constructing knowledge difficult. The MCDA-C is a multicriteria method with a mixed approach, qualitative and quantitative, that focuses on knowledge construction, listening to all interested parties in several organizational levels, and brings as a result, the performance points, maximization and minimization of information security controls. In this work, it is proposed the use of MCDA -C as a method that helps information security managers to prioritize controls, the NIST CSF was used as a good practice base for this work. Finally, the work demonstrates that the use of MCDA-C is capable of understanding the problem at all organizational levels, building knowledge so that managers can understand where resources should be applied and prioritized.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

Siglas

ABNT	*Associação Brasileira de Normas Técnicas*
AHP	*Processo de Análise Hierárquicas*(Processo de Análise Hierárquicas)
ANP	*Analytic network process*(Processo de rede Analítica)
BWM	*Best-Worst Method*(Método Melhor-pior)
CIST	*Conferência Ibérica de Sistemas e Tecnologias de Informação*
CSF	*Cybersecurity Framework*(Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica)
DEMATEL	*Decision Making Trial and Evaluation Laboratory* (Laboratório de Julgamento e Avaliação da Tomada de Decisão)
ENISA	*European Union Agency for Cybersecurity* (Guia De Aperfeiçoamento Da Segurança Cibernética Para Infraestrutura Crítica)
EPV	Elemental Points of View(Ponto de vista elementar)
FAP-DF	*Fundação de Apoio a Pesquisa do Distrito Federal*
FPV	Fundamental Points of View(Ponto de vista fundamental)
GDPR	General Data Protection Regulation(Regulamento Geral de Proteção de Dados)
IEEE	*Institute of Electrical and Electronic Engineers*(Instituto de Engenheiros Eletricistas e Eletrônicos)
ISO	*International Organization for Standardization*(Organização Internacional de Normalização)
LGPD	Lei Geral de Proteção de Dados Pessoais
MACBETH	Measuring Attractiveness by a Categorical Based Evaluation Technique (Medindo a Atratividade por uma Técnica de Avaliação de Base Categórica)
MCDA	Multicriteria Decision Analysis (Análise de Decisão Multicritérios)
MCDA-C	*Multicriteria Decision Aid Constructivist Approach* (Metodologia Multicritério de Apoio à Decisão Construtivista)
MCDM	*Multiple-criteria decision analysis*(Método de decisão multi-critério)
NIST	*National Institute of Standards and Technology*(Instituto Nacional de Padrões e Tecnologia)
PIBIT	Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico
TOPSIS	*Technique for Order of Preference by Similarity to Ideal Solution*(Técnica para Ordem de Preferência por Similaridade com a Solução Ideal)
UNB	*Universidade de Brasília*

1 INTRODUÇÃO

O número crescente de ataques cibernéticos demonstra a gravidade do cenário atual no âmbito da segurança da informação [1]. Com isso, a segurança da informação tornou-se um problema importante para as empresas, demonstrando a necessidade de investimentos para mitigar riscos e se manterem seguras diante desse desafio [2] [1]. Portanto, realizar uma gestão de riscos de segurança da informação de forma sistêmica é fundamental para que as empresas encontrem os requisitos necessários no que tange o sistema de gestão de segurança da informação [3].

Realizar uma gestão de riscos de segurança da informação não somente é uma boa prática, mas também existe uma crescente demanda por transparência que parte pelo mercado financeiro e por órgãos reguladores [4]. Desta forma, fica evidente que uma gestão de riscos é importante tanto em organizações privadas quanto em organizações da administração pública [5].

A gestão de riscos da segurança da informação exige que as organizações façam uma avaliação de seu cenário, tendo a ciência que os riscos possuem diferentes naturezas e efeitos, podendo ocorrer em qualquer nível organizacional [6]. Essa avaliação de riscos pode auxiliar as empresas a desenvolver uma estratégia para mitigar e priorizar os seus tratamentos, elaborando um planejamento que auxilie na tomada de decisão e permita obter uma melhor relação risco e retorno [7].

Entretanto, realizar uma avaliação de riscos baseada em controles nos diversos níveis organizacionais é um problema que as instituições possuem, onde existe uma dificuldade de priorizá-los [7] [8]. Por exemplo, o "Framework for Improving Critical Infrastructure Cybersecurity"do NIST traz 108 controles para auxiliar nos riscos de cibersegurança, mas não diz onde iniciar um plano de risco com esses controles [9] [8]. Um outro exemplo é a ISO 27001:2013 que traz consigo 113 controles que podem ser usados para reduzir os riscos de segurança [10]. Portanto, os gestores de segurança se vêem diante de um problema de tomada de decisão de quais controles priorizar.

Tomar decisões que envolvam riscos cibernéticos são complexos por haver várias variáveis ou critérios que necessitam ser estruturados e analisados. Esse tipo de problema é caracterizado como um processo de tomada de decisão multicritério que necessitam de métodos específicos para sua resolução [11].Esses métodos podem ser encontrados em normas como por exemplo a ISO 31.010:2012 que apontam os métodos multicritérios como um método de decisão que pode ser muito aplicável na identificação, análise e avaliação de riscos [12].

A norma ISO 31.010:2012 indica que a adoção dos métodos multicritério conseguem auxiliar gestores produzindo uma ordem de priorizações em relação as alternativas e critérios adotados, sendo assim uma ferramenta de gestão de riscos. As vantagens de adotar esses métodos são: fornecer uma forma simples de tomada de decisão, descomplicar o problema tornando gerenciável e com complexidade menor, auxiliar na análise de custo benefício, e por fim, encontrar uma solução ótima entre as possíveis alternativas [12].

Os métodos de decisão multicritérios têm sido aplicados para auxiliar na avaliação de riscos em diversas áreas como desenvolvimento de negócios eletrônicos, contaminação de águas subterrâneas, desenvolvimento de *software* entre outros [7]. Esses métodos também podem ser aplicados para avaliação dos riscos

da segurança da informação, fornecendo uma estrutura apropriada para a melhoria do gerenciamento de riscos e auxiliando na tomada de decisão por parte de gestores [13].

Neste trabalho, foi realizada uma proposta da utilização de métodos multicritério para a priorização de controles de segurança cibernética utilizando um *framework* como referência. Usando esta abordagem, foi possível priorizar e mostrar o quanto cada controle poderia colaborar para mitigar os riscos cibernéticos, auxiliando gestores no processo de tomada de decisão .

1.1 HIPÓTESE

Com base nesse cenário, é possível utilizar de uma abordagem multicritério construtivista, que não somente utilize os métodos convencionais de gestão de riscos, mas o desafio da construção do conhecimento em relação aos riscos, onde o gestor consiga visualizar os pontos de melhorias. Neste modelo, tanto gestores e as partes interessadas expõem seus pontos de vista, contribuindo para a compreensão do problema.

1.2 MOTIVAÇÃO E PROBLEMA

O crescente número de crimes cibernéticos, assim como o aumento dos valores em perdas financeiras, demonstram a necessidade de utilizar de ferramentas de gestão de riscos para a segurança cibernética, buscando as melhores práticas e aumentando a segurança neste meio.

As abordagens multicritério utilizadas no contexto da segurança da informação não apresentam a compre ensão do problema, e construção do conhecimento. Essas abordagens focam somente na precisão dos cálculos, não indicando a situação real da organização perante os controles de segurança e apontando os pontos de melhoria.

Outrossim, a crescente demanda por transparência que as instituições enfrentam junto a órgãos regulamentadores e o mercado financeiro, também é um fator motivacional para a construção deste trabalho.

Portanto, diante desse cenário, a utilização de um método eficaz e confiável é considerada a motivação para que os gestores procurem uma abordagem de gestão de riscos multicritério diferente das convencionais. Nela, o foco recai sobre a construção do conhecimento e o gestor conhece a situação real, os pontos de priorização dos controles de segurança, o que auxilia o processo de tomada de decisão.

1.3 OBJETIVO GERAL

Propor e avaliar o método de decisão multicritério MCDA-C em um *framework* de segurança da cibernética utilizando os conceitos e princípos da gestão de riscos.

1.3.1 Objetivos específicos

Com o objetivo geral proposto, os objetivos específicos foram definidos e cumpridos, quais sejam:

- Utilizar dos controles de um *framework* de segurança da informação como boa prática de mitigação de riscos .
- Envolver todas as partes interessadas no processo de gestão de risco.
- Identificar os controles de segurança que devem ser priorizados.
- Aplicar o método MCDA-C abordando os princípios da gestão de riscos, permitindo medir a efiência dos objetivos descritos.

1.4 JUSTIFICATIVAS

Os modelos comuns de gestão de riscos se baseiam na subjetividade da ocorrência de um evento, deixando os gestores em situação de dificuldade para priorizar riscos e realizar o processo de tomada de decisões.

Os métodos multicritério mais utilizados que poderiam colaborar com os gestores não focam na construção do conhecimento, limitando-se somente à execução e precisão dos cálculos, deixando de fora pontos de vista que poderiam colaborar para a compreensão do problema.

Com a adoção de um modelo que empregue a compreensão do problema e a construção do conhecimento, diversos pontos de vista podem ser abordados para auxiliar no processo de gestão de riscos. A partir do momento em que as partes interessadas são incluídas nesse processo, a visão dos gestores começa a se confrontar com a dos *stakeholders*, indicando os pontos de priorização e de possíveis melhorias, resultando e um problema estruturado e compreendido.

1.5 PUBLICAÇÕES RESULTANTES DESSE TRABALHO

- Publicação do artigo *"Optimization of the performance of an online payment application by the improviment of its infrastructure" 2020 15th Iberian Conference on Information Systems and Technologies* (CISTI) [14].
- Uma Análise das Aplicabilidades de Métodos Multicritérios no Contexto da Segurança da Informação no 32º Encontro Nacional de Cursos de Graduação em Administração 2021 [15].
- A Utilização dos *frameworks* NIST CSF E Da Série NBR ABNT ISO 27.000 no Contexto da Gestão da Segurança da Informação 32º Encontro Nacional de Cursos de Graduação em Administração 2021 [16].
- Certificado de Mérito - Melhores Artigos - Área Temática: Administração da Informação, 32o ENANGRAD, Associação Nacional dos Cursos de Graduação em Administração [16].

- Publicação do artigo *"Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology"* na Revista IEEE *Access* [8].

1.6 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está dividida da seguinte maneira: No capítulo 2 são abordados os principais conceitos e definições a respeito do tema deste trabalho. Primeiramente, apresenta-se uma descrição sobre o processo de gestão de riscos é apresentada, seguida de uma explicação sobre os principais *frameworks* de segurança da informação bem como sua utilização no mundo. Os conceitos, definições e cenário de aplicabilidade dos métodos multicritério também estão nesse capítulo. Além disso, explica-se brevemente o *software* utilizado nesta pesquisa. Ainda nesse capítulo, os principais trabalhos relacionados são descritos e comparados com o trabalho proposto no que tange os *frameworks* de segurança da informação e métodos multicritério utilizados.

O capítulo 3 descreve a metodologia utilizada neste trabalho, de modo que a classificação da pesquisa é explicada. Também nesse capítulo, outros conceitos são definidos como lócus, sujeitos e objetos da pesquisa. O capítulo 4 discute os resultados obtidos a partir da aplicação do método multicritério MCDA-C, que procurou compreender o problema e identificar o controles de segurança que podem ser priorizados em uma possível implementação. Por fim, o trabalho apresenta as Conclusões no capítulo 5 e elenca as premissas para os trabalhos futuros que podem ser realizados a partir desta pesquisa.

2 REFERENCIAL TEÓRICO E TRABALHOS CORRELATOS

Nesta seção serão abordados os principais conceitos pertinente deste trabalho. Por fim, uma subseção de trabalhos correlatos será apresentada.

2.1 PRINCÍPIOS DA GESTÃO DE RISCOS

De acordo com [17], O risco é definido como o efeito da incerteza nos objetivos. Este efeito trata -se de um desvio em relação ao caminho que é esperado, podendo ser positivo, negativo ou que se traduz em oportunidades e ameaças [17].

O processo de gerenciamento de riscos se apresenta de forma iterativa e tem como objetivo auxiliar as organizações a atingir seus objetivos e tomar decisões. Este processo é parte da governança e liderança e deve envolver todas as atividades da organização, incluindo todas as partes interessadas.

Ao realizar um gerenciamento de riscos, diversos fatores devem ser considerados, entre eles, o contexto interno e externo da organização, fatores humanos e culturais [17]. Gerenciar riscos baseia-se em 8 princípios conforme Figura 2.1: [17]:

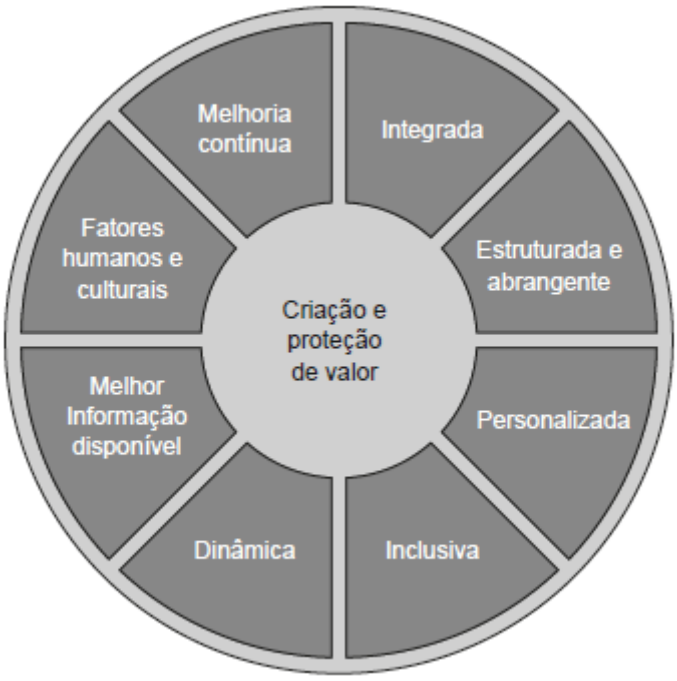

Figura 2.1: Principios da gestão de riscos. Retirado de [17]

Esses princípios podem ser especificados da seguinte forma 2.1:

- Integrada: gestão de riscos deve envolver todas as partes da organização;
- Estruturada e abrangente: O processo de gestão de riscos deve possuir uma abordagem estruturada contribuindo para resultados consistentes e comparáveis;
- Personalizada: Este processo deve ser personalizado podendo relacionar os contextos externos e internos da organização com os objetivos;
- Inclusiva: O processo de gestão de riscos deve envolver todas as partes interessadas de forma que os pontos de vistas e percepções sejam considerados;
- Dinâmica: O processo de gestão de riscos deve ser dinâmico pois riscos podem surgir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem;
- Melhor informação disponível: As entradas de dados para a estão de riscos são baseadas em históricos e expectativas futuras, considerando quaisquer limitações e incertezas associadas a estas informações e expectativas. Importante ressaltar que a informação deve ser clara e disponível para todos os stakeholders;
- Fatores humanos e culturais: O fator humano e cultural deve ser levando em consideração pois influenciam em todos os riscos em cada nível de estágio;
- Melhoria contínua: o processo de gestão de riscos deve ser melhorado conforme aprendizado e experiencias adquiridas.

A norma ISO/IEC 31010 foi criada para listar técnicas para o processo de avaliação de riscos abordando 8 princípios [12]. Ela foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos - ABNT/CEE-63 - que tem como representantes, integrantes de partes interessadas dos setores envolvidos, podendo ser citados: produtores, consumidores e neutros (universidades, laboratórios e outros)[12].

A ISO/IEC 31010 apresenta os métodos multicritério como um método proposto para a gestão de riscos. Assim, neste trabalho, os princípios da gestão de riscos foram abordados durante a aplicação do MCDA -C, que será discutido adiante,

2.2 *FRAMEWORKS* DE SEGURANÇA DA INFORMAÇÃO

Nesta seção serão abordados dois dos principais *frameworks* para a implementação de controles de segurança. Esses *frameworks* são o NIST CSF e a ISO 27000 series, que foram estudados e analisados para a aplicação e realização desta pesquisa.

2.2.1 NIST - *CYBERSECURITY FRAMEWORK* (CSF)

O Framework CSF *Cybersecurity Framework* criado pela NIST *National Institute of Standards and Technology* - Instituto Nacional de Padrões e Tecnologia tem como objetivo auxiliar operadores de infra-

estrutura crítica. Ele auxilia na Identificação e o desenvolvimento de diretrizes para enfrentar riscos de segurança cibernética [9].

A definição de Infraestrutura crítica está no *US Patriot Act* de 2001 que define sistemas e ativos, sejam físicos ou virtuais, que a incapacidade ou destruição de tais teria um impacto debilitante. Seja esse impacto sobre as áreas da saúde, segurança pública nacional, economia ou até mesmo na combinação dessas áreas [9].

O CSF pode ser utilizado tanto na área privada quanto pública e proprietários de empresas e entidades com a função de proteger qualquer tipo de organização. Este guia não substitui o processo de segurança cibernética de uma organização, mas ele procura complementa lo. Guia é composto por três partes: Estrutura básica; os níveis de implementação; Avaliação da estrutura [9].

A Estrutura Básica oferece os padrões e diretrizes para a toda a organização, passando desde o nível executivo até o nível de implementação ou operacional. Esta Estrutura Básica é composta por quatro elementos: Funções; Categorias; Subcategorias; Referências Informativas [9].

1. Funções: organizam atividades básicas de segurança cibernética em seu nível mais alto;
2. Categorias: subdivisões denominadas das funções;
3. Subcategorias: são as subdivisões das categorias sendo o resultado específicos das atividades técnicas e de gerenciamento a serem implementadas;
4. Referências informativas: São as referências de onde são retirados os controles para implementação.

A Figura 2.2 ilustra como é realizada e dividida essa estrutura.

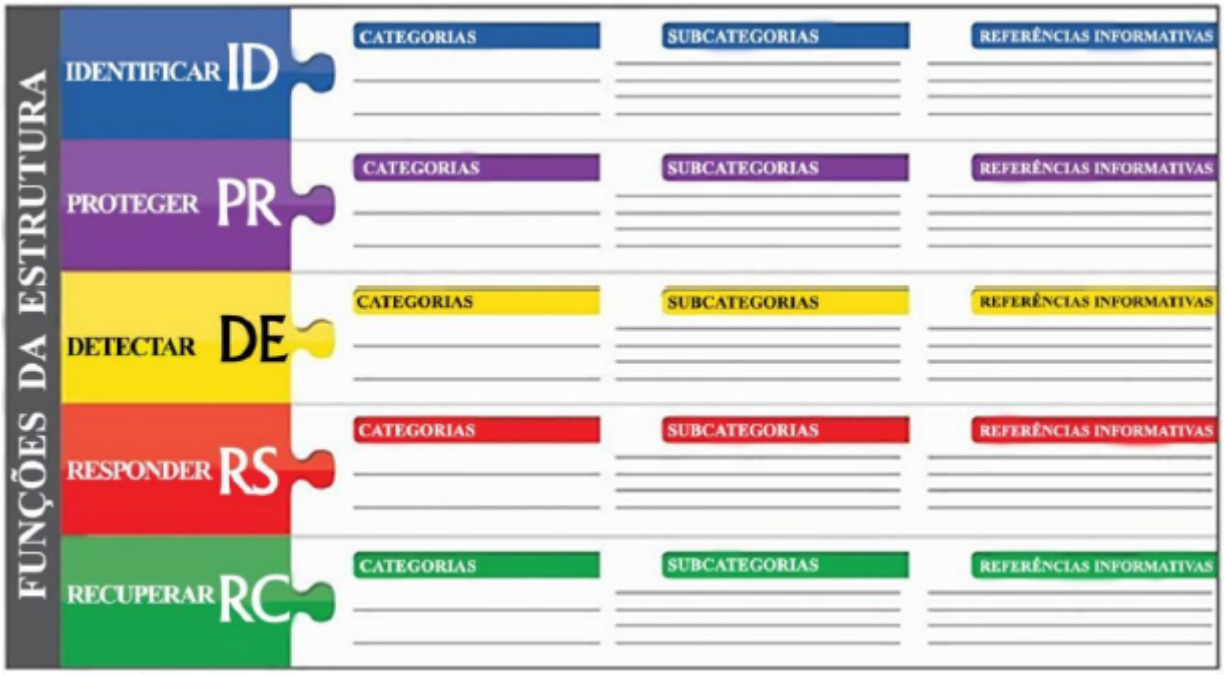

Figura 2.2: Estrutura NIST e as taxas de colaboração. Retirado de [9]

As funções são respectivamente [9]:

- Identificar - Essa função tem como objetivo desenvolver uma compreensão organizacional para gerenciar os riscos de segurança. Com a finalidade de tanger sistemas, pessoas, ativos e recursos. Entre as categorias dessa função pode -se citar: desta Função incluem: Gerenciamento de Ativos; Ambiente Empresarial; Governança; Avaliação de Risco; e Estratégia de Gerenciamento de Risco;
- Proteger - Esta função é responsável por desenvolver e implementar as proteções necessários para garantir que os serviços continuem em funcionamento. Ela procura limitar ocorrências de segurança cibernética Entre as categorias desta Função incluem: Gerenciamento de Identidade e Controle de Acesso; Conscientização e Treinamento; Segurança de dados; Processos e Procedimentos de Proteção da Informação; Manutenção; e Tecnologia de Proteção;
- Detectar - Esta função tem como objetivo desenvolver e implementar os controles necessários para realizar a identificação e ocorrência de um evento de segurança cibernética. As categorias desta função são: Anomalias e Ocorrências; Monitoramento Contínuo de Segurança; e Processos de Detecção;
- Responder - Esta procura e implementar atividade apropriadas para efetuar algum tipo de ação quando um incidente de segurança cibernética detectado. Exemplos de Categorias desta Função incluem: Planejamento;
- Recuperar - Esta função procura realizar as atividades e a manutenção de planos de resiliência para restaurar qualquer serviço inoperante devido a um incidente de segurança cibernética. Os exemplos de Categorias de resultados dentro desta Função incluem: Planejamento de Restabelecimento; Aperfeiçoamentos; e Notificações.

Os níveis de implementação do Guia fornecem uma abordagem de avaliar como a organização trata o risco de segurança cibernética bem como avaliar o seu grau de maturidade. Estes variam de nível 1 considerado "Parcial" até nível 4 que é o "Adaptável" que se apresentam de forma crescente a medida que a organização se apresenta madura no processo de gestão de riscos da segurança cibernética [9]. A maturidade é avalidada da seguinte forma incremental:

- Nível 1: Não existe formalização, o risco é gerenciado de maneira reativa. A organização realiza o gerenciamento de riscos cibernéticos de maneira irregular, de acordo com a experiência ou informações obtidas de fontes externas. A organização não colabora com ou recebe informações de outras entidades, nem compartilha informações. A organização geralmente não possui consciência dos riscos da cadeia de suprimentos cibernéticos [9];

- Nível 2: Os processos de gerenciamento de risco são aprovadas pela administração, abrangendo toda a organização. Existe uma preocupação em relação à segurança cibernética em alguns, mas não em todos os níveis da organização. Existe a avaliação do risco cibernético de ativos organizacionais e externos, entretanto, não é tipicamente reproduzível ou recorrente. A organização começa a colaborar e receber algumas informações de outras enteidades gerando informações, mas não repassa para outras organizações [9];

- Nível 3: Existe um processo formalizado e aprovado expresso como política. As práticas organizacionais de cibersegurança são atualizadas de acordo com às mudanças nos requisitos de negócios/missão em cenário dinâmico de ameaças e tecnologia. Políticas, processos e procedimentos de conhecimento de riscos são definidos, implementados e revisados. A instituição possui métodos para responder de forma eficaz as mudanças no risco. A organização realiza a monitoração de forma consistente e precisa do risco de cibe segurança. Ela colabora e recebe informações de outras entidades bem como, compartilha suas informações [9];

- Nível 4:A organização consegue adaptar suas práticas de segurança cibernética com base em nas atividades de segurança cibernética anteriores e atuais. A empresa possui um processo de lições aprendidas e indicadores preditivos além de possuir um processo de aperfeiçoamento contínuo incorporando tecnologia, práticas avançadas de segurança cibernéticas. Este nível também contempla a consciência da relação entre risco de segurança cibernética com os objetivos organizacionais, e estes, passam a ser analisados durante o processo de tomada de decisões. Os executivos da organização, monitoram esses riscos no mesmo contexto que riscos financeiros. Ela entende seu papel em um ecossistema maior contribuindo para a comunidade no que tange a riscos cibernéticos gerando, recebendo, analisando informações bem como compartilhando de forma interna e externa a outros colaboradores [9].

Avaliação da Estrutura procura realizar uma avaliação das Funções, categorias e subcategorias do guia com os requisitos do negócio da organização. Essa avaliação procura encontra lacunas a serem preenchidas e que podem ser resolvidas satisfazendo uma determinada Categoria ou subacategoria [9].

2.2.2 ISO 27000 SERIES

A série ISO 27000 é um *framework* que foi desenvolvido pela *International Organization for Standardization*. Esta organização é responsável por criar padrões de boas práticas em diversas áreas. A norma ISO/IEC 27000 é responsável por guiar as organizações no gerenciamento de segurança da informação fornecendo controles para a implementação das boas práticas deste processo [18].

Este padrão traz consigo os controles necessários para implementar um SGSI Sistema de Gestão de Segurança da Informação. Com a utilização destes padrões é possível que uma organização consiga preservar os princípios da segurança da informação como a confidencialidade, integridade e disponibilidade. Esse processo passa por meio da utilização e aplicação de gestão de riscos, oferecendo confiança para todos as partes interessadas participantes deste processo [18].

Ao utilizar este padrão a organização deve analisar os fatores internos e externos que influenciam e são relevantes para atingir os objetivos pretendidos na gestão de segurança de informação. Os padrões das séries ISO/IEC 27000 são separados da seguinte maneira:

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

Este padrão é importante pois outros *frameworks* utilizaram a ISO 27000 como referência para criar seu próprio modelo. Um exemplo é o CSF NIST, ele contém diversos controles de segurança da informação retirados e tendo como inspiração a ISO 27000 [18].

2.2.3 A UTILIZAÇÃO DE FRAMEWORKS NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Para entender o cénario da utilização dos frameworks NIST CSF x ISO 27000 SERIES no contexto da segurança da informação, foi realizada um levantamento bibliográfico de 50 trabalhos a respeito desse tema [16].

A coleta de artigos foi feita entre os meses de fevereiro de 2021 e março de 2021, que foram relativos aos últimos 10 anos [16].

A Figura 2.3 mostra uma série temporal dos 50 artigos coletados e publicados de cada *framework* ISO e NIST por ano. É possível notar um crescimento de estudos na área de segurança cibernética. Importante notar que já no primeiro bimestre de 2021 existem de três artigos utilizando o CSF da NIST [16].

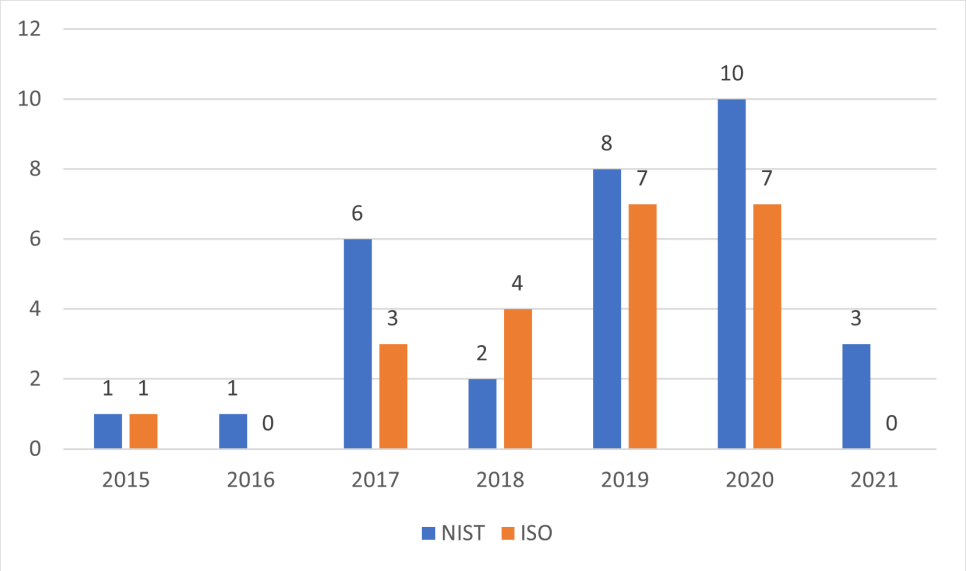

Figura 2.3: Série temporal dos 50 artigos coletados e publicados de cada *framework*. Retirado de [16]

Aplicando uma correlação e regressão linear sob os resultados obtidos desprezando 2021 é possível ver duas curvas de alta tanto para a NIST quanto para ISO com R = 0,85 e R = 0,94 respectivamente. Esses números podem ser caracterizados com uma forte correlação [19]. Esses valores reforçam que existe uma tendência do aumento do uso desses *frameworks* com o passar dos anos. Também é possível verificar que a curva de tendência para o uso da NIST tem sido maior, colaborada pelo alto índice de publicações ao longo dos dois últimos anos. A Figura 2.4 ilustra esse cenário.

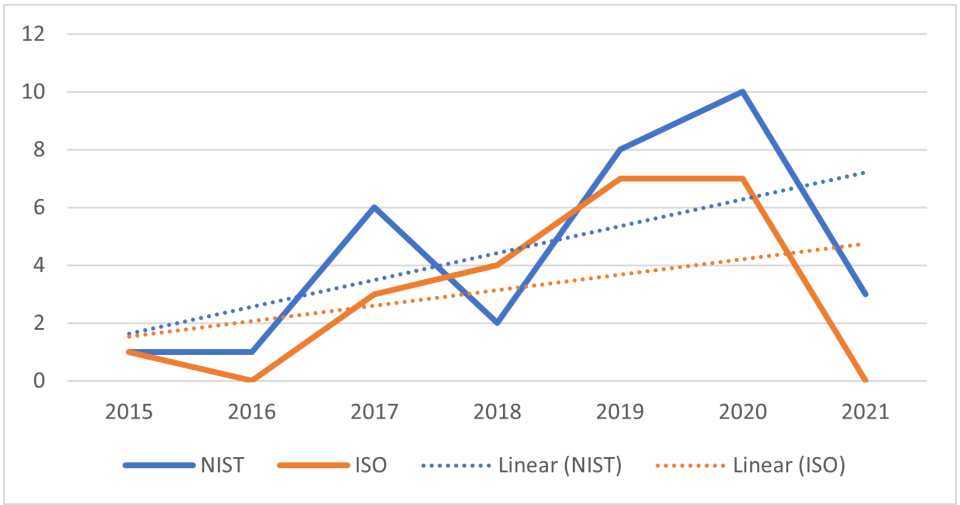

Figura 2.4: Aplicação da regressão linea. Retirado de [16]

O relatório técnico *"The Life and Times of Cybersecurity Professionals"* elaborado pela ESG - (*The Enterprise Strategy Group*) de 2017 também mostrou esse fenômeno. Entrevistando empresas do mundo todo qual foi a ação tomada em relação a segurança da informação nos últimos anos, 52% das grandes organizações responderam que adotaram alguma parte do NIST CSF [16] [20].

Esta informação contida nesse relatório técnico publicado no próprio site da NIST ao encontro ao fenômeno encontrado neste estudo . A Figura 2.5 mostra uma forte disparidade da adoção do CSF NIST

nos Estados Unidos, um domínio da ISO na Indonésia e um equilíbrio maior nos países Europeus [16]. Dados que serão discutidos nos próximos parágrafos.

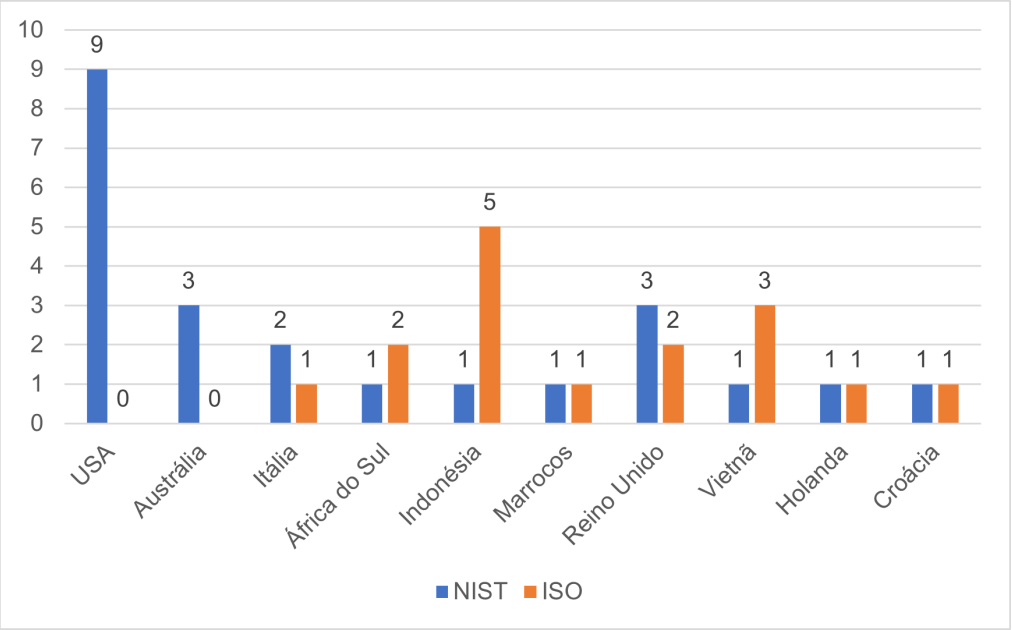

Figura 2.5: Artigos coletados por países. Retirado de [16]

O equilíbrio na adoção desses dois *frameworks* na Europa passa pela importância que a ISO 27000 tem cumprido no aspecto da GDPR - *General Data Protection Regulation*, a Lei Geral de Proteção de dados da Europa. A ISO 27000 cumpre cerca de 75% a 80% nos cumprimentos legais da lei conforme mostrados em estudos [16] [21].

Ainda sob essa ótica, existe um incentivo da própria GDPR para que as empresas adquiram a certificação na ISO 27001 auxiliando assim, a entrar em conformidade com a lei [16] [22]. Aproximadamente 73% das empresas que utilizaram este *framework* concorda que este tem colaborado nos objetivos exigidos pela GDPR [22]..

Já o relatório técnico *"Trends In Security Framework Adoption"*, elaborado em 2016 ouvindo somente empresas nos Estados Unidos, justificam o alto número da adoção do CSF nesse mesmo país. Aproximadamente 70% das empresas que utilizam o CSF consideram uma boa prática, enquanto 29% utilizaram por motivos negociais, e 28% porque um contrato federal exigia a adoção de controles do CSF [16] [23].

Neste mesmo relatório é possível ver que o CSF da NIST estava somente em quarto lugar em preferência nos Estados Unidos, importante ressaltar que as empresas podem adotar mais de um *framework*, de acordo o entendimento da organização [23]. A Figura 2.6 mostra essa informação.

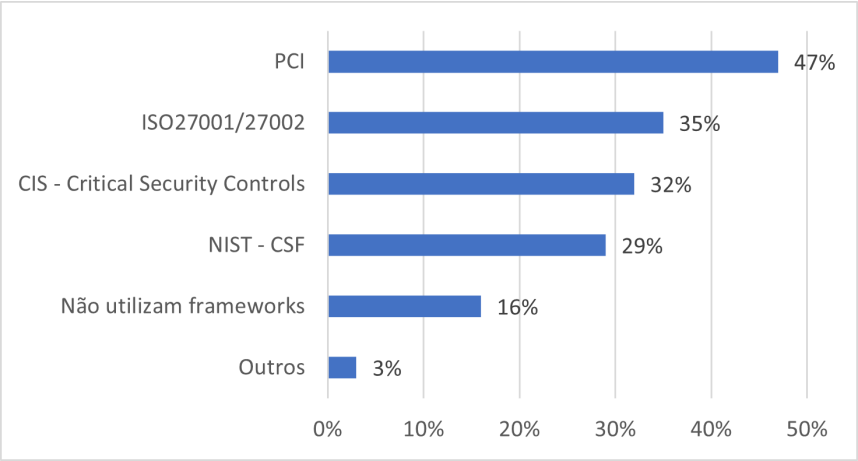

Figura 2.6: Preferência de *frameworks* nos Estados Unidos em 2016. Adaptado de [23]. Retirado de [16]

No ano de 2016 o CSF não estava em primeiro lugar pelo fato de o PCI ser um *framework* voltado para o varejo e foi relatado uma necessidade de alto investimento para abordar todos os controles do NIST [16] . A ISO também estava se destacando em relação ao CSF devido ao maior conhecimento da sua existência em relação a primeiro por parte das empresas [16] [23].

Este relatório técnico foi obtido em 2016, mas já apontava projeções de alta em relação a uma maior adesão ao NIST, fato que foi ilustrado nesse presente trabalho [23]. A Figura 2.7 mostra esse cenário[16] .

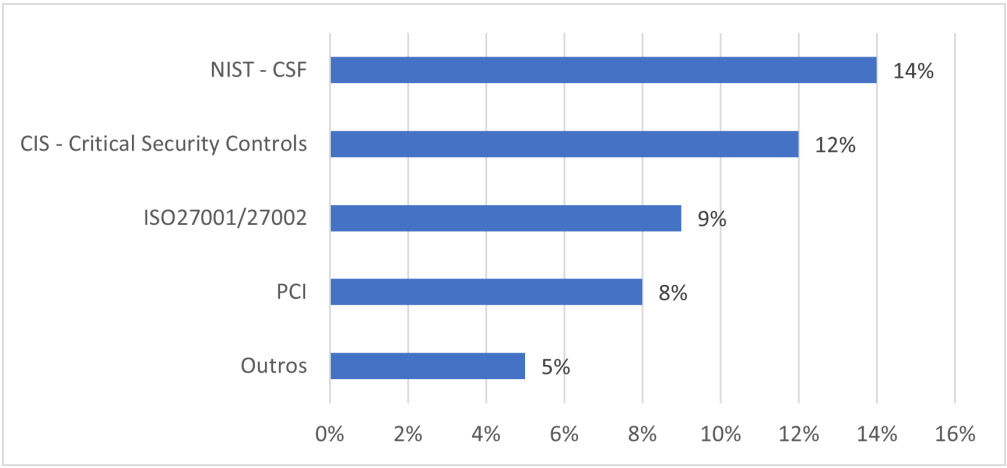

Figura 2.7: Preferência de *frameworks* nos Estados Unidos em 2016.Adaptado de [23]. Retirado de [16]

O levantamento bibliográfico também mostra a relação de trabalhos publicados por setores da economia. Importante ressaltar que os trabalhos podem possuir mais de um setor econômico pertencente. Alguns trabalhos não relataram a qual setor da economia pertencem[16]. A Figura 2.8 apresenta esse cenário.

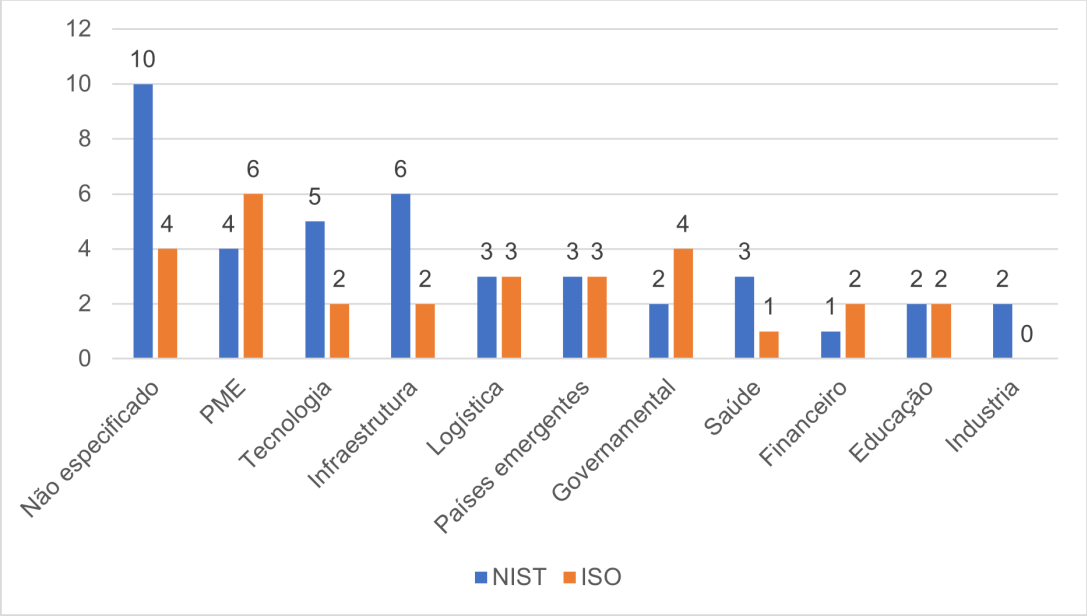

Figura 2.8: Preferência de setores da economia por Framework. Retirado de [16]

Um ponto positivo constato no trabalho é a preocupação das PME - Pequenas e Médias Empresas em relação a sua segurança cibernética. Nessa categoria é possível ver que existe uma preferência pela ISO, e isso pode ser visto também no relatório técnico *"Trends In Security Framework Adoption"*. Como citado anteriormente devido ao alto custo para a implantação das diretrizes da NIST, esta pode ser uma justificativa para a preferência do uso dessas categorias pela ISO [16]. A Figura 2.9 mostra esse cenário também encontrado no relatório [23].

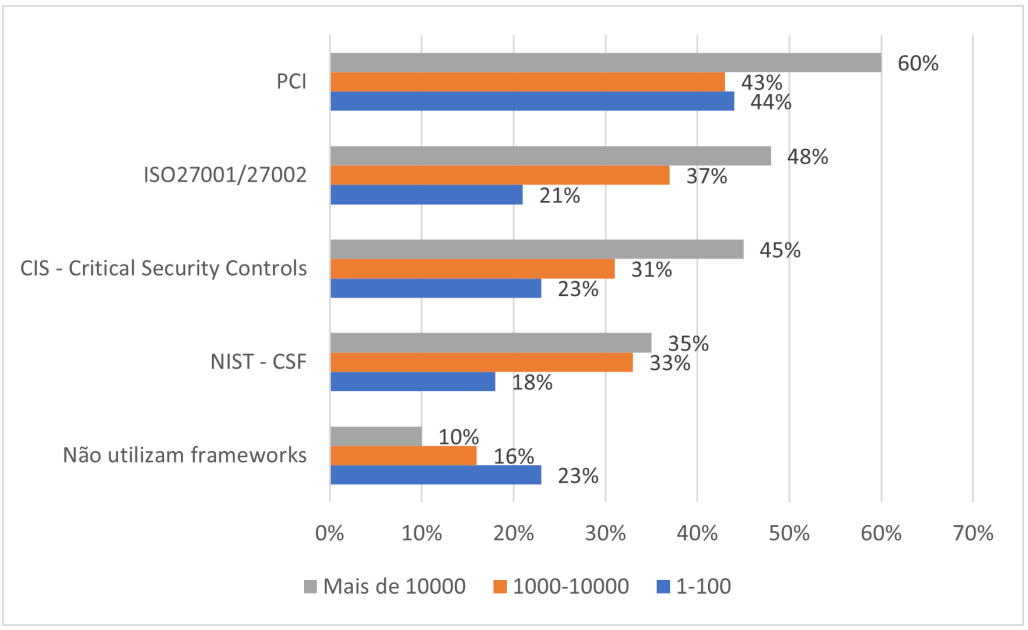

Figura 2.9: Tamanho de empresas por framework.Adaptado de [23]. Retirado de [16]

Assim como o presente trabalho mostrou a adoção do CSF a escala global em diversos setores da economia, este relatório mostra ainda a presença do uso do CSF nos Estados Unidos[16]. É possível verificar a presença de vários setores em comum, destacando a Tecnologia da Informação, Governamental

e o setor Bancário. A Figura 2.10 ilustra esse cenário.

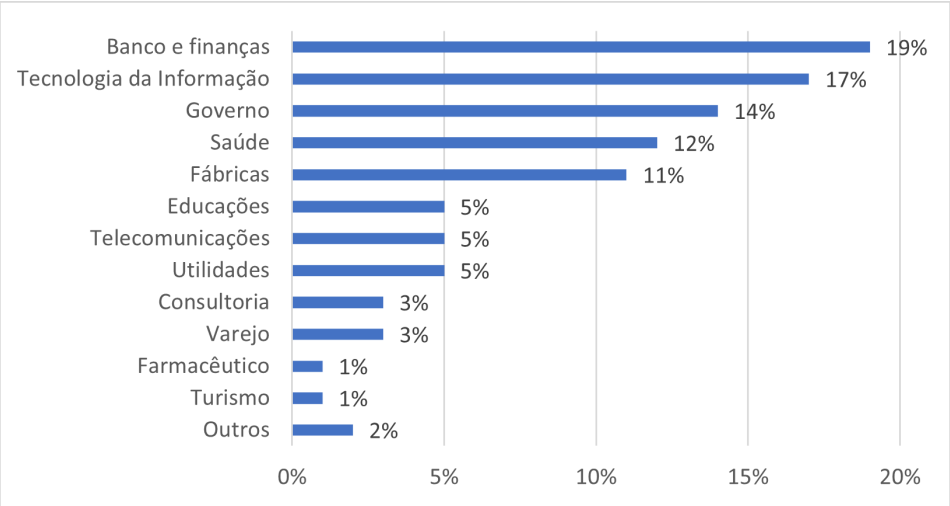

Figura 2.10: Tamanho de empresas por framework. Adaptado de [23]. Retirado de [16]

Os *frameworks* de segurança da informação foram utilizados neste trabalho como referência de controles para a aplicação do método MCDA -C. Por se tratar de um *framework* novo, que demonstrou uma curva de crescimento maior em relação a ISO 27000 series, que utiliza de várias fontes para sua criação incluindo a própria ISO, o *framework* escolhido foi o CSF NIST.

2.3 MCDM - *MULTIPLE-CRITERIA DECISION ANALYSIS* MÉTODOS MULTICRITÉRIOS

Após a segunda guerra mundial houve um crescimento do uso de métodos de pesquisas operacionais com o objetivo de encontrar soluções ótimas para problemas multidimensionais de alta complexidade do cotidiano. Ao longo dos anos a ciência começou a se questionar sobre as reais vantagens de se utilizar esses tipos de métodos para auxiliar na tomada de decisões [24].

Quando se fala em processo de tomada de decisão, é importante ressaltar que este se torna intrínseco a qualquer tipo de atividade. À medida que os anos passam, o ritmo das mudanças tecnológicas se acelera, o mercado e os clientes ficam cada vez mais exigentes e com isso tomar decisões se torna um processo crítico e complexo exigindo com que a melhor alternativa sempre seja escolhida não abrindo margem para falhas [25].

Uma das formas de tomar decisões é a adoção de MCDM - Métodos de Decisão Multicritérios. Quanto se utiliza esses métodos, um problema de alta complexidade, deve ser estruturado, melhorando entendimento, e auxiliando no processo de tomada de decisão. [25].

Esses métodos auxiliam os gestores otimizando o tempo e custos, melhorando a precisão para tomadas de decisões [12]. Os métodos MCDM são ferramentas úteis auxiliar no gerenciamento de riscos da segurança da informação por fornecer uma estrutura apropriada para tal, podendo ser úteis para medir a eficácia dos controles de riscos [12] [13].

Geralmente os MCDM se baseiam em uma avaliação de critérios e alternativas em cenários que englobem muitas variáveis para serem analisadas [25].

Os métodos multicritérios estão listados na ISO 31.010:2012 como uma ferramenta que engloba todo o processo de gestão de riscos abordando todas as suas fases conforme ilustrado na tabela 2.1.

Tabela 2.1: Métodos multicritério no processo de Gestão de Riscos. Retirado e adaptado de [12]

Ferramentas e Técnicas	Processo de Gestão de Riscos				
	Identificação de Riscos	Análise de Riscos			Avaliação de Riscos
		Consequência	Probabilidade	Nível de Risco	
Análise de decisão por Multicritério	A	FA	A	FA	A

- FA - Fortemente aplicável;
- A - Aplicável.

A ISO 31.010:2012 também demonstra que ao avaliar uma série de alternativas, critérios devem ser escolhidos para auxiliar neste processo. Um dos resultados é uma ordem de preferência com uma pontuação entre as alternativas a serem avaliadas [12]. Ao utilizar essa metodologia, uma matriz com uma série de opções é feita com classificações e pontuação para cada alternativa e critério. Esta norma descreve que a aplicação de um método multicritério deve envolver os seguintes passos [12]:

- Definir um objetivo;
- Determinar critérios e medidas de desempenho para cada objetivo;
- Estruturar os atributos e os riscos em hierarquia;
- Desenvolver opções para serem avaliadas em relação aos critérios determinando a importância dos critérios e suas ponderações;
- Avaliar as alterativas em relação aos critérios;
- Avaliando os resultados;
- Diretrizes gerais;
- Diretrizes específicas de setores.

Os pontos fortes dos métodos multicritérios são [12]:

- O fornecimento de uma estrutura para auxiliar na tomada de decisão
- Tornar os problemas complexos em mais gerenciáveis;
- Considerar onde os trade offs precisam ser efetuados;
- Auxiliar a atingir um acordo onde os stakeholders possuem objetivos e critérios de análise diferentes.

2.3.1 AHP - *ANALYTIC HIERARCHY PROCESS*

O método AHP - Analytic Hierarchy Process é um MCDM que se apresenta como um método que estabelece uma ordem de preferência de alternativas e critérios, de acordo com a percepção, avaliação e julgamento de especialistas em um determinado assunto [26].

O método AHP consegue fazer a redução de um problema multidimensional em um problema unidimensional, permitindo que decisões complexas sejam reduzidas para um único número, ou seja, permitindo a seleção do melhor resultado dentre uma gama de critérios [26].

O AHP depende para sua aplicação que exista uma hierarquia entre os critérios. Uma hierarquia é composta por um objetivo e abaixo diversos níveis, sendo o primeiro nível chamado de critérios e o segundo chamado de alternativas, com conexões de nível superior para inferior [26]. A Figura 2.11 apresenta uma hierarquia do processo de decisão da escolha da melhor escola. Por exemplo, a figura traz o processo decisório com os critérios: Aprendizado, Amigos, Vida escolar, Treinamento Vocacional, Colegas e Aulas de música. Entre as alternativas, se encontram: Escola A, Escola B e Escola C, que serão julgadas perante os critérios escolhidos.

Figura 2.11: Hierarquia de decisão. Retirado e adaptado de [27]

O AHP utiliza uma abordagem baseada em cálculos para se atribuir pesos para cada um dos critérios. Esses cálculos são realizados por meio da escala de Saaty, onde os especialistas atribuem uma nota ao comparar e julgar critérios e alternativas uns contra os outros. A Tabela 2.2 detalha a escala de Saaty. Como exemplo, em determinado momento um decisor pode comparar a Escola A em relação a B utilizando o critério Aprendizado, atribuindo uma nota 9 para a Escola A, o que significaria que A possui uma preferência Extrema em relação a B no que tange a Aprendizado.

Tabela 2.2: Escala de Saaty. Retirado e adaptado de [26]

Escala Saaty	Valor
Igual Preferência (importância)	1
Intermediário	2
Preferência (importância) moderada	3
Intermediário	4
Preferência (importância) forte	5
Intermediário	6
Preferência (importância) muito forte	7
Intermediário	8
Preferência (importância) extrema	9

Após o julgamento de todos os critérios, um contra os outros, o AHP realiza uma série de cálculos matriciais, encontrando uma ordem de preferência da alternativas e indicando a solução ideal.

As fases do AHP podem ser sintetizadas da seguinte maneira:

1. Definição da árvore de critério e alternativas;
2. Realização dos julgamentos de forma pareada usando a escala de Saaty;
3. Realização do cálculo de prioridades e do índice de julgamentos;
4. Realização do cálculo das alternativas.

Ao final o AHP exibirá uma tabela com a ordem de preferência das alternativas onde uma tabela conterá os valores obtidos pelos cálculo matriciais, os níveis de porcentagem de cada alternativa em escala global do problema [27].

2.3.2 ANP - *ANALYTIC NETWORK PROCESS*

O método ANP - Analytic Network Process é uma generalização do AHP que considera a dependência entre os elementos da hierarquia. Todas as avaliações são estabelecidas da mesma maneira que no processo do AHP através do julgamento dos especialistas [27].

Nem todos os critérios conseguem ser estruturados e apresentar em forma hierárquica, isto porque alguns elementos muitas vezes envolvem interação e dependência de elementos entre níveis superiores de forma lateral.

Desta forma, diferentemente de uma hierarquia, o ANP apresenta-se como um MCDM para ser aplicado quando os critérios envolvam uma forma de rede. [27]. A Figura 2.12 apresenta uma estrutura em rede.

Portanto, a principal diferença entre o AHP e o ANP é a forma de como o problema está estruturado. Enquanto o AHP está voltado para uma estrutura em árvore hierárquica, o ANP é feito em rede apresentando um grau de complexidade maior.

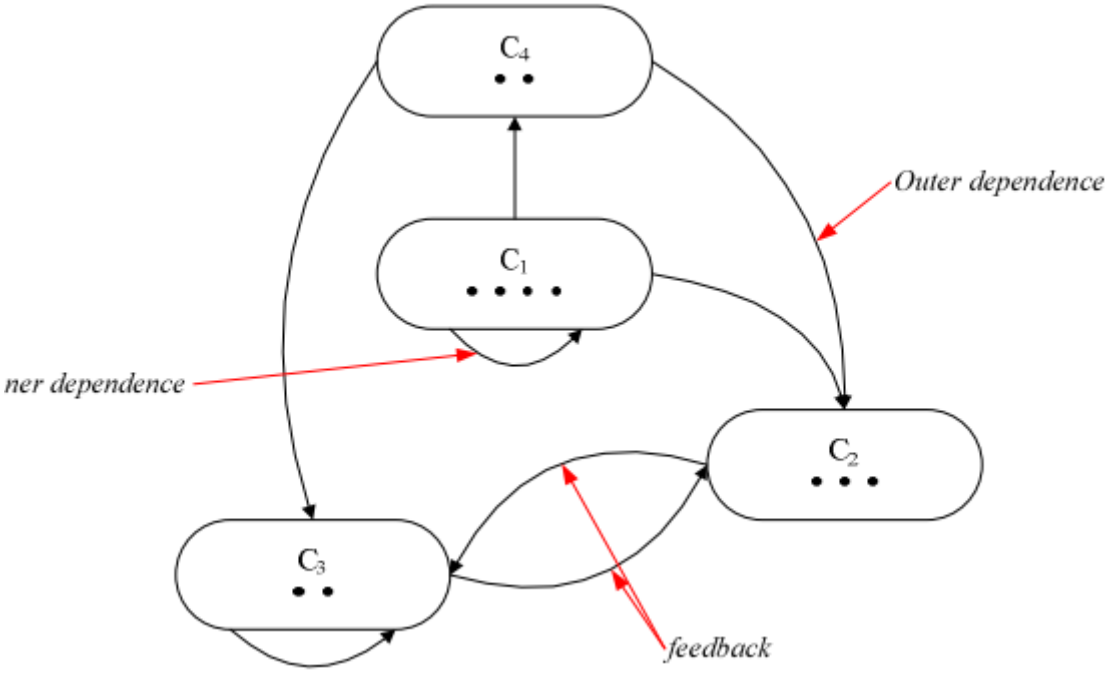

Figura 2.12: Estrutura em rede. Retirado e adadptado de [28]

2.3.3 TOPSIS - *TECHNIQUE FOR ORDER PREFERENCE BY SIMILARITY TO IDEAL SOLUTION*

O método TOPSIS - Technique for Order Preference by Similarity to Ideal Solution é um MCDM que tem como objetivo realizar a escolha da solução ideal por meio de critérios a serem avaliados por um conjunto de especialistas[29]. Entretanto, diferentemente do AHP e ANP por exemplo, este método utiliza de cálculos vetoriais para encontrar a diferença da alternativa avaliada em relação que possui o melhor desempenho em diante de um critério.

Assim, ele funciona por meio da realização da comparação de um conjunto de alternativas, identificando cada critério, aplicando as suas devidas normalizações e pontuações e por fim calculada a distância geométrica entre cada alternativa e a alternativa ideal para cada critério [29].

As etapas do TOPSIS podem ser sintetizadas da seguinte maneira [29]:

1. Avaliar fatores com especialistas: escolher o grupo de especialistas para avaliar os fatores do sistema de estudo. Sempre dois fatores serão escolhidos e confrontados em pares. Para este confronto, uma escala deve ser utilizada de 0 a 4, na qual, 0 representa o menor grau de influência e o 4 o maior;
2. Criação da matriz de decisão: cria -se uma matriz de decisão compostas por critérios e alternativas a serem analisadas;
3. Normaliza -se a matriz de decisão: Assim como outros métodos, também é necessário efetuar esse processo. Essa normalização pode ser realizada de diversas maneiras. Um exemplo é a realização por vetor;

4. Realização do cálculo da matriz com os respectivos pesos: nesta etapa, a matriz normalizada é multiplicada pelos pesos dos critérios. Os pesos dos critérios são obtidos de acordo com o ponto de vista dos decisores;

5. Identificação da Solução ideal positiva e da Solução ideal negativa: nessa etapa é determinado a escolha das melhores alternativas para cada um dos critérios, e então uma solução ideal é encontrada positivamente. Esse mesmo processo é feito para determinar a solução ideal negativa;

6. Cálculo das distancias: Calcula -se a distância euclidiana de cada alternativa em relação a solução ideal positiva e negativa;

7. Similaridade para a posição ideal positiva: Por fim, calcula -se a aproximação das alternativas em relação a situação ideal definindo a hierarquização das alternativas.

2.3.4 DEMATEL - *DECISION MAKING TRIAL AND EVALUATION LABORATORY*

O método Decision Making Trial and Evaluation Laboratory (DEMATEL) é um MCDM que tem sido utilizado para auxiliar na tomada de decisão, capaz de realizar a análise das relações diretas e indiretas entre diversos componentes de um sistema complexo [30] [31].

Construído baseado na teoria dos grafos, o DEMATEL avalia efetivamente todas as relações, construindo um mapa entre os sistemas e através da matriz de relação entre os componentes desses sistemas, permitindo obter um melhor entendimento da inter-relação dos componentes [30] [31].

Os passos do DEMATEL podem ser sintetizados da seguinte maneira:

1. Avaliar fatores com especialistas: escolher o grupo de especialistas para avaliar os fatores do sistema de estudo. Sempre dois fatores serão escolhidos e confrontados em pares. Para este confronto, uma escala deve ser utilizada de 0 a 4, na qual, 0 representa o menor grau de influência e o 4 o maior;

2. Normalizar a Matriz Média : Em seguida cria -se uma matriz com as médias das respostas de todos os envolvidos. Esta matriz deve ser normalizada através do uso de uma constante;

3. Quantificar a influência total entre os fatores: Os fatores provocam efeitos diretos e indiretos entre si. Portanto, nessa etapa quantifica -se quantas influências estão entre os fatores, de forma direta e indireta;

4. Calcular intensidade de efeitos provocados e recebidos: Cria se então uma matriz de efeitos totais, onde o somatório de uma linha representa os efeitos provocados por determinado fator;

5. Definir um limiar de análise para o mapa de influência: Então cria -se um limiar que tem por responsabilidade definir quais efeitos não serão apresentados de acordo com suas intensidades;

6. Construir mapa de influência: Na última fase do processo, cria -se um mapa de influência. Este mapa trata -se de um diagrama de relação causa e efeito. Ele apresenta ilustrativamente a complexidade nas relações entre fatores analisados e intensidades. A figura 2.13 apresenta um exemplo dos diagrama de relação causa e efeito produzido pelo DEMATEL.

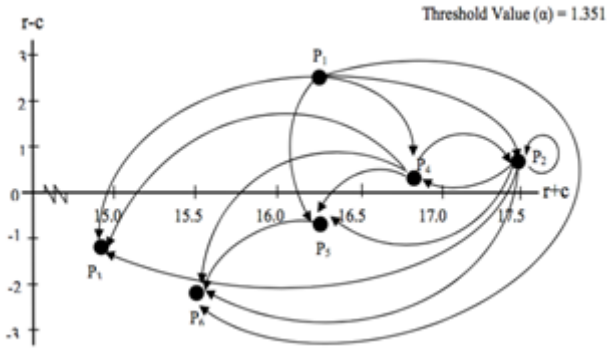

Figura 2.13: Hierarquia de decisão. Retirado e adaptado de [32]

2.3.5 BWM - *BEST-WORST METHOD*

O BWM - Best-Worst Method trata -se de um método desenvolvido por [33]. Este método trata se de escolher a melhor e a mais importante dentre as alternativas bem como a pior e menos importante dentre as alternativas [33].

Primeiramente uma série de alternativas são identificadas pelo tomador de decisão, posteriormente uma série de comparações em pares são realizadas entre cada um dos dois critérios sendo melhor ou pior ou outro critério. Em seguida um problema de maximização e minimização é realizado e resolvido determinando os pesos dos diferentes critérios [33].

Ao final, cada alternativa possuirá uma pontuação agregando os diferentes pesos, e a melhor e pior alternativa é selecionada [33].

As fases do BWM podem ser sintetizadas da seguinte forma:

1. Determinar um conjunto de critérios para se tomar uma decisão. Nesta etapa, consideramos os critérios que devem ser usados para se chegar a uma decisão;
2. Determinar o melhor e o pior critério;
3. Determinar o melhor e o pior critério;
4. Determinar a preferência de todos os critérios em relação ao pior. Utilizando uma escala de 1 a 9;
5. Encontrar os pesos ideais.

2.3.6 *CHOQUET INTEGRAL*

O uso do Choquet Integrais tem como função realizar uma agregação dos critérios. Em Seguida ele realiza uma combinação dos escores de acordo com o uso de uma abordagem fuzzy. Este MCDM é indicado para problemas de natureza quantitativa [34].

O que diferencia o uso da Choquet Integral em relação aos outros métodos multicritérios é a sua abordagem. Enquanto vários outros métodos multicritérios não consideram a relação entre dependência dos

parâmetros passados para o método, o Choquet Integral utiliza de um parâmetro chamado "Índice de Interação" que indica a dependência entre os diversos fatores a serem avaliados [35].

2.3.7 MACBETH - *Measuring Attractiveness by a Categorical Based Evaluation Technique*

O MACBETH é um método multicritério que permite avaliar diversas alternativas diante de vários critérios. Ele possui como destaque diante dos outros métodos, a possibilidade de realizar a avaliação através do uso de julgamentos qualitativos [36].

Assim como em outros métodos, o MACBETH conta com a participação dos decisores, mas ao contrário dos anteriores, este possui um processo de construção dos descritores qualitativos, que estão associados a uma escala cardinal (quantitativa), referindo -se aos valores a serem utilizados durante a aplicação do método. [37].

Este MCDM foi desenvolvido com o objetivo de construir uma função de valor intracritério. Desta forma ele atende o julgamento dos decisores, que por sua vez, atribuem os pesos aos critérios a serem analisados. Esses pesos são atribuidos de acordo com as opiniões dos decisores [36].

O método utiliza do método de programação linar para sugerir a escala de notas, e os intervalos em que elas podem variar apontando os pontos de maximização, minimização e desempenho de uma alternativa [37].

2.3.8 MCDA-C - *METHODOLOGY MULTICRITERIA DECISION AID – CONSTRUCTIVIST*

Diferentemente dos métodos multicritério tradicionais que possuem foco nos cálculos e são oriundos da escola americana, método multicritério de Apoio a Decisão construtivista é um método oriundo da escola européia que possui foco voltado para a criação do conhecimento e compreensão do problema [38].

Esta metodologia tem como premissa a aplicação deste método em problemas de alta complexidade e a busca por uma melhor solução que se enquadre nas necessidades do decisor [39].

Partindo desse ponto as principais características dessa metodologia são:

- Aceitação da subjetividade e reconhecimento dos limites da objetividade;
- Implementação de um modelo construtivista que visa a evolução do processo decisório;
- A não divisão de elementos subjetivos dos objetivos;
- Melhoria do processo de tomada decisão, onde este modelo faz frente a outras metodologias;
- Apoio em todas as etapas da metodologia onde o processo decisório se encontra em todas as fases do método [38], [36] , [40] e [41].

[38] e [41] descrevem o processo de tomada de decisão como uma atividade que tem como objetivo atender os questionamentos das partes interessadas envolvidas no processo. Assim, o MCDA-C consegue

auxiliar e facilitar o processo de tomada de decisão não a encontrar uma solução ótima, mas melhorar o entendimento do problema respondendo aos questionamentos dos envolvidos. Desta forma que o MCDA-C, lida com esses problemas e situações de alta complexidade [39].

[42] aponta que o processo decisório é um problema que se apresenta de uma forma não estruturada. Portanto, quando se utiliza um método focado em entender o problema como faz o MCDA-C, este vai se estruturando e tornando gerenciável [39].

Por se derivar de uma escola europeia focada na construção do conhecimento, o objetivo do MCDA-C e não apresentar uma lista de prioridades assim como o AHP, por exemplo. O modelo construtivista auxilia no processo decisório contribuindo para a construção do conhecimento em cenários complexos baseados nos sistemas de valor que se apresentam no processo decisório [43].

Assim o MCDA-C também contribui para deixar mais claro o entendimento do problema e o processo de tomada de decisão por parte dos atores. O MCDA-C contribui para a esta evolução através da presença dos objetivos e ponto de vistas, assim incluindo também o papel de um facilitador além do decisor no processo [39].

É importante citar que o MCDA-C não procura substituir qualquer tipo de processo de tomada de decisão, mas fomenta o entendimento do problema, deixando a tomada de decisão somente para o gestor. Um processo decisório possui um alto nível de subjetividade por envolver diversos pontos de vistas, e portanto necessita da utilização decisores, que tem como papel avaliar e escolher alternativas e critérios. O MCDA-C colabora diretamente para a construção e elaboração de critérios e modelagem das preferencias apresentando um resultado para que o decisor tome a decisão final [39].

Segundo [43] a aplicação do MCDA-C é dividida em três grupos principais sendo eles a fase da Estruturação, Avaliação e Recomendação.A fase da Estruturação é onde o decisor considera suas maiores preocupações onde são identificadas, organizadas e mensuradas.

A segunda fase, é onde são elaborados as escalas e os pesos taxas de substituição que atribuem valor de acordo com as preferencias do decisor.

A última etapa se denomina como Fase de Elaboração de Recomendações que procura realizar o entendimento das consequências das decisões a serem tomadas. A Figura 2.14 demonstra como estão estruturadas essas 3 fases:

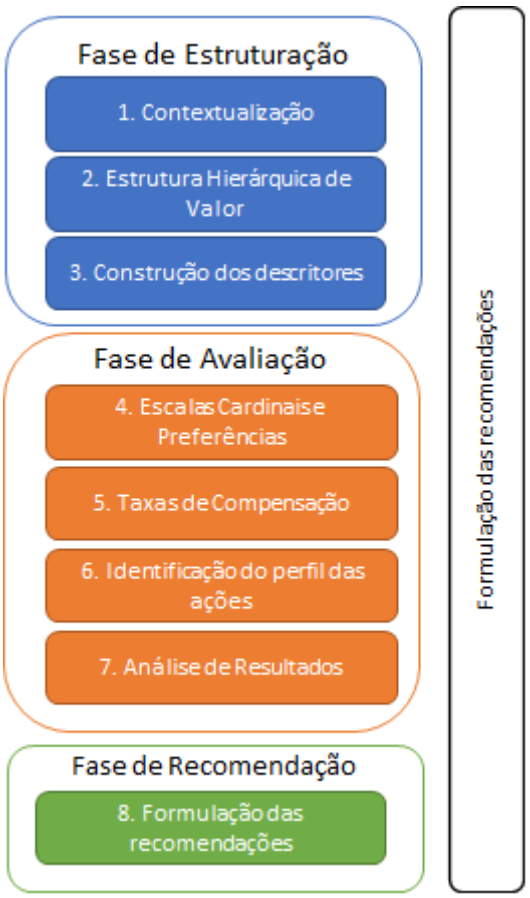

Figura 2.14: Fases do MCDA-C. Retirado e adaptado de [8]

Os valores e indicadores obtidos pelo MCDA-C são realizados através de escalas e teorias de medições e propriedades de operacionalizações sendo construídas a partir dos seguintes passos [44], [45],[46].

1. Entender a contextualização do problema e definir o rótulo da pesquisa [8];
2. Determinar uma estrutura hierárquica de valores de acordo com as preocupações do decisor [47],[48]. Nesta fase se faz a divisão e construção dos FPV's *Fundamental Point View* - Pontos de Vista Fundamentais , e EPV. *Elementar Point View* (Pontos de Vista Elementares), nomenclaturas que fazem parte dos termos utilizados pelo MCDA-C para definir o primeiro e segundo níveis da estrutura, respectivamente;
3. Criar e desenvolver os descritores, ou seja, realizar a escala ordinal [44]. Identificar as referências de forma que o decisor aponte as referências de inferioridade e excelência, [44];
4. Realizar a construção de uma escala cardinal através dos dados incorporados de acordo com os níveis declarados pelo decisor [49];
5. Determinar o peso dos critérios de acordo com o ponto de vista do decisor [8];
6. Realizar a coleta das medianas de acordo com o ponto de vista dos *stakeholders*, na qual, medianas com o valores acima de 0,5 tem seu valor arredondado para cima [8];

7. Analisar os resultados obtidos [8];

8. Realizar a formulação de recomendações [8].

Ao abordar todas as fases do MCDA-C é possível averiguar que este está alinhado com o processo e princípios de gerenciamento e avaliação de risco [17].

2.3.9 MÉTODOS HÍBRIDOS

Os gestores também podem utilizar da combinação de dois ou mais MCDM para retirar o que tem de vantagem de cada método, utilizando assim uma abordagem híbrida para obter mais precisão nos resultados [50].

Desta forma, autores têm adotado esse tipo de abordagem, onde eles retiram cada parte vantajosa de um método agregam com outros métodos, ou somente a parte deste outro método. Desta forma criando uma metodologia única de caráter híbrido totalmente diferente das abordagens comuns e com resultados interessantes [51].

2.3.10 APLICAÇÃO DOS MÉTODOS MULTICRITÉRIO NO CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

Nesta seção será demonstrada uma revisão bibliométrica a respeito da aplicação dos métodos multicritério no contexto da segurança da informação. Foram analisados 31 artigos em um período de cinco meses, abrangendo os meses de abril a agosto de 2020.

A Figura 2.15 exibe a distribuição de artigos publicados no contexto da segurança da informação que utilizaram métodos multicritérios ao longo dos anos mostrando uma série temporal de janeiro de 2008 a maio de 2020 com um aumento ao longo dos anos [15].

Esse aumento pode ser percebido através dos dois últimos anos da análise que consta um aumento quando comparado aos primeiros anos. De 2008 a 2016 é possível verificar que houve uma estabilidade de publicações, variando de 0 a 3 artigos por ano. No ano de 2017 houve um incremento bastante significativo enquanto 2018 volta ao padrão dos anos iniciais. Já de 2019 até abril de 2020 foram publicados 8 e 6 artigos demonstrando uma tendencia de aumento novamente [15].

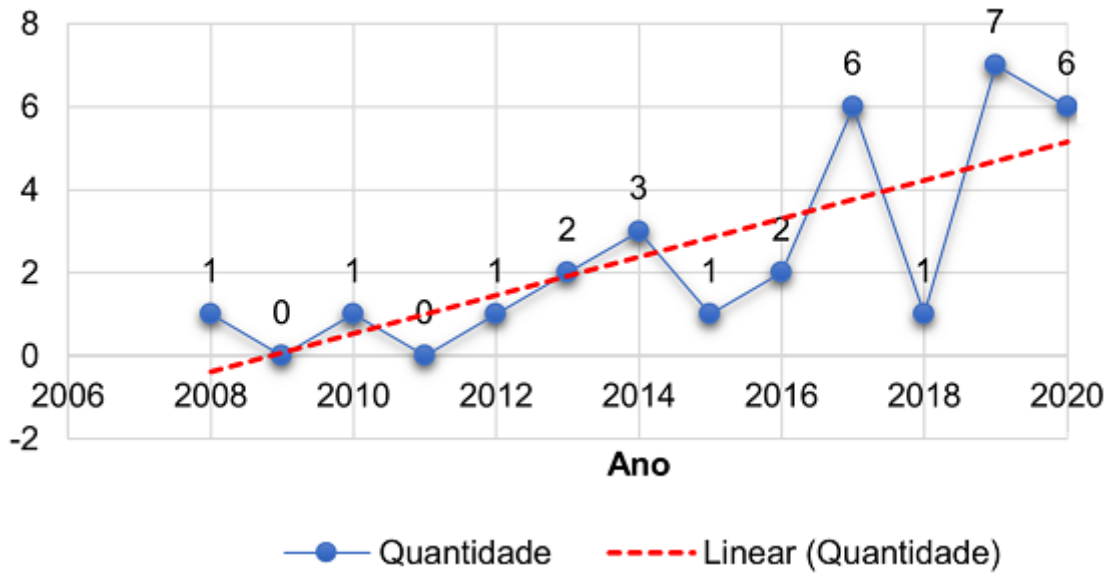

Figura 2.15: O uso das metodologias multicritério no âmbito da segurança da informação por ano [15]

A Tabela 2.3 realiza uma condensação dos artigos coletados por país e continente. Ela exibe uma ampla vantagem do continente asiático com a maioria das publicações, sendo a Índia o maior protagonista. Em segundo lugar aparece a América do Norte como continente que mais colabora com essas publicações. A Ásia representa 81% dos trabalhos publicados enquanto o americano e europeu obtiveram 13% e 2% respectivamente. Os continentes África e Oceania não obtiveram publicações [15].

Detalhando melhor esses fatos, é possível ver que a Índia possui cerca de 25% das publicações, já a Coreia do Sul constitui 16% enquanto a China 13%. A composição dos valores desses três países constitui mais de 50% dos trabalhos publicados [15].

Ao analisar a América, especificamente América do sul, é possível ver que a Colômbia foi o único a apresentar um trabalho voltado para a segurança da informação. Esses dados demonstram um desequilíbrio nesse ramo de pesquisa entre os países e continentes, principalmente quando se comparado a América do Sul que possui países importantes como o Brasil [15].

Tabela 2.3: Total de artigos por continente e país

Continente	Total por continente	País	Total por País
Ásia	25	Índia	8
		Coreia do Sul	5
		China	4
		Paquistão	3
		Outros	5
América	4	Estados Unidos	2
		Canadá	1
		Colômbia	1
Europa	2	França	1
		Lituânia	1

A Figura 2.16 ilustra a aplicação dos métodos multicritérios em diversas áreas da atividade de tec-

nologia da informação que necessita de segurança da informação. O destaque entre os temas de *Cloud Computing*, Infraestrutura, Segurança de *software* e Riscos Organizacionais [15].

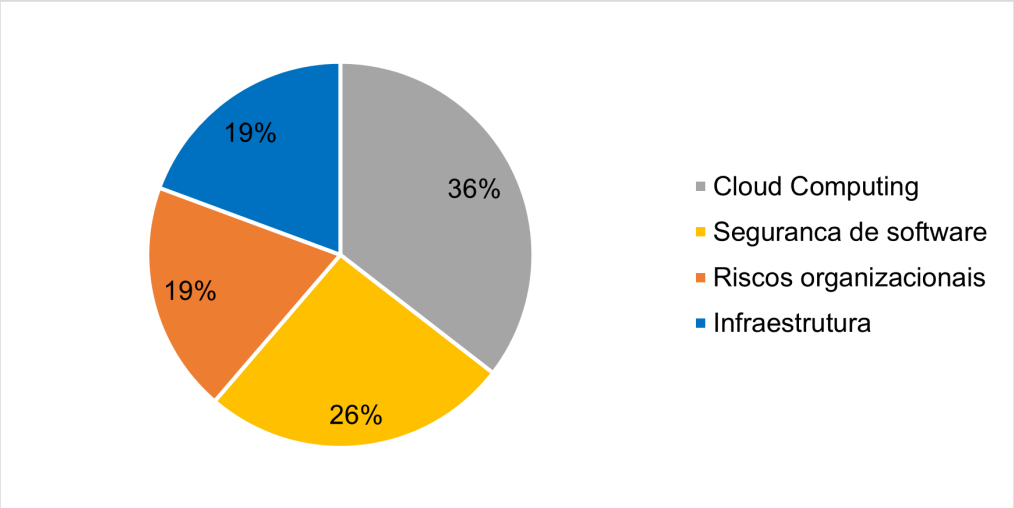

Figura 2.16: Aplicabilidade dos métodos multicritério por tema. Retirado de [15]

No que tange o crescimento das aplicações dos métodos multicritérios ao longo dos anos e área de aplicação, é possível ver um aumento do uso MCDM em *Cloud Computing* e Segurança de *software* principalmente de 2017 até 2020. Já nos primeiros anos é possível ver um destaque para riscos organizacionais. Já a infraestrutura se mostra bem distribuído ao longo dos anos.O crescimento da Segurança de *software* nos últimos anos demonstra que a segurança tem sido objeto de preocupação dos autores [15]. A Figura 2.17 ilustra esse cenário.

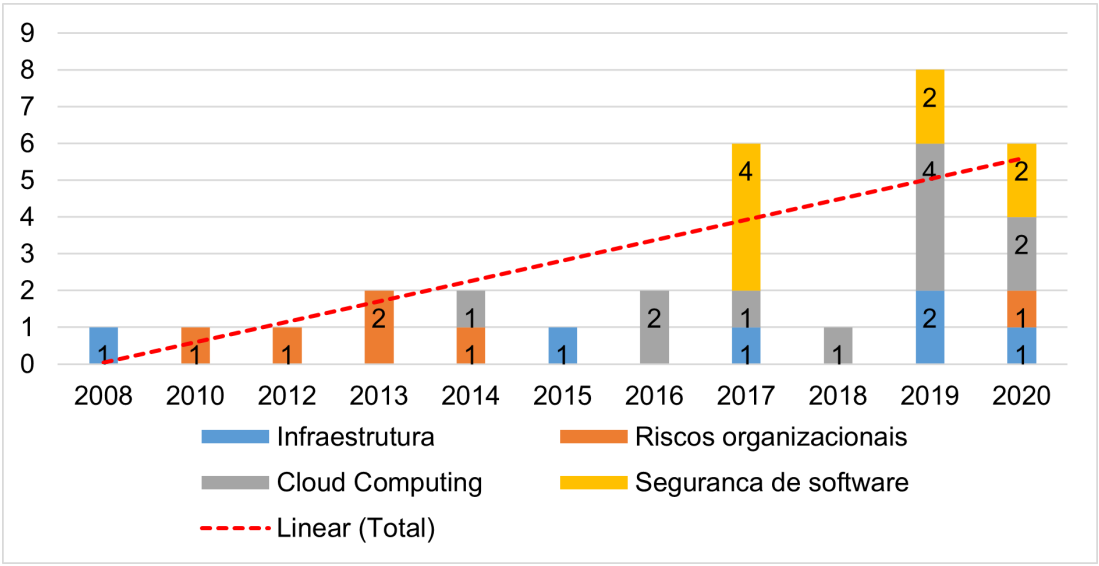

Figura 2.17: Aplicabilidade dos métodos multicritério por tema. Retirado de [15]

Sobre o tipo de aplicação dos métodos, a Figura 2.18 mostra uma série temporal da utilização dos métodos multicritérios envolvendo a aplicabilidade híbrida e não híbrida. A figura 2.18 ilustra um equilíbrio nas duas abordagens sendo que a híbrida se apresenta mais distribuída ao longo dos anos enquanto a não híbrida se destaca nos últimos. anos[15].

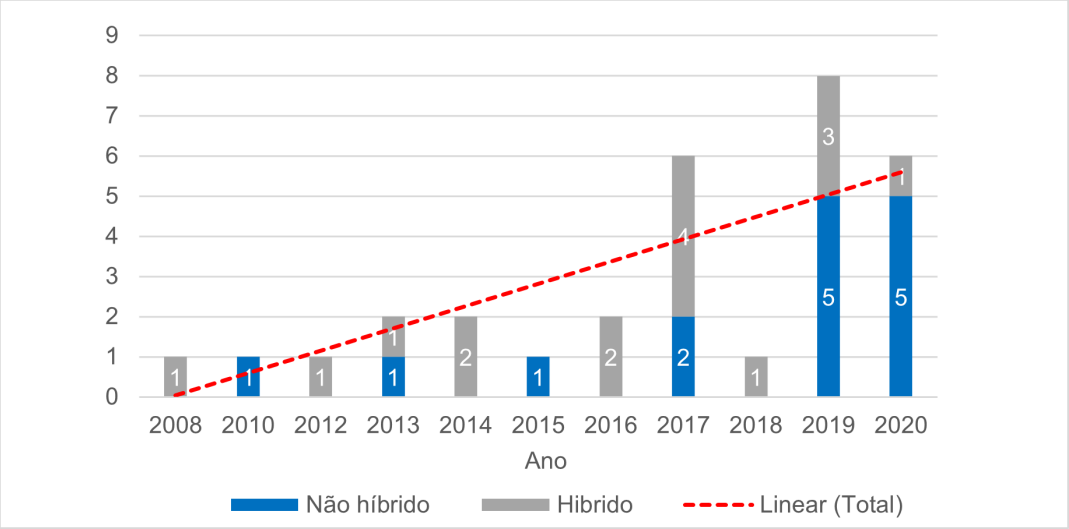

Figura 2.18: Tipo de aplicabilidade dos métodos multicritérios ao longo dos anos. Retirado de [15]

A Figura 2.19 exibe a distribuição e preferência das escolhas de métodos multicritérios ao longo dos anos. O que pode -se perceber é que uma ampla utilização de diversos métodos multicritérios como o ANP - *Analytic Network Process* - Processo de Rede Analítica, TOPSIS - *Technique for Order Preference by Similarity to Ideal Solution* - Técnica para Ordem de Preferência por Similaridade como a solução Ideal e Integrais Choquet. O AHP aparece com um leve destaque em relação ao TOPSIS [15].

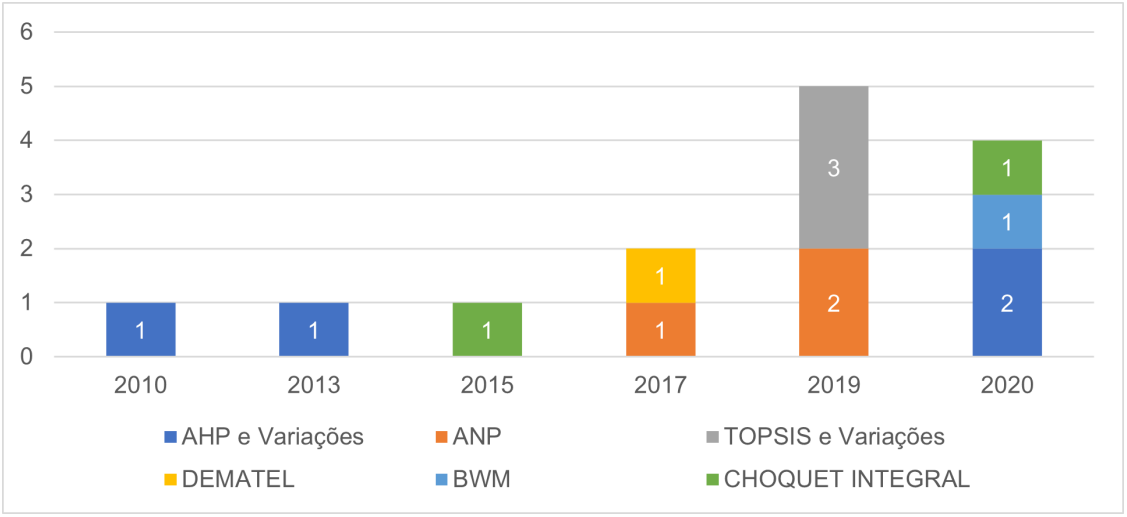

Figura 2.19: Aplicabilidade dos métodos multicritério por tema ao longo dos anos. Retirado de [15]

A Figura 2.20 demonstra um detalhamento na preferência das escolhas dos métodos multicritério pelos autores. É possível demonstrar qual tem sido o método preferido para a realização das pesquisas. É possível ver uma tendencia de escolha para métodos como AHP, TOPSIS, ANP e DEMATEL [15].

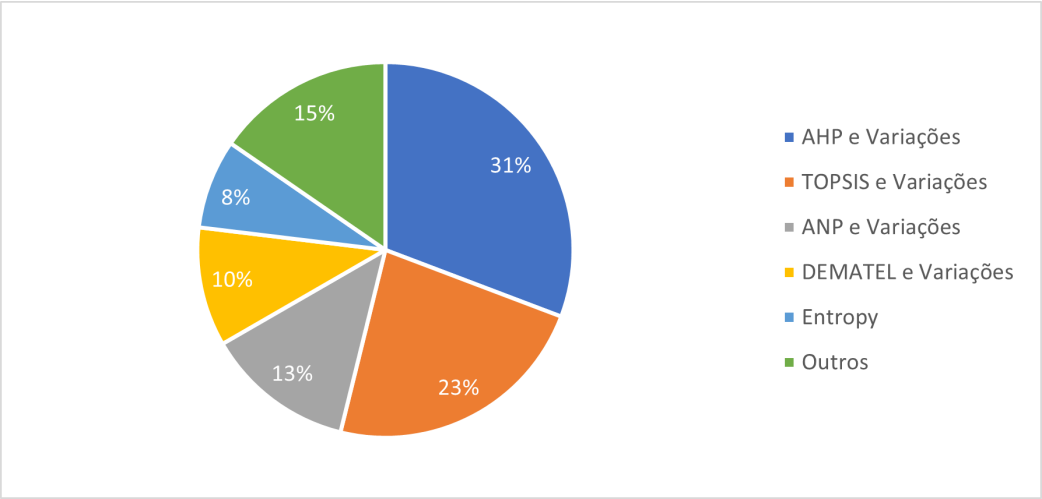

Figura 2.20: Preferência na escolhas de Métodos multicritério para aplicação híbrida. Retirado de [15]

É possível ver que o método AHP e suas variações possuem um destaque em relação aos outros métodos com doze escolhas enquanto o TOPSIS e suas variações ontem nove escolhas. Esses métodos juntos correspondem a mais de 50% das escolhas pela preferência dos autores ao aplicar uma metodologia híbrida [15].

Ao analisar detalhadamente o motivo da preferência pelo método multicritério AHP em uma metodologia híbrida, é possível ver claramente que o uso de comparações pareadas permitindo um cálculo consistência dos critérios de menos de 10% traz mais segurança para os autores [15].

Esse índice de consistência é extremamente importante, pois, caso a avaliação dos critérios por parte dos especialistas obtenham mais de 10% estes são rejeitados, necessitando fazer uma nova reavaliação. Assim os autores têm procurado esse método AHP para obter os pesos dos critérios com confiabilidade e em seguida utilizam esses pesos em outros métodos para obter seus resultados.

A Figura2.21 procura ilustrar a preferência dos métodos multicritério por área de aplicabilidade. É possível ver que o método AHP com suas variações e o TOPSIS possuem um destaque maior quando o tema se refere a *Cloud Computing*. Já em relação aos outros métodos existe uma equivalência nessa distribuição [15].

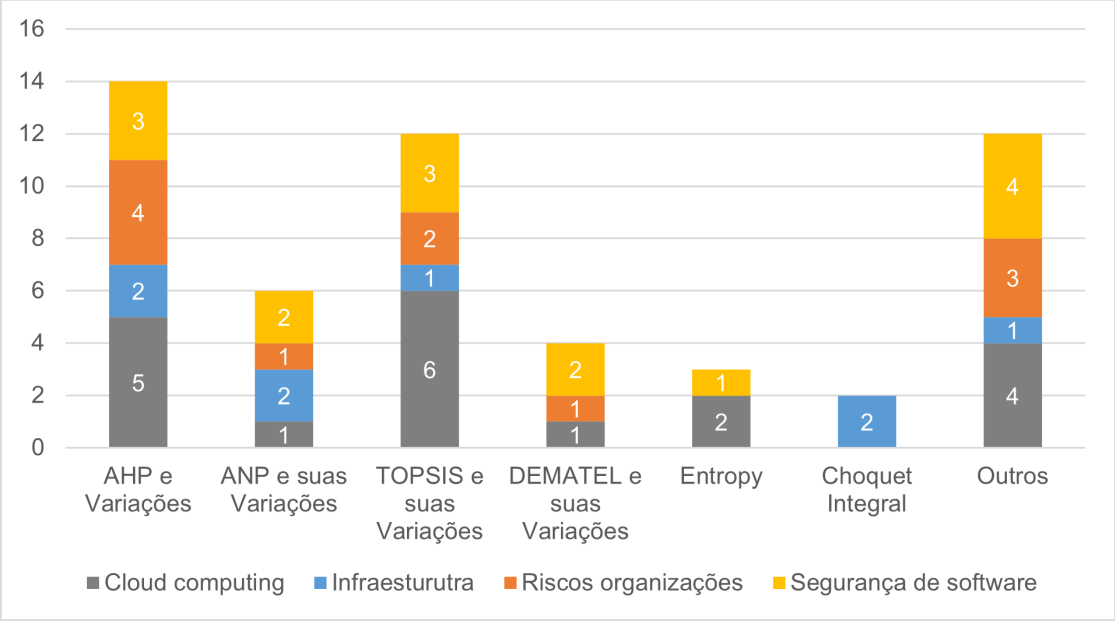

Figura 2.21: Preferência Métodos multicritério para aplicação por tema. Retirado de [15]

Os métodos multicritério foram utilizados neste trabalho como uma forma de priorizar os controles de segurança. Como citado pela ISO/IEC 31010:2018 estes métodos podem ser utilizados no processo de gestão de riscos, abordando os oito princípios do processo [12].

O que os dados mostram é uma utilização em massa de métodos multicritérios derivados da escola americana que possuem mais foco voltados para a precisão dos cálculos. Esses dados mostram uma adesão em massa dos métodos multicritério no oriente. O MCDA-C não foi citado nos artigos coletados o que mostra uma lacuna no estado da arte a ser preenchido.

Partindo desses fatos, e da necessidade de um método que realize a gestão de riscos da segurança da informação que contemple os diversos pontos de vistas de uma empresa em diversos níveis organizacional, o MCDA-C foi escolhido como objeto de estudo.

2.4 MYMCDA-C

MyMCDA-C é um *software* desenvolvido na UnB – Universidade de Brasília com o fomento da FAP-DF (Fundação de Apoio a Pesquisa do Distrito Federal) e PIBIT (Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico) que implementa o método multicritério MCDA-C.

Este *software* auxilia gestores que usam esse método para a tomada de decisão. O MyMCDA-C tem como características ser um *software* livre e que permite a geração de gráficos e tabelas para auxiliar o processo de decisão levando em conta os requisitos da análise multicritério construtivista [8][52].

Diversas pesquisas têm sido realizadas através da utilização deste *software* e em diversos setores. Na literatura, é possível encontrar trabalhos nos quais o *software* foi utilizado:

- Segurança da informação [8];

- Logística Reversa [53],[54];
- Contabilidade Pública Gerencial [55];
- Análise de usabilidade de websites [56], [57];
- Análise da influência do Instagram sobre os consumidores. [52]

Esta ferramenta realiza a transformação de uma análise subjetiva qualitativa em quantitativa adotando modelos matemáticos inspirados no já consolidado e conhecido método MACBETH [58].

O MyMCDA-C consegue obter os pontos de maximização e minimização para cada critério de acordo com o peso aplicado a eles[40]. Em seguida ele realiza a compilação dos cálculos transformando em valores quantitativos. Também, o software e exibe os resultados em forma de gráficos, mostrando os pontos de melhorias e de consolidação. Os modelos matemáticos adotados pelo MyMCDA-C procuram realizar uma associação das percepções dos decisores sob a ótica das partes interessadas nos critérios. De acordo com o método MACBETH os valores qualitativos "Neutro" e "Bom" correspondem a 0 e 100 respectivamente em forma quantitativa.

Para obter os pontos de minimização é utilizado a fórmula [8]:

$$\sum_{i=1}^{n} NV = 0 - \frac{WN(N-1)}{PS} \tag{1}$$

Para obter os valores acima do nível considerado "Bom" [8]:

$$\sum_{i=1}^{n} PV = 100 + \frac{WN(N-1)}{PS} \tag{2}$$

Para obter o ponto de maximização[8]:

$$\sum_{i=1}^{n} PV = 100 + WN(N-(PS-1)) \tag{3}$$

Onde [8]:

- NV - Valor negativo de uma ação na escala dos descritores de um critério;
- PV - Valor positivo de uma ação na escala de descritores de um critério;
- WN - Número de peso;
- N - Número de critérios do projeto;
- PS - Posição da ação na escala de descritores. A ordem de esforço.

Para valores intermediários as fórmulas apresentadas acima e que não correspondem aos níveis "Neutro" e "Bom" é adotado uma programação linear de acordo com a função [59]:

$$f(x) = \alpha x + \beta \tag{4}$$

Já para obter os valores globais, ou seja, os valores dos critérios é utilizado a fórmula [8]:

$$GV(a) = \sum_{i=1}^{n} RR_i \times PV_i(a) \tag{5}$$

Onde [8]:

- GV - Valor Global do desempenho potencial 'a';
- RR - Taxa de substituição correspondente ao critério;
- V(a) - Valor Parcial de uma ação potencial 'a' no critério.

2.5 TRABALHOS RELACIONADOS

Nesta pesquisa diversos trabalhos correlacionados foram encontrados, conforme visto na subseção 2.3.10 - Aplicação dos Métodos Multicritério no Contexto da Segurança da Informação. Entretanto, alguns trabalhos obtiveram um destaque maior e serão discutidos e comparados com o trabalho proposto nessa seção.

O primeiro trabalho relacionado desenvolveu uma estrutura de mitigação de segurança cibernética através de um paradigma empírico chamado CyFEr. Este paradigma empírico utiliza um método multicritério para realizar a análise de decisão, exigindo que as entradas sejam diversos critérios ponderados. A utilização de um método multicritério neste contexto se justifica devido ao fato de que a decisão de pesos e a subjetividade levam a tomada de decisões erradas, e a utilização deste método mitiga esse problema. O trabalho utilizou uma estrutura chamada BC2F como base, que foi criada e baseada no NIST [60].

Embora o trabalho de [60] tenha utilizado um MCDA, O trabalho proposto difere totalmente na questão do método. O MCDA-C baseia -se na compreensão do problema, na qual, decisores e agidos participam do método. O trabalho de [60] utiliza o BC2F como controles de segurança, já o presente trabalho utilizou o CSF NIST.

O segundo trabalho utilizou dos métodos multicritério para priorizar táticas de segurança com o objetivo de mitigar as vulnerabilidades e ataque. Eles utilizaram uma metodologia híbrida Fuzzy AHP-TOPSIS para realizar este trabalho. Esta metodologia foi aplicada em um *software* web que processa dados em tempo real na Índia. O método indicou que testes de acesso especializados são as primeiras táticas que devem ser adotadas devido ao fato de a indústria de *software* ter desenvolvido sistemas com vulnerabilidades. O estudo conclui que o método ajuda a indicar para arquitetos e desenvolvedores quais seriam os melhores pontos que devem ser priorizados em seus sistemas [61].

O trabalho de [61] utiliza uma metodologia híbrida utilizando uma lógica Fuzzy junto ao AHP para definir o peso dos critérios, por fim utilizou o TOPSIS para obter a ordem de prefência, desta forma focando

na precisão dos cálculos. Já o método multicritério utilizado no presente trabalho, foi o MCDA-C que não gera uma ordem de preferência, mas sim fornece conhecimento para a tomada de decisão para os gestores.

O terceiro trabalho procurou realizar uma investigação sobre as vulnerabilidades, riscos e ameaças considerando a implementação, orçamento da organização. Os autores utilizaram o método multicritério AHP para priorizar controles de segurança cibernética que possam colaborar para o cumprimento dos objetivos da organização, nesse sentido foram utilizados padrões de segurança da 27001:2013 como base para o trabalho [51].

O trabalho de [51] assim como o de [61] procurou utilizar o AHP. Isso significa que houve uma preocupação por parte dos pesquisadores em focar na precisão dos cálculos e estabelecer uma lista de prioridades.

Quarto em destaque utiliza os métodos multicritério para realizar uma gestão de riscos cibernéticos. O autor realizou essa análise através da quantificação de ameaça, vulnerabilidade e consequência sob a ótica de um conjunto de critérios a serem avaliados. O trabalho permite que o analista assegure um processo de forma estruturada e transparente, selecionando alternativas para o seu gerenciamento de risco. O trabalho fez um estudo de caso hipotético onde ele exemplifica e avalia a classificação de cinco estratégias de melhoria de cibersegurança. A abordagem fornece ações de gestão de riscos consistentes auxiliando os tomadores de decisão [62].

O trabalho de [62] utiliza o MCDA como referência para realizar uma gestão de riscos cibernéticos assim como o presente trabalho. Entretanto, o presente trabalho utilizou o CSF NIST como controles a serem utilizados para mitigar os riscos. [62] preferiu utilizar a quantificação de ameaça, vulnerabilidade e consequência para priorizar os riscos.

O quinto trabalho utilizou o método multicritério BWM para a priorização de vulnerabilidades de softwares [63]. Os autores neste trabalho inovaram fazendo uma pequena alteração no BWM, levando em conta os ponto de vistas dos gestores, desenvolvedores quanto das partes interessadas no que tange a gravidade das vulnerabilidades. Desta forma os autores conseguiram reduzir o risco dos ativos corporativos.

Embora o trabalho de [63] utilize do BWM que possuí uma visão semelhante ao AHP, utilizando de escalas para escolha de preferências, os autores inovaram conseguindo aplicar este método de uma forma semlhante ao trabalho proposto ouvindo os diversos pontos de vista.

[64] utiliza de uma abordagem MCDM híbrida para definir quais são os requisitos críticos a serem considerados para as medidas de segurança nos serviços de Internet das Coisas. Os autores utilizaram do fuzzy DEMATEL e o fuzzy ANP para refletir as dependências e inter-relações entre os critérios de segurança, pesando -os e priorizando -os de acordo com o ponto de vista de 38 especialistas.

Tanto o DEMATEL quanto o ANP possuem uma abordagem diferentes do que o presente trabalho propõe. Enquanto o objetivo de [64] ao utilizar o DEMATEL foi estabelecer a relação da influência de um critério em relação ao outro, o presente trabalho usa o MCDA-C para indicar os pontos de melhoria do critério em relação a si mesmo.

O trabalho proposto contribui preenchendo lacunas existentes quando se trata da aplicação do método MCDA-C. Nenhum dos trabalhos citados anteriormente utiliza dessa abordagem construtivista, que possui foco na compreensão do problema, procurando entender os diversos pontos de vistas no que tange a segurança cibernética entre decisores e partes interessadas. Diversos trabalhos citados anteriormente utilizam

métodos multicritérios que possuem foco na precisão dos cálculos e priorização de alternativas. Sendo assim o trabalho traz essa inovação de avaliar a viabilidade do MCDA-C. Uma outra lacuna a ser preenchida é a utilização do NIST CSF como base alinhado a metodologia construtivista. A tabela 2.4 sintetiza a diferença dos trabalhos relacionados.

Tabela 2.4: Síntese dos trabalhos relacionados

Trabalho	**Critérios utilizados**	**Método Multicritério**	**Metodologia Híbrida**
Trabalho 1 - [60]	Controles do BC2F - Baseado CSF NIST	Não especificado	Não
Trabalho 2 - [61]	Táticas de segurança para mitigar vulnerabilidades em software	Fuzzy-AHP-TOPSIS	Sim
Trabalho 3 - [51]	Controles da ISO 27001:2013	AHP	Não
Trabalho 4 [62]	Ameaça, vulnerabilidades e consequências	Não especificado	Não
Trabalho 5 - [63]	Vulnerabilidade de Software	BWM	Não
Trabalho 6 - [64]	Requisitos de Segurança	Fuzzy Dematel - Fuzzy ANP	Sim
Trabalho Proposto	Controles de detecção do CSF NIST	MCDA-C	Não

Diversos trabalhos utilizando métodos multicritério foram coletados e estudados, o artigo “Uma Análise das Aplicabilidades de Métodos Multicritérios no Contexto da Segurança da Informação” apresenta uma revisão sistemática condensando como aplicação dos métodos multicritério tem sido utilizados no âmbito da segurança da informação [15].

3 METODOLOGIA

Para desenvolver trabalhos acadêmicos é necessário que se faça um planejamento abordando métodos e técnicas de pesquisa para que se obtenha dados concretos e resultados eficientes [65]. Portanto, os resultados e as conclusões do presente estudo são fortalecidos de acordo com os procedimentos e estratégias abordadas durante a aplicação do trabalho. Este capítulo elenca quais foram as etapas desenvolvidas durante a aplicação do trabalho: características e classificação da pesquisa, população e amostra, os procedimentos de análise e coleta de dados e o apoio da estrutura de Metodologia Multicritério de Apoio à Decisão - Construtivista (MCDA-C).

3.1 OBJETO DE PESQUISA

O objeto desta pesquisa consiste no gerenciamento de riscos cibernéticos utilizando uma metodologia multicritério que envolva os pontos de vistas de profissionais da tecnologia da informação de uma organização.

3.2 SUJEITOS DA PESQUISA

Os sujeitos da pesquisa são compostos pela descrição das características dos diversos perfis de cada um que está envolvido neste processo. No presente estudo os aspectos que compõe a pesquisa podem ser descritos da seguinte maneira:

- Decisores: são os que possuem conhecimento e estratégias de uma organização, contribuindo para o objeto da pesquisa porque vivenciam na prática os processos organizacionais.
- Agidos: são aqueles que participam da pesquisa, mas não possuem o poder de decisão.
- Pesquisador: assume o papel de facilitador, procura mediar e conduzir as etapas da pesquisa.

3.3 LÓCUS DA PESQUISA

A pesquisa está ancorada em um grande banco brasileiro. A área de tecnologia internacional desta instituição foi escolhida para analisar a viabilidade deste método, uma vez que esta área possui um escopo menor. Este setor movimenta aproximadamente US$ 150.000.000,00 por hora. A equipe total participante desta pesquisa foi 18 funcionários com perfis e cargos diferentes.

3.4 CLASSIFICAÇÃO DA PESQUISA

O trabalho propôs um modelo de avaliação, e implementação de controles de segurança cibernética do CSF NIST para esta instituição. Assim, a instituição teria uma lista de prioridades para a implementação destes controles, o que mostra que esta pesquisa é uma pesquisa aplicada.

Pesquisas aplicadas são incentivadas para auxiliar a resolver problemas concretos de forma imediata ou não. Dessa forma, tem como finalidade incentivar o uso de práticas e conhecimentos numa realidade circunstancial do que desenvolver teorias a nível universal [66] [67].

O objetivo da pesquisa é descritivo e exploratório. A primeira se justifica porque descreve a população de um determinado fenômeno. Já a segunda porque adentra em algo que não é conhecido [68].

O presente trabalho também se característica por ser desenvolvido em etapas, sendo a primeira realizada através de uma pesquisa documental bibliográfica para se entender o problema. A segunda etapa consiste em encontrar métodos para a coleta de dados, analisar os resultados e em seguida as conclusões dos estudos. Assim, a pesquisa pode ser caracterizada como uma pesquisa de campo [69].

A forma desta pesquisa é mista sendo qualitativa e quantitativa. Ela é quantitativa na fase de avaliação pois possui modelos matemáticos, métricas, fórmulas estatísticas. E qualitativa devido a fase de Estruturação devido a identificação de controles e valores de escalas.

Abordagem qualitativa está correlacionada em relação a capacidade humana de compreender e perceber determinados fenômenos e teorias. Nesta abordagem o próprio pesquisador possui um papel subjetivo, pois observa o ambiente realizando suas observações e de acordo com seu ponto de vista fazendo interpretações. Métodos mais comuns qualitativos são entrevistas, trabalho de campo, análise de material documental [70].

No que tange a abordagem quantitativa, esta considera tudo que é quantificável, e mensurável, podendo assim se traduzir em números. Muitas técnicas dessa abordagem utilizam estatística, porcentagem, tendencias e análise de variáveis de precisão [70].

A coleta de dados da pesquisa foi considerada mista sendo primária e secundaria. A primeira se justifica pela utilização de formulários e questionários aplicados juntos ao decisores e agidos do trabalho, a segunda se justifica pela utilização de um framework como base.

Fontes primárias são dados brutos que não possuem nenhum tipo de análise, julgamento ou interpretação por uma segunda parte. Estes são geralmente são obtidos principalmente através das aplicações de formulários de coleta de dados [71].

Já os dados de cunho secundário está correlacionada a acessos a livros, revistas, periódicos bem como revisões sistemáticas da literatura. O principal objetivo dessa linha de fontes secundárias é obter algo que já foi realizado, escrito ou digitalmente, para que possa conduzir o pesquisador em sua pesquisa[69].

No que diz respeito a temporalidade, a pesquisa está caracterizada como transversal. Isto porque ela retrata somente a dimensão do tempo de um determinado momento [71].

O estudo utilizou uma estrutura de controles retirados do NIST e durante a aplicação do MCDA-C ouviu especialistas, criou -se plano de riscos e com isso todos os princípios de gerenciamento de riscos foram abordados. As fases abordadas durante a aplicação do MCDA-C foram realizadas de acordo com a

figura 2.14 contida no Referencial teórico deste trabalho. Os resultados obtidos em cada uma destas fases estão contidos na seção de Resultados e Discussões desse presente trabalho.

A metodologia do presente estudo fica sob avaliar se a aplicação do método MCDA-C é viável cumpre os princípios de gestão de risco. Assim essa pesquisa foi estruturada em etapas de revisão da literatura ou análise documental conforme levantados na seção do referencial teórico. O método escolhido para a aplicação da pesquisa foi o MCDA-C, cuja escolha se justificou porque não foi citado na revisão sistemática. O Framework NIST CSF foi escolhido como base para este estudo pois mostrou em tendência de alta, mas com uma concentração somente na América do Norte.

4 RESULTADOS E DISCUSSÕES

Neste capítulo, serão abordados os resultados e discussões obtidos neste trabalho através da aplicação do MCDA-C com o framework da NIST CSF sob a ótica dos princípios da gestão de riscos [8].

Nesta seção serão descritos os resultados da aplicação do CSF NIST. Assim como o MCDA-C solicita, várias partes interessadas participaram do processo. Isto é extremamente importante para refletir suas percepções de acordo com a análise final do MCDA-C. O primeiro passo para aplicar essa metodologia é identificar os papéis que os atores terão na pesquisa [8] [38]. Os atores ficaram divididos da seguinte forma:

- Três tomadores de decisão: Desenvolvedor de *software*, gerente de equipe de TI, analista de infraestrutura de TI.
- Facilitadores: Pesquisadores.
- Quinze *stakeholders*: funcionários da área internacional de TI
- Destinatários: Clientes.

Os três tomadores de decisão foram escolhidos de acordo com sua experiencia, são funcionários de nível sênior. Estes foram responsáveis por realizar a modelagem e análise do problema de tomada de decisão

Os *stakeholders* que participaram do processo são os demais funcionários da gerência internacional de TI. Estes são funcionários que trabalham na área com diversos tipos de cargos e exercem papéis diferentes na gerência. A Figura 4.1 apresenta a distribuição dos *stakeholders* por cargo:

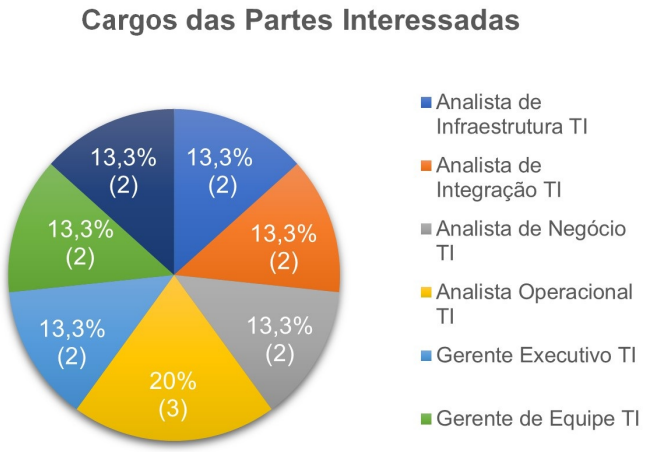

Figura 4.1: Cargos das partes interessadas. Retirado e adaptado de [8]

A partes interessadas possuem as seguintes responsabilidades:

- Analista de Infraestrutura de TI: responsável por manter a infraestrutura de TI da empresa no que tange a servidores *web*;
- Analista de Integração de TI: responsável por arquitetar toda a estrutura de comunicação entre os sistemas do banco;
- Analista de Negócio TI: possui a responsabilidade de replicar as regras de negócio nos sistemas bancários;
- Analista de Operacional TI: responsável por executar rotinas nos sistemas bem como auxiliar na resolução de incidentes de TI;
- Gerente de Equipe de TI: líder de uma equipe específica que possui diversos analistas;
- Gerente executivo de TI: possui o papel de gestor de toda uma gerência com diversas equipes.

A escolha por optar os tomadores de decisão e as partes interessadas com perfil e cargos diferentes foi intencional. O motivo é encontrar um ponto ótimo em comum entre eles na resolução do problema. Também é importante salientar que os tomadores de decisão não foram incluídos no grupo das partes interessadas para evitar que os mesmo que modelassem o problema enviesassem os dados coletados e calculados de acordo com o ponto de vista dos *stakeholders*. Neste processo de tomada de decisão existem dois grupos distintos que participaram em momentos distintos com objetivos e funções diferentes [8].

Os grupo de pesquisadores que são os facilitadores, não respondem a perguntas e também não modelam o processo. Eles têm como objetivo apenas conduzir o processo fase por fase, inserindo os dados no *software* e realizando as recomendações necessárias. E o grupo de clientes são os beneficiários finais da melhoria do processo de cibersegurança, portanto não participam do processo[8]. A Tabela 4.1 apresenta o envolvimento dos atores nas fases do MCDA-C.

Tabela 4.1: Fases do método MCDA-C e a participação dos atores

Fase	**Atores envolvidos**
1. Contextualização	Pesquisador e Decisores
2. Estrutura de valor hierárquico	Pesquisador e Decisores
3. Construção dos descritores	Pesquisador e Decisores
4. Escalas cardinais e preferências	Pesquisador e Decisores
5. Taxas de compensação	Pesquisador e Decisores
6. Identificação do perfil dos atores	Pesquisador e Stakeholders
7. Análise dos resultados	Pesquisador
8. Recomendações	Pesquisador

Após definir os atores e suas atribuições o método solicita que um rótulo da pesquisa seja criado. Os tomadores de decisão escolheram o seguinte rótulo: "O quanto dos controles da função de Detecção do NIST CSF poderia contribuir para a ciber-segurança do banco?"[8].

Em seguida o número do esforço para atingir o ponto de maximização foi definido. Esse peso é importante por refletir o nível de esforço do projeto. O *software* MyMCDA-C possui essa entrada como fundamental para efetuar os cálculos. Esses esforços podem ser traduzido como uma forma de realizar uma análise de qual critério deve concentrar mais esses recursos, impactando no esforço que controle de segurança deve fazer para atingir o seu ponto de maximização. Isso significa que, um peso maior, aumenta o rigor da avaliação, dificultando o encontro da performance com o ponto de maximização. O MyMCDA-C possui o nível 3 como padrão, valor da escolha feita pelos tomadores de decisão [8].

O passo seguinte foi definir uma estrutura hierárquica de valor com os controles a serem avaliados. Como o NIST CSF já possuí uma estrutura hierárquica com seus controles, esta foi aproveitada. Para esta fase foi escolhida a função "Detect" do *framework* [9]. A principal justificativa para utilizar essa função é o objetivo de melhorar as atividades de identificação de ocorrência em cibersegurança. Esta função possui 3 categorias e 18 categorias com os respectivos controles a serem avaliados [9].

Na fase de construção dos descritores, fase 3, houve a necessidade de estruturar os FPV's *Fundamental Point View* - Pontos de Vista Fundamentais , e EPV. *Elementar Point View* (Pontos de Vista Elementares) . Essas nomenclaturas fazem parte dos termos utilizados pelo MCDA-C que definem o primeiro e segundo níveis, respectivamente. Na Figura 4.2, dentro do diagrama cinza claro, há as FPV's que são as categorias do CSF NIST que contêm seus respectivos EPV's agrupados. Já os EPV's são de fato os controles de cibersegurança do NIST que tiveram sua avaliação, estes estão dentro do diagrama cinza escuro. É importante ver que neste momento é possível ver o MCDA-C abordando os princípios personalizados, estruturados, abrangentes e dinâmicos de gerenciamento de risco [8]. A Figura 4.2 ilustra a estrutura da função de detecção de acordo com [9]. Esta estrutura foi replicada no MyMCDA-C para que ele receba os dados obtidos nas próximas fases.

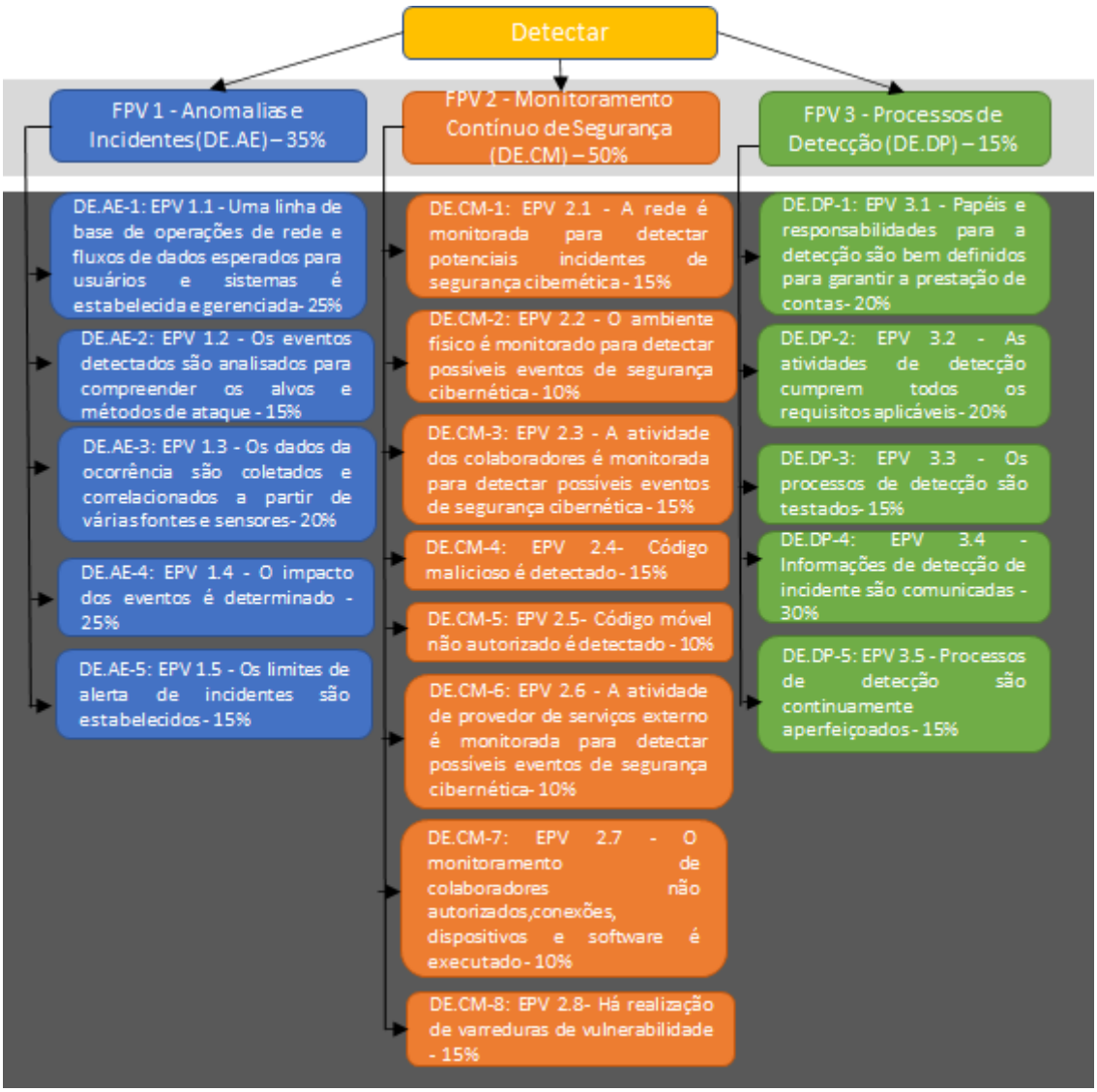

Figura 4.2: Estrutura hierárquica de valor da Função Detectar. Retirado e adaptado de [8]

Ainda na terceira fase do método, criou -se uma escala de preferência subjetiva para avaliação de acordo com os tomadores de decisão. Os decisores escolheram cinco níveis: "Neutro"como o pior nível, seguido por "Mínima colaboração", "Pouca colaboração", e "Boa colaboração"com "Excelente colaboração"como o melhor nível.

O motivo explicado para iniciar em “Neutro” de acordo com os tomadores de decisão é que a implementação de um controle não afetaria de forma negativa sendo o pior cenário não resultar em algum efeito. A tabela 4.2 mostra a escala de preferência para avaliação [8]. Desta forma N1 foi como "Neutro", e N4 "Boa colaboração"definido como bom. A Tabela 4.2 exibe essa escala.

Tabela 4.2: Escala de avaliação utilizada na pesquisa. Retirado de [8]

Nível	Descritor	Neutro	Bom
N1	Neutro	X	
N2	Mínima colaboração		
N3	Pouca colaboração		
N4	Boa colaboração		X
N5	Excelente colaboração		

O *software* MyMCDA-C realizou os cálculos converteu os valores qualitativos em valores quantitativos. Desta forma permitindo a criação de uma escala para determinar o nível de cada elemento.

A tabela 4.3 mostra um exemplo das escalas convertidas de ordinal para cardinal para o “EPV 2.5” É importante ressaltar que cada EPV e FPV possui sua respectiva escala calculada e arredondada pelo MyMCDA-C [8]. A Tabela 4.3 mostra esse cenário.

Tabela 4.3: Conversão da escala em qualitativa para quantitativa. Retirado de [8]

Nível	Descritor	Escala
N1	Neutro	0
N2	Mínima colaboração	33
N3	Pouca colaboração	67
N4	Boa colaboração	100
N5	Excelente colaboração	154

Primeiramente o método adota os valores para N1 "Neutro"como 0 e N4 "Bom"[59] [8]:

$$\begin{aligned} \mathrm{N1} &= 0 \\ \mathrm{N4} &= 100 \end{aligned}$$

Então um método de programação linear inspirado no MACBETH foi adotado baseado nos valores citados acima [8] [59].

$$\begin{aligned} \alpha \times 1 + \beta &= 0 \\ \alpha &= -\beta \end{aligned}$$

Encontrando alfa e beta substituindo do valor de N4’s na equação [8]:

$$\begin{aligned} \alpha \times 4 + \beta &= 100 \\ -4\beta + \beta &= 100 \\ \beta &= -33,33 \end{aligned}$$

Substituindo os valores obtidos anteriormente é possível obter os valores de N2 e N3 [8]:

$$
\begin{aligned}
\mathrm{N}\,(\mathrm{x}) =& \alpha x + \beta \\
\mathrm{N}\,(2) =& 33,33 \times 2 + (-33,33) \\
\mathrm{N}\,(2) =& 33,33 \\
\mathrm{N}(\mathrm{x}) =& \alpha x + \beta \\
\mathrm{N}\,(3) =& 33,33 \times 3 + (-33,33) \\
\mathrm{N}\,(3) =& 66,66
\end{aligned}
$$

Por fim, obtem se o ponto de maximização:

$$
\begin{aligned}
N5 =& PV + WN\,(N - (PS - 1)) \\
N5 =& 100 + 3\,(18 - (1 - 1)) \\
N5 =& 154
\end{aligned}
$$

Iniciou -se então a fase 4, a escolha e definição das taxas de compensação. Essas taxas foram escolhidas através de um ponto de vista em comum entre os tomadores de decisão. A Figura 4.2 demonstra as taxas de compensação para cada controle. Essas taxas são definidas de baixo pra cima da árvore começando dos níveis mais baixos EPV's até os FPV's. Em seguida essas taxas foram inseridas no MyMCDA-C[8].

Em seguida os tomadores de decisão determinaram a ordem de esforço dos controles. A tabela 4.4 demonstra como ficaram definidos esses controles. Importante ressaltar que esse esforço se não trata da implementação, mas sim de atingir um nível de maximização em relação a este controle. Esses valores foram inseridos no MyMCDA-C, assim o controle "EPV 2.5: Código móvel não autorizado é detectado"liderou como o controle com mais esforço de atingir o ponto de maximização, enquanto o controle "EPV 3.3: Os processos de detecção são testados"recebendo menos esforço[8]. A Tabela 4.4 mostra essa ordenação.

Tabela 4.4: Ordem de esforço. Retirado de [8]

Ordem	Controle
1	EPV 2.5: Código móvel não autorizado é detectado
2	EPV 2.4: Código malicioso é detectado
3	EPV 2.8: Realização de varreduras de vulnerabilidade
4	EPV 2.1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética
5	EPV 3.1: Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas
6	EPV2.3: A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética
7	EPV 2.6: A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética
8	EPV2.7:O monitoramento de colaboradores não autorizados,conexões, dispositivos e *software* é executado
9	EPV 2.2:O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética
10	EPV 1.2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque
11	EPV 1.1:Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada
12	EPV 1.3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores
13	EPV 1.4: O impacto dos eventos é determinado
14	EPV 1.5: Os limites de alerta de incidentes são estabelecidos
15	EPV 3.2: As atividades de detecção cumprem todos os requisitos aplicáveis
16	EPV 3.4: Informações de detecção de incidente são comunicadas
17	EPV 3.5: Processos de detecção são continuamente aperfeiçoados
18	EPV 3.3: Os processos de detecção são testados

Após todas as escala de avaliação, taxas de compensação e ordem de esforço definidos, iniciou -se a fase 6 do MCDA-C. Um questionário foi aplicado ao grupo das partes interessadas com o rótulo definido na pesquisa. As respostas para cada EPV e FPV foram coletadas, e a mediana para cada um foi calculada. [8].

Respostas do tipo "Eu não sei"foram descartadas não pontuando no cálculo da mediana. A Tabela 4.5 demostra como foi realizado este cálculo para o "EPV 2,5". O valor final da mediana foi arredondando porque o MyMCDA não funciona com casas decimais [8]. Como o valor final para este EPV foi 5, equivalente a N5 “Excelente Colaboração” , este equivale ao respectivo 154 valor cardinal contido na Tabela 4.2.

Tabela 4.5: Cálculo da mediana para o controle EPV 2.5: Código móvel não autorizado é detectado. Retirado de [8]

Stakeholder	**Descritor selecionado**	**Nível correspondente**
Stakeholder 1	Eu não sei	
Stakeholder 2	Eu não sei	
Stakeholder 3	Boa Colaboração	4
Stakeholder 4	Eu não sei	
Stakeholder 5	Boa Colaboração	4
Stakeholder 6	Eu não sei	
Stakeholder 7	Excelente Colaboração	5
Stakeholder 8	Excelente Colaboração	5
Stakeholder 9	Excelente Colaboração	5
Stakeholder 10	Excelente Colaboração	5
Stakeholder 11	Boa Colaboração	4
Stakeholder 12	Eu não sei	
Stakeholder 13	Boa Colaboração	4
Stakeholder 14	Boa Colaboração	4
Stakeholder 15	Excelente Colaboração	5
Mediana dos níveis		4,5

Embora a organização possua um organograma, todas as respostas possuem um mesmo peso e valor no cálculo da mediana. Isto significa que a avaliação de um gerente possui o mesmo peso de um analista. Neste ponto conseguimos ver mais três pilares da gestão de riscos sendo abordados: integrados, inclusivos, humanos e culturais [8].

Então foi realizado o cálculo da Mediana obtidas através do ponto de vista dos *stakeholders* das partes. A Tabela 4.6 ilustra esses valores. Importante ressaltar que cada linha corresponde a um controle com sua respectiva escala cardinal, nível e mediana obtida de acordo com os cálculos feitos pelo MyMCDA-C.

Veja que para cada controle que obteve uma classificação como Excelente possui uma escala divergente, isto varia de acordo com a modelagem do problema e devido a classificação de esforço citadas na Tabela 4.4. Ao analisar os valores para boa colaboração é possível ver que todos os valores estão atingindo o valor de 100, isto porque o método MACBETH usa esse valor como padrão. Em relaçao aos valores de "Pouca colaboração", estes foram obtidos através de programação linear conforme funcionamento do próprio MACBETH.

Tabela 4.6: Medianas obtidas através do ponto de vista dos *stakeholders*. Retirado de [8]

Controle	Nível	Descritor	Valor
EPV 2.5: Código móvel não autorizado é detectado	N5	Excelente colaboração	154
EPV 2.4: Código malicioso é detectado	N4	Boa colaboração	100
EPV 2.8: Realização de varreduras de vulnerabilidade	N5	Excelente colaboração	148
EPV 2.1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética	N5	Excelente colaboração	145
EPV 3.1: Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas	N4	Boa colaboração	100
EPV 2.3: A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética	N4	Boa colaboração	100
EPV 2.6:A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética	N4	Boa colaboração	100
EPV 2.7: O monitoramento de colaboradores não autorizados,conexões, dispositivos e *software* é executado	N4	Boa colaboração	100
EPV 2.2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética	N3	Pouca colaboração	67
EPV 1.2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	N5	Excelente colaboração	127
EPV 1.1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	N4	Boa colaboração	100
EPV 1.3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores	N5	Excelente colaboração	121
EPV 1.4: O impacto dos eventos é determinado	N5	Excelente colaboração	118
EPV 1.5: Os limites de alerta de incidentes são estabelecidos	N3	Pouca colaboração	67
EPV 3.2: As atividades de detecção cumprem todos os requisitos aplicáveis	N4	Boa colaboração	100
EPV 3.4: Informações de detecção de incidente são comunicadas	N5	Excelente colaboração	109
EPV 3.5: Processos de detecção são continuamente aperfeiçoados	N5	Excelente colaboração	106
EPV 3.3: Os processos de detecção são testados	N5	Excelente colaboração	103

Com os dados processados, os resultados foram gerados para auxiliar no processo de tomada de decisão e serão discutidos nos próximos parágrafos.

Primeiramente é possível observar que todos os pontos de minimização foram zero porque a escala começou no N1 Neutro, então não houve valores negativos. Também é possível ver diferentes pontos de maximização para cada controle. Nesse estágio é possível perceber um outro princípio do gerenciamento de risco sendo abordado: melhor informação disponível [8].

Ao analisar para a categoria “FPV Anomalias e Incidentes", é possível perceber que o "EPV 1.2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque"obteve um pequeno destaque em relação aos outros. Importante ver que este obteve uma compensação mais baixa. Este EPV atingiu o seu ponto de maximização mostrando que tende muito a contribuir.

Olhando para os pontos negativos o "EPV 1.5: Os limites de alerta de incidentes são estabelecidos” mostrou que poderia contribuir pouco, devido a sua performace ter ficado distante do ponto de maximi-

zação, com 48 degraus de diferença, fazendo com que os tomadores de decisão revisem sobre a implementação deste controle. Outros controles obtiveram um desempenho equivalente, mostrando que sua implementação pode ter um impacto significativo na ciber-segurança do banco [8]. A Figura 4.3 mostra esse cenário.

Figura 4.3: Resultados para a categoria FPV. Anomalias e Incidentes. Retirado de [8]

Na categoria "FPV 2 - Monitoramento Contínuo de Segurança (DE.CM)", é possível perceber que o "EPV 2.5: Código móvel não autorizado é detectado"conseguiu atingir seu ponto máximo de maximização. Isto significa que ele mostrando que ele tende a contribuir muito para a segurança do banco. Já outros controles também se destacaram desta forma, mas com um desempenho um pouco inferior [8].

Olhando para o ponto negativo o "EPV 2.2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética"ficou muito longe de seu ponto de maximização, com aproximadamente 63 degraus de diferença. Isto faz com que os tomadores de decisão tenham que revisar sobre a implementação deste controle e como poderiam fazer de forma que colaborasse mais para a instituição [8]. Esse resultado chama muito a atenção visto que a segurança física é extremamente importante para as instituições. A Figura 4.4 ilustra esse cenário.

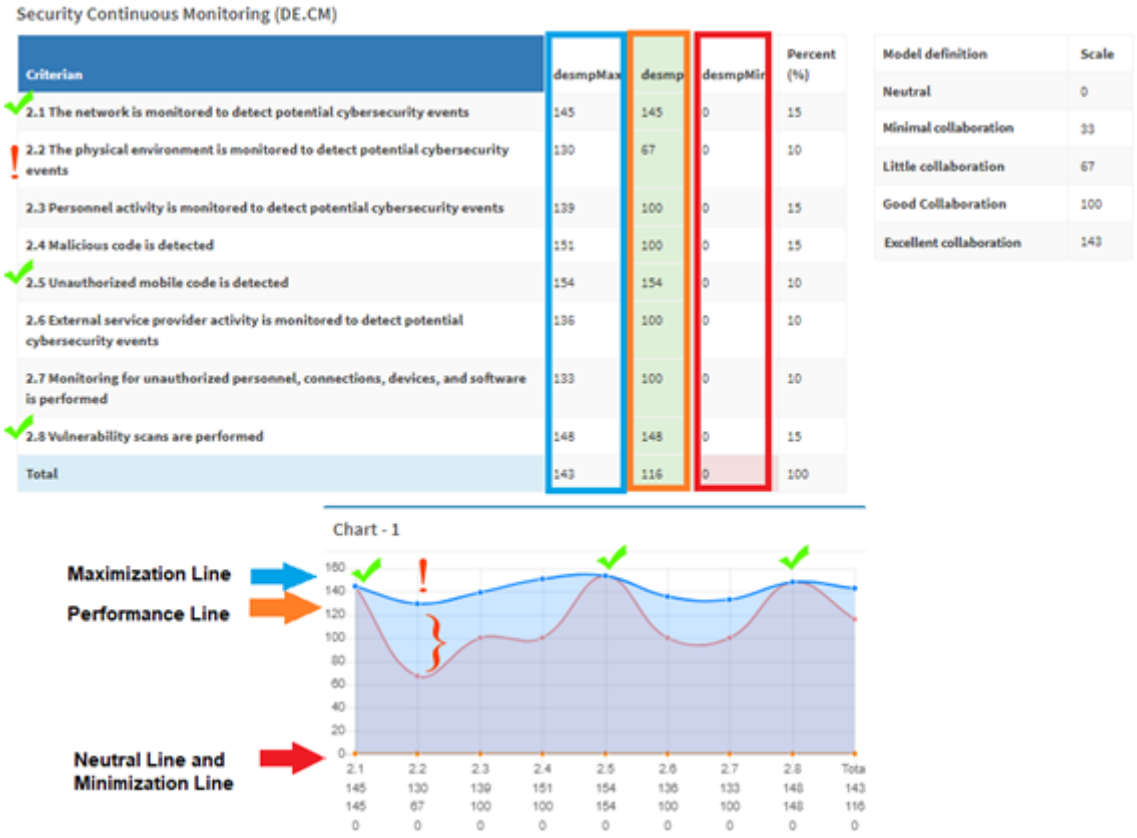

Figura 4.4: Resultados para a categoria FPV. Monitoramento Contínuo de Segurança. Retirado de [8]

Ao analisar a categoria "FPV 3 - Processos de Detecção (DE. DP)", é possível ver um cenário que mostra um destaque para o "EPV 3.4: Informações de detecção de incidente são comunicadas"que obteve seu ponto de maximização. Demonstrando que pode ser priorizado na sua implementação. Também é importante ressaltar que esse controle detém o maior peso em relação aos outros controles desta categoria[8].

Olhando o lado negativo o "EPV 3.1: Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas"ficou longe do seu ponto de maximização. Isso significa que este controle tem que melhorar mais para colaborar de acordo com o ponto de vista dos tomadores de decisão. Este controle ficou a 42 degraus do seu ponto de maximização. Portanto, este controle deve ser analisado com mais atenção pelos tomadores de decisão [8]. A Fig. 4.5 ilustra o cenário descrito.

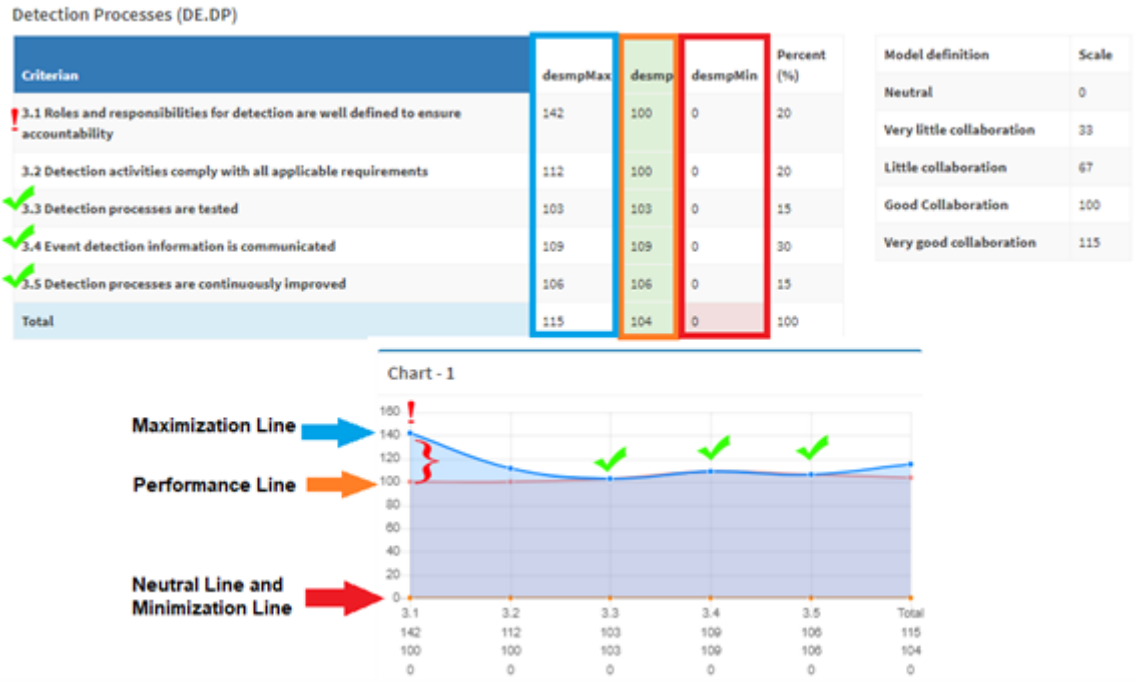

Figura 4.5: Resultados para a categoria FPV. Processos de Detecção. Retirado de [8]

Analisando de forma global a nível de FPV's ou seja, categorias, é possível ver que a categoria FPV 2 -Monitoramento Contínuo de Segurança (DE. CM)"obteve o mais alto desempenho. Curiosamente ela foi a que ficou mais longe do seu ponto de maximização com uma diferença de 27 degraus, demonstrando que os controles desta categoria tendem muito a colaborar para o banco mas que ainda poderiam colaborar mais. Isto significa que alguns controles nesta categoria devem ser revistos [8] .

Ao analisar a categoria "FPV 3 - Processos de Detecção (DE. DP)", é possível constatar que este controle foi o que mais se aproximou do seu ponto de maximização, mostrando que seus controles podem ser eficientes para a instituição [8]. A Figura 4.6 ilustra esse cenário.

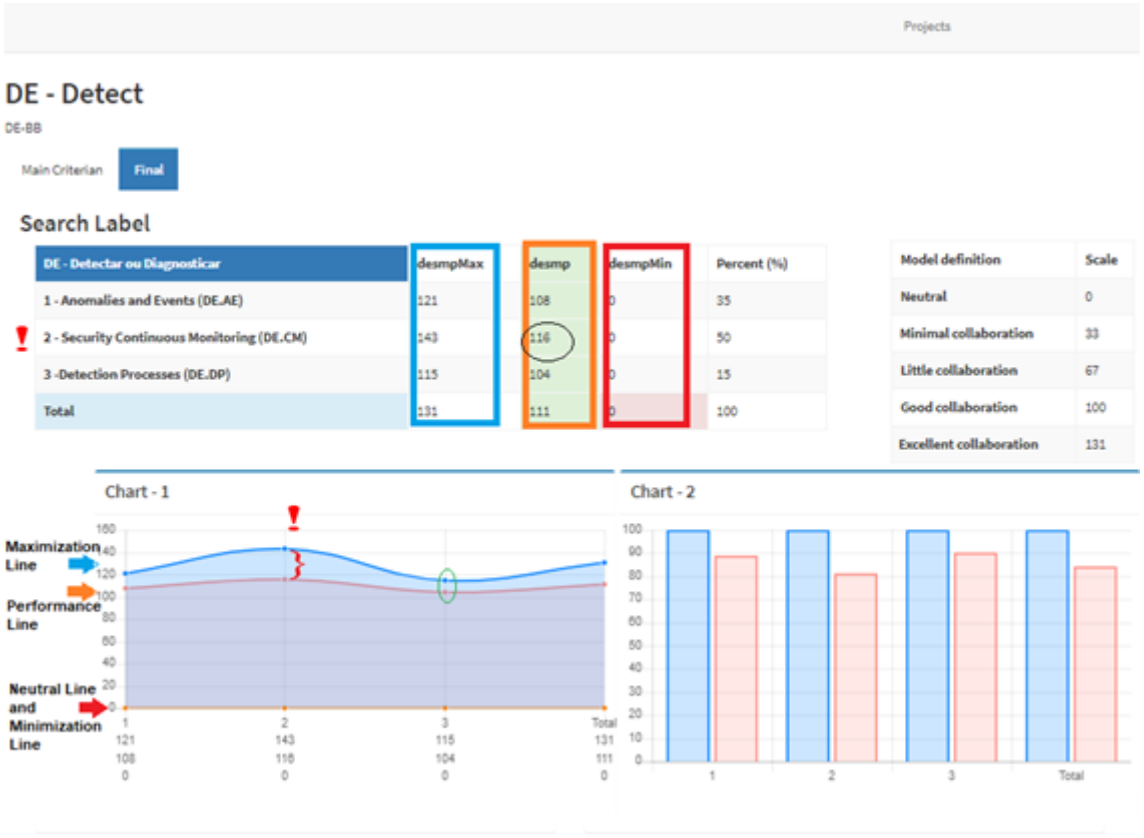

Figura 4.6: Resultados para análise global da função Detectar Retirado de [8]

Controles que não obtiveram destaques positivos ou negativos devem ser avaliados se devem ou não ser implementados ou revisados. Caso optem por uma implementação, estes não devem ser prioridade, assim como os que obtiveram seu ponto de maximização [8].

É importante ressaltar que, para uma boa gestão de riscos, esse processo deve ser sempre revisto concomitantemente para que obedeça um outro pilar da gestão de riscos a “Melhoria Contínua”, sendo assim o MCDA-C pode ser reaplicado novamente [8].

5 CONCLUSÃO E TRABALHOS FUTUROS

Gerenciar riscos de segurança tem se mostrado importante para as organizações. Além de permitir que as instituições se preparem para responder aos riscos levantados, também é fundamental no processo de transparência junto ao mercado financeiro e órgãos regulamentadores.

É importante ressaltar a quantidade de controles contidos nos *frameworks* de segurança da informação, que, muitas vezes, trazem dificuldades por parte dos gestores na escolha e priorização de quais implementar. Isso acontece porque existe uma complexidade no processo de tomada de decisão que envolve riscos da segurança da informação, onde muitas variáveis e critérios devem ser analisados diante destes controles.

Considerando a hipótese discutida neste trabalho, a proposta de aplicar um método multicritério, que possui foco na compreensão do problema e construção do conhecimento, se mostrou eficiente. A compreensão dos problemas enfrentados por gestores em priorizar os riscos cibernéticos foi fundamental para a confecção deste trabalho.

O objetivo deste trabalho foi propor e avaliar o método de decisão multicritério MCDA-C em um *framework* de segurança da cibernética utilizando os conceitos e princípios da gestão de riscos. Através de uma aplicação deste método em um ambiente real, um banco brasileiro, foi possível identificar as vantagens deste MCDM. O fato de o método identificar os pontos de desempenho, maximização e minimização é uma avalição perante os outros métodos. O uso de escalas de avaliação qualitativa, torna mais fácil a avaliação dos controles por parte das partes interessadas. E a conversão dos valores qualitativos em quantitativos utilizados pelo método também consegue oferecer uma nova visão dos resultados para os gestores no processo de tomada de decisão.

Problemas relatados em relação à priorização de controles de segurança da informação para mitigar riscos e evitar perdas financeiras são relevantes, merecendo uma atenção especial, entretanto, realizar uma gestão de riscos para cada organização apresenta diferentes variáveis e critérios devido ao mundo em que estão imersas. Assim, realizar uma gestão de risco que envolve controles de segurança da informação não é trivial, pois muitas vezes os gestores não detêm o conhecimento e o cenário do problema enfrentado pela própria instituição nos diversos níveis organizacionais, podendo realizar assim, uma priorização errada.

Uma limitação deste estudo é que somente a função de Detectar do CSF NIST foi aplicada, isso porque houve um entendimento por parte dos tomadores de decisão de que os controles mais críticos para aquele cenário enfrentado pela instituição se adequavam melhor naquele momento. Entretanto, essa dificuldade não inviabiliza a aplicação do método, uma vez que o próprio CSF NIST destaca que, os controles podem ser utilizados e selecionados de acordo com o cenário que a organização está envolvida.

5.1 VANTAGENS DO MCDA-C

A utilização do MCDA-C no processo de tomada de decisão na Gestão de Riscos da segurança da informação é eficaz. Isso porque,o método demonstrou abordar em suas fases os princípios de Gestão de

Riscos. Portanto, a transparência junto aos órgãos regulamentadores e o mercado não é mais um desafio. O uso da escala qualitativa facilita a avaliação das partes interessadas neste processo. Muitas vezes realizar um julgamento quantitativo a respeito da situação de um controle de segurança da informação não é trivial.

O cálculo de programação linear que converte os valores qualitativos em quantitativos é fundamental, pois o resultado para cada controle se torna três valores, que indicam o desempenho, ponto de maximização e minimização. Desta forma, os gestores não somente têm uma visão da situação atual dos controles de segurança, mas também onde deve concentrar os recursos até chegar nos níveis de maximização.

Tomadas de decisões baseadas somente na subjetividade dos gestores que muitas vezes não conhecem os desafios enfrentados em cada nível organizacional passam a não ser um problema. Isso porque o método consegue ouvir os diversos pontos de vista da organização, abordando os princípios da Integração, Fatores Humanos e Culturais, e Inclusivos.

O MCDA -C foca na construção do conhecimento e compreensão do problema e, para isso, ele envolve os diversos pontos de vista das partes interessadas, o que foi demonstrado neste trabalho. Portanto, realizar uma gestão de riscos baseada em controles de segurança da informação de forma eficaz, que aborde todos os requisitos necessários para o cumprimento de todas as fases desse processo não é mais um problema.

5.2 TRABALHOS FUTUROS

Este trabalho gerou várias ideias para trabalhos futuros, um deles seria a melhoria no cálculo de obtenção das taxas de compensação do MCDA-C. Essa taxa é obtida através da convicção e subjetividade dos tomadores de decisão. Esses valores poderiam ser obtidos através da comparação pareada utilizada no AHP, a partir índice de consistência para avaliar se os julgamentos estão coerentes. Desta forma poderia se dizer que seria adotada uma abordagem híbrida, chamada de AHP-MCDA-C.

Outro trabalho é realizar a aplicação do MCDA-C em tempo real para medir as vulnerabilidades de ferramentas em instituições. Os tomadores modelariam os problemas e, de acordo com os dados coletados de ferramentas de teste de segurança automatizados, o MCDA-C exibiria o índice de performance de segurança da instituição, mostrando os pontos de maximização.

Também seria interessante auxiliar pequenas e médias empresas na gestão de riscos cibernéticos utilizando o MCDA-C. A ideia é ajudar na implementação de controles de segurança de baixo custo para evitar que prejuízos financeiros decorrentes de ataques cibernéticos que venham a acontecer.

Um outro trabalho futuro importante seria a utilização do MCDA-C para auxiliar pequenas e médias empresas no âmbito da LGPD. O método é gratuito e não custou nenhum valor para a instituição financeira. Alénm disso, o MyMCDA-C é livre. Este trabalho futuro consistiria em uma primeira etapa levantar os requisitos necessários para se obter a conformidade com a LGPD utilizando algum framework como referência ou até mesmo criando um próprio. Em seguida, seria aplicado o MCDA-C mostrando quais seriam os pontos que deveriam ser priorizados para atingir o ponto de maximização para que as empresas entrem em conformidade com a lei.

REFERÊNCIAS BIBLIOGRÁFICAS

1 BUNKER, G. Targeted cyber attacks: how to mitigate the increasing risk. *Network Security*, v. 2020, n. 1, p. 17–19, 2020. ISSN 1353-4858. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1353485820300106>.

2 MELO, L. P. d. Proposta de metodologia de gestão de risco em ambientes corporativos na área de ti. 2008.

3 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *NBR Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação*. Rio de Janeiro, 2019. 70 p.

4 PEOTTA, L.; GONDIM, P. A framework for risk assessment of information technology in the corporate environment. *FORENSIC COMPUTER SCIENCE IJoFCS*, p. 75, 2007.

5 CANEDO., E.; Morais do Vale., A.; GRAVINA., R.; PATRãO., R.; Camargo de Souza., L.; REIS., V.; MENDONCA., F.; Sousa Jr.., R. An applied risk identification approach in the ict governance and management macroprocesses of a brazilian federal government agency. In: INSTICC. *Proceedings of the 23rd International Conference on Enterprise Information Systems - Volume 1: ICEIS,*. [S.l.]: SciTePress, 2021. p. 272–279. ISBN 978-989-758-509-8. ISSN 2184-4992.

6 MOHYEDDIN, M.; GHARAEE, H. Fahp-topsis risks ranking models in isms. In: IST. *7th International Symposium on Telecommunications*. [S.l.], 2014. p. 879–882.

7 SHAMELI-SENDI, A.; SHAJARI, M.; HASANABADI, M.; JABBARIFAR, M.; DAGENIAS, M. Fuzzy multi-criteria decision-making for information security risk assessment. In: *The Open Cybernetics Systemics Journal*. [S.l.: s.n.], 2012. p. 26–37.

8 MOREIRA, F. R.; FILHO, D. A. D. S.; NZE, G. D. A.; JúNIOR, R. T. de S.; NUNES, R. R. Evaluating the performance of nist's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access*, v. 9, p. 129605–129618, 2021.

9 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, 2018. 110 p.

10 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *NBR 27001: Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos*. Rio de Janeiro, 2013. 34 p.

11 SYAMSUDDIN, I.; HWANG, J. A new fuzzy mcdm framework to evaluate e-government security strategy. In: *4th International Conference on Application of Information and Communication Technologies*. [S.l.: s.n.], 2010. p. 1–5.

12 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *NBR Gestão de riscos - Técnicas para o processo de avaliação de riscos: ISO/IEC 31010:2012*. Rio de Janeiro, 2012. 110 p.

13 MEER, J. van der. *Multi-criteria decision model inference and application in information security risk classification*. [S.l.]: Master Thesis, Dept. of Computational Economics, Erasmus University Rotterdam, 2012.

14 MOREIRA, F. R.; NUNES, R. R.; GIOZZA, W. F.; NZE, G. A. Optimization of the performance of an online payment application by the improviment of its infrastructure. p. 1–2, 2020.

15 MOREIRA, F. R.; LIMA, E. D. O.; NUNES, R. R.; GIOZZA, W. F.; NZE, G. D. A. Uma análise das aplicabilidades de métodos multicritérios no contexto da segurança da informação. In: ANGRAD. *32º ENCONTRO NACIONAL DE CURSOS DE GRADUAÇÃO EM ADMINISTRAÇÃO (ENANGRAD)*. [S.l.], 2021. p. 1 –17.

16 BUENO, P. H. M.; MOREIRA, F. R.; LIMA, E. D. O.; NUNES, R. R. A utilização dos frameworks nist csf e da série nbr abnt iso 27.000 no contexto da gestão da segurança da informação. In: ANGRAD. *32º ENCONTRO NACIONAL DE CURSOS DE GRADUAÇÃO EM ADMINISTRAÇÃO (ENANGRAD)*. [S.l.], 2021. p. 1 –17.

17 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *ISO 31000:2018. Risk Management – Guidelines International Organization for Standardization*. Rio de Janeiro, 2018. 22 p.

18 ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *NBR 27002: Tecnologia da Informação: Técnicas de Segurança: Código de prática para controles de segurança da informação*. Rio de Janeiro, 2013. 112 p.

19 COHEN, J. *Statistical Power Analysis for the Behavioral Sciences. Second Edition*. [S.l.]: Mahwah, NJ: Lawrence Erlbaum Associates, 1998.

20 OLTSIK, J. *The Life and Times of Cybersecurity Professionals: a cooperative research project by esg and issa*. [S.l.]: The Enterprise Strategy Group, 2017.

21 NAKAMURA, E.; FILHO, J. R. F.; IDE, M. C. Metodologia de avaliação de riscos e medidas de segurança na proteção de dados pessoais. SBC, Porto Alegre, RS, Brasil, p. 11–16, 2019. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/wrac/article/view/14032>.

22 LOPES, I. M.; GUARDA, T.; OLIVEIRA, P. How iso 27001 can help achieve gdpr compliance. p. 1–6, 2019.

23 RESEARCH, D. *Trends in Security Framework Adoption: a survey of it and security professionals*. [S.l.]: Dimensional Research, 2016.

24 HILLIER F.S. LIEBERMAN, G. *Introdução à Pesquisa Operacional*. [S.l.]: 8ed. São Paulo: Ed.McGraw-Hill,, 2006.

25 LONGARAY, A. A.; TONDOLO, V. G.; MUNHOZ, P. R.; TONDOLO, R. P. Emprego de métodos multicritério em decisões gerenciais: uma análise bibliométrica da produção científica brasileira. *Revista Contemporânea de Contabilidade*, v. 13, n. 29, p. 113–128, 2016.

26 T, S. *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*. [S.l.]: RWS Publications, 2000.

27 SAATY, T.; VARGAS, L. *The Analytic Network Process*. [S.l.: s.n.], 2006. 1–26 p. ISBN 978-0-387-33859-0.

28 SAATY, T. L. *Theory and applications of the analytic network process: decision making with benefits, opportunities, costs, and risks*. [S.l.]: RWS publications, 2005.

29 HWANG, C.; YOON, K. *Multiple Attribute Decision Making: Methods and Applications*. [S.l.]: Springer-Verlag, New York, 1981.

30 E, G. A. F. *The DEMATEL Observer*. [S.l.]: Battelle Geneva Research Center, Geneva, 1976.

31 A, F. E. G. *World Problems, an Invitation to further thought within the framework of DEMATEL*. [S.l.]: Battelle Geneva Research Center, Geneva, 1972.

32 SUMRIT, D.; ANUNTAVORANICH, P. Using dematel method to analyze the causal relations on technological innovation capability evaluation factors in thai technology-based firms. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, v. 4, n. 2, p. 81–103, 2013.

33 REZAEI, J. Best-worst multi-criteria decision-making method. *Omega*, v. 53, p. 49–57, 2015. ISSN 0305-0483. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0305048314001480>.

34 SMOLIKOVA, R.; WACHOWIAK, M. P. Aggregation operators for selection problems. *Fuzzy Sets and Systems*, Elsevier, v. 131, n. 1, p. 23–34, 2002.

35 GRABISCH, M. A graphical interpretation of the choquet integral. *IEEE Transactions on Fuzzy Systems*, IEEE, v. 8, n. 5, p. 627–631, 2000.

36 BANAECOSTA, C. A. Introdução geral às abordagens multicritério de apoio à tomada de decisão. *Investigação Operacional*, v. 66, p. 117–139, 1988.

37 COSTA C.A., V. J. B. E. 01 1999.

38 ROY, B. Decision science or decision-aid science? *European Journal of Operational Research*, v. 66, n. 2, p. 184–203, 1993. ISSN 0377-2217. Model Validation.

39 DUTRA, A.; LIMA, M.; LOPES, A.; SERRA, F. Uso da metodologia multicritério de apoio à decisão construtivista - mcda-c para a incorporação da dimensão integrativa nos processos de avaliação de desempenho organizacional. *I Encontro da Administração da Informação*, v. 66, 2007.

40 BANAECOSTA, C. A. Três convicções fundamentais na prática do apoio à decisão. pesquisa operacional. *Pesquisa Operacional*, v. 13, p. 09–20, 1993.

41 BANAECOSTA, C. A.; VINCKE, P. Multiple criteria decision aid: an verview. in: Bana e costa, c. a. readings in multiple criteria decision aid. *Springer- Verlag*, v. 13, p. 101–118, 1990.

42 BANAECOSTA, C. A. *Processo de apoio à decisão: problemáticas, actores e acções. Apostila do Curso Metodologias Multicritério de Apoio à Decisão*. [S.l.]: ENE/UFSC, 1995.

43 ENSSLIN, L.; GIFFHORN, E.; ENSSLIN, S. R.; PETRI, S. M.; VIANNA, W. B. Avaliação do desempenho de empresas terceirizadas como o uso da metodologia multicritério de apoio à decisão – construtivista. *Pesquisa Operacional*, v. 30, p. 125–152, 2010.

44 LONGARAY, A. A.; ENSSLIN, L.; DUTRA, A.; ENSSLIN, S.; BRASIL, R.; MUNHOZ, P. Using mcda-c to assess the organizational performance of industries operating at brazilian maritime port terminals. *Operations Research Perspectives,*, v. 6, p. 100109, 2019. ISSN 2214-7160.

45 ENSSLIN, L.; MONTIBELLER, G.; NORONHA, S. Apoio à decisão: metodologias para estruturação de problemas e avaliação multicritério de alternativas. *Insular*, 2001.

46 BARZILAI, J. Measurement and preference function modeling. *International Transactions in Operational Research*, v. 12, p. 173 – 183, 03 2005.

47 KEENEY, R. *Value-focused thinking: a path to creative decision making*. [S.l.]: Harvard University Press, 1992.

48 BANAECOSTA, C. A.; BEINAT, E. *Model-structuring in public decision-aiding*. [S.l.: s.n.], 2005.

49 ROGERIO, A.; LACERDA, R.; ENSSLIN, L.; JUNGLES, A.; ENSSLIN, S. Performance measurement to aid decision making in the budgeting process for apartment building construction: A case study using mcda-c. *Journal of Construction Engineering and Management*, v. 139, p. 225–235, 02 2013.

50 SINGH, S.; MISRA, S. C.; KUMAR, S. Identification and ranking of the risk factors involved in plm implementation. *International Journal of Production Economics*, Elsevier, v. 222, p. 107496, 2020.

51 TARIQ, M. I.; AHMED, S.; MEMON, N. A.; TAYYABA, S.; ASHRAF, M. W.; NAZIR, M.; HUSSAIN, A.; BALAS, V. E.; BALAS, M. M. Prioritization of information security controls through fuzzy ahp for cloud computing networks and wireless sensor networks. *Sensors*, v. 20, n. 5, 2020. ISSN 1424-8220.

52 BRAGA., P. L.; LIMA., C. M.; C., R. E. C. Influência do instagram no comportamento do consumidor. *Faces: Revista De Administração*, v. 19, p. 15–28, 2020.

53 BARROS, G. L.; RODRIGUES, E. C. C.; LIMA, C. M. Logística reversa de pós-consumo: Análise das práticas em unidades escolares públicas do distrito federal. *Revista Negócios Em Projeção*, v. 9, p. 45–65, 2018.

54 BARBALHO, L. R.; RODRIGUES, E. C. C.; LIMA, C. M. Análise multicritério das lacunas entre logística reversa e processamento de bens. *Rea. Revista Eletrônica De Administração*, v. 19, p. 301–322, 2020.

55 CARDOSO, G. P.; RODRIGUES, E. C. C. Contabilidade pública gerencial - uma análise da informação de custos à luz da percepção dos gestores públicos. *International Conference in Management and Accounting (ICMA/COGECONT)*, v. 19, 2020.

56 JúNIOR, A. S.; RODRIGUES, E. C. C.; LIMA, C. M.; ., R. R. N.; WIELEWSKI, G. L. Análise da usabilidade do marketiplace ifood pela Ótica do consumidor. *30th Enangrad, Uberlândia Brazil*, 2019.

57 AMARAL, E. R.; JúNIOR, A. S.; WIELEWSKI, G. L.; RODRIGUES, E. C. C.; LIMA, C. M. A usabilidade de um site de compras e vendas no brasil. *30th Enangrad, Uberlândia Brazil*, 2019.

58 BANAECOSTA, C.; VANSNICK, J.-C. The macbeth approach: basic ideas, software, and an application. v. 4, 01 1999.

59 BANAECOSTA, C. A.; CORTE, J. D.; VANSNICK, J. Macbeth. *International Journal of Information Technology Decision Making (IJITDM), World Scientific Publishing Co. Pte. Ltd.*, p. 359–387, 2003.

60 GOURISETTI, N. G.; MYLREA, M.; PATANGIA, H. Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. p. 0206–0213, 2019.

61 ALENEZI, M.; ALKA, A.; KUMAR, R.; AHMAD, K. R. Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective. *IEEE Access*, v. 8, p. 25543–25556, 2020.

62 GANIN, A. A.; QUACH, P.; PANWAR, M.; COLLIER, Z. A.; KEISLER, J. M.; MARCHESE, D.; LINKOV, I. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, v. 40, n. 1, p. 183–199, 2020.

63 ANJUM, M.; KAPUR, P.; AGARWAL, V.; KHATRI, S. K. Assessment of software vulnerabilities using best-worst method and two-way analysis. *International Journal of Mathematical, Engineering and Management Sciences*, International Journal of Mathematical, Engineering and Management Sciences, v. 5, n. 2, p. 328–342, 2020.

64 PARK, K. C.; SHIN, D.-H. Security assessment framework for iot service. *Telecommunication Systems*, Springer, v. 64, n. 1, p. 193–209, 2017.

65 HÅKANSSON, A. Portal of research methods and methodologies for research projects and degree projects. p. 67–73, 2013.

66 VERGARA, S. C. Projetos e relatórios de pesquisa. *São Paulo: Atlas*, 2006.

67 GIL, A. C. *Métodos e técnicas de pesquisa social*. [S.l.]: 6. ed. Ediitora Atlas SA, 2008.

68 GIL, C.; PESQUISA, A. C. E. P. de. 6 edição. *São Paulo, Atlas*, 2017.

69 MARCONI, M. L.; CIENTIFICA, E. F. da M. 5ª edição, editora atas sa. *São Paulo*, 2003.

70 PRODANOV, C. C.; FREITAS, E. C. D. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição*. [S.l.]: Editora Feevale, 2013.

71 COOPER, D. R.; SCHINDLER, P. S. *Métodos de Pesquisa em Administração-12ª edição*. [S.l.]: McGraw Hill Brasil, 2016.