DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE MÉTODO DE PRIORIZAÇÃO DE CONTROLES PARA IMPLEMENTAÇÃO DA ARQUITETURA ZERO TRUST UTILIZANDO MÉTODOS MULTICRITÉRIOS

Luiz Guilherme Schiefler de Arruda

Brasília, junho de 2023

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

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE MÉTODO DE PRIORIZAÇÃO DE CONTROLES PARA IMPLEMENTAÇÃO DA ARQUITETURA ZERO TRUST UTILIZANDO MÉTODOS MULTICRITÉRIOS

Luiz Guilherme Schiefler de Arruda

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. Clóvis Neumann, Ph.D, FT/UnB _____
Examinador Interno

Prof. Dino Macedo Amaral, Ph.D, BB _____
Examinador externo

FICHA CATALOGRÁFICA

ARRUDA, LUIZ GUILHERME SCHIEFLER DE
PROPOSTA DE MÉTODO DE PRIORIZAÇÃO DE CONTROLES PARA IMPLEMENTAÇÃO DA ARQUITETURA ZERO TRUST UTILIZANDO MÉTODOS MULTICRITÉRIOS [Distrito Federal] 2023.
xvi, 66 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. *Zero Trust* 2. Método Multicritério
3. Revisão Sistemática de Literatura 4. Segurança Cibernética
I. ENE/FT/UnB II. Título (série)
Publicação: PPEE.MP.052

REFERÊNCIA BIBLIOGRÁFICA

ARRUDA, L. G. S. (2023). *PROPOSTA DE MÉTODO DE PRIORIZAÇÃO DE CONTROLES PARA IMPLEMENTAÇÃO DA ARQUITETURA ZERO TRUST UTILIZANDO MÉTODOS MULTICRITÉRIOS.* Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 66 p.

CESSÃO DE DIREITOS

AUTOR: Luiz Guilherme Schiefler de Arruda
TÍTULO: PROPOSTA DE MÉTODO DE PRIORIZAÇÃO DE CONTROLES PARA IMPLEMENTAÇÃO DA ARQUITETURA ZERO TRUST UTILIZANDO MÉTODOS MULTICRITÉRIOS.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

Luiz Guilherme Schiefler de Arruda
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho ao meu querido pai, Paulo Gilberto, e à minha mãe, Wanda Eunice (*in memorian*) por todo estudo e educação que me proporcionaram. A minha querida esposa Camila que sempre me apoiou, sendo um grande alicerce para mais esta conquista. Finalmente, dedico ao meu orientador Rafael Rabelo e co-orientador William Giozza, pela dedicação e esforço em compartilhar seus conhecimentos para a conclusão deste trabalho.

AGRADECIMENTOS

Agradeço à Deus pelo dom da vida, pela saúde e motivação que me permitiu ultrapassar todas as barreiras e obstáculos e chegar ao final deste trabalho.

À toda equipe da Secretaria do PPEE, nas pessoas da Adriana, Cristiana e Tayná, por todo suporte e orientação. Vocês facilitaram muito nossa vida acadêmica.

À minha família pelas oportunidades dadas para eu chegar até aqui, pelo apoio incondicional e pela compreensão em minhas ausências.

À Camila, por todo amor e carinho durante todo este tempo. Sua colaboração e compreensão nas noites mal dormidas foram fundamentais para chegar ao término desta fase. Obrigado sempre.

Ao meu orientador Prof. Dr. Rafael Rabelo Nunes e a meu co-orientador Prof. Dr. William Ferreira Giozza por todo suporte e confiança durante o curso e a elaboração deste trabalho, permitindo-me chegar a esta etapa. Foi um prazer ser orientado por você durante esse percurso.

Aos professores da UnB que, mesmo com a mudança da metodologia de ensino causada pela COVID-19, ministraram as disciplinas deste curso. Seus ensinamentos foram fundamentais para meu amadurecimento e na criação deste trabalho

Aos meus amigos do curso (Edvan, Fernando, Leandro, Lucas, Marcos, Solimar, Zottmann, entre outros), meus sinceros agradecimentos pelo tempo que dedicaram com as correções de artigos e deste trabalho, bem como pelos momentos que passamos conversando e trocando informações e ideias.

Finalmente a ABIN e UnB, pela iniciativa deste acordo. Desejo que esta parceria continue produzindo frutos em prol da difusão dos conhecimentos acadêmicos dentro da área de inteligência e da sociedade brasileira.

RESUMO

A evolução das redes de computadores fez com que elas se tornassem cada vez mais complexas e aumentassem sua superfície de ataque, tornando a proteção de bordas menos eficaz. Nesse contexto, surgiu o conceito de *Zero Trust* (ZT), que é um novo modelo de confiança. Esse conceito amplo apresenta diversos controles para sua implementação, o que torna a gestão de riscos um desafio, pois os gestores precisam priorizar esses controles. De acordo com a ISO 31000, a metodologia multicritério de apoio à decisão pode auxiliar os decisores na modelagem de problemas e na priorização de ações a serem tomadas. O conceito multicritério é baseado em duas escolas: a americana, que foca na precisão dos cálculos para priorizar os controles, e a europeia, que considera a decisão como uma atividade humana. O MCDA-C, que vem da escola europeia, tem a capacidade de agregar diversos níveis dentro de uma organização na busca pela construção do conhecimento, facilitando a tomada de decisão pelos decisores. Neste trabalho, propõe-se a utilização dos controles descritos no Modelo de Maturidade de ZT da CISA em conjunto com o MCDA-C, pois isso permite a clareza na visualização do desempenho ideal, na perspectiva dos decisores, e na priorização para a implementação dos controles da ZT. Por fim, considerando os controles propostos, este estudo demonstra a capacidade do MCDA-C em auxiliar na compreensão do problema dentro da organização e na construção do conhecimento por meio da análise dos dados coletados. Dessa forma, foi possível apresentar aos decisores quais controles devem ser priorizados no início da implementação da ZT.

ABSTRACT

The evolution of computer networks has made them increasingly complex and expanded their attack surface, rendering traditional perimeter protection less secure. In this context, a new trust model called Zero Trust (ZT) emerged. This concept, encompassing various controls for its implementation, makes risk management a challenging task, as managers face the challenge of prioritizing these controls. ISO 31000 describes how the multicriteria decision-making methodology can assist decision-makers in problem modeling and action prioritization. The multicriteria concept is based on two schools of thought: the American approach, which focuses on precise calculations to prioritize controls, and the European approach, which views decision-making as a human activity. MCDA-C, originating from the European school, has the capability to incorporate multiple levels within an organization to facilitate knowledge construction and decision-making for decision-makers. This study proposes the utilization of controls described in the CISA's Zero Trust Architecture (ZTA) Maturity Model in conjunction with MCDA-C. This approach provides clarity in visualizing the ideal performance from decision-makers' perspectives and facilitates prioritization for ZTA control implementation. Finally, considering the proposed controls, this study demonstrates the capability of MCDA-C in aiding the understanding of the problem within the organization and constructing knowledge through the analysis of collected data. Consequently, it becomes possible to present decision-makers with the controls that should be prioritized at the outset of a ZTA implementation.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas
AHP	*Analytic Hierarchy Process*
APF	Administração Pública Federal
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CISA	*Cybersecurity and Infrastructure Security Agency*
COMET	*Characteristic Objects Method*
DevSecOps	*Development, Security and Operation*
DAAS	*Desktop as a Service*
DoD	*Department of Defense*
ELECTRE	*Elimination et Choix Traduisant la Réalité*
EPV	*Elementar Point of View*
EVAMIX	*Multi-criteria evaluation with mixed qualitative-quantitative data*
FPV	*Fundamental Point of View*
IC	Infraestruturas Críticas
IDS	*Intrusion Detection System*
IoT	*Internet of Things*
IPS	*Intrusion Protection System*
ISO	*International Organization for Standardization*
MACBETH	*Measuring Attractiveness by a Categorical Based Evaluation Technique*
MAUT	*Multiple Atribute Utiliiy Theory*
MCDA	*MultiCriteria Decision Analysis*
MCDA-C	*MultiCriteria Decision Aid Constructivist*
MCDM	*MultiCriteria Decision Making*
NSTAC	*National Security Telecommunications Advisory Committee*
NIST	*National Institute of Standards and Technology*
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*
PROMETHEE	*Preference Ranking Method for Enrichment Evaluation*
RADIUS	*Remote Authentication Dial In User Service*
RR	*Rank Reversal*
RSL	Revisão Sistemática de Literatura
SIEM	*Security Information and Event Management*

SIMUS	*Sequential Interactive Modelling for Urban Systems*
SPOTIS	*Stable Preference Ordering Towards Ideal Solution*
TOPSIS	*Technique for Order Preference by Similarity to ideal Solution*
UnB	Universidade de Brasília
VLAN	*Virtual Local Area Network*
ZT	*Zero Trust*
ZTA	*Zero Trust Architecture*
ZTMM	*Zero Trust Maturity Model*

1 INTRODUÇÃO

O mundo vive sob a ameaça de uma onda crescente de ataques cibernéticos. Das pessoas físicas às organizações, de entidades sociais a governos, todos estão expostos a riscos ainda não completamente avaliados se estiverem presentes no espaço cibernético [1].

Quando a Internet surgiu, no final da década de 60, as redes de computadores, além de simples, eram pequenas e restritas. Entretanto, a evolução das redes de computadores trouxe um aumento em seu tamanho, tornando-as cada vez mais complexas e dificultando o monitoramento do fluxo de dados [2]. Contudo, algumas mudanças ocorreram na computação empresarial nas últimas duas décadas, principalmente com o surgimento de novas abordagens, como por exemplo a nuvem, a computação de ponta e a *Internet of Things* (IoT) [3]. Além disso, com a proliferação da tecnologia das redes e IoT, observou-se alterações no âmbito dos sistemas de tecnologias da informação [4].

Ataques perpetrados no espaço cibernético podem refletir no ambiente físico das Infraestruturas Críticas (IC) de um país, interferindo, assim, em assuntos internos, ao buscar frustrar ou impedir um dos objetivos fundamentais do Estado brasileiro: a autodeterminação [1].

A tradicional abordagem de proteção das bordas acaba dividindo as redes em duas: internas e externas [4, 5]. Esta divisão pode ser observada com a utilização de controles de segurança como *firewall*, *Intrusion Detection System* (IDS), *Intrusion Protection System* (IPS), entre outros [4]. Entretanto, esta arquitetura de segurança de rede, apresenta dois grandes riscos: ausência de defesa contra-ataques oriundos internamente a rede; e uma dependência dos dispositivos de segurança existentes nas bordas [5, 6].

Embora a literatura apresente informações sobre estruturas para trocas de dados, há uma falta de abordagens para a proteção de IC, o que pode ser causado por conta da criticidade dessas infraestruturas ou por preocupações com a adoção de uma tecnologia nova e ainda não totalmente explorada [7].

Conforme [8] a segurança de informações tem sido definida nos termos da Confidencialidade, Integridade e Disponibilidade. A confidencialidade tem relação com a garantia de que apenas pessoas autorizadas podem acessar determinada informação, a integridade garante que a informação não sofreu alteração não autorizada e a disponibilidade é a propriedade da informação ser acessível e modificável em momento oportuno por aqueles que estejam autorizados a fazê-lo.

Incidentes cibernéticos recentes destacam o desafio de proporcionar uma segurança cibernética eficaz dentro do território nacional, como acontece com grandes empresas, demonstrando que a abordagem tradicional pode não ser mais eficiente para proteger um país contra ameaças cibernéticas [9].

Em respostas às crescentes ameaças cibernéticas e à necessidade de proteger efetivamente os sistemas de informação em um ambiente cada vez mais complexo e interconectado, um paradigma de segurança, conhecido como *Zero Trust* (ZT) e sua correspondente arquitetura, *Zero Trust Architecture* (ZTA) foi desenvolvido. Esta nova abordagem rompe com a ideia tradicional de confiar automaticamente na segurança dos sistemas internos e na rede corporativa, adotando o princípio de "*Never Trust, Always Verify*"(Nunca Confie, Sempre Verifique) [10].

Esse novo conceito descreve que a confiança inerente aos sistemas tradicionais permitia que as ameaças internas se propagassem facilmente, resultando em violações de segurança significativas. Ao invés disso, o ZT propõe a implementação de rigorosos controles de segurança e autenticação em todas as etapas da comunicação, independentemente da localização ou origem do usuário ou dispositivo [10, 11].

Além disso, uma organização deve ser capaz de realizar ações para verificar as possíveis fontes de risco e suas consequências. Neste diapasão, com uma gestão de risco eficaz, a organização tem a capacidade de avaliar os possíveis riscos que ela pode sofrer ou se seus gestores seriam capazes de tomar decisões fundamentadas para mitigar este risco [12]. Nesse sentido, como suporte ao processo de avaliação de risco, o método multicritério apresenta-se como uma solução capaz de, a partir de um conjunto de informações, fornecer uma priorização de controles para a solução de um problema [13].

As aplicações da tomada de decisão baseada em risco usando a Análise de Decisão Multicritério (MCDA) dentro do governo federal americano incluem a avaliação de segurança portuária, a Iniciativa de Segurança de Áreas Urbanas, e a gestão de rejeitos de engenharia. Revisões recentes do MCDA mostram que sua aplicação tem sido cada vez mais difundida dentro do governo americano bem como na literatura acadêmica em geral [14].

1.1 HIPÓTESE

Considerando a evolução da tecnologia e por consequência o aumento do número de dispositivos conectados em rede, aliado à possibilidade de que vazamentos ocorram por conta de público interno, a utilização de uma metodologia multicritério construtivista pode auxiliar na priorização da implementação dos controles de uma ZTA dentro de uma corporação. A utilização deste modelo arquitetural traz soluções considerando o ponto de vista não apenas dos gestores e decisores, mas de todos os envolvidos no processo, melhorando o entendimento do problema.

1.2 MOTIVAÇÃO E PROBLEMAS

As vulnerabilidades naturais de um conjunto complexo de redes informatizadas, como a encontrada na Administração Pública federal (APF), são agravadas por fatores como a pouca cultura em segurança da informação e comunicações, o apoio tímido da alta administração para o assunto e a baixa articulação entre os órgãos e entidades públicos que têm a responsabilidade de defender a parcela do espaço cibernético, sob suas responsabilidades contra ataques cibernéticos [1].

Os vazamentos de dados oriundos de ataques cibernéticos, assim como problemas ocorridos com interrupção de serviços realizados em IC, podem trazer problemas graves a corporações e até uma nação.

Considerando a evolução observada dentro da área de Tecnologia da Informação, uma tecnologia com pouco mais de 10 anos pode ser considerada ultrapassada. Entretanto poucos são os estudos sobre a ZTA que abordam sua implementação. Nesse contexto, os métodos multicritérios podem ser analisados como uma possível solução à priorização da implementação da ZTA. Entretanto, fruto da baixa quantidade de

publicações, torna-se necessário a construção de uma base de conhecimentos por parte dos decisores para, então, sentirem-se mais confortáveis no rumo escolhido.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

A presente pesquisa tem como objetivo avaliar e priorizar controles de segurança da informação baseados na ZTA, utilizando um método de decisão multicritério.

1.3.2 Objetivos Específicos

A partir deste objetivo geral, os seguintes objetivos foram propostos:

- Identificar os modelos de ZTA disponíveis na literatura
- Verificar a necessidade de um estudo voltado a implementação da ZTA dentro de organizações;
- Verificar a aplicabilidade dos métodos multicritério na priorização dos controles a ser implementados;
- Identificar e elaborar critérios e subcritérios a ser analisado acerca dos controles implementados em uma ZTA; e
- Verificar como os *stakeholders* de uma organização percebem o impacto dos controles na mitigação dos riscos de segurança da informação em uma organização.

1.4 JUSTIFICATIVAS

O aumento das redes de computadores trouxe evoluções para diferentes áreas, contudo tornou seu monitoramento mais complexo e difícil. Além disso, informações sensíveis trafegam nos sistemas de informação em maior quantidades. Por conseguinte, o processo de identificação, análise, resposta e monitoração dos riscos fica mais complexo.

Dentre as maneiras para a proteção dos dados dentro de uma organização, pode-se utilizar o ZTA. O fato desta arquitetura ser composta por diversos controles, dificulta sua implementação, uma vez que dificulta os gestores no estabelecimento da prioridade de implementação do controle com o foco na mitigação dos riscos para o caso de um vazamento de dados.

Assim, os métodos multicritérios podem contribuir para a definição desta priorização. Entretanto, mesmo existindo uma diversidade de métodos, grande parte delas utiliza-se de modelos matemáticos para a ordenação, não agregando conhecimentos aos decisores.

Considerando que o conceito do ZT é relativamente novo e desconhecido, torna-se necessário a construção de um conhecimento, através da inclusão no processo de gestão de risco, não apenas do tomadores de decisão, mas também das partes interessadas, com o propósito de gerar novos conhecimentos. O fato de não se ter encontrado na literatura informações sobre o emprego do método multicritério na implementação da ZTA, mostra a necessidade de um estudo com este enfoque.

1.5 PUBLICAÇÕES DECORRENTES DO TRABALHO

Os artigos abaixo foram escritos e publicados no decorrer dos estudos, servindo de alicerce não apenas para o referencial teórico, como também na divulgação dos resultados obtidos.

1.5.1 9ª Conferência Ibero-Americana Computação Aplicada 2022 (CIACA)

Título: O método multicritério no apoio à priorização na implementação do *Zero Trust* [15]

Ano Publicação: 2022

Local: Lisboa - Portugal

DOI: http://www.doi.org/10.33965/CIACA_CIAWI2022_202209C021

1.5.2 6th *International Conference on Information Technology & Systems* (ICITS)

Título: Implementação da Arquitetura *Zero Trust*: Uma Revisão Sistemática de Literatura [16]

Ano Publicação: 2023

Local: Cusco - Peru

DOI: http://www.doi.org/10.5281/zenodo.8032943

1.6 ESTRUTURA DA DISSERTAÇÃO

A presente dissertação está dividida da seguinte maneira: No Capítulo 2 são abordados os tópicos que serviram como referencial teórico para o trabalho. Inicialmente, são apresentados os dez princípios de Saltzer & Schroeder sobre segurança da informação. Na sequência é introduzido o conceito de ZT e ZTA, algumas de suas aplicações e os modelos de ZTA desenvolvidos por grandes empresas internacionais bem como padronizações definidas. Além disso, fruto de uma das publicações, é apresentada uma revisão sistemática de literatura onde foi possível observar uma lacuna na literatura que foi explorada nesta dissertação. Finalizando o Capítulo 2, são apresentados os métodos multicritério e o *software* utilizado.

O Capítulo 3 apresenta a metodologia utilizada na elaboração do estudo. O Capítulo 4 mostra a aplicação do método multicritério e os resultados obtidos com sua aplicação dentro de uma corporação de

maneira a entender, na visão das pessoas que responderam ao questionário, a priorização dos controles no caso de uma implementação da ZTA dentro de uma organização. Finalizando com o Capítulo 5 são apresentadas as conclusões do estudo e enumerados possíveis trabalhos futuros baseados nesta pesquisa.

2 REFERENCIAL TEÓRICO

Este Capítulo aborda o referencial teórico envolvendo os assuntos tratados nesta dissertação. Assim, além dos princípios de Saltzer e Schroeder, serão abordados as propostas de ZTA da Google, Microsoft, *National Institute of Standardization and Tecnology* (NIST), *Departament of Defense* dos Estados Unidos da América (DoD) e da *Cybersecurity and Infrastructure Security Agency* (CISA em inglês); a Revisão Sistemática de Literatura que norteou a sequência do trabalho; e os métodos multicritérios de apoio à decisão. Este Capítulo inclui também uma Seção abordando a utilização dos métodos multicritério na implementação do ZT.

2.1 PRINCÍPIOS DE SALTZER & SCHROEDER

Em 1975 Saltzer & Schroeder escreveram um artigo entitulado *The Protection of Information in Computer Systems* [17] onde descrevem oito princípios básicos relacionados à Segurança Cibernética. Interessante perceber que pouco tempo depois do início da Internet, ocorrida em 1969 com a Arpanet, autores já pensavam nessa temática. Além disso, mesmo os princípios sendo antigos, ainda nos dias atuais são importantes e debatidos em artigos e livros, conforme pode-se observar em [17, 18].

A seguir são explicados, de maneira sucinta, cada um dos princípios, retirados do [17, 18]:

- **Economia de mecanismo**: Este princípio enfatiza a simplicidade no desenvolvimento de projetos e implementação de medidas de segurança pois é especialmente importante dentro do domínio da segurança. Segundo os autores, quanto mais simples e fácil de raciocinar for o modelo de um sistema, torna-se mais fácil a tarefa de auditar ou verificar manualmente o mesmo para garantir um nível mais alto de segurança. Além disso, quanto menor for o tamanho do projeto, consegue-se aumentar a garantia de que ele mantenha as propriedades mínimas de segurança esperadas. Na prática, isso se traduz em evitar soluções complicadas e preferir abordagens simples, eficientes e confiáveis. Um exemplo seria a implementação de criptografia usando algoritmos padrão bem estabelecidos em vez de criar algoritmos proprietários complexos.
- ***Defaults* seguros contra falhas**: Este princípio estabelece que a configuração padrão de um sistema deve ser um esquema de proteção conservador, ou seja, atribuir um nível mínimo de direitos ao usuário, desativando recursos não essenciais que possam representar riscos. Isso ocorre porque, na escolha entre segurança e usabilidade, normalmente opta-se pelo segundo em detrimento do primeiro. Além disso, é preferível construir os controles de segurança levando em consideração o comportamento adequado conhecido, o que reduz a chance de possíveis erros decorrentes da exclusão da violação detectada. Este princípio está relacionado à configuração de *firewalls*, que pode ser ajustada para permitir o acesso somente a serviços essenciais, bloqueando outros tipos de acesso.
- **Mediação completa**: Este princípio considera que todo acesso a um determinado recurso deve ser verificado e confrontado com um esquema de proteção baseado em políticas, de maneira a garantir

que a tentativa de acesso ocorra conforme uma política de segurança. Assim, consegue-se verificar se a tentativa de acesso a um determinado recurso está de acordo ou não antes de conceder o acesso, utilizando, para isso, sistemas robustos de autenticação. A implementação de controles de acesso tipo *Policy-based Access Control* (PBAC), onde a concessão do acesso ocorre apenas após a verificação da permissão e *Role-Based Access Control* (RBAC) onde a autorização está relacionado a funções específicas da tentativa de acesso, são exemplos da utilização deste princípio.

- **Projeto aberto**: Defende que a segurança de um sistema não deve depender da obscuridade do seu projeto, ou seja, não deve ser baseada na ideia de que a segurança está garantida pelo fato de que os detalhes do sistema são desconhecidos ou mantidos em segredo. Em vez disso, a segurança deve ser alcançada através de mecanismos e algoritmos amplamente conhecidos, que sejam abertos e transparentes para análise e avaliação pela comunidade de especialistas em segurança. Assim é possível que especialistas em segurança verifiquem os aspectos relevantes do projeto, como ocorre na adoção de padrões e algoritmos criptográficos abertos, no desenvolvimento de *software* livre (como o SO Linux).

- **Separação de privilégio**: Este princípio estabelece que várias condições devem ser requeridas para que entidades (usuários, processos, dispositivos, ...) obtenham acesso a recursos restritos ou sejam capaz de fazer um programa realizar alguma ação. Desde a publicação do artigo de Saltzer-Schroeder, o termo também significa a separação dos componentes de um sistema, para limitar o dano causado por uma brecha de segurança de qualquer componente individual. Esta ação limita o impacto potencial de um usuário mal-intencionado ou de um programa comprometido. Por exemplo, separar as funções de administrador e usuário comum dentro de um SO é uma aplicação pratica desse princípio.

- **Menor privilégio**: A concessão de um conjunto mínimo de privilégios assegura que possíveis abusos de privilégios sejam evitados, reduzindo, assim, os danos causados por um usuário mal intencionado. Assim, organizações com grandes sistemas, podem segregá-los em componentes menores e com privilégios reduzidos, garantindo uma maior segmentação e aumentando a segurança global do sistema como um todo. A configuração dos usuários de um SO, a liberação de acesso a determinadas páginas na Web apenas após a autenticação e autorização do usuário, e até o controle no acesso à redes podem ser exemplos da utilização deste princípio.

- **Mecanismo comum mínimo**: O compartilhamento de recursos entre diferentes entidades deve ser o mínimo possível, caso isso seja necessário, eles devem ter maneiras de acesso diferentes. Este compartilhamento pode ser um vetor crucial de fuga de informação. Entretanto existem exceções, como o próprio caso da utilização da Internet ou SO com diversos usuários. Isto pode ser observado dentro de uma rede de computadores, quando diferentes setores de uma organização tem suas redes lógicas segregadas, reduzindo a superfície de ataque.

- **Aceitação psicológica**: Para que o usuário comece a utilizar medidas de segurança, estas devem ser projetadas de maneira a ser intuitivas e atrativas. Desta maneira, os usuários comuns não ficam com medo de utilizar ou não utilizam as medidas de segurança por desconhecimento dos procedimentos para sua configuração. Assim, ao considerar as necessidades e as percepções dos usuários, é pos-

sível aumentar a eficácia das medidas de segurança e fortalecer a postura geral de segurança de um sistema. Isto pode ser obtido através do desenvolvimento da aplicações amigáveis e intuitivas.

Além destes oito princípios, analistas de sistemas de segurança sugeriram outros dois princípios que, na visão dos autores, são aplicáveis de maneira imperfeita a sistemas de computadores:

- **Fator de trabalho**: O custo para fraudar um mecanismo de segurança está ligado tanto à sensibilidade dos dados armazenados neles quanto aos recursos disponíveis para um possível atacante tentar corromper seu sistema. Entretanto, há situações onde esse custo torna-se difícil de ser mensurado, como por exemplo na busca por *bugs* dentro de um *software*.
- **Registro de comprometimento**: Envolve o monitoramento e registro de atividades suspeitas ou comprometedoras em um sistema. Com isso, dependendo do tipo de sistema, é mais desejável registrar os detalhes de uma intrusão do que adotar medidas mais sofisticadas para evitá-la. Assim, sugere-se por vezes que registros confiáveis ou *logs*, que permitem a detecção de um comprometimento, ou a trilha de auditoria e evidências devem ser usados ao invés de controles que previnam um comprometimento.

Os princípios estão sintetizados na Figura 2.1:

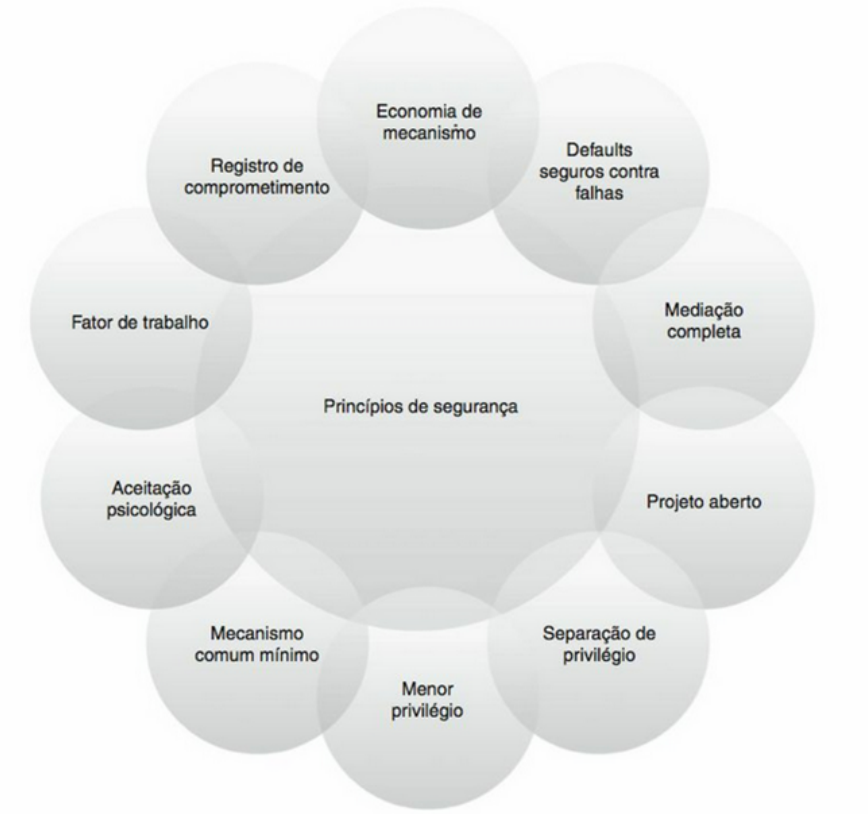

Figura 2.1: Princípios de Saltzer e Schroeder. Fonte: [8]

2.2 *ZERO TRUST*

O conceito conhecido como *Zero Trust* (ZT) foi inicialmente apresentado em 2004, durante o Fórum de Jericho, onde executivos de diversas empresas do Reino Unido reuniram-se para discutir acerca da manutenção dos protocolos de segurança a época. Neste Fórum foi reconhecido que o modelo de segurança, então conhecida como castelo e fosso, estava deixando de funcionar em face do crescente número de dispositivos interligado em rede dentro deste ”castelo” [19].

Em 2010, John Kindervag, então analista da Forrester, percebeu que o conceito de realizar a proteção no perímetro, capaz de segregar uma rede em interna e externa, garantindo que os usuários e dispositivos que estavam dentro do perímetro estavam seguros e os do lado de fora inseguros, apresentava algumas armadilhas. Assim, considerando que o modelo vigente de segurança apresentava falhas, introduziu um novo modelo de confiança. Neste novo modelo, chamado de ZT, os profissionais de segurança deveriam parar de confiar nos pacotes como se fossem pessoas e começar a verificar todos os acessos, considerando, assim todo o tráfego dentro da rede como não confiável [10].

Este novo modelo de confiança apresenta três conceitos básicos [10]:

1. Garantir que todos os recursos são acessados de maneira segura, independente da localização do acesso;
2. Adotar uma estratégia de menor privilégios e aplicar rigorosamente o controle de acessos; e
3. Inspecionar e registrar todo o tráfego na rede.

Com o modelo ZT deve-se considerar que não existe interfaces, rede e usuários confiáveis e não confiáveis. Entretanto, é importante levar em consideração que o ZT não diz que os funcionários de uma organização deixaram de ser confiáveis, mas guia os profissionais de segurança da informação a não confiar mais nos pacotes, tráfego na rede e dados [11].

A realidade da existência de atacantes oriundos do interior das redes contribuiu para uma mudança no modelo de confiança. Com isso, é possível detectar uma tentativa interna por conta de mau uso da Internet, aumentando as chances da descoberta de um crime cibernético antes que ele tenha sucesso [11].

No ano de 2014, a Google iniciou uma ação interna, que implementou elementos fundamentais do ZT que efetivamente removeram os limites de sua rede corporativa. Esta plataforma foi chamada de BeyondCorp e influenciou o setor. Sua implementação foi documentada através de uma série de artigos que serão abordados na Seção 2.2.1 [20].

O conceito apresentado por Kindervag em 2010 foi sendo estudado e aprimorado dentro da empresa Forrester e no ano de 2018, o conceito ZT sofreu uma atualização. Na visão da Forrester, em virtude do crescimento da quantidade de dados localmente e na nuvem, os dados passaram a ser o ponto central do ZT, devendo ser protegido e as pessoas (*people*), dispositivos (*devices*), redes (*networks*) e carga de trabalhos (*workloads*), os elementos nas imediações que dão acesso aos dados, devendo, também, ser protegidos [21].

Na sequência, em 2020, o NIST apresentou sua padronização chamada de SP 800-207 *Zero Trust*

Architecture, sendo o primeiro instituto de padronização internacional a publicar uma orientação sobre a ZTA [22].

O governo dos Estados Unidos da América emitiu um decreto (*Executive Order 14028*) que adota o ZT como um modelo de segurança desejado dentro do governo federal. Neste sentido, o Gabinete Executivo do Presidente dos EUA emitiu um memorando (M-22-09 - *Moving U.S. Government Towards Zero Trust Cybersecurity Principles*) onde determina que todos os órgãos do executivo norte americano implemente o ZT até o final do ano fiscal de 2024 [9].

A Figura 2.2 representa graficamente uma linha do tempo com os principais eventos do ZT.

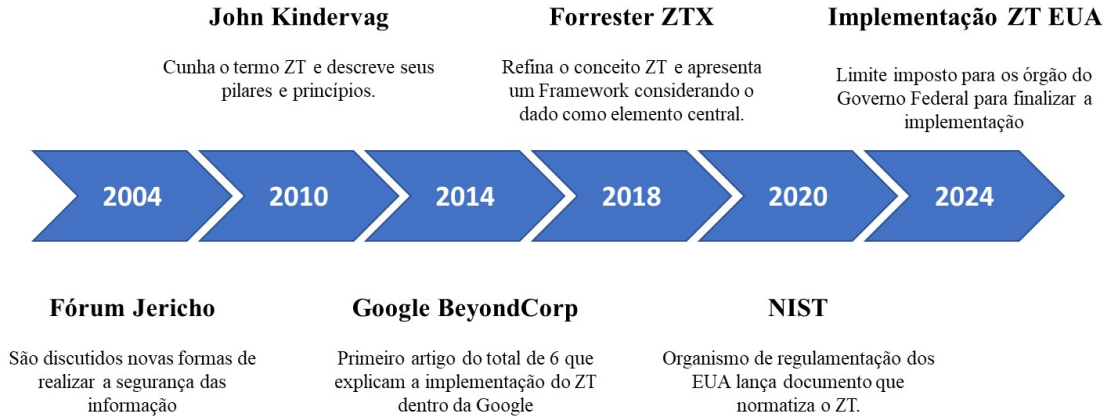

Figura 2.2: *Timeline* eventos ZT.

Conforme descrito pelo NIST, o ZT fornece uma coleção de conceitos e ideias destinadas a minimizar a incerteza na aplicação de decisões precisas e menos privilegiadas de acesso por solicitação em sistemas e serviços de informação, diante de uma rede vista como comprometida [22].

O *National Security Telecommunications Advisory Committee* (NSTAC) apresenta o ZT como um uma estratégia de segurança cibernética suportada pela premissa que nenhum usuário ou ativo devem possuir uma confiança implícita. Pelo contrário, ele considera que uma falha de segurança já ocorreu ou está prestes a ocorrer, desta maneira um usuário não deve receber permissão de acesso a informações sensíveis simplesmente com uma simples verificação no perímetro de uma organização [9].

A ZTA é uma estratégia de segurança cibernética adotada por organizações que se baseia nos princípios do ZT e engloba a interconexão entre os componentes, o planejamento dos fluxos de trabalho e as políticas de acesso. Dessa forma, em uma empresa que implementa o ZT, a infraestrutura de rede e as políticas operacionais vigentes são consideradas elementos essenciais de uma estratégia de ZTA. A abordagem da ZTA reflete a tendência de focar na proteção dos recursos, em vez de depender exclusivamente de perímetros de rede, uma vez que a localização da rede já não é considerada o principal fator para garantir uma postura de segurança adequada [16, 22].

2.2.1 Google BeyondCorp

A Google, no decorrer de sua implementação, descreve em seis artigos como realizou a implementação da ZTA dentro de sua corporação:

1. Apresenta as dificuldades observadas com o crescimento de tecnologias, onde a segurança de perímetro começou a se tornar cada vez mais difícil. Assim, a Google começou a mudar seu conceito de segurança transferindo suas aplicações para a Internet, dispensando a necessidade de se ter uma rede cheia de privilégios. Esta nova estrutura, representada na Figura 2.3 é composta de diversos componentes atuando em conjunto, com o propósito de realizar um controle de acesso às aplicações apenas a pessoas e equipamentos autorizados. As verificações ocorrem de modo que se identifique de maneira segura os dispositivos e usuários; remova a confiança da rede; externalize as aplicações e fluxos de trabalho; e implemente um controle de acesso baseados em inventário [23].

2. Resume a maneira na qual a Google mudou sua infraestrutura de segurança tradicional para o modelo BeyondCorp, os desafios encontrados e as lições aprendidas com o processo [24].

3. Descreve a infraestrutura de *front-end* focada em um Proxy de Acesso. Também descreve alguns projetos que estão em andamento no intuito de melhorar a experiência do usuário para seus funcionários acessando aplicações internas [25].

4. Discute como a Google saiu de uma rede legada para o modelo BeyondCorp, mudando os fundamentos de acesso à rede, sem a redução de produtividade [26].

5. Aborda a experiência do usuário com a implementação do Google BeyondCorp [27].

6. Descreve sobre como manter um parque computacional seguro [28].

Desta maneira, os seguintes controles foram observados pela Google durante sua jornada de implementação de sua ZTA [23]:

- **Dispositivo**: A identificação segura do dispositivo (*Securely Identifying the Device*) consiste de dois processos. Neste diapasão é utilizado o conceito de dispositivo gerenciado, sendo estes dispositivos os únicos capazes de acessar suas aplicações corporativas. Aliado ao conceito de dispositivo gerenciado, cada dispositivo tem um certificado específico.

- **Usuário**: Da mesma maneira, a identificação segura do usuário (*Securely Identifying the User*) é realizada em duas etapas. Todos os funcionários são cadastrados em um banco de dados de usuários e de grupos, sob a supervisão do departamento de Recursos Humanos (RH). Assim, consegue-se manter o banco de dados sempre atualizado, garantindo, desta maneira, informações precisas sobre os usuários que necessitam acessar as informações da empresa. A partir dai vem a próxima etapa, um portal de autenticação valida as credenciais e um segundo fator para as solicitações de acesso. Com a confirmação das informações, um *token* de curta duração é gerado como parte do processo de autorização para recursos específicos.

- **Rede**: Em se tratando de rede, a remoção da confiança das redes (*Removing Trust from Network*) cria uma rede sem privilégios semelhante a redes externas, embora dentro de um espaço privado. Nela o acesso a Internet é realizado de maneira limitada a alguns serviços (DNS, DHCP e NTP, por exemplo) e a um sistema de gerenciamento de conexão. Além disso, servidores RADIUS são utilizados para atribuir dinamicamente dispositivos a uma Rede Local Virtual (VLAN em inglês)

apropriada. Os certificados dos dispositivos gerenciados são enviados durante a conexão utilizando o protocolo 802.1x.

- **Aplicações**: Para que se tenha uma externalização de aplicações e fluxo de trabalho (*Externalizing Applications and Workflows*) elas são acessadas através de um *proxy* de acesso voltado para a Internet com utilização de criptografia entre o cliente e a aplicação. Ele que distribui de maneira adequada as solicitações à aplicação após uma verificação de controle de acesso. Todas estas aplicações são hospedadas na Internet, possuindo DNS próprio e CNAME apontando para o proxy de acesso voltado à Internet.

- **Controle de Acesso**: Finalmente para a implementação do controle de acesso baseado em inventário (*Implementing Inventory-Based Access Control*) considera-se que o nível de acesso concedido a um simples usuário pode mudar durante o tempo, sendo este utilizado na verificação de controle de acesso. Um mecanismo de controle de acesso fornece autorização de nível de serviço para aplicativos corporativos por solicitação. A decisão de autorização faz verificações sobre o usuário, os grupos aos quais o usuário pertence, o certificado do dispositivo e os artefatos do dispositivo do banco de dados de inventário de dispositivos. Os níveis de confiança do usuário e do dispositivo também fazem parte desta verificação. Além disso, este mecanismo é capaz de restringir o acesso a partes de uma aplicação.

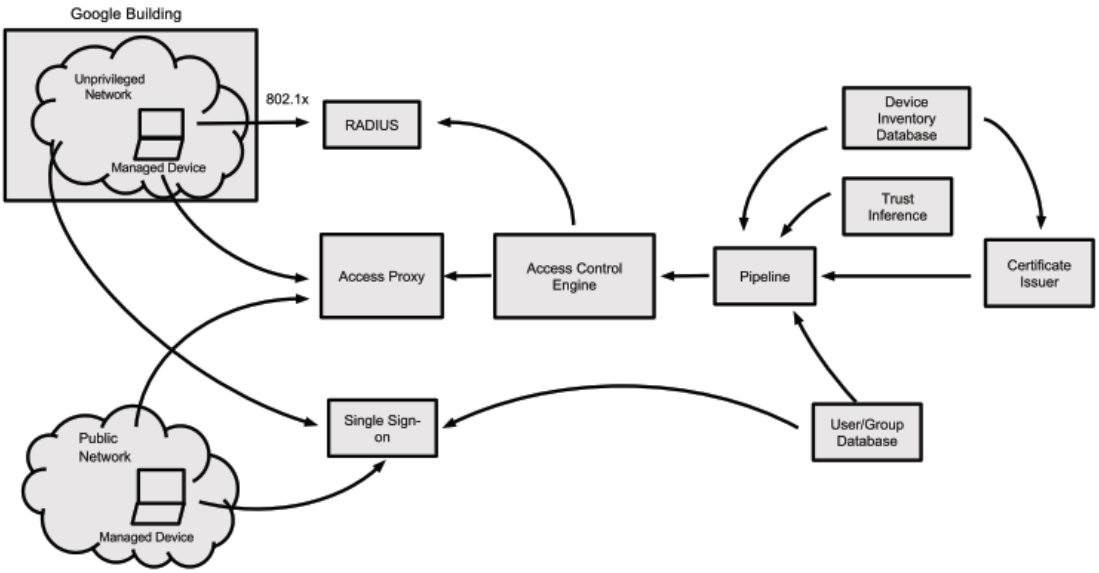

Figura 2.3: Diagrama Google BeyondCorp. Fonte: [23]

2.2.2 Microsoft e sua ZTA

A ZTA proposta pela Microsoft pode ser representada pelo diagrama, apresentado na Figura 2.4, cujos principais pilares são os seguintes [29]:

- **Identidade**: Algumas organizações confiam em sistemas de gerenciamento de identidades antigos.

Estes tornam difícil para as pessoas acessarem aplicativos e dados que precisam e criam brechas de segurança ao conceder privilégios excessivos.

- ***Endpoints***: As empresas atuais têm uma diversidade de equipamentos e dispositivos acessando seus dados, entretanto nem todos eles pertencem à corporação ou são gerenciados por elas. Com isso, uma superfície de ataque pode surgir visto que nem todos acabam tendo as soluções de segurança atualizadas.
- **Rede**: Não estamos mais em uma era de rede claramente definida para um determinado local. Proteger esse portfólio é um desafio para muitas empresas, que geralmente têm pouca segurança de rede, além de proteção mínima contra ameaças e tráfego interno não criptografado.
- **Aplicações**: Com as aplicações agora sendo acessadas através da nuvem e de dispositivos móveis, a superfície de ataque expandiu consideravelmente. Para protegê-la são necessárias modernas capacidades de detecção de ameaças.
- **Dados**: O crescimento do número de pessoas utilizando o teletrabalho aliado com o avanço em aplicações na nuvem, torna-se necessário novas ferramentas para proteger os dados que trafegam fora dos perímetros de segurança das corporações. Desta forma, para garantir uma proteção e acesso aos dados restrito apenas a pessoas credenciadas, eles devem ser classificados, etiquetados e, na medida do possível, criptografados.
- **Infraestrutura**: A dificuldade na proteção deste ambiente decorre do gerenciamento manual de permissões e de uma falta na configuração eficaz de máquinas virtuais e servidores. Assim, cresce de importância a proteção da infraestrutura com soluções de segurança que reconheçam ameaças conhecidas e desconhecidas e se adaptem para preveni-las em tempo real.

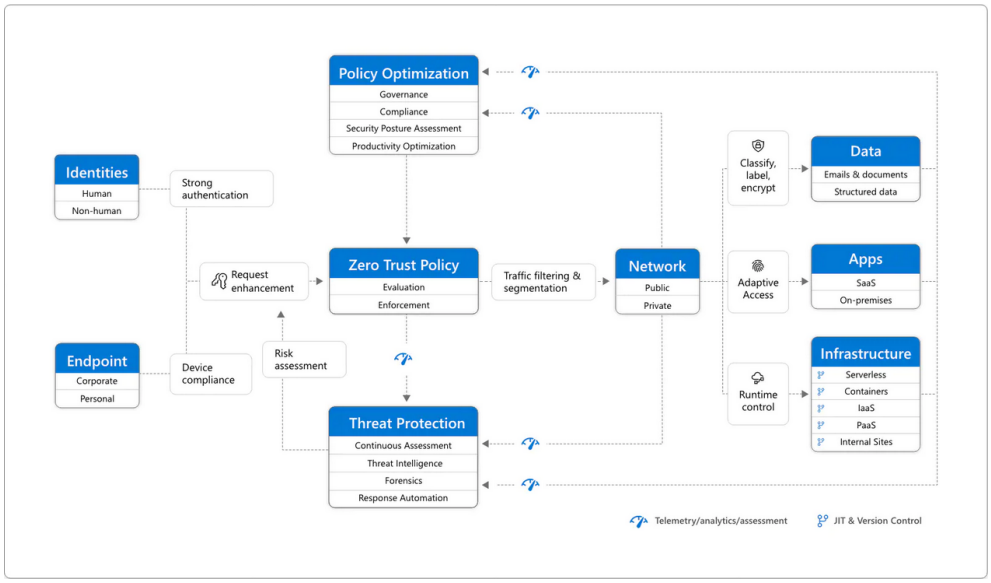

Figura 2.4: Diagrama ZT da Microsoft. Fonte: [30]

A Microsoft, em dois anos de utilização de seu modelo ZT (de 2019 a 2021), reporta que aprendeu cinco lições importantes [30]:

1. É possível melhorar a experiência do usuário e a produtividade utilizando o ZT;
2. Deve-se implementar o ZT em todo seu patrimônio digital;
3. Deve-se integrar a verificação e controles através de pilares de segurança;
4. Deve-se monitorar sua postura de segurança através de uma governança forte; e
5. Deve-se automatizar para simplificar e fortalecer sua postura de segurança.

2.2.3 *National Institute of Standards and Technology* (NIST)

O NIST definiu ZT e ZTA em termos dos seguintes princípios básicos, como sendo um objetivo, mas sabendo que dependendo da estratégia a ser tomada nem todos os princípios serão plenamente implementados [22]:

1. Todas as fontes de dados e serviços de computação são considerados recursos;
2. Toda a comunicação é segura, independentemente da localização da rede;
3. O acesso a recursos empresariais individuais é concedido por sessão;
4. O acesso aos recursos é determinado pela política dinâmica - incluindo o estado observável da identidade do cliente, aplicativo/serviço e o ativo solicitante - e pode incluir outros atributos comportamentais e ambientais;
5. A empresa monitora e mede a integridade e a postura de segurança de todos os ativos de propriedade e associados;
6. Todas as autenticações e autorizações de recursos são dinâmicas e rigorosamente aplicadas antes que o acesso seja permitido; e
7. A empresa coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as usa para melhorar sua postura de segurança.

Em sua padronização, a ZTA do NIST foi dividida em dois grandes planos: Plano de Controle, responsável por realizar as transmissões relacionada às solicitações de acesso; e Plano de Dados que realiza tarefas de controle de acesso [22]. A Figura 2.5 ilustra o *framework* conceitual e as relações básicas entre os componentes e suas interações.

O Plano de controle apresenta um componente central, chamado de *Police Decision Point* (PDP), composto pelos seguintes componentes: *Policy Administrator* (PA) (responsável por estabelecer ou finalizar o caminho de comunicação entre um sujeito e um recurso) e *Policy Engine* (PE) (responsável pela decisão final de conceder ou não o acesso a um determinado recurso). A atuação do PA e PE é conjunta, ou seja, enquanto o PE decide aprovar ou rejeitar uma solicitação de conexão e registrar sua ação, o PA, baseado nesta decisão, configura ou não o *Police Enforcement Point* (PEP) para realizar a seção [22].

O Plano de Dados tem como principal componente o PEP. Sua atribuição é habilitar, monitorar e eventualmente encerrar as conexões entre os sujeitos e os recursos de organização [22].

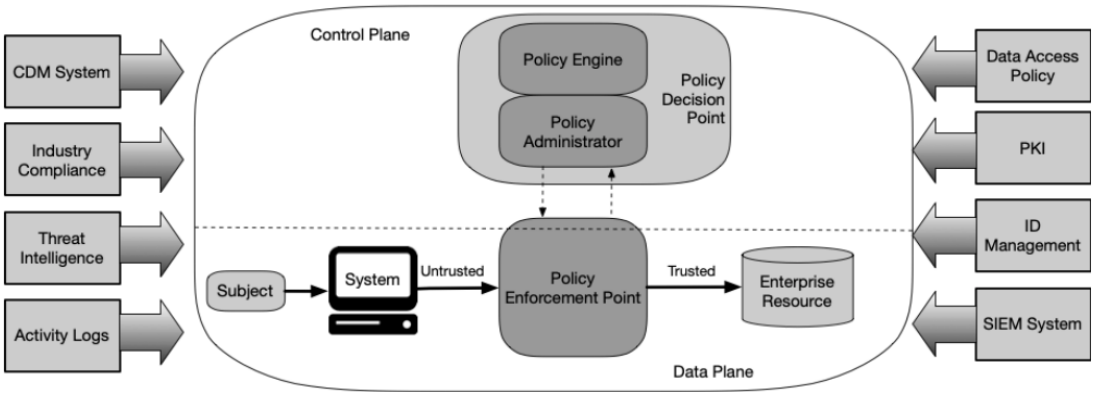

Figura 2.5: Componentes Lógicos *Zero Trust* do NIST. Fonte: [22]

2.2.4 ZTA proposta pelo DoD

Vulnerabilidades expostas por violações de dados dentro e fora de uma corporação demonstram a necessidade de um modelo de segurança cibernética novo e mais robusto que facilite decisões baseadas em risco bem informadas [6]. Neste pensamento, o *Department of Defense* (DoD) [6] define o ZT como uma estratégia de segurança cibernética que incorpora princípios de segurança em toda a corporação para prevenir, detectar, responder e recuperar-se de atividades cibernéticas maliciosas.

Em seu conceito de ZTA, o DoD cita cinco princípios: Assuma um ambiente hostil; Presumir violação; Nunca confie, sempre verifique; Examinar Explicitamente; e Aplicar Análise Unificada [6]. Ainda segundo [6], sua arquitetura é baseada nos seguintes pilares, que permitem o máximo de visibilidade e proteção dos dados (foco principal de qualquer implementação do ZT), conforme mostrado na Figura 2.6:

- **Usuário**: As organizações precisam da capacidade de autenticar, autorizar e monitorar continuamente os padrões de atividade para controlar o acesso e os privilégios dos usuários, protegendo e protegendo todas as interações.
- **Dispositivo**: Ter a capacidade de identificar, autenticar, autorizar, inventariar, isolar, proteger, remediar e controlar todos os dispositivos é essencial em uma abordagem ZT. A certificação em tempo real e a correção de dispositivos em uma empresa são funções críticas. Algumas soluções como os programas *Mobile Device Managers* ou *Comply to Connect* fornecem dados que podem ser úteis para a avaliação da confiança dos dispositivos. Outras avaliações devem ser realizadas para cada solicitação de acesso (por exemplo, exames de estado de compromisso, detecção de anomalias, versões de software, status de proteção, habilitação de criptografia, etc.).
- **Network/Environment**: Segmentar (tanto lógica como fisicamente), isolar e controlar a rede/ambiente (no local e fora do local) com acesso granular e restrições políticas. Como o perímetro se torna mais granular através da macro-segmentação, a micro-segmentação proporciona maiores proteções e controles sobre o *Desktop as a Service* (DAAS). É fundamental para: Controlar acesso privilegiado; Gerenciar fluxos de dados internos e externos; e Evitar movimentos laterais.
- **Application & Workload**: As aplicações e cargas de trabalho incluem tarefas em sistemas ou ser-

viços no local, bem como aplicações ou serviços executados em um ambiente de nuvem. As cargas de trabalho do ZT abrangem toda a pilha de aplicações desde a camada de aplicação até o hipervisor. A segurança e o gerenciamento adequado da camada de aplicação, bem como os contêineres de computação e as máquinas virtuais, são fundamentais para a adoção do ZT. Métodos de entrega de aplicações, tais como tecnologias *proxy*, permitem que proteções adicionais incluam pontos de decisão e aplicação do ZT. O código fonte desenvolvido e as bibliotecas comuns são controlados através das práticas de Desenvolvimento, Segurança e Operações (DevSecOps em inglês) para proteger as aplicações desde o início.

- **Dados**: O ZT protege dados, ativos, aplicações e serviços críticos. Um entendimento claro do DAAS de uma organização é fundamental para uma implementação bem sucedida de uma arquitetura ZT. As organizações precisam categorizar seu DAAS em termos de criticidade de missão e usar essas informações para desenvolver uma estratégia abrangente de gerenciamento de dados como parte de sua abordagem geral do ZT. Isto pode ser alcançado através da categorização dos dados, desenvolvendo esquemas e criptografando os dados em repouso e em trânsito. Soluções como *Data Rigths Managements* (DRM), *Data Loss Prevention* (DLP), *Software Defined Storage* (SDS) e marcação de dados granulares são relevantes na proteção de dados críticos.

- **Visibility & Analytics**: Os detalhes vitais e contextuais proporcionam uma maior compreensão do desempenho, comportamento e linha de base da atividade em outros pilares do ZT. Esta visibilidade melhora a detecção de comportamentos anômalos e proporciona a capacidade de fazer mudanças dinâmicas na política de segurança e decisões de acesso em tempo real. Além disso, outros sistemas de monitoramento, tais como dados de sensores, além da telemetria, serão usados e ajudarão a preencher a imagem do que está acontecendo com o ambiente e ajudarão no acionamento do uso de alertas para resposta. Uma empresa com ZT capturará e inspecionará o tráfego, olhando além da telemetria da rede e dentro dos próprios, pacotes para descobrir com precisão o tráfego na rede e observar as ameaças que estão presentes e orientar as defesas de forma mais inteligente.

- **Automation & Orchestration**: Automatizar os processos manuais de segurança para tomar ações baseadas em políticas em toda a empresa com rapidez e em escala. *Security Orchestration Automation Response* (SOAR) melhora a segurança e diminui o tempo de resposta. A orquestração de segurança integra o *Security Information and Event Management* (SIEM) e outras ferramentas automatizadas de segurança e auxilia no gerenciamento de sistemas de segurança díspares. A resposta automatizada de segurança requer processos definidos e aplicação consistente da política de segurança em todos os ambientes de uma empresa com ZT para fornecer comando e controle pró-ativos.

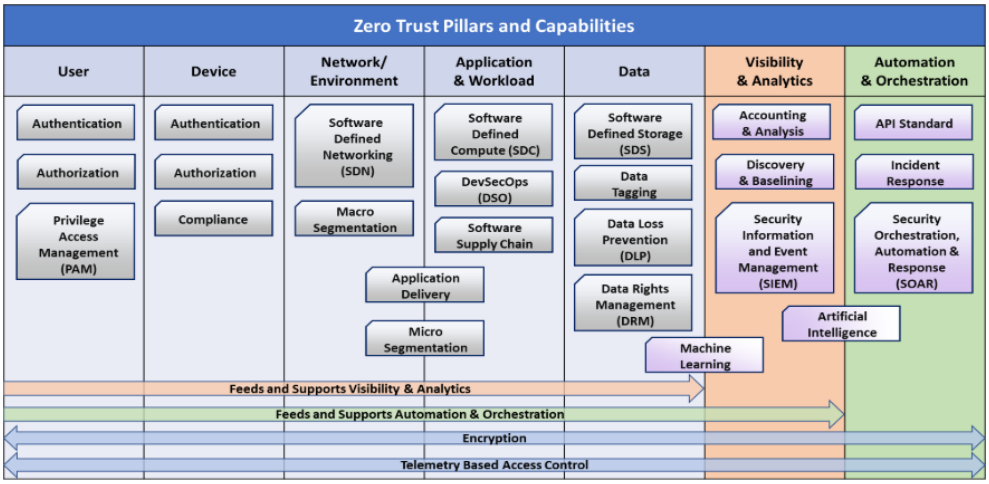

Figura 2.6: Pilares e capacidades do ZT do DoD. Fonte: [6]

2.2.5 O modelo de maturidade da *Cybersecurity and Infrastructure Security Agency* (CISA)

O *Zero Trust Maturity Model* (ZTMM) da *Cybersecurity and Infrastructure Security Agency* (CISA) representa uma implementação gradativa suportada em cinco pilares: Identidade, Dispositivos, Rede, Aplicativos e Carga de Trabalho e Dados, ilustrados na Figura 2.7 [9]:

- **Identidade**: Uma identidade refere-se a um atributo ou conjunto de atributos que descreve exclusivamente um usuário ou entidade da organização, incluindo entidades não pessoais;
- **Dispositivos**: Um dispositivo refere-se a qualquer ativo (incluindo seu hardware, software, firmware etc.) que pode se conectar a uma rede, incluindo servidores, desktops e laptops, impressoras, telefones celulares, dispositivos IoT, equipamentos de rede e muito mais;
- **Rede**: Uma rede refere-se a um meio de comunicação aberto, incluindo canais típicos, como redes internas do organizações, redes sem fio, redes e a Internet, bem como outros canais potenciais, como canais celulares e de nível de aplicativo usados para transportar mensagens;
- **Aplicativos e Carga de Trabalho**: Os aplicativos e as cargas de trabalho incluem sistemas da organização, programas de computador e serviços executados no local, em dispositivos móveis e em ambientes de nuvem; e
- **Dados**: Os dados incluem todos os arquivos e fragmentos estruturados e não estruturados que residem ou residiram em sistemas, dispositivos, redes, aplicativos, bancos de dados, infraestrutura e backups (incluindo ambientes locais e virtuais), bem como os metadados associados.

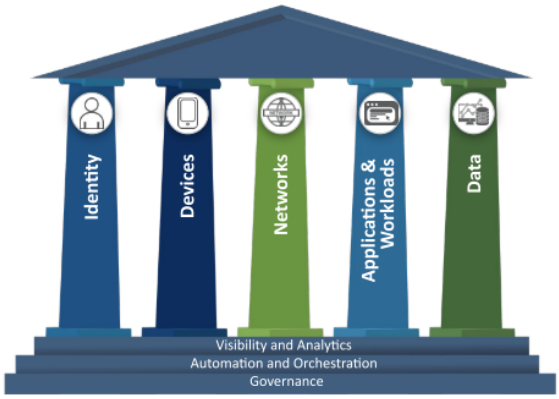

Figura 2.7: Pilares do Modelo de Maturidade da CISA. Fonte: [9]

A jornada de implementação do ZTMM da CISA ocorre em três etapas, de modo a facilitar seu desenvolvimento, com o ponto inicial partindo da implementação tradicional, subindo para a inicial, avançada e ótima. Além disso, à medida que um estágio é alcançado, níveis mais altos de proteção são necessários para alcançar o próximo ponto [9].

As organizações devem usar os seguintes critérios orientadores de cada estágio para identificar a maturidade para cada pilar de tecnologia de confiança zero e fornecer consistência em todo o modelo de maturidade[9]:

- **Tradicional**: Quando os controles dos pilares são implementados de maneira manual, assim como as políticas e soluções de segurança são aplicadas a um pilar, com pouca dependência de sistemas externos;
- **Inicial**: Há um início da utilização de automação dos processos. Além disso, começa a ocorrer uma interoperabilidade entre os pilares a partir da integração com sistemas externos;
- **Avançada**: Onde é possível, utiliza-se controles automatizados para a atribuição de controles e políticas, com uma integração entre os pilares. Há uma mudança para reduzir o privilégio baseada em avaliação de risco e da postura do usuário; e
- **Ótima**: Controles são completamente automatizados concedendo atributos a ativos e recursos com autorrelação à políticas dinâmicas. Esta automatização ocorre, também, na definição de privilégios mínimos para acesso aos ativos da organização.

2.2.6 Resumo dos controles utilizados nas implementações descritas

Os controles encontrados nas implementações da ZTA da Google e da Microsoft, bem como aqueles apresentados nas padronizações do NIST, DoD e CISA, estão resumidos na Tabela 2.1. O NIST não considera, em sua padronização, controles bem específicos, mas sim componentes que realizam determinadas ações. Assim, não foi contemplado na Tabela.

Tabela 2.1: Resumo dos controles citados em cada modelo.

Controle	Google	Microsoft	NIST	DoD	CISA
Identidade	X	X	X	X	X
Dispositivo	X	X	X	X	X
Rede	X	X	X	X	X
Dados		X		X	X
Aplicações	X	X		X	X
Infraestrutura		X			
Controle de Acesso	X		X		

A partir desta tabela observa-se que os controles Identidade, Dispositivo, Rede e Aplicações são considerandos na implementação da ZTA da Google, Microsoft e nas padronizações do DoD e CISA, representando sua importância relacionado ao conceito ZT.

Em que pese a Google não considerar o controle Dados em sua implementação, ele é importante, visto que a Microsoft, o DoD e a CISA o fizeram. De certa forma isto é interessante, visto que os Dados podem ser considerados ums dos principais ativos que a implementação do ZTA pretente proteger.

2.2.7 Emprego do Zero Trust na proteção dos dados

Nesta seção será apresentada a evolução nas pesquisas sobre ZT no decorrer dos anos, entre 2010 e 2022. Assim, foram realizadas pesquisas com o termo ”Zero Trust” em quatro grandes bases de dados: ACM Digital Library, IEEE Xplore, Scopus e Web of Science. Os resultados obtidos nas pesquisas estão descritos na Tabela 2.2.

Analisando o resultado, observa-se que, somando as quatro base de dados consideradas, encontrou-se 1396 trabalhos escritos com a temática ZT. Além disso, depreende-se que até 2015 foram apenas 20 trabalhos escritos (cerca de 1,4% do total de trabalhos encontrados), mostrando que o assunto passou a ser mais pesquisado a partir de 2016, pouco depois que a Google começou a divulgar seus artigos.

Tabela 2.2: Evolução de trabalhos em Zero Trust

ACM Digital Library
Total: 123 artigos

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
0	1	1	2	1	2	5	1	5	9	11	24	61

IEEE Xplore
Total: 255 artigos

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
0	0	0	1	0	0	2	3	29	3	14	61	142

Scopus
Total: 827 artigos

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
0	0	1	2	5	4	8	10	26	32	79	225	435

Web of Science
Total: 191 artigos

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
0	0	0	0	0	0	2	3	6	4	13	60	103

A partir da Tabela 2.2, foi realizada a soma por ano e desenhada a linha de tendência dos artigos encontrados, representado pela Figura 2.8. Observa-se que o total de artigos escritos entre 2011 e 2015 apresenta uma certa estabilidade, variando entre 1 e 6 artigos e a partir de 2016 esse total passa a crescer. Além disso, há uma tendência positiva, representada pela linha laranja, no total de artigos escritos no decorrer dos anos sobre o ZT.

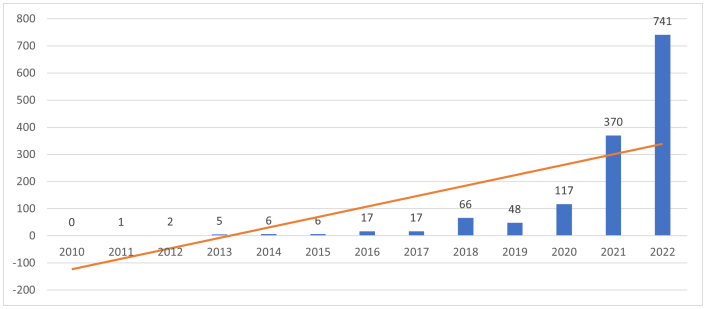

Figura 2.8: Total artigos encontrados por ano.

A partir dos dados apresentados na Tabela 2.2, foi gerada a Figura 2.9 que apresenta a média de artigos produzidos até o ano de 2022, ou seja, somou-se o total de artigos encontrados nas quatro bases de dados pesquisados e dividiu-se pelo total de anos. Percebe-se que mesmo tendo um crescimento na média de trabalhos escritos, este valor foi aparentemente constante e de certa forma baixo até o ano 2016/2017, aproximadamente, onde pode-se observar uma evolução na média. Assim, o ano de 2016 aparenta ser um marco histórico para os estudos sobre o ZT.

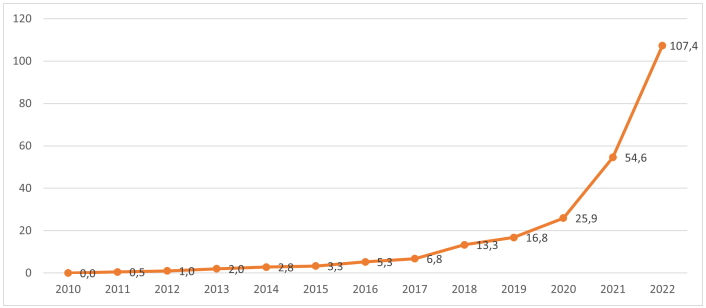

Figura 2.9: Média de artigos escritos.

2.2.7.1 Revisão Sistemática de Literatura (RSL)

Existem três grandes métodos para se realizar uma revisão: Análise Bibliométrica, Meta-Análise e Revisão Sistemática de Literatura. Dentre suas diferenças, o escopo do tema e o conjunto de dados estudados na Análise Bibliométrica e Meta-Análise são maiores que na Revisão Sistemática de Literatura [31].

Também, [31] descreve que não devemos utilizar a Análise Bibliométrica e a Meta-Análise quando o escopo de estudo é muito específico ou seu conjunto de dados é pequeno o suficiente de maneira que possa ser revisado manualmente. Assim, realizou-se uma RSL na busca de aumentar os conhecimentos sobre como ocorre a implementação da ZTA.

Além disso, segundo [16] dentre os diversos motivos para a realização de uma RSL, utiliza-se esse método de revisão para, após vasta busca em base de dados, entender como funciona um determinado assunto, sintetizando as informações em um conjunto de evidências a fim de obter-se conclusões robustas e sem viés.

Entretanto, a realização de uma RSL pode apresentar formatos diferentes, com conclusões distintas. Assim, alguns padrões para a RSL como PRISMA, CASP e MMAT foram descritos em[32]. Dentre esses padrões, o PRISMA é o mais utilizado nas mais diversas áreas de conhecimento [33], sendo ele o procedimento que foi utilizado no trabalho.

Observando as duas implementações anteriormente apresentadas (Google e Microsoft) e as duas padronizações (NIST e DoD), foi possível identificar uma separação em sete controles distintos que podem ser empregados na implementação de uma ZTA: Autenticação, Identidade, *Endpoints*, Dados, Rede, Aplicações e Infraestrutura [16].

2.2.7.2 Método PRISMA

O método PRISMA apresenta uma relação de procedimentos e itens que devem ser seguidos de maneira que, caso qualquer pesquisador deseje refazer a RSL, este consiga obter os mesmos resultados obtidos [32]. A última versão do método, apresentada em 2020, apresenta um *checklist* com 27 tópicos divididos em sete seções: Título, Resumo, Introdução, Metodologia, Resultados, Discussões e Outras Informações [34].

Inicialmente foi necessário estabelecer o objetivo principal da busca. No caso, tendo como base os sete controles encontrados, o foco foi verificar na literatura as diferentes maneiras de realizar a implementação da ZTA [16].

Sabendo qual o objetivo da pesquisa, estabeleceu-se as bases de dados para realizar a pesquisa. Dentre as diversas bases de dados disponíveis no acesso disponibilizado no portal da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), definiu-se as bases da IEEE Xplore e ACM Digital. Além delas terem seus artigos disponibilizados em sua integralidade no referido portal, a temáticas principal delas está relacionadas à assuntos ligados à Tecnologia da Informação [16].

O próximo passo foi estabelecer um intervalo de tempo. Considerando que o ano de 2016 apresentou o início do aumento dos estudos relacionados ao tema ZT, foi definido o intervalo entre Janeiro de 2016 e Junho de 2022 para a realização da RSL [16].

A etapa de elaboração da estratégia de busca é necessário estabelecer uma estratégia que envolva um conjunto de procedimentos capaz de localizar o máximo de artigos com a informação desejada [32]. Assim, considerando o objetivo da busca, os termos **implementação** e ***Zero Trust*** surgem como palavras chaves iniciais [16]. Contudo, as bases de dados utilizadas apresentam artigos, em sua maioria, no idioma inglês, o que nos remete a utilizar a palavra *implementation* no lugar de implementação. Além disso, para aumentar o retorno de artigos buscados, utilizou-se os seguintes sinônimos da palavra implementação: *deployment* e *development* [16].

Alguns operadores *booleanos* são utilizado para concatenar as palavras-chave de maneira a gerar estratégias avançadas de busca. Assim foram utilizados os operadores * e *AND*, para substituir partes da palavra e gerar a intersecção entre as palavras, respectivamente [32]. Com isso os termos utilizados nas buscas foram: *"zero trust" AND implement**, *"zero trust" AND deploy** e *"zero trust" AND develop** [16]. Foram realizadas três pesquisas distintas em cada base de dados, sendo a distribuição no decorrer do período selecionado apresentada na Figura 2.10 e totalizando 268 artigos encontrados.

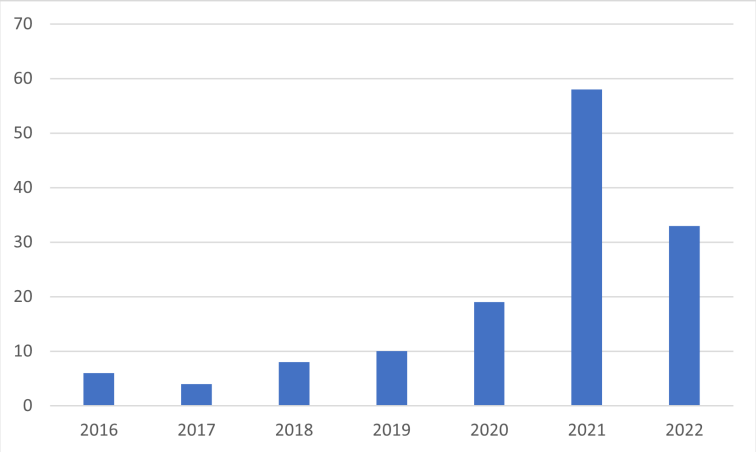

Figura 2.10: Distribuição do resultado da pesquisa entre 2016 e 2022.

Na sequência, o [34] estabelece um procedimento de avaliação dos artigos até chegar ao conjunto final de artigos selecionados. Os procedimentos estão sintetizados na Figura 2.11 e descritos abaixo. Para a caracterização de cada artigo, utilizou-se o Rayyan, uma plataforma integrada com inteligência artificial desenvolvida para o auxílio na realização de RSL [35]. Ela é capaz de atribuir etiquetas aos arquivos importados de maneira automática, segundo padrão estabelecidos pelo utilizador e observados de maneira automática. O funcionamento da plataforma acontece através da importação de um arquivo contendo as principais informações de cada artigo: Título, Nome dos Autores, Ano de Publicação, Local de Publicação,

entre outros. A partir da importação, o sistema de inteligência artificial do site, realiza relacionamento e atribuição de etiquetas, que podem ser editadas para melhorar/alterar os dados categorizados pelo sistema.

Assim o processo de exclusão dos artigos foi realizado em uma etapa automática e três etapas manuais. Inicialmente, de maneira automática, retirou-se do cômputo total 130 artigos que foram retornados da busca de maneira duplicada, pois foram realizadas três buscas em cada base, conforme citado anteriormente. O processo é realizado através da comparação de informações de cada artigo, como por exemplo, título, autor e DOI, características únicas de cada um [16].

Uma primeira filtragem, já manual, consistiu na busca no título, resumo e palavras-chave dos artigos, das palavras-chave utilizadas nas buscas, sendo retirados aqueles que não continham pelo menos uma das palavras-chave utilizadas: *Zero Trust*, *implementation*, *deployment* e *development* [16].

A segunda passagem buscou retirar artigos não disponibilizados de maneira integral e textos de revistas e livros. Para esta etapa, foi necessário realizar o *download* de cada artigo das duas bases de dados consultadas [16]. O acesso ao repertório das bases de dados utilizando o portal da CAPES facilitou bastante esta etapa, considerando a possibilidade de realizar o *download* de múltiplos trabalhos de uma única vez.

Finalmente, ocorreu a leitura do resumos dos artigos. A busca foi por textos que, mesmo apresentando pelo menos uma das palavras utilizadas na busca, não apresentavam semelhança com o contexto da pesquisa [16]. Isto mostra que o termo ZT também é empregado em outros contextos, não apenas relacionados à segurança cibernética.

O processo descrito está apresentado, de maneira sintética, na Figura 2.11.

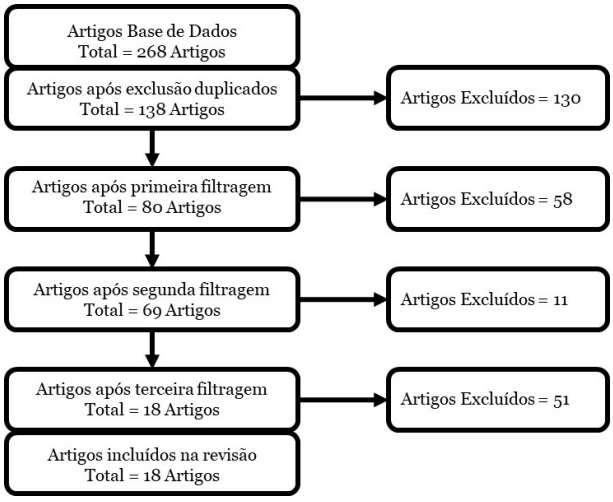

Figura 2.11: Fluxograma da Revisão. Fonte: [16]

Realizando uma comparação entre o total de artigos encontrados inicialmente (total de 138 artigos, desconsiderando os duplicados) e o resultado final (18 artigos), observa-se que apenas 15% do total de artigos encontrados foram incluídos na RSL. Isso ocorreu pois o termo ZT não é empregado apenas na temática de Segurança Cibernética, fato este observado durante a leitura dos trabalhos.

Além disso, a Figura 2.12 nos mostra que o espectro de artigos encontrados e filtrados cresceu no decorrer dos anos. Isto nos mostra uma maior busca no conhecimento acerca desta nova maneira de realizar a Segurança Cibernética, considerando seu pouco tempo que foi "criada".

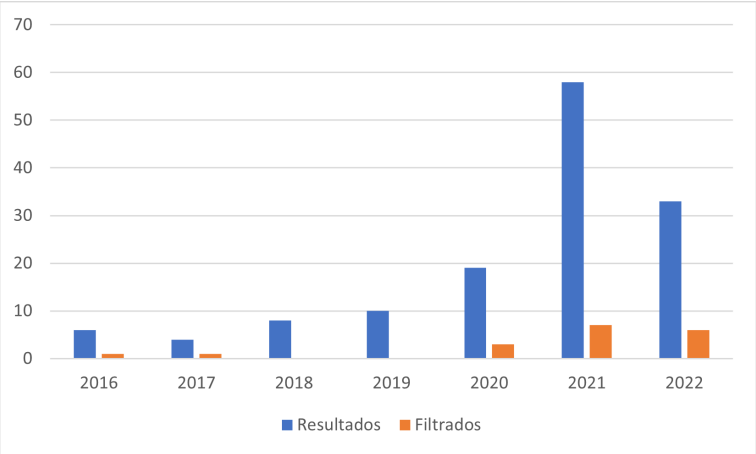

Figura 2.12: Gráfico comparação resultado e filtrados.

2.2.7.3 Resultados obtidos

Após o término da última filtragem, iniciou-se uma leitura mais aprofundado de cada um dos 18 artigos, com o propósito de levantar qual das sete dimensões o artigo aborda. Com isso, a Tabela 2.3 apresenta, em totais e percentual, o número de artigos e os autores considerados. Interessante perceber que, um artigo pode abordar mais de uma dimensão, desta maneira, a soma dos artigos e de seu percentual extrapola 18 e 100% respectivamente [16].

Tabela 2.3: Visão Global dos tópicos

Dimensões	Total de Artigos	Autores
Autenticação	10 (56%)	[36, 37, 38, 39, 40, 41, 42, 43, 44, 45]
Identidade	05 (28%)	[36, 38, 46, 47, 48]
Endpoints	02 (11%)	[36, 38]
Dados	05 (28%)	[36, 38, 41, 43, 44]
Rede	11 (61%)	[38, 49, 39, 41, 50, 43, 47, 51, 52, 44, 53]
Aplicações	04 (22%)	[36, 38, 43, 47]
Infraestrutura	00 (00%)	

Fonte: Adaptado de [16]

A partir dos dados observados na Tabela 2.3, os autores [16] concluíram que, dentro das bases de dados buscadas, existe a ausência de dois tópicos:

- Artigos descrevendo, mesmo que de maneira sucinta a implementação do controle Infraestrutura; e
- Maneiras de gerenciar e organizar a implementação dos controles do ZT, utilizando-se de métodos estruturados e sistematizados. Dessa maneira, mostra-se, também, uma outra lacuna.

Esta segunda conclusão é interessante e gerou o contexto inicial do artigo [15].

2.3 GESTÃO DE RISCOS

A ISO 31000 é uma norma internacional criada em 2009 pela *International Organization for Standardization* (ISO) que apresenta diretrizes para a gestão de riscos dentro de empresas de qualquer segmento e tamanho. Ela teve sua redação revisada e atualizada em 2018 [12].

O risco é definido como o efeito da incerteza sobre os objetivos. Já a gestão de risco são as atividades coordenadas para dirigir e controlar uma organização no tocante a riscos, tendo como propósito a criação e proteção de valor, melhorando o desempenho no alcance de objetivos [12].

A gestão de risco é orientada por 8 princípios capazes de proporcionar uma base sólida para o sucesso da implementação da gestão de risco em uma corporação [12, 54]. Sumarizados na Figura 2.13, os princípios são:

1. Integrada: A gestão de risco deve ser parte integrante de todos os processos organizacionais e tomada de decisão, em todos os níveis.
2. Estruturada e abrangente: A gestão de risco deve ser um processo sistemático, estruturado e abrangente de maneira a gerar resultados consistentes e comparáveis.
3. Personalizada: A gestão de risco deve considerar tanto o contexto interno quanto o externo em que a organização opera, relacionando-os com seus objetivos.
4. Inclusiva: A gestão de risco deve procurar envolver todos os interessados, levando em consideração suas experiências.
5. Dinâmica: A gestão de risco deve estar atenta às mudanças que os riscos podem sofrer, sendo capaz de atuar antecipadamente de uma maneira oportuna.
6. Melhor informação disponível: A gestão de risco deve incluir uma comunicação clara e transparente em todos os níveis da organização, bem como com partes interessadas pertinentes.
7. Fatores humanos e culturais: A gestão de risco deve envolver a participação e consulta de todas as partes interessadas relevantes, incluindo funcionários, clientes, fornecedores e outras partes externas.
8. Melhoria contínua: A gestão de risco deve ser parte de um processo de melhoria contínua da organização, visando aprimorar a eficácia, eficiência e adaptabilidade da gestão de risco.

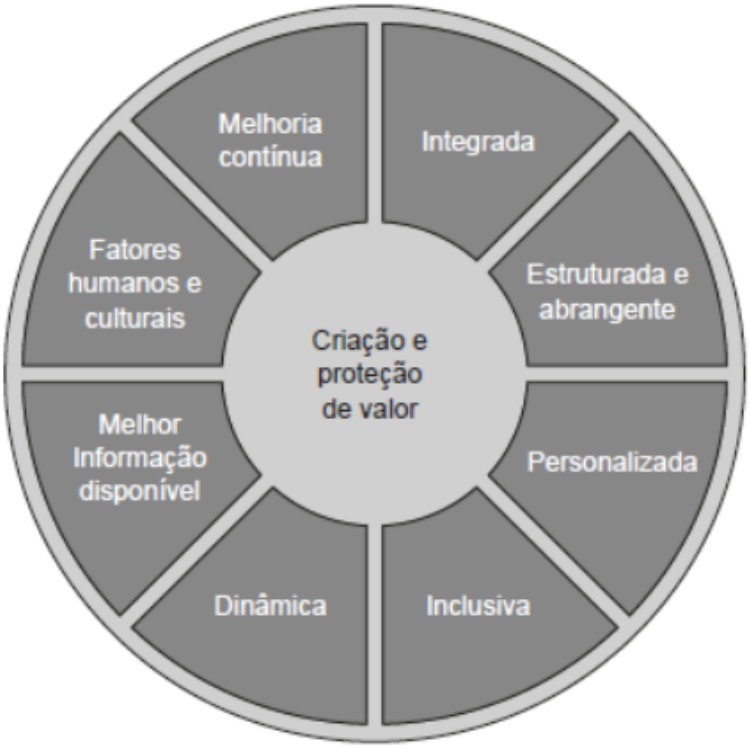

Figura 2.13: Princípios da gestão de riscos. Fonte: [12]

Como um suporte aos conceitos apresentados na ISO 31000, a ISO 31010 foi elaborada com o propósito de orientar os decisores com a seleção de procedimentos e técnicas para o processo de avaliação de riscos [13].

Dentre as mais de 30 ferramentas utilizadas no processo de avaliação de riscos, é descrito a análise de decisão por multicritério, cujo principal objetivo é, a partir de um conjunto de critérios estabelecidos, apresentar uma ordem de preferência entre as opções disponíveis [13].

O processo de avaliação de riscos é capaz de fornecer aos decisores conhecimentos acerca dos riscos que podem afetar os objetivos de uma corporação. Além disso, proporciona informações sobre os controles que estão em uso. Assim, é possível tomar uma decisão mais precisa na prevenção de um determinado risco [13].

Este processo é realizado em três etapas: Identificação de Risco, Análise de Risco e Avaliação de Riscos. Conforme apresentado na Tabela 2.4, o MCDA apresenta-se como uma ferramenta apta a ser utilizada nestas etapas [13].

Este método pode ser utilizado para [13]:

- comparar múltiplas opções para uma primeira análise para determinar opções preferenciais e potenciais e as inapropriadas;
- comparar opções onde existam critérios múltiplos e, algumas vezes, conflitantes; e
- alcançar um consenso sobre uma decisão onde diferentes partes interessadas têm objetivos ou valores conflitantes.

Tabela 2.4: Aplicabilidade do MCDA no processo de avaliação de riscos

Ferramenta e técnica	Processo de avaliação de riscos				
	Identificação de riscos	Análise de riscos			Avaliação de riscos
		Consequência	Probabilidade	Nível de risco	
Análise de decisão por multicritérios (MCDA)	A	FA	A	FA	A

FA - Fortemente aplicável
A - Aplicável
NA - Não Aplicável
Fonte: [13]

Os métodos multicritérios apresentam os seguintes pontos fortes [13]:

- fornece uma estrutura simples para uma tomada de decisão eficaz e apresentação de premissas e conclusões;
- pode tornar mais gerenciáveis os problemas de decisão complexos, que não são passíveis de aná- lise de custo/benefício;
- pode auxiliar a considerar racionalmente os problemas onde concessões (trade offs) precisam ser efetuadas; e
- pode auxiliar a atingir um acordo quando as partes interessadas têm objetivos e, consequente- mente, critérios diferentes.

Como pontos fracos, a mesma norma descreve [13]:

- pode ser afetada por viés e por má seleção dos critérios de decisão;
- a maioria dos problemas da MCDA não tem uma solução conclusiva ou única; e
- algoritmos de agregação que calculam os critérios de ponderação a partir de preferências estabelecidas ou agregam diferentes pontos de vista podem obscurecer a verdadeira base da decisão.

2.4 MÉTODOS MULTICRITÉRIO DE APOIO À DECISÃO

A Seção 2.3, apresentou o Método Multicritério de Apoio à Decisão como uma possível solução no processo de avaliação de riscos. Além disso, a Seção 2.2.7 apresentou uma lacuna importante no emprego do ZT na proteção dos dados, visto que não foi encontrado artigo publicado nas bases de dados buscadas que orientam a implementação dos controles de uma ZTA. Os modelos apresentados, trazem um conjunto de controles que devem ser implementados com o propósito de garantir uma segurança mínima dos dados dentro de uma organização. Portanto, torna-se necessário aprofundar os conceitos sobre os diversos MCDA.

Os métodos multicritério começaram a ser estudados a partir década de 1970. Até este período, acreditava-se que existia uma solução ótima perante as demais, baseada em um único critério. Deste modo, estudos começaram a ser realizados com o propósito de gerar conhecimentos sobre cenários complexos de modo para auxiliar os tomadores de decisão, mudando, assim, o maneira de assessorar os tomadores de decisão [55, 56].

Nesta época, duas comunidades científicas começaram a se consolidar em pesquisas realizadas com o foco na utilização de metodologias multicritérios: a americana (MCDM) e a europeia (MCDA). Elas foram influenciadas por suas diversidades culturais e ambientais [55].

A literatura atual apresenta diversas metodologias para a solução de problemas que envolvem múltiplos critérios. Contudo elas apresentam como fundamento umas destas duas escolas. A diferença principal entre as duas são [55]:

- **MCDM (Escola Americana)**: Como o ambiente científico era dominado por paradigmas mais racionais, esta metodologia tinha como foco a busca por uma solução ótima e uma informação objetiva quantitativa; e
- **MCDA (Escola Europeia):** Ela reconhecia os limites de uma abordagem puramente objetiva, visto que não era dominada por um paradigma racional. Assim, considerava que a tomada de decisão é uma atividade humana informada pela noção de valor.

Os diferentes MCDA são realizados de maneira que as partes interessadas realizem um processo onde os critérios são analisados de distintas maneira, conforme a metodologia empregada, e obtenham como saída do processo, uma ordenação das opções disponíveis [13].

Contudo, depois do emprego da metodologia, um novo critério pode surgir. Com esse novo dado, o ordenamento final dos critérios pode mudar. Alguns casos, após a inclusão deste novo critério gera uma alteração no resultado final, o que não é desejável pois pode mostrar uma fraqueza da metodologia utilizada. A alteração na ordenação final das opções é chamada de *Rank Reversal* (RR) [57].

Por exemplo, após a aplicação de uma metodologia multicritério, chegou-se a conclusão que A > B > C > D, ou seja que a situação A é melhor que a B, e assim por diante. O fenômeno conhecido como RR, ocorre quando, eu adiciono uma situação E, sabidamente pior que D, onde ela deve ficar após a opção D e isso não ocorre ou a sequência é alterada [57].

Com o passar dos anos, o MCDA desenvolveu diversos métodos e *software* para solução de problemas. Para utilização dos referidos métodos, procedimentos básicos tornam-se necessários: definição do problema, alternativas e critérios [58].

Os diferentes métodos existentes podem ser agrupados conforme distintos parâmetros. Isto ocorre uma vez que cada metodologia utilizada emprega sua própria forma de cálculo. Além disso, utilizando um mesmo conjunto de alternativas relacionadas a um determinado problema com diferentes metodologias não garante a obtenção de um mesmo resultado [58].

Os métodos multicritérios são amplamente utilizados nos mais variados setores, como por exemplo na aviação [59], educação [60], gestão de riscos [14, 61] transporte [62, 63], entre outros.

2.4.1 *Analytic Hierarchy Process* (AHP)

O AHP *Analytic Hierarchy Process* é um método multicritério utilizado na tomada de decisão, com origem na década de 1970 por Thomas Saaty, auxiliando os gestores a escolher e justificar sua escolha. Sua lógica esta lastreada na ideia de decompor um problema de tal maneira que se tenha um nível onde pode ser possível realizar comparações na definição da melhor opção [56]

A partir desta decomposição hierárquica, o AHP é realizado em três etapas principais [64]:

1. **Estruturação hierárquica**: Início do processo, onde a partir da identificação do decisor do problema a ser definido, são definidos os objetivos (nível mais alto), critérios e alternativas envolvidas na decisão;

2. **Comparação paritária**: Etapa onde são realizadas as comparações entre os elementos da estrutura hierárquica elaborada na etapa anterior. A comparação é realizada utilizando a Escala Fundamental de Saaty, apresentada na Tabela 2.5, onde é avaliado a importância de um elemento em relação ao outro; e

3. **Cálculo das propriedades**: Etapa na qual um conjunto de cálculos matemáticos é realizado para determinar as prioridades dos elementos a partir das comparações realizadas. Assim, um valor numérico é atribuído a um elemento, permitindo que os elementos possam ser ordenados de modo que o decisor consiga escolher a melhor solução do problema.

Tabela 2.5: Escala fundamental de Saaty.

Valor	Definição	Comentário
1	Igual importância	Os dois critérios contribuem igualmente para o objetivo.
3	Importância pequena de um para o outro	A experiência e o julgamento favorecem levemente um critério em relação ao outro.
5	Importância grande ou essencial	A experiência e o julgamento favorecem fortemente um critério em relação ao outro.
7	Importância muito grande ou demonstrada	O critério é muito fortemente favorecido em relação ao outro.
9	Importância absoluta	A evidência favorece um critério em relação ao outro com o mais alto grau de certeza.
2, 4, 6, 8	Valores intermediários	Quando se procura uma condição de compromisso entre as duas definições.

Fonte: Traduzido de [64]

2.4.2 *Characteristic Objects Method* (COMET)

O método COMET *Characteristic Objects Method* tem como objetivo encontrar os objetos característicos, ou seja, as alternativas que possuem características únicas em relação aos critérios de decisão. Para

isto, ele utiliza a teoria dos Conjuntos *Fuzzy* para analisar as relações entre as alternativas avaliadas e os critérios de decisão. Pode-se dizer que, por estes motivos, o método COMET é livre do problema de RR [65].

O método COMET é realizado em cinco etapas conforme descrito abaixo [66]:

1. **Definir o escopo do problema**: etapa onde são determinados a dimensão do problema, selecionado o total de critérios e após a seleção, um conjunto de números *Fuzzy*, obtido através da função de pertinência triangular *Fuzzy* são selecionados para cada critério;
2. **Gerar dos Objetos Característicos (OC)**: os OC são definidas realizando o produto cartesiano dos números triangulares de *Fuzzy* sendo obtido ao final um conjunto de OC;
3. **Ordenação e avaliação dos OC**: momento onde é definido pelos especialistas uma Matriz de Julgamento de Especialistas (MJE), que é o resultado da comparação dos OC com o conhecimento dos especialistas. Caso um OC tenha uma maior preferência, ele recebe 1 ponto. Caso a preferência seja igual, cada um recebe 0,5. O que não tem preferência, recebe 0.
4. **A regra básica**: cada OC e o valor de preferência, obtido na etapa anterior, são convertidos em uma regra *Fuzzy* e ordenados num vetor de Julgamentos Somados (JS).
5. **Interferência e o ordenamento final**: nesta última etapa são apresentados os valores finais, correspondendo ao conjunto de critérios definidos inicialmente, após a ordenação dos JS, que representam um valor aproximado da preferência para o CO.

Dentre as vantagens da utilização do COMET, pode-se citar que ele usa mais pontos de referência, sem necessitar da definição de pesos por parte dos decisores [65].

2.4.3 *Multi-Criteria Decision Aid - Constructivist* (MCDA-C)

O Método Multicritério de Apoio à Decisão Construtivista (MCDA-C) segue a linha de pensamento da escola europeia segundo uma vertente construtivista [67]. Diferentemente do conceito racionalista para a tomada de decisão, onde busca-se uma solução ótima para o problema, o construtivismo tem como objetivo apresentar informações para a construção do conhecimento do decisor para que ele tenha uma base sólida para tomar sua decisão [56, 68]

Assim, o MCDA-C é realizado em três fases distintas, a saber: Elaboração, onde o problema é estruturado e modelado; Avaliação, quando são construídos os critérios de avaliação; e Recomendações, onde são apresentados os entendimentos das fases anteriores [69]; e um total de 8 etapas, conforme ilustrado na Figura 2.14.

A fase da Elaboração visa fundamentalmente o estabelecimento de um mecanismo de comunicação entre os diversos atores envolvidos, que promova um entendimento, levando a uma linguagem comum entre eles. Ela é dividida em três etapas [70]:

- **Contextualização:** onde, após conversas e discussão é definido o tópico do problema [70] assim como a identificação dos atores envolvidos no processo decisório [67];

- **Hierarquização dos Valores:** quando o tópico do problema é dividido em *Fundamental Point of View* (FPV) e seus *Elementar Point of View* (EPV), construindo uma árvore hierárquica que serão utilizados como variáveis, ou controles, dentro do método multicritério. O detalhamento deve ser feito ao ponto que seja possível transformar o critério em escala ordinal [70]; e
- **Construção dos Descritores:** Transformação da estrutura hierárquica construída na etapa anterior em uma escala ordinal, devendo, ainda, ser definidos os níveis mínimo e bom para cada um dos EPV definidos [68].

Ao final desta fase, será possível observar uma estrutura contendo os pontos considerados importantes pelos decisores de modo a se ter uma avaliação da problemática considerada [68]

A fase da Avaliação visa fundamentalmente a construção de um modelo quantitativo multidimensional, onde, a partir de modelos matemáticos, cada controle é ponderado de acordo com a sua contribuição para a avaliação do desempenho global dos servidores em estudo. Ela é dividida em quatro etapas [70]:

- **Construção de Escala Cardinal e de Preferência:** A partir dos descritores elaborados na última etapa da fase anterior, é determinado o grau de atratividade entre os níveis dos descritores, ou seja, atribuído um valor numérico para cada descritor. Neste desenvolvimento, devem, também, ser definidos os pontos onde o descritor é neutro e bom [67];
- **Determinação das Taxas de Compensação:** Definição de valores que informam o grau de importância relativa que o decisor tem para um determinado FPV em comparação com outro FPV, bem como entre os EPV dentro de um determinado FPV [67]
- **Identificação do Perfil de Desempenho das Ações:** A partir do modelo finalizado, são enviados questionários para avaliar o ponto de vista dos *stakeholders* e, assim, ser capaz de analisar de maneira individual e global, cada um dos controles e dimensões do modelo [70].
- **Análise dos Resultados:** A partir das respostas e das Funções de Valor criadas no decorrer do processo, é calculado o valor global de cada EPV e FPV e apresentados graficamente para comparar o resultado obtido com a performance esperada [70].

Finalmente, a fase da Recomendação busca ajudar o decisor com subsídios sobre formas que para melhorar o desempenho do que está sendo avaliado. Vale a pena ressaltar que o objetivo desta fase não é prescritivo, mas sim de apoio na construção de ações e suas possíveis consequências. É composta de uma única etapa [68]:

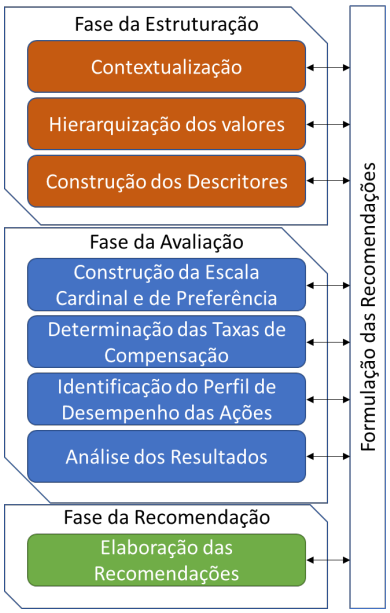

Figura 2.14: Fases do MCDA-C. Fonte: Adaptado de [68]

2.4.4 *Sequential Interactive Modelling for Urban Systems* (SIMUS)

Este método foi desenvolvido por Nolberto Munier, sendo testado na solução de diversos problemas relacionados à mobilidade urbana [63].

O SIMUS *Sequential Interactive Modelling for Urban Systems* é um método multicritério híbrido baseado em Programação Linear para ajudar na tomada de decisão de problemas multicritérios para contribuir no planejamento e tomada de decisão em sistemas urbanos [63]. O método não utiliza uma abordagem subjetiva, pelo contrário, os critérios são considerados como os objetivos e, através da utilização da Programação Linear, eles são otimizados. Além disso, a importância relativa de cada critério é calculada internamente, não necessitado da utilização de pesos [62]. Os critérios assumem uma dupla função: podem ser considerados objetivos ou restrições [71].

O método é dividido em 3 fases e cada uma tem alguns passos conforme descrito abaixo [62]:

1. **Formulação dos parâmetros do método multicritério**: Esta fase é dividida em três etapas. A primeira (Formulação da Matriz de Decisão Inicial) gera uma matriz, onde as linhas representam as médias dos valores de uma matriz auxiliar, composta pelos valores (Mínimo, Médio e Máximo do critério para cada alternativa) de cada critério. Na próxima etapa (Determinação da Matriz Normatizada) é gerada a normatização das matrizes da etapa anterior, são estabelecidas, ao total, quatro matrizes. Finalmente, na última etapa (Determinação dos valores limites dos critérios) são definidos os limites para cada critério. Caso deseje-se obter o máximo de um critério, é utilizado o valor mais alto dentre os valores obtidos nas matrizes normatizadas. Caso seja um mínimo, utiliza-se o valor mais baixo.

2. **Formulação do modelo *Fuzzy* para cada objetivo**: Fase dividida em duas etapas. Na etapa inicial (Resolvendo o procedimento SIMUS para as matrizes iniciais de decisão superior e inferior) são re-

alizadas sucessivas operações lineares para se obter os valores ótimos máximos e mínimos para cada critério. Os dois valores são utilizados na próxima etapa. A última etapa desta fase (Resolvendo os modelos lineares de otimização) é quando são formados, para cada objetivo, modelos de otimização linear utilizando a função de pertencimento linear de *Fuzzy*, gerando uma Matriz de Eficiência *Fuzzy*. Esta é a etapa mais importante visto que os valores máximos e mínimos são obtidos a partir de um ponto de vista de otimização.

3. **Classificação das alternativas**: Inicialmente a Matriz de Eficiência *Fuzzy* deve ser normalizada, através do método da soma, por exemplo e a partir destes valores, as alternativas são ordenadas.

2.4.5 *Stable Preference Ordering Towards Ideal Solution* (SPOTIS)

Os autores em [72], apresentaram um novo MCDM, livre do RR, de baixa complexidade, nomeado *Stable Preference Ordering Towards Ideal Solution* (SPOTIS), utilizando menos informações, comparado com o método COMET.

Assim como os demais métodos multicritério da escola americana, o SPOTIS precisa de uma matriz de decisão e de um conjunto de pesos para ser definido [73].

O método tem como base um modelo que leva em conta a preferência do decisor em relação aos critérios e as relações entre os critérios, tendo como resultado final uma ordenação estável da alternativas.

O princípio do método SPOTIS é baseado no cálculo da distância normalizada de cada alternativa com relação à solução ideal (melhor valor dentre o intervalo de valores considerados) [72].

Ele é desenvolvido em cinco etapas [72]:

1. Definir os limites mínimos e máximos para cada um dos critérios representada pela Equação 2.1.

$$\left[S_n^{min}, S_n^{max}\right] = [x_1, x_2] \tag{2.1}$$

   Onde:

   - n - Número do critério
   - x_1 - Limite mínimo
   - x_2 - Limite superior

2. Definir o ponto de solução ideal baseado na ordem de preferência de cada critério.

3. Calcular a distância normalizada para cada alternativa $A_i(i = 1, 2, ..., M)$ considerando a solução ideal para cada critério $C_j(j = 1, 2, ..., N)$ utilizando as Equações 2.2 e 2.3.

$$d_{ij}(A_i, S_j^*) = \left|S_{ij} - S_j^*\right| \tag{2.2}$$

$$\tilde{d}(A_i, S_j^*) = \frac{d_{ij}(A_i, S^*) - d_j^{min}}{d_j^{max} - d_j^{min}} \tag{2.3}$$

4. Para cada alternativa, computar a distância média normalizada em relação à solução multicritério ideal utilizando a Equação 2.4.

$$d(A_i, s^*) = \sum_{j=1}^{N} w_j d_{ij}(A_i, S_j^*) \tag{2.4}$$

5. Ordenar as alternativas, em ordem crescente considerando os valores obtidos com a utilização da Equação 2.4. O último valor, corresponde a melhor solução.

2.4.6 *Technique for Order of Preferences by Similarity to Ideal Solution* (TOPSIS)

O TOPSIS *Technique for Order of Preferences by Similarity to Ideal Solution* é um método que tem como objetivo determinar a alternativa que se encontra mais próxima de uma solução de ideal e mais distante da solução antagônica. É útil para apoiar decisões complexas que envolvem múltiplos critérios e alternativas [73].

A solução ideal é aquela que maximiza os critérios de benefícios e minimiza os custos. Já a solução antagônica minimiza os benefícios e maximiza os custos [66]. Com isso, entende-se que o método não leva em consideração a opinião do decisor.

Ele é desenvolvido a partir de uma matriz de decisão, composta por um conjunto de alternativas e critérios; da normalização das pontuações das alternativas e critérios; cálculo das distâncias dos pontos ideal e negativo; cálculo da proximidade relativa (utilizando a distância Euclidiana), ordenação das alternativas e análise de sensibilidade [65].

2.4.7 Emprego do Método Multicritério na implementação do ZT

Conforme observado na Figura 2.2, o ZT foi desenvolvido há pouco mais de dez anos. Com isso, as buscas por informações e maneiras diferente de realizar sua implementação, apresentam resultados, de certa maneira, escassos.

Além disso, a implementação da ZTA leva em consideração alguns controles, conforme apresentado na Seção 2.2. Pensando em uma implementação específica, o gestor pode planejar de diversas formas e sequências na qual ele pode implementar tais controles em sua corporação [22]. Conforme [13] este é um caso típico onde torna-se necessário comparar diversas opções (controles) através de procedimentos específicos utilizados em cada uma das opções.

De acordo com a Seção 2.4, existem diversos método de apoio a decisão, por exemplo: AHP, COMET, MCDA-C, SPOTIS, SIMUS, e TOPSIS.. Desta maneira, levando em consideração estes métodos e as diversas formas de realizar a implementação da ZTA, aliado à conclusão observada na Subseção 2.2.7.3, buscou-se na presente Seção aprofundar a revisão dos trabalhos que descrevem como um método multicritério pode ser empregado no apoio a escolha dos controles que devem ser priorizados conforme a necessidade de uma corporação.

De mesmo modo, considerando os motivos apresentados por [31] e descritos na Seção 2.2.7.1, foi

realizada uma RSL com o propósito de apurar a utilização dos métodos multicritérios na implementação da ZTA. Da mesma maneira, foi utilizado o Método PRISMA de RSL.

Considerando esse método, realizou-se uma busca nas seguintes base de dados: ACM Digital Library, IEEE Xplorer, Scopus e Web of Science. Além disso, como observado anteriormente, 2010 foi o ano que o termo foi desenvolvido e iniciaram-se os estudos sobre esta nova forma de proteger dados. Logo, o período considerado para a busca foi de Janeiro de 2010 a Dezembro de 2022.

Tendo o propósito, as bases de dados e o intervalo de pesquisa definidos, torna-se necessário a definição dos termos de busca. Inicialmente realizou-se uma busca apenas com o Método Multicritério considerado (AHP, COMET, MCDA-C, SIMUS, SPOTIS, TOPSIS). A Tabela 2.6 resume o resultado encontrado em cada base de dados para cada termo buscado. Importante perceber que, o método COMET, pode ser confundido com pesquisas que falem sobre ”cometa”, visto que essa é uma possível tradução para a sigla do método. Assim, para evitar este tipo de situação, não apenas neste método, como também nos métodos SIMUS, e SPOTIS que pode ser confundido com outras palavras, a pesquisa foi realizada utilizando o nome por extenso do método, não sua sigla.

Tabela 2.6: Resultado da Busca dos Métodos Multicritério

	ACM Digital	IEEE Explorer	Scopus	WoS	Total
MCDM	4.502	1.060	37.525	8.970	52.057
MCDA	996	218	12.004	3.274	16.492
AHP	6.348	4.351	128.869	25.584	167.058
COMET	34	3	210	20	267
MCDA-C	4	3	111	37	155
SIMUS	2	1	11	5	19
SPOTIS	11	6	45	15	77
TOPSIS	278	1604	69614	12968	84464

Para se ter uma noção da quantidade de artigos com o conjunto de palavras *Zero Trust*, antes de realizar uma pesquisa conjugando esta expressão com os métodos multicritério, foi realizada uma pesquisa nas bases de dados com este conjunto de palavras. Na sequência, fez-se a conjugação das palavras-chave considerando o termo "*Zero Trust*"e o método multicritério, sendo realizado, assim, 5 consultas. A pesquisa utilizou o operador & para que o sistema da base de dados considerado retorne apenas trabalhos que contenham os dois conjuntos de palavras. Além disso, o termo *Zero Trust* foi pesquisando entre ” ”, uma maneira para não retornar o conjunto de palavras separadas. Para estas buscas, considerou-se o mesmo período citado anteriormente, de Janeiro de 2010 a Dezembro de 2022. A Tabela 2.7 apresenta o retrato do resultado alcançado.

Além da utilização dos métodos multicritérios, realizou-se, também, a pesquisa utilizando as duas escolas conhecidas, a americana e europeia, MCDM e MCDA respectivamente. Considerou-se utilizar a pesquisa com as escolas por conta da diversidade de métodos existentes e que não foram abordados neste trabalho. Com isso, é possível observar se, algum outro método não citado anteriormente, foi utilizado para descrever uma possível solução para a implementação da ZTA em uma organização.

Em que pese a busca apresentada na Tabela 2.6 tenha retornado um número vasto de publicações acerca de trabalhos elaborados com os métodos multicritério, ao conjugar-se a busca do método com a expressão

Tabela 2.7: Resultado da Busca de Trabalho sobre ZT e Métodos Multicritério

	ACM Digital	IEEE Explorer	Scopus	WoS
Zero Trust	323	259	838	198
MCDM	0	0	5	0
MCDA	0	0	0	0
AHP	4	0	6	0
COMET	0	0	0	0
MCDA-C	0	0	0	0
SIMUS	0	0	0	0
SPOTIS	0	0	0	0
TOPSIS	1	0	6	0

Zero Trust, pode-se observar uma redução grande no total de artigos retornados da pesquisa. A partir deste resultados, iniciou-se a verificação de cada artigo retornado.

Entre os 4 artigos da ACM Digital Library relacionados ao ZT e AHP: 1 é artigo e 3 encontram-se em anais de conferências. Nenhum dos resultados dos anais de conferência foi possível acessar o texto inteiro do trabalho, sendo a análise realizada através da leitura do resumo e palavras-chave:

- Artigo que cita o ZT como sendo um abordagem de segurança cibernética que previne que atores maliciosos obtenham acesso a dados sensíveis. Ele utiliza o AHP para avaliar a influência de indicadores de qualidade na arquitetura proposta usando o AHP [74];
- **HP3C '22: Proceedings of the 6th International Conference on High Performance Compilation, Computing and Communications:** Há 1 artigo que fala sobre a utilização do ZT e 2 artigos que falam sobre o AHP, mas não há artigo que fale tanto de ZT quanto de AHP [75];
- **ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security:** Há 5 artigos que falam sobre a utilização do ZT e 1 artigo que fala sobre o AHP, mas não há artigo que fale tanto de ZT quando de AHP [76]; e
- **CSSE '22: Proceedings of the 5th International Conference on Computer Science and Software Engineering:** Há 1 artigo que fala sobre a utilização do ZT e 1 artigos que fala sobre o AHP, mas não há artigo que fale tanto de ZT quanto de AHP [77].

Ainda sobre a busca na ACM Digital Library, a busca considerando o método TOPSIS apresentou 1 resultado nos anais da **ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security**. Entretanto o artigo que cita a utilização do TOPSIS para a solução de um problema, não descreve nada relacionado com o ZT.

Além disso, a Scopus retornou 5 trabalhos que citam a MCDM e o ZT sendo 4 artigos (dois deles repetido da consulta anterior [78, 79]) e 1 anal de conferência (não disponível):

- Apresenta um sistema de gerenciamento de confiança na computação industrial armazenada na nuvem utilizando uma abordagem da tomada de decisão utilizando o método multicritério. Apresenta, no decorrer do texto o que é a abordagem do ZT, mas a utilização do método multicritério não tem relação com a implementação dos controles [80];

- Artigo que utiliza o paradigma do ZT para apresentar uma nova metodologia para a avaliação antecipada combinada de segurança e proteção, focado nos fatores que contribuem para a estimativa das probabilidades de ataques bem-sucedidos aos componentes de um sistema. Não considera os métodos multicritério no desenvolvimento de seu trabalho, apenas cita uma referência que tem, em seu título o MCDM [81]; e

- **ASME 2020 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference:** Artigo que serviu como base para a escrita do artigo citado no linha anterior. Não está disponível para acesso no portal da CAPES, apenas de maneira paga, porém pela leitura do resumo, apresenta as mesmas informações [82].

Considerando os 6 artigos encontrados na Scopus que apresentam relação do ZT com o AHP temos 1 livro e 1 *paper* de conferência (ambos sem disponibilidade de acesso, sendo disponibilizado apenas o resumo e sua bibliografia) e 4 artigos:

- Livro que apresenta uma combinação de engenharia, pesquisa operacional e ciências políticas, com o objetivo de proporcionar aos alunos um entendimento completo do conceito de sustentabilidade e dos ciclos de vida sustentáveis dos produtos, além de uma apreciação da importância da sustentação de sistemas críticos [83];

- **ICAIS 2022: Advances in Artificial Intelligence and Security:** Artigo do congresso que a partir do objetivo de analisar os possíveis riscos na segurança da rede, propõe um AHP aprimorado para avaliar de forma abrangente as informações de consciência situacional [84];

- Artigo que descreve uma metodologia para a avaliação de risco baseado nas características dos dispositivos IoT. Cita o método AHP no título de uma das referências utilizadas no trabalho mas não o utiliza no decorrer do texto [85];

- Trabalho que utiliza o método multicritério para analisar os fatores que afetam o comportamento e a coordenação sustentável de uma cadeia de suprimentos no contexto da digitalização. Contudo não aborda o ZT em seu conteúdo [78];

- O artigo apresenta a utilização do AHP para avaliar os fatores de risco do marketing verde dentro da indústria de laticínios. Da mesma maneira, não aborda o ZT em seu conteúdo [79]; e Este estudo aborda a avaliação de riscos na implementação do marketing verde na indústria de laticínios. Utilizando uma metodologia de tomada de decisão fuzzy integrada, são identificados os fatores de risco e propostas estratégias de mitigação. Os resultados destacam o nível de consciência ambiental como o fator de risco mais importante, seguido por políticas e regulamentos governamentais.

- Propõe um modelo de controle e prevenção de risco dentro de uma cadeia de suprimentos utilizando o diagrama de influência *Fuzzy*. Não cita nada sobre o ZT e AHP em seu corpo, apenas no título de trabalhos descrito em suas referências bibliográficas [86].

Ainda na base de dados da Scopus, a busca do método TOPSIS retornou 6 artigos, dois deles repetidos da pesquisa utilizando ZT e o AHP [78, 79]. Além disso, 1 artigo não está disponível de maneira com-

pleta, apenas seu resumo e referencial teórico (primeiro item descrito abaixo) e 1 que consta em anais de conferência:

- Este artigo aborda a importância do gerenciamento de confiança na computação em nuvem e a necessidade de uma avaliação precisa. Propõe um método de média ponderada utilizando funções *Weighted Moving Average - Ordered Weighted Averaging* (WMA-OWA) para atribuição de pesos dinâmicos aos fatores envolvidos nessa avaliação. O método supera a inflexibilidade dos métodos subjetivos de atribuição de peso e demonstra maior flexibilidade e adaptabilidade na computação em nuvem, conforme evidenciado por resultados experimentais [87];
- **WorldCIST 2022: Information Systems and Technologies** O artigo aborda o problema da necessidade de medir o desempenho das equipes *Development and Operations* (DevOps) nas organizações. Propõe-se uma Revisão Sistemática da Literatura que identificou 13 Indicadores Chave de Desempenho. Os resultados destacam que os indicadores relacionados à qualidade e resultados dos testes são os mais mencionados e implementados. [88];
- O artigo um mecanismo de consenso chamado *Proof by Earnestness* (PoE) que determina a veracidade da informação subjetiva antes do processamento posterior e formalização em *blockchains*. Não cita nada sobre o ZT e TOPSIS em seu corpo, apenas no título de trabalhos descrito em suas referências bibliográficas [89]; e
- Artigo que apresentar uma RSL para fornecer um levantamento da literatura existente sobre os mecanismos de defesa contra *Advanced Persistent Threats* (APT). Eles descrevem que o ZT é um dos mecanismos de segurança baseado em confiança. Ao final, é sugerido a utilização do ZT na etapa da proteção das informações pelo fato do ZT ser utilizado para evitar o risco de vazamento de dados. Os autores não citam o TOPSIS em seu trabalho, aparece apenas no título de um dos trabalhos citados no referencial teórico [90].

Observa-se que ao especificar mais a busca, conjugando a expressão ZT com um método multicritério, o total de artigos encontrados nas base de dados buscadas reduziu de mais de 1660 artigos encontrados para apenas 22. Além disso, a partir da leitura dos textos encontrados e disponibilizados e do resumo daqueles indisponível, notou-se que não há, dentro do espaço amostral de base de dados buscada, no período de 12 anos, entre 2010 e 2022, nada que descreva uma maneira de conjugar a implementação de uma ZTA utilizando as diretrizes de escolha de controles resultantes de uma avaliação realizada por meio de um Método Multicritério de decisão.

2.5 *MYMCDA*

O *software* foi idealizado por dois professores da UnB e desenvolvido por um aluno do curso de Engenharia da Computação, com fomento da Fundação de Apoio a Pesquisa do Distrito Federal (FAP-DF) e do Programa Institucional de Bolsas de Iniciação em Desenvolvimento Tecnológico (PIBTI). O propósito do *software* é facilitar e impulsionar a utilização do MCDA-C na busca de possíveis soluções de problemas onde existem várias variáveis de escolha.

Sua origem se deu pela dificuldade de disseminação do *software* MAMADECISÃO, visto que ele foi desenvolvido utilizando o *software* de planilha de texto Excel. Desta maneira, viu-se como oportunidade a reconstrução do MAMADECISÃO em uma plataforma de código aberto e de fácil acesso tanto por pesquisadores quanto por organizações.

O MyMCDA é voltado para gestores que utilizam o MCDA-C para auxiliar na tomada de decisões, sendo empregado em uma variedade de estudos e setores, conforme evidenciado em [61].

Uma das principais características do MyMCDA-C reside na sua capacidade de identificar os pontos de maximização e minimização para cada critério, levando em consideração os respectivos pesos atribuídos. Isto é possível através da transformação das informações qualitativos obtidas nas primeiras etapas do MCDA-C em dados quantitativos. Além disso, após a identificação dos valores máximos e mínimos, ele é capaz de gerar gráficos e tabelas para auxiliar o processo de decisão, levando em consideração os requisitos da análise multicritério construtivista.

Ao adotar os modelos matemáticos do MyMCDA-C, é possível estabelecer uma associação sólida entre as percepções dos tomadores de decisão e as perspectivas das partes interessadas nos critérios considerados.

Além disso, o software consolida os cálculos realizados, conferindo-lhes expressão numérica. Os resultados obtidos são apresentados de forma visualmente elucidativa, por meio de gráficos que permitem a identificação de áreas passíveis de melhoria e consolidação. [61] destaca que, no método MACBETH, os valores qualitativos "NEUTRO"e "BOM"são convertidos em representações quantitativas correspondentes a 0 e 100, respectivamente.

Abaixo são descritas as Equações 2.5, que representa o cálculo dos pontos de minimização (valores negativos), 2.6 para os valores de maximização (acima do nível considerado Bom) e 2.7 para obter o ponto de maximização [61]:

$$\sum_{i=1}^{n} NV = 0 - \frac{WN * (N-1)}{PS} \tag{2.5}$$

$$\sum_{i=1}^{n} PV = 100 + \frac{WN * (N-1)}{PS} \tag{2.6}$$

$$\sum_{i=1}^{n} PV = 100 + WN * (N - (PS-1)) \tag{2.7}$$

Onde [61]:

- NV - Valor negativo de uma ação na escala dos descritores de um critério
- PV - Valor positivo de uma ação na escala dos descritores de um critério
- WN - Número e peso
- N - Número de critérios da avaliação
- PS - Posição da ação dentro da escala de descritores

Considerando os valores qualitativos definidos para os níveis NEUTRO e BOM, torna-se necessário encontrar os valores intermediários. Isto é realizado através da Equação 2.8 [61]:

$$N(X) = \alpha * X + \beta \tag{2.8}$$

Finalmente, os valores globais para os critérios é definido pela Equação 2.9 [61]:

$$G(a) = \sum_{i=1}^{n} RR_i * V_i(a) \tag{2.9}$$

Onde [61]:

- G(a) - Valor Global do desempenho de 'a'
- n - Total de critérios
- RR - Taxa de substituição correspondente ao critério
- V(a) - Valor parcial de uma ação potencial 'a' no critério

3 METODOLOGIA

O desenvolvimento de trabalhos acadêmicos segue um rito, no qual processos e procedimentos são seguidos. Desta forma, o presente capítulo visa explicar a metodologia empregada na solução do problema proposto, bem como possíveis formas de empregar uma metodologia Multicritério na solução de um problema complexo.

3.1 CLASSIFICAÇÃO DA PESQUISA

A pesquisa é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos, sendo realizada quando se tem um problema e não se têm informações para solucioná-lo [91]. Nesta linha de pensamento, as pesquisas podem ser classificadas de diversas formas, sintetizadas na Figura 3.1:

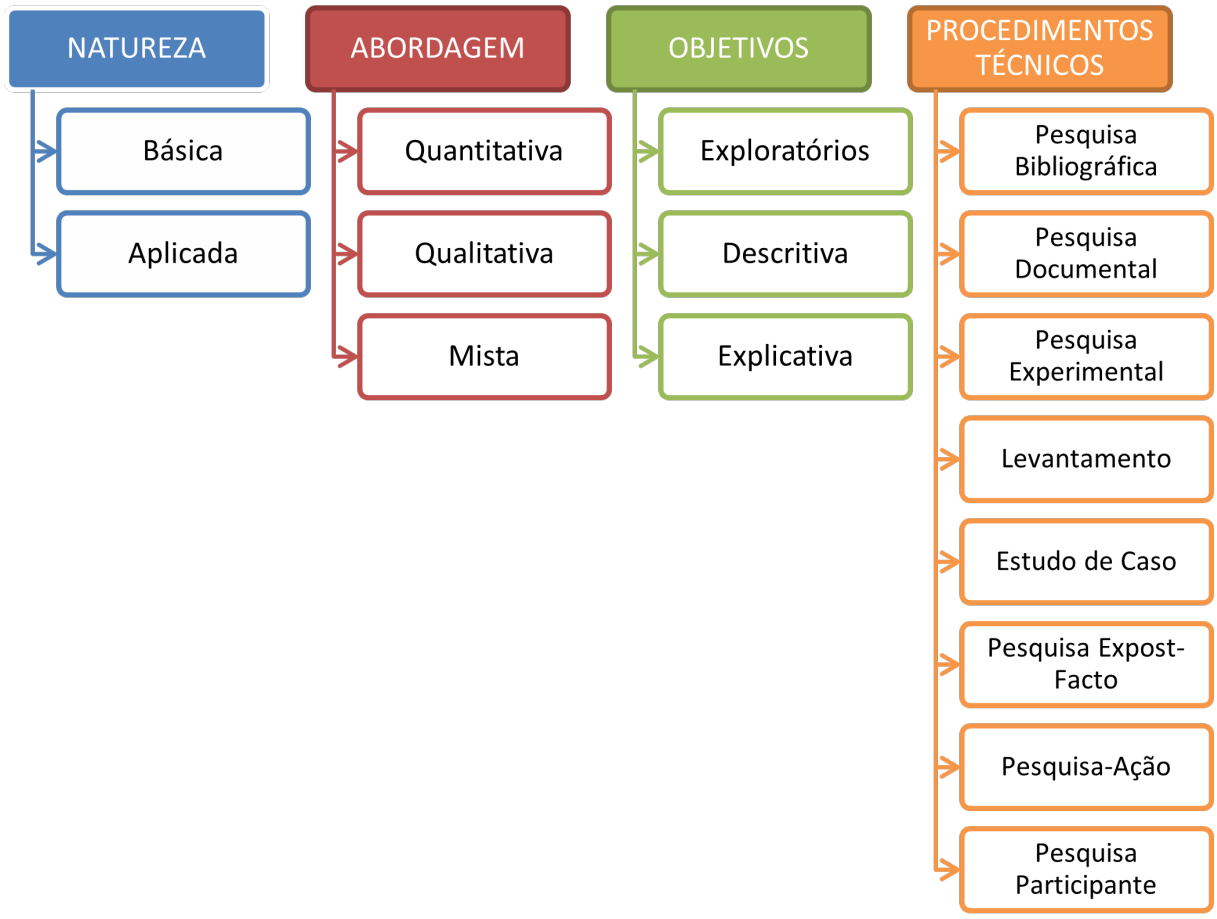

Figura 3.1: Classificação dos Tipos de Pesquisa. Fonte: Adaptado de [91, 92, 93]

Como se pode observar através da revisão sistemática de literatura apresentada na Seção 2.2.7.1, há uma lacuna dentro da literatura acerca da maneira na qual as dimensões observadas em uma implementação ZTA

devem ser implementadas. Conforme esta lacuna, o trabalho propõe um método capaz de avaliar em uma organização qual o status da implementação da ZT, listando, em ordem de prioridades, quais os controles de segurança devem ser implementados. Assim, segundo [91] pode-se dizer que o trabalho tem a finalidade aplicada pois busca gerar conhecimentos para aplicar de maneira prática e dirigida à solução de problemas.

A execução do MCDA-C é realizada em três fases, conforme ilustrado na Figura 2.14. Inicialmente, na fase da estruturação, a pesquisa é montada e discutida com tomadores de decisão, de modo que controles e funções de valor sejam definidos. Ou seja, conforme explicado em [92], considera-se que a abordagem da pesquisa é qualitativa, uma vez que o pesquisador, através da coleta de dados do mundo real, é capaz de analisar os dados intuitivamente.

Por outro lado, na segunda fase do método, as funções valor são desenvolvidas e, através de funções matemáticas e estatística, a opinião de pessoas é traduzida em números. Com isso, segundo [92] expõe em seu livro, a abordagem quantitativa da pesquisa pode ser definida como a capacidade de quantificar opiniões e informações em números. Com isso, a pesquisa pode ser considerado mista, como relação à abordagem.

Segundo mostrada na Figura 2.2, o assunto ZT é relativamente novo, carecendo de um aprofundamento no tema, conforme observado nas duas revisões sistemáticas de literatura, para se trazer uma maior familiaridade com o tema. Com isso, esta pesquisa apresenta um objetivo exploratório, pois aborda um assunto desconhecido [93].

Além disso, no decorrer do trabalho, houve interação com grupos de pessoas (decisores e *stakeholders*) com o propósito de compreender seus pontos de vista sobre a importância de diversos controles para a implementação do ZT. Demonstrando o que [91] identifica como um objetivo descritivo, pois esta se buscando descrever o estabelecimento de relações entre os controles e a implementação da ZTA.

A Seção 2 apresenta definições e conceitos, bem como o contexto histórico do desenvolvimento de um padrão de segurança cibernética recente. Assim, segundo [93] este procedimento caracteriza o que a literatura chama de Pesquisa Bibliográfica, que apresenta como vantagem a possibilidade de se cobrir uma ampla gama de assuntos. O autor descreve, ainda, que não se pode confundir a Pesquisa Bibliográfica, aquela onde a busca ocorre em bibliotecas e base de dados, com a Pesquisa Documental, na qual o material consultado é interno a organização.

Durante a realização de uma das etapas do método multicritério considerado, elaborou-se um questionário padrão, com perguntas fechadas, que foi enviado a *stakeholders* de modo que coletar informações sobre sua visão acerca da implementação dos controles ZTA proposta. [93] descreve este procedimento técnico como sendo um levantamento.

Considerando o observado na Seção 2, dentre as implementações do ZTA apresentadas, utilizou-se a ZTMM apresentada pela CISA por apresentar um modelo de maturidade com dimensões e controles bem definidos e descrever, de maneira detalhada o que é necessário para se atingir cada nível (tradicional, inicial, avançada e ótima).

Com relação aos MCDA, método descrito em [13] para o apoio na tomada de decisão que envolve diversos critérios, dentre as formas apresentados, considerou-se a utilização do MCDA-C. Por ser um tema relativamente novo, tendo pouco mais de 10 anos desde sua criação, não encontrou-se nas base

de dados buscadas trabalhos considerando a utilização do MCDA-C na priorização dos controles a ser implementados em uma ZTA, conforme descrito na Seção 2.4.7 do Capítulo do Referencial Teórico. Assim, pela sua característica construtivista de gerar conhecimento para os decisores no decorrer de sua realização, esta metodologia foi a empregada.

4 RESULTADOS OBTIDOS

Capítulo exclusivo para discutir os resultados obtidos com a aplicação do MCDA-C dentro de uma organização e propor sugestões para melhorar a Segurança Cibernética através da implementação da ZTA.

Conforme descrito na Seção 2.4.7 pouco se estudou até o momento sobre como se pode implementar uma ZTA utilizando métodos multicritérios. Desta maneira, vamos discorrer uma proposta da implementação da ZTA utilizando os conceitos e procedimentos da estrutura do MCDA-C considerando os pilares e controles descritos no ZTMM da CISA.

4.1 ETAPA 1 - CONTEXTUALIZAÇÃO

A aplicação do MCDA-C ocorre conforme descrito na Seção 2.4.3. Diversos atores fazem parte deste processo que tem como objetivo final construir um nível de conhecimento aos decisores para assessorá-los na tomada de decisão. Assim, torna-se necessário, definir quem são os atores envolvidos neste processo, que foram divididos em três grupos distintos (decisores, facilitadores, stakeholders), abaixo definidos:

- **Decisores:** Coordenador de segurança da informação e comunicações, Coordenador de Governança de TI e Coordenador de Sistemas de Informação;
- **Facilitadores:** Os pesquisadores; e
- ***Stakeholders*:** Integrantes da área de gestão de banco de dados, governança de TI, Infraestrutura de TI e Segurança da Informação e Comunicações.

A escolha dos decisores aconteceu por dois motivos: suas experiências dentro de sua área de atuação e pelo cargo gerencial que ocupam. Dentro das oito etapas do processo do MCDA-C, os decisores participam apenas das etapas de 1 a 5, contribuindo com a modelagem de todo o processo.

Os *Stakeholders* são funcionários da área de TI da organização, não apenas da mesma área dos decisores. A participação dos *Stakeholders* ocorre exclusivamente na etapa 6 do processo, onde são apresentados os pontos de vista dos *stakeholders* relacionados ao problema de pesquisa através da resposta, individual, de um questionário elaborado nas etapas anteriores. Para não haver contaminação das respostas, apenas eles respondem ao questionário. Eles possuem as seguintes responsabilidades dentro da organização:

- **Gestão de banco de dados**: Realizar e gerenciar o processo de identificação, definição, implementação e manutenção de padrões, metodologias e tecnologias para integrar, formatar, capturar e armazenar informações provenientes de diversas fontes de dados;
- **Governança de TI**: Monitorar a implementação das ações planejadas no portfólio, avaliando o desempenho das estruturas envolvidas e o progresso em relação às metas estabelecidas. Identificar e propor soluções concretas para resolver problemas que possam afetar os resultados almejados;

- **Infraestrutura de TI**: Definir soluções para assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos serviços de tecnologia da informação da organização. Supervisionar a infraestrutura de conectividade para garantir o desempenho dos links de comunicação de dados e gerenciar a infraestrutura de rede; e
- **Segurança da Informação e Comunicações**: Desenvolver planos estratégicos e coordenar as atividades de auditoria e verificação de conformidade da segurança da informação e comunicações (SIC). Gerenciar as práticas de gestão de riscos e assegurar a continuidade dos negócios.

A distribuição dos 12 *stakeholders* que contribuíram com a pesquisa está representada na Figura 4.1:

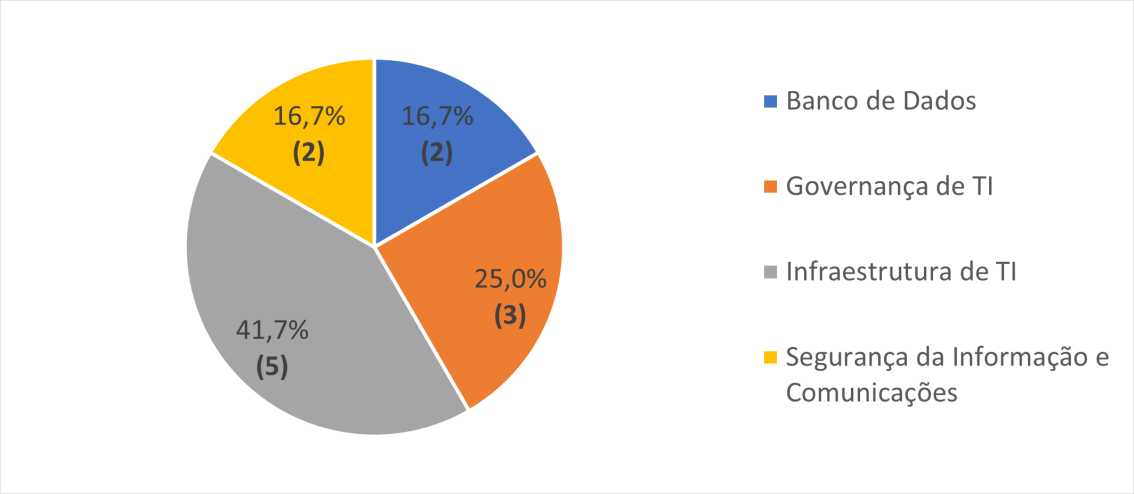

Figura 4.1: Área de Atuação.

Os pesquisadores participam de todas as etapas do processo. Nas etapas de 1 a 5, sua participação ocorre na condução/auxílio da elaboração do processo por parte dos decisores. Na etapa 6 através do envio dos questionários e consolidação das respostas por parte dos *Stakeholders*. Finalmente nas etapas 7 e 8, está envolvido, desta vez sozinho, no registro das informações obtidas na etapa 6 em software específico, na análise dos dados e apresentação dos resultados aos decisores. A Tabela 4.1 resume a participação dos atores em cada uma das etapas:

Tabela 4.1: Resumo da participação dos atores em cada etapa do MCDA-C

Etapa	Descrição	Ator Envolvido
1	Contextualização	Pesquisador e Decisores
2	Hierarquização dos valores	Pesquisador e Decisores
3	Construção dos descritores	Pesquisador e Decisores
4	Construção das escalas cardinal e de preferência	Pesquisador e Decisores
5	Determinação das taxas de compensação	Pesquisador e Decisores
6	Identificação do Perfil de Desempenho das Ações	Pesquisador e *Stakeholders*
7	Análise de resultados	Pesquisador
8	Elaboração das recomendações	Pesquisador

Desta maneira, observa-se que com a participação dos atores no transcurso do processo, onde suas opiniões são escutadas e consideradas, estamos utilizando o princípio da Gestão de Riscos da inclusão, descrito na Seção 2.

Com a definição das partes envolvidas no processo e suas responsabilidades, o método solicita que seja definido o rótulo do trabalho. Este rótulo servirá como orientador das demais etapas do processo. Considerando o ZTMM proposto pela CISA, o rótulo do escolhido foi: ”Como a implementação dos controles podem mitigar riscos de segurança da informação na organização?”

4.2 ETAPA 2 - HIERARQUIZAÇÃO DOS VALORES

A partir deste rótulo, inicia-se o processo de criar a estrutura hierárquica do método. Inicialmente, o Ponto de Vista, descrito na azul, tem o ZT. À direita, na segunda coluna, são apresentadas os cinco pilares do ZTMM, considerado no trabalho as dimensões, e segundo o MCDA-C são denominados Pontos de Vista Fundamental (FPV). Cada dimensão é dividida em controles, denominados Ponto de Vista Elementar (EPV). Os EPV estão descritos na terceira coluna, sendo apresentados na mesma cor de seu FPV para facilitar o entendimento. As dimensões e controles apresentados estão definidos em [9]. Ao total, as cinco dimensões apresentam 22 controles. Assim, é possível elaborar uma árvore estruturada, representada na Figura 4.2.

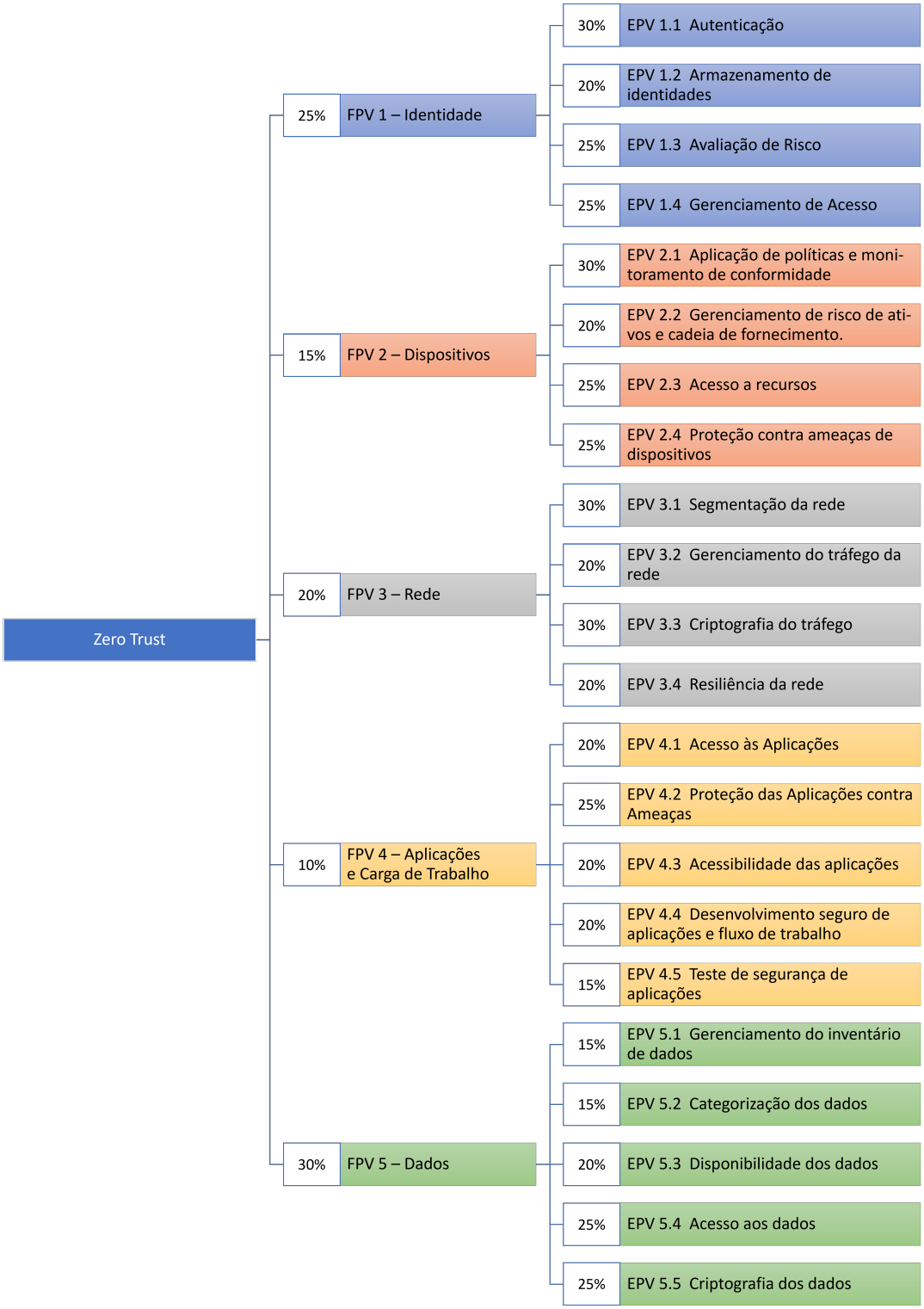

Figura 4.2: Estrutura hierárquica de valores do ZTMM com seus FPV e EPV. Fonte: Adaptado de [9]

4.3 ETAPA 3 - CONSTRUÇÃO DOS DESCRITORES

Na terceira etapa, último estágio para finalizar a primeira fase do processo, torna-se necessário criar os descritores. Nesta parte, uma escala subjetiva de cinco níveis de considerações foi definida pelos decisores. Além disso, foi realizado o posicionamento dos níveis considerados "NEUTRO" e "BOM" pelos decisores. Esta definição é importante pois, conforme [69] os descritores servem para descrever uma performance das ações potenciais de cada EPV. Os níveis propostos, bem como a posição dos níveis de controle (NEUTRO e BOM) estão apresentados na Tabela 4.2.

Tabela 4.2: Escala de avaliação dos descritores.

Nível	Descritor	Neutro	Bom
N1	Indiferente	X	
N2	Fraco		
N3	Moderado		
N4	Forte		X
N5	Muito Forte		

4.4 ETAPA 4 - CONSTRUÇÃO DA ESCALA CARDINAL E DE PREFERÊNCIA

Iniciando-se a quarta etapa, primeira da fase da Avaliação, definiu-se os graus de atratividade entre os descritores. Assim, considerou-se os valores NEUTRO (N1) e BOM (N4), apresentados na Tabela 4.2 como sendo 0 e 100, respectivamente. Isto porque não faz sentido eu implementar algo em um modelo de proteção que tenha influência negativa na segurança cibernética de uma organização.

Desta maneira, segundo a teoria do método MACBETH, a definição dos valores entre os níveis "NEUTRO" e "BOM" é definida por uma escala linear, ou seja, a fórmula para encontrar os valores de N2 e N3 é representada pela Equação 2.8 [61].

Substituindo os valores para N1 e N4, encontramos a relação entre α e β.

$$\begin{aligned} N(X) &= \alpha * X + \beta \\ N1 &= \alpha * 1 + \beta \\ 0 &= \alpha * 1 + \beta \\ \alpha &= -\beta \end{aligned}$$

A partir do valor de α encontra-se o valor de β.

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

Substituindo na Equação 2.8, define-se os valores (arredondados) de N2 = 33 e N3 = 67. Além destes valores, é necessário encontrar o valor para o qual o esforço é acima do bom, ou seja, o ponto de maximização. Quando este valor é atingido, significa que o determinado EPV, na visão dos *stakeholders*, apresenta o máximo de influência na implementação da ZTA. Para encontrar esse valor de maximização, o MyMCDA utiliza-se de um peso, que representa o nível de esforço necessário para maximizar o controle [61]. O software utiliza o valor 3 como padrão para este valor, sendo este o considerado entre os decisores.

Além disso, antes de definir o valor máximo para cada EPV, os decisores definiram uma ordem de prioridade para se alcançar a maximização. Ou seja, enquanto o EPV com número de ordem 1 é aquele que necessita mais esforço para ser alcançado, o EPV com número de ordem 22 apresenta o mínimo de esforço. Importante perceber que esse ordenamento não tem relação com o nível de importância do EPV, mas sim a quantidade de esforço necessário para atingí-lo.

Desta maneira, os valores de maximização não apresentam valores iguais para todos os controles, como ocorre para os níveis de 1 a 4 (N1, N2, N3 e N4). Isto pode ser observado ao analisar a Equação 2.7 [61] que demonstra que o valor de maximização esta relacionado com a posição do controle dentro da escala de prioridade. Ou seja, quanto menor o número (ter uma ordem de prioridade maior), mais distante do valor bom (N4) ele se encontra. Por exemplo, a distancia entre N4 e N5 para o controle de ordem 1 é praticamente a mesma entre N2 e N4, ou seja 66 pontos.

A Tabela 4.3 resume a ordem de preferência, e os valores ordinais para os descritores (N1 a N5) em cada um dos EPV.

Tabela 4.3: Ordem de esforço de implementação do controle.

Ordem	Controle	N1	N2	N3	N4	N5
1	EPV 2.4 - Proteção contra ameaças de dispositivos	0	33	67	100	166
2	EPV 4.2 - Proteção das aplicações contra ameaças	0	33	67	100	163
3	EPV 3.3 - Criptografia do tráfego	0	33	67	100	160
4	EPV 5.5 - Criptografia dos dados	0	33	67	100	157
5	EPV 4.5 - Teste de segurança das aplicações	0	33	67	100	154
6	EPV 1.3 - Avaliação de risco	0	33	67	100	151
7	EPV 4.4 - Desenvolvimento seguro de aplicações e fluxo de trabalho	0	33	67	100	148
8	EPV 2.1 - Aplicação de políticas e monitoramento de conformidade	0	33	67	100	145

Continua na próxima página.

Continuação da Tabela 4.3

Ordem	Controle	N1	N2	N3	N4	N5
9	EPV 3.1 - Segmentação da rede	0	33	67	100	142
10	EPV 1.4 - Gerenciamento de acesso	0	33	67	100	139
11	EPV 5.1 - Gerenciamento de inventário de dados	0	33	67	100	136
12	EPV 1.1 - Autenticação	0	33	67	100	133
13	EPV 2.2 - Gerenciamento de risco de ativos e cadeia de fornecimento	0	33	67	100	130
14	EPV 5.2 - Categorização dos dados	0	33	67	100	127
15	EPV 2.3 - Acesso a recursos	0	33	67	100	124
16	EPV 4.1 - Acesso às aplicações	0	33	67	100	121
17	EPV 5.4 - Acesso aos dados	0	33	67	100	118
18	EPV 4.3 - Acessibilidade das aplicações	0	33	67	100	115
19	EPV 3.2 - Gerenciamento do tráfego da rede	0	33	67	100	112
20	EPV 3.4 - Resiliência da rede	0	33	67	100	109
21	EPV 1.2 - Armazenamento de identidades	0	33	67	100	106
22	EPV 5.3 - Disponibilidade dos dados	0	33	67	100	103

4.5 ETAPA 5 - DETERMINAÇÃO DAS TAXAS DE COMPENSAÇÃO

Na quinta etapa do processo, os decisores definiram a taxa de compensação dos PFV e EPV. Esta taxa, apresentada na Figura 4.2, é utilizada para se obter não só uma avaliação global dos EPV dentro de um determinado FPV bem como a avaliação global dos FPV. Assim, é possível, após a aplicação dos questionários, realizada na próxima etapa, encontrar, segundo a visão dos *stakeholders*, como cada controle pode afetar a implementação do ZTA dentro da organização, a partir da utilização da taxa de compensação do valor obtido na realização do questionário e a posição do EPV dentro da ordem de esforço de implementação, utilizando-se da Equação 2.9 .

4.6 ETAPA 6 - IDENTIFICAÇÃO DO PERFIL DE DESEMPENHO DAS AÇÕES

Na sequência, foi realizada a coleta de dados, através de um questionário enviado aos *stakeholders*. A elaboração deste método de coleta de dados aconteceu com a transcrição das dimensões e controles à um formulário na Plataforma Microsoft Forms. Foi solicitado às pessoas que responderam ao questionário que apresentassem seus pontos de vista com relação a contribuição que o determinado controle tem para a implementação da ZTA. As respostas possíveis ao questionamento foram os descritores apresentados na Tabela 4.2. Com o questionário elaborado, o mesmo foi enviado aos funcionários das áreas de TI, descritas na Etapa 1 do processo.

4.7 ETAPA 7 - ANÁLISE DOS RESULTADOS

A medida que os formulários foram sendo respondidos, os dados coletados foram tabulados. Aos níveis dos descritores foi atribuída uma pontuação de 1 a 5, conforme cada nível. O nível de contribuição foi encontrado utilizando a mediana dos valores obtidas, sendo desconsideras as repostas "Não sei responder", de modo a não contaminar o resultado final. Para critério de arredondamento, foi considerado a primeira casa decimal, sendo arredondado para cima o valor igual ou maior a 5 pontos decimais (0,5). A Tabela 4.4 ilustra a maneira na qual a mediana de um dos controles foi encontrada.

Tabela 4.4: Cálculo da contribuição para o critério EPV 1.1 - Autenticação.

Stakeholder	Resposta	Nível
1	Forte	4
2	Não sei responder	
3	Forte	4
4	Forte	4
5	Muito Forte	5
6	Muito Forte	5
7	Muito Forte	5
8	Forte	4
9	Muito Forte	5
10	Muito Forte	5
11	Muito Forte	5
12	Forte	4
Mediana		5

Conforme mostrado na Tabela 4.5 pode-se observar o valor obtido, em todos os controles apresentados, após a realização das pesquisa e cálculo das contribuições.

Tabela 4.5: Nível de contribuição obtida dos controles.

Ordem	Controle	Nível	Descritor	Valor
1	EPV 2.4 - Proteção contra ameaças de dispositivos	N5	Muito Forte	166
2	EPV 4.2 - Proteção das aplicações contra ameaças	N4	Forte	100
3	EPV 3.3 - Criptografia do tráfego	N5	Muito Forte	160
4	EPV 5.5 - Criptografia dos dados	N5	Muito Forte	157
5	EPV 4.5 - Teste de segurança das aplicações	N5	Muito Forte	154
6	EPV 1.3 - Avaliação de risco	N4	Forte	100
7	EPV 4.4 - Desenvolvimento seguro de aplicações e fluxo de trabalho	N5	Muito Forte	148
8	EPV 2.1 - Aplicação de políticas e monitoramento de conformidade	N5	Muito Forte	145

Continua na próxima página.

Continuação da Tabela 4.5

Ordem	Controle	Nível	Descritor	Valor
9	EPV 3.1 - Segmentação da rede	N4	Forte	100
10	EPV 1.4 - Gerenciamento de acesso	N4	Forte	100
11	EPV 5.1 - Gerenciamento de inventário de dados	N4	Forte	100
12	EPV 1.1 - Autenticação	N5	Muito Forte	133
13	EPV 2.2 - Gerenciamento de risco de ativos e cadeia de fornecimento	N4	Forte	100
14	EPV 5.2 - Categorização dos dados	N4	Forte	100
15	EPV 2.3 - Acesso a recursos	N4	Forte	100
16	EPV 4.1 - Acesso às aplicações	N5	Muito Forte	121
17	EPV 5.4 - Acesso aos dados	N4	Forte	100
18	EPV 4.3 - Acessibilidade das aplicações	N4	Forte	100
19	EPV 3.2 - Gerenciamento do tráfego da rede	N5	Muito Forte	112
20	EPV 3.4 - Resiliência da rede	N5	Muito Forte	109
21	EPV 1.2 - Armazenamento de identidades	N4	Forte	100
22	EPV 5.3 - Disponibilidade dos dados	N4	Forte	100

4.8 ETAPA 8 - ELABORAÇÃO DAS RECOMENDAÇÕES

Com as informações tabuladas e as representações gráficas apresentadas, foi possível gerar os conhecimentos que servirão como base para a tomada de decisão dos gestores. Desta maneira, nas imagens abaixo, serão analisados os pontos obtidos, ou seja, aqueles que, contribuem mais com a implementação do ZT e aqueles que apresentam uma contribuição menor.

Da primeira dimensão ”FPV 1 - Identidade” observa-se que o ”EPV 1.1 - Autenticação” foi o único controle que apresentou um nível máximo de contribuição. Além disso, seu percentual de compensação perante os demais EPV é o mais alto, demonstrando a grande contribuição que este controle tem na implementação do ZT.

Os demais controles obtiveram o descritor de avaliação ”BOM”. Entretanto, analisa-se que o ”EPV 1.4 - Gerenciamento de acesso” apresentou um resultado com 48 pontos de diferença entre o nível obtido e seu ponto de maximização. Além da diferença na pontuação obtida e a máxima, este EPV é, juntamente com o EPV 1.3, o que possui a menor taxa de compensação, ou seja, sua implementação pode contribuir pouco. A Figura 4.3 apresenta os resultados para o ”FPV 1 - Identidade”:

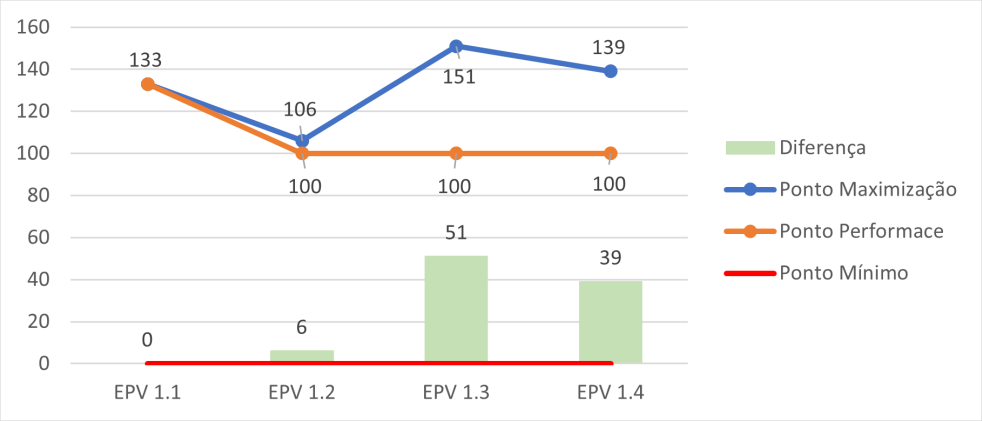

Figura 4.3: Resultado Dimensão FPV 1 - Identidade.

Na segunda dimensão, ”FPV 2 - Dispositivos” tanto o ”EPV 2.1 - Aplicação de politicas e monitoramento de conformidade” quanto o ”EPV 2.4 - Proteção contra ameaças de Dispositivos” obtiveram resultados máximos. Contudo, o percentual de compensação do primeiro é maior (30%) que a do segundo (25%). Em contrapartida, o EPV 2.4 foi definido pelos decisores como o controle que demanda um maior esforço para atingir seu ponto de maximização.

Em que pese os dois controles tenham apresentado o nível ”BOM” dentre os descritores, o ”EPV 2.2 - Gerenciamento de risco de ativos e cadeia de fornecimento” apresentou uma mediana de 3,5, sendo, por conta do arredondamento, atribuído o N4. Também, ele é o que apresenta o menor percentual de compensação, ou seja, aparenta ser um controle com pouco contribuição para a implementação da ZTA. A Figura 4.4 apresenta os resultados para o ”FPV 2 - Dispositivos”:

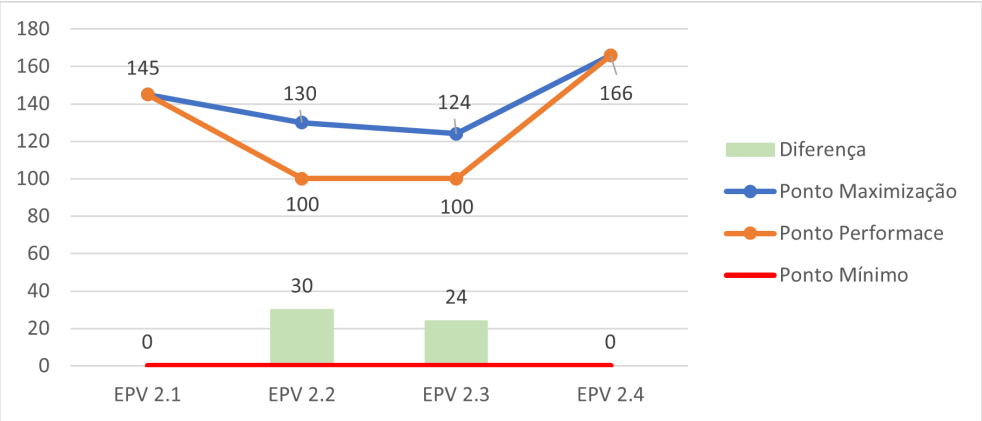

Figura 4.4: Resultado Dimensão FPV 2 - Dispositivos.

Analisando a terceira dimensão, ”FPV 3 - Rede” observa-se que apenas um controle, o ”EPV 3.1 - Segmentação de Rede” não teve como resultado o descritor ”MUITO FORTE”. Este fato é interessante pois a segmentação da rede, na visão do pesquisador, aparentava ser um fator de grande importância na implementação da ZTA. A Figura 4.5 apresenta os resultados para o ”FPV 3 - Rede”:

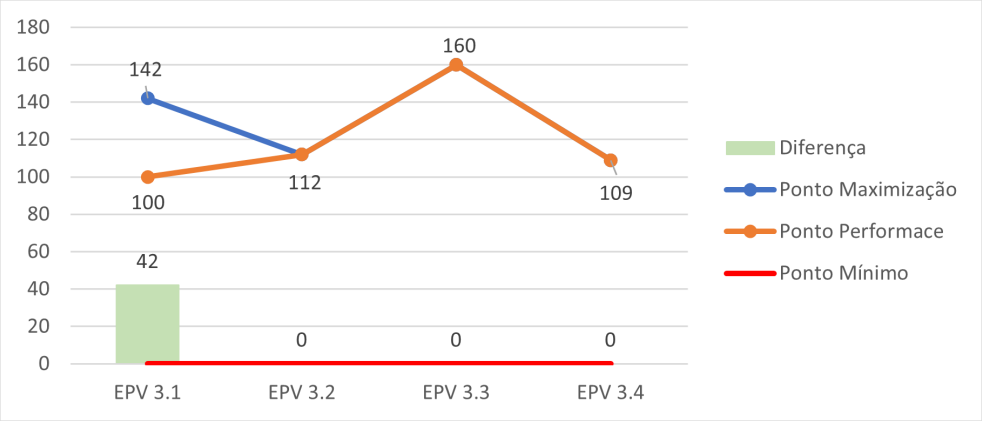

Figura 4.5: Resultado Dimensão FPV 3 - Rede.

A avaliação do ”FPV 4 - Apelações e Carga de Trabalho” esta focada na maneira pela qual a organização desenvolve e protege seus programas e serviços executados, independentemente da localização. Assim, o ”EPV 4.1 - Acesso às aplicações” apresentou um leve destaque em comparação com os demais controles.

Por outro lado, o ”EPV 4.2 - Proteção das aplicações contra ameaças”, com uma distância de 63 unidades, foi o controle que apresentou a maior distância entre o valor obtido após as entrevistas e seu ponto de maximização. Isto pode trazer uma reflexão aos decisores sobre sua importância na implementação. A Figura 4.6 apresenta os resultados para o ”FPV 4 - Aplicações e Carga de Trabalho”:

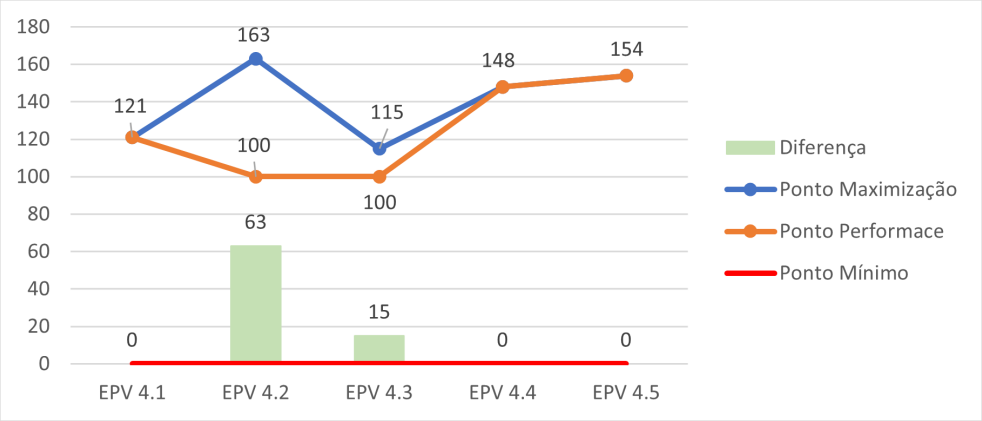

Figura 4.6: Resultado Dimensão FPV 4 - Aplicações e Carga de Trabalho.

Finalizando com o ”FPV 5 - Dados” o ”EPV 5.5 - Criptografia dos dados” apresentou um destaque perante os demais, por ser o único controle que atingiu o ponto de maximização nesta dimensão. Além disso, ele tem a maior contribuição dentro da dimensão, demonstrando a preocupação que os tomadores de decisão devem ter com relação à sua implementação.

Em contrapartida, o ”EPV 5.1 - Gerenciamento de inventário de dados” foi o que apresentou a maior distância para o ponto ideal. Também, sua contribuição é a mais baixa, em se comparar com as demais. Assim, os decisores conseguem avaliar, comparando de uma maneira geral, o quanto vale a pena investir na implementação deste controle. A Figura 4.7 apresenta os resultados para o ”FPV 5 - Dados”:

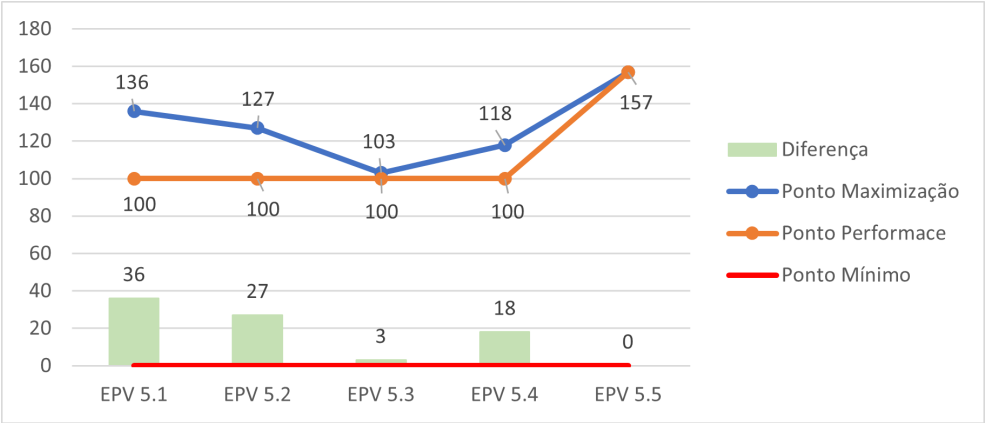

Figura 4.7: Resultado Dimensão FPV 5 - Dados.

Faz-se mister destacar que, analisando separadamente cada dimensão, após a tabulação das respostas e da realização do cálculo de contribuição, os controles de maneira individual apresentam apenas 5 possibilidades, que são os níveis (N1 a N5) com a pontuação atribuída a cada um a partir dos valores obtidos após a resposta aos questionários.

Contudo, esse valores podem ser analisados de uma maneira mais macro, os seja, avaliando a contribuição que cada dimensão tem para a implementação de uma ZTA. Assim, para obter tanto os valores de maximização das dimensões e a pontuação obtida, utiliza-se a Equação 2.9. Esta fórmula leva em consideração a contribuição de cada controle, conforme descrito na Figura 4.2 e o valor obtido ou valor de maximização, dependendo de qual contribuição esta se calculando.

Abaixo é demonstrado o cálculo do ponto de maximização do FPV 1:

$$
\begin{aligned}
G(a) &= \sum_{i=1}^{n} RR_i * V_i(a) \\
G(1) &= \sum_{i=1}^{4} RR_i * V_i(a) \\
G(1) &= RR_1 * V_1(a) + RR_2 * V_2(a) + RR_3 * V_3(a) + RR_4 * V_4(a) \\
G(1) &= 0,30 * 133 + 0,20 * 106 + 0,25 * 100 + 0,25 * 100 \\
G(1) &= 134
\end{aligned}
$$

Após a aplicação da Equação 2.9 para os pontos de maximização e os pontos obtidos nas cinco dimensões, obteve-se a Figura 4.8. A análise dele mostra que a ”FPV 2 - Dispositivo” apresenta uma contribuição maior dentre todas as dimensões, por conta de sua menor diferença entre o ponto de maximização e a pontuação obtida, mesmo não sendo esta a dimensão que apresenta o melhor desempenho, no caso a ”FPV 3 - Rede”.

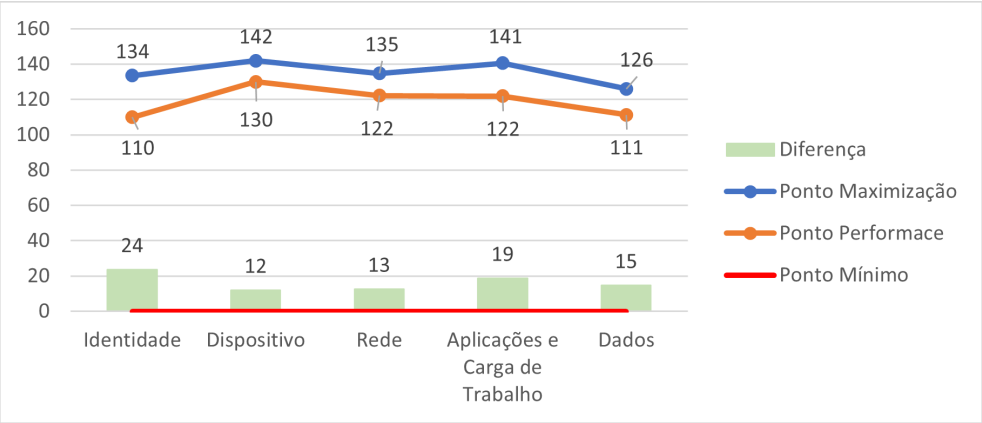

Figura 4.8: Resultado das Dimensões.

Finalmente, de uma maneira geral, a contribuição de todos os controles, apresentou um resultado interessante. O ponto de desempenho máximo para a implementação é de 134 unidades, e a pontuação obtida foi de 117. Ou seja, o resultado obtido encontra-se mais próximo de sua maximização do que estar no nível bom. A Figura 4.9 representa este resultado obtido.

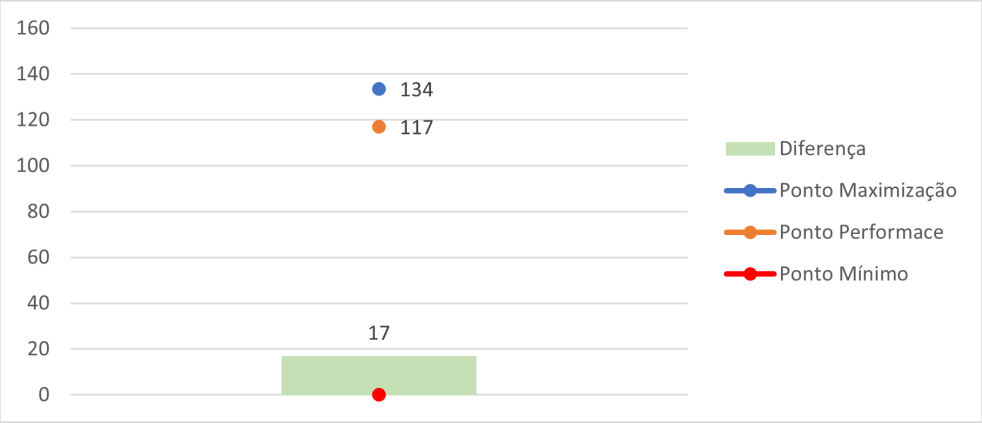

Figura 4.9: Resultado Geral.

De uma maneira geral, 10 dos 22 (45% do total) dos controle estudados obtiveram a pontuação máxima, em que pese, fazendo uma análise das medianas sem considerar o arredondamento da casa decimal, apenas 5 tenham alcançado a pontuação máxima. Isto mostra aos tomadores de decisão por onde iniciar a implementação de uma ZTA. Não quer dizer que os demais controles não devam ser implementados e ter uma atenção especial. Como descrito no pelo NIST [22] as implementações são dinâmicas e distintas, tendo forte ligação com a organização onde serão desenvolvidas.

A abordagem realizada no estudo teve como propósito entender como cada controle contribui para a implementação da ZTA dentro de uma organização. Com o início da implementação da ZTA na organização, o processo pode ser realizado novamente, porém com uma mudança de abordagem.

Inicialmente, deseja-se entender como cada controle pode contribuir. Já a partir do início da implementação, pode-se buscar entender o quanto já foi implementado ou se, com o desenvolvimento da noção do ZT, a visão dos *stakeholders* sofreu alteração ou melhoria.

Assim, levando em consideração uma evolução constante que uma organização deve ter quando se fala em segurança cibernética, o pilar da Gestão de Risco da melhoria contínua esta sendo aplicado.

5 CONCLUSÕES

A Segurança Cibernética apresenta-se como um tema debatido há bastante tempo. Conforme observado nos princípios de Saltzer & Schroeder, alguns princípios escritos naquela época, são válidos até os tempos atuais, sendo, inclusive, considerados dentro do conceito do ZT, como por exemplo o "*Default* seguro contra falhas". Além deste, o princípio da "Mediação Completa" pode ser considerado com uma boa relação com o ZT, visto que a ideia principal do ZT é de nunca confiar e sempre verificar. Outro importante princípio destacado pelos autores e que apresenta ligação direta com o conceito do ZT é o "Mecanismo comum mínimo".

Considerando o curto período que se passou desde o surgimento da ideia do ZT, é possível observar dentro da literatura, duas implementações e três padronizações distintas. No entanto, essas implementações variam amplamente nas organizações. Por outro lado, a diversidade de abordagens de implementação pode levar os gestores a terem pouco conhecimento sobre o assunto, o que dificulta a adoção de ações adequadas para promover uma mudança no paradigma de segurança dentro da organização.

Estas implementações e padronizações, levam em consideração dimensões e controles que devem ser utilizados. Assim, através de uma RSL realizada, é possível observar a necessidade e um estudo voltado para a implementação da ZTA, visto que os trabalhos encontrados no espectro buscado, não apresentaram estudos que apresentam a implementação de uma maneira geral, apenas de dimensões específicas.

A aplicação da metodologia multicritério construtivista para a priorização dos controles na implementação de uma ZTA dentro da organização demonstrou resultados positivos. Através da análise dos dados coletados e do envolvimento de todos os participantes do processo, foi possível constatar que essa abordagem promoveu uma melhora na compreensão do problema sobre a priorização para a implementação de soluções efetivas de segurança por parte dos decisores. A confirmação dessa hipótese fortalece a importância do uso desse modelo arquitetural para garantir a proteção e integridade dos recursos tecnológicos da organização diante do crescente número de ameaças cibernéticas que as organizações vem sofrendo.

A pesquisa apresentou como objetivo geral a avaliação e priorização de controles de segurança da informação baseados na ZTA, utilizando um método de decisão multicritério. O MCDA-C, com sua característica construtivista, foi o método escolhido para ser utilizado em um órgão da APF, onde foi possível observar as vantagens de seu emprego. No decorrer das etapas, os *stakeholders* usam as escalas qualitativas para apresentar seus pontos de vista. A partir desta escala qualitativa, uma escala quantitativa é obtida de modo a apresentar aos tomadores de decisão os pontos de minimização, maximização e o de performance dos controles considerados. Desta maneira, após a análise apresentada, os tomadores de decisão são capazes de visualizar melhor as informações para tomar melhores decisões.

As ameaças cibernéticas têm apresentado uma evolução, fazendo com que as organizações realizem medidas de maneira a mitigar os riscos de vazamento de informações sigilosas ou o sequestro de dados, por exemplo. A implementação da ZTA nas organizações, contribui para um aumento na eficiência da segurança cibernética e apresentando uma melhora na gestão de riscos. No decorrer da execução das etapas do MCDA-C, alguns princípios da gestão de riscos foram observados: Inclusão, Personalização, Dinâmico,

e Estruturado e Abrangente. Com isso, pode-se observar que utilização de um método multicritério como o utilizado contribui para que uma organização tenha uma melhor gestão de riscos

Uma das limitações encontradas neste trabalho é o fato de se ter poucas padronizações sobre a implementação de uma ZTA. Outra limitação encontrada foi a reduzida quantidade de trabalhos disponíveis na literatura. Além disso, por ser um tema relativamente novo e que tem pouco tempo que organismos internacionais desenvolveram suas padronizações, NIST em 2020, DoD em 2022 e CISA em 2023, poucos são os gestores que tem conhecimento sobre o assunto. Isto, não inviabilizou a aplicação do MCDA-C, uma vez que está intrínseco em seu processo a construção do conhecimento por parte de todos os envolvidos no processo.

5.1 TRABALHOS FUTUROS

O processo de definição dos pesos e suas contribuições foi realizado utilizado, exclusivamente, o pensamento do gestor de maneira individualizada a cada dimensão e controle. Existem outras maneiras para se realizar a definição, assim, pode-se considerar a utilização dos outros métodos multicritérios apresentados (AHP, COMET, SPOTIS, TOPSIS) para a definição da importância dos critérios na implementação da ZTA.

O processo de transformação das escalas qualitativas em quantitativas, foi realizado considerando um intervalo linear entre os pontos considerados ”NEUTRO” e ”BOM”. Isto pode trazer algum viés no resultado final, uma vez que cada controle tem seu grau de importância, conforme observado na etapa onde eles são ordenados em níveis de esforço. Desta maneira, com o propósito de trazer uma melhor clareza nesta definição, um trabalho possível pode ser a utilização da comparação em pares, utilizada no MACBETH para chegar a valores específicos para cada controle.

A partir da realização deste trabalho, os tomadores de decisão tem um caminho a ser trilhado, com a priorização para a implementação de uma ZTA. Porém, a medida que a ZTA é implementada, mudanças no pensamentos tantos dos gestores quanto dos demais integrantes da organização podem ocorre. Assim, a reaplicação da metodologia, com um *label* diferente, pode acontecer de modo a verificar como está a implementação deste conceito. Assim, é possível descobrir os possíveis claros encontrados neste processo de melhoria da segurança cibernética.

REFERÊNCIAS BIBLIOGRÁFICAS

1 JUNIOR, R. M. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Editora Cubzac, 2010. 182 p. ISBN 9788561293130.

2 SKOPIK, F.; LANDAUER, M.; WURZENBERGER, M. Blind Spots of Security Monitoring in Enterprise Infrastructures: A Survey. *IEEE Security and Privacy*, IEEE, p. 2–10, 2022. ISSN 15584046.

3 VANICKIS, R.; JACOB, P.; DEHGHANZADEH, S.; LEE, B. Access control policy enforcement for zero-trust-networking. In: . [S.l.: s.n.], 2018. ISBN 9781538660461.

4 TEERAKANOK, S.; UEHARA, T.; INOMATA, A. Migrating to zero trust architecture: Reviews and challenges. In: . [S.l.: s.n.], 2021. v. 2021. ISSN 19390122.

5 CHUAN, T.; LV, Y.; QI, Z.; XIE, L.; GUO, W. An implementation method of zero-trust architecture. In: . [S.l.: s.n.], 2020. v. 1651, n. 1. ISSN 17426596.

6 DISA, D. I. S. A.; NSA, N. S. A. *Department of Defense (DoD) Zero Trust Reference Architecture*. Washington, DC: USA: [s.n.], 2021 [Online]. Disponível em: <https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf>.

7 BUCK, C.; OLENBERGER, C.; SCHWEIZER, A.; VÖLTER, F.; EYMANN, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers and Security*, Elsevier Ltd, v. 110, p. 102436, 2021. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2021.102436>.

8 GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013. 550 p. ISBN 9788540701939.

9 AGENCY, C.; SECURITY, I. *Zero Trust Maturity Model*. [S.l.], 2023. 32 p. Disponível em: <https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf>.

10 KINDERVAG, J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. *Forrester Research, Inc.*, 2010. Disponível em: <'https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf>.

11 KINDERVAG, J. Build Security Into Your Network´s DNA: The Zero Trust Network Architecture. *Forrester Research, Inc.*, 2010. Disponível em: <https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf>.

12 ASSOCIACAO BRASILEIRA DE NORMAS TECNICAS. *ABNT 31000 Gestão de Riscos*: Principios e diretrizes. Rio de Janeiro, 2018. 17 p.

13 ASSOCIACAO BRASILEIRA DE NORMAS TECNICAS. *ABNT 31010 Gestão de Riscos*: Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012. 96 p.

14 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, p. 183–199, 2020. ISSN 15396924.

15 ARRUDA, L. G. S. d.; GIOZZA, W. F.; NUNES, R. R. O MÉTODO MULTICRITÉRIO NO APOIO À PRIORIZAÇÃO NA IMPLEMENTAÇÃO DO ZERO TRUST. In: *Proceedings of the Ibero American Conferences on Applied Computing 2022 and WWW/Internet 2022*.

IADIS Press, 2022. p. 171–175. Disponível em: <https://www.iadisportal.org/digital-library/o-método-multicritério-no-apoio-à-priorizaç~ao-na-implementaç~ao-do-zero-trust>.

16 ARRUDA, L. G. S. d.; GIOZZA, W. F.; NZE, G. D. A.; NUNES, R. R. Implementação da Arquitetura Zero Trust : uma Revisão Sistemática de Literatura. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n. 56, p. 261–275, 2023.

17 SALTZER, J. H.; SCHROEDER, M. D. The Protection of Information in Computer Systems. *Proceedings of the IEEE*, v. 63, n. 9, p. 1278–1308, 1975. ISSN 15582256.

18 RASHID, A.; CHIVERS, H.; DANEZIS, G.; LUPU, E.; MARTIN, A. The Cyber Security Body of Knowledge (CyBoK) 1.0. *CyBOKVersion 1.0 The National Cyber Security Centre 2019*, p. 808, 2019. Disponível em: <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>.

19 NACE, L. Securing Trajectory based Operations through a Zero Trust Framework in the NAS. *Integrated Communications, Navigation and Surveillance Conference, ICNS*, v. 2020-Septe, p. 1–8, 2020. ISSN 21554951.

20 GARBIS, J.; CHAPMAN, J. W. *Zero Trust Security*. Berkeley, CA: Apress, 2021. ISBN 978-1-4842-6701-1.

21 CUNNINGHAM, C. The-Zero-Trust-eXtended-ZTX-Ecosystem. *Forrester Research, Inc.*, p. 1–15, 2018.

22 ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. *Zero Trust Architecture*. Gaithersburg, MD, 2020. 1–6 p. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

23 WARD, R.; BEYER, B. Beyondcorp: A new approach to enterprise security. *;login:*, December 2014, Vol. 39, No. 6, p. 6–11, 2014. Disponível em: <https://www.usenix.org/publications/login/dec14/ward>.

24 OSBORN, B.; MCWILLIAMS, J.; BEYER, B.; SALTONSTALL, M. Beyondcorp: Design to deployment at google. *;login:*, Spring 2016, Vol. 41, No. 1, p. 28–34, 2016. Disponível em: <https://www.usenix.org/publications/login/spring2016/osborn>.

25 CITTADINI BATZ SPEAR, B. B. L.; SALTONSTALL, M. Beyondcorp part iii: The access proxy. *;login:*, Winter 2016, Vol. 41, No. 4, p. 28–33, 2016. Disponível em: <https://www.usenix.org/publications/login/winter2016/cittadini>.

26 PECK BETSY BEYER, C. B. J.; SALTONSTALL, M. Migrating to beyondcorp: Maintaining productivity while improving security. *;login:*, Summer 2017, Vol. 42, No. 2, p. 49–55, 2017. Disponível em: <https://www.usenix.org/publications/login/summer2017/peck>.

27 ESCOBEDO BETSY BEYER, M. S. V.; ZYZNIEWSKI, F. Beyondcorp 5: The user experience. *;login:*, Fall 2017, Vol. 42, No. 3, p. 38–43, 2017. Disponível em: <https://www.usenix.org/publications/login/fall2017/escobedo>.

28 JANOSKO, M.; KING, H.; BEYER, B. A. E.; SALTONSTALL, M. Beyondcorp 6: Building a healthy fleet. *;login:*, Fall 2018, Vol. 43, No. 3, p. 24–30, 2018. Disponível em: <https://www.usenix.org/publications/login/fall2018/king>.

29 MICROSOFT. *The Comprehensive Playbook for Implementing Zero Trust Security*. 2021. Disponível em: <https://clouddamcdnprodep.azureedge.net/gdc/gdctT4SO0/original>.

30 MICROSOFT. *Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies*. 2021. Disponível em: <https://www.microsoft.com/pt-br/security/business/zero-trust>.

31 DONTHU, N.; KUMAR, S.; MUKHERJEE, D.; PANDEY, N.; LIM, W. M. How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, Elsevier Inc., v. 133, n. May, p. 285–296, sep 2021. ISSN 01482963.

32 GALVÃO, M. C. B.; RICARTE, I. L. M. REVISÃO SISTEMÁTICA DA LITERATURA: CONCEITUAÇÃO, PRODUÇÃO E PUBLICAÇÃO. *Logeion: Filosofia da Informação*, v. 6, n. 1, p. 57–73, sep 2019. ISSN 2358-7806.

33 SIDDAWAY, A. P.; WOOD, A. M.; HEDGES, L. V. How to Do a Systematic Review: A Best Practice Guide for Conducting and Reporting Narrative Reviews, Meta-Analyses, and Meta-Syntheses. *Annual Review of Psychology*, v. 70, p. 747–770, 2019. ISSN 15452085.

34 PRISMA, G. *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*. University of Ottawa/Oxford University, 2020. Disponível em: <https://prisma-statement.org/>.

35 OUZZANI, M.; HAMMADY, H.; FEDOROWICZ, Z.; ELMAGARMID, A. Rayyan—a web and mobile app for systematic reviews. *Systematic Reviews*, Systematic Reviews, v. 5, n. 1, p. 210, dec 2016.

36 AMEER, S.; GUPTA, M.; BHATT, S.; SANDHU, R. Bluesky: Towards convergence of zero trust principles and score-based authorization for iot enabled smart systems. In: *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. New York, NY, USA: ACM, 2022. p. 235–244. Disponível em: <https://dl.acm.org/doi/10.1145/3532105.3535020>.

37 BELLO, Y.; REFAEY, A.; ULEMA, M.; KOLIPALI, J. On sustained zero trust conceptualization security for mobile core networks in 5g and beyond. *IEEE Transactions on Network and Service Management*, IEEE, 2022. ISSN 19324537.

38 CHEN, B.; QIAO, S.; ZHAO, J.; LIU, D.; SHI, X.; LYU, M.; CHEN, H.; LU, H.; ZHAI, Y. A security awareness and protection system for 5g smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, IEEE, v. 8, n. 13, p. 10248–10263, 2021. ISSN 23274662.

39 DECUSATIS, C.; LIENGTIRAPHAN, P.; SAGER, A.; PINELLI, M. Implementing zero trust cloud networks with transport access control and first packet authentication. *Proceedings - 2016 IEEE International Conference on Smart Cloud, SmartCloud 2016*, IEEE, p. 5–10, 2016.

40 DIMITRAKOS, T.; DILSHENER, T.; KRAVTSOV, A.; La Marra, A.; MARTINELLI, F.; RIZOS, A.; ROSETT, A.; SARACINO, A. Trust aware continuous authorization for zero trust in consumer internet of things. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, p. 1801–1812, 2020.

41 D'SILVA, D.; AMBAWADE, D. D. Building a zero trust architecture using kubernetes. *2021 6th International Conference for Convergence in Technology, I2CT 2021*, p. 1–8, 2021.

42 EIDLE, D.; NI, S. Y.; DECUSATIS, C.; SAGER, A. Autonomic security for zero trust networks. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017*, v. 2018-Janua, n. Area 4, p. 288–293, 2017.

43 FANG, W.; GUAN, X. Research on ios remote security access technology based on zero trust. *IEEE 6th Information Technology and Mechatronics Engineering Conference, ITOEC 2022*, IEEE, p. 238–241, 2022.

44 WANG, J.; CHEN, J.; XIONG, N.; ALFARRAJ, O.; TOLBA, A.; REN, Y. S-bds: An effective blockchain-based data storage scheme in zero-trust iot. *ACM Transactions on Internet Technology*, 2022. ISSN 1533-5399.

45 YAO, Q.; WANG, Q.; ZHANG, X.; FEI, J. Dynamic access control and authorization system based on zero-trust architecture. *ACM International Conference Proceeding Series*, p. 123–127, 2020.

46 HATAKEYAMA, K.; KOTANI, D.; OKABE, Y. Zero trust federation: Sharing context under user control towards zero trust in identity federation. *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2021*, p. 514–519, 2021.

47 HOSNEY, E. S.; HALIM, I. T. A.; YOUSEF, A. H. An artificial intelligence approach for deploying zero trust architecture (zta). *5th International Conference on Computing and Informatics, ICCI 2022*, IEEE, p. 343–350, 2022.

48 WU, Y. G.; YAN, W. H.; WANG, J. Z. Real identity based access control technology under zero trust architecture. *Proceedings - 2021 International Conference on Wireless Communications and Smart Grid, ICWCSG 2021*, p. 18–22, 2021.

49 Da Rocha, B. C.; De Melo, L. P.; De Sousa, R. T. Preventing apt attacks on lan networks with connected iot devices using a zero trust based security model. *2021 Workshop on Communication Networks and Power Systems, WCNPS 2021*, 2021.

50 DZOGOVIC, B.; SANTOS, B.; HASSAN, I.; FENG, B.; DO, V. T.; JACOT, N.; Van Do, T. Zero-trust cybersecurity approach for dynamic 5g network slicing with network service mesh and segment-routing over ipv6. IEEE, p. 105–114, 2022.

51 LI, Z.; DING, Y.; GAO, H.; QU, B.; WANG, Y.; LI, J. A highly compatible verification framework with minimal upgrades to secure an existing edge network. *ACM Transactions on Internet Technology*, 2022. ISSN 1533-5399.

52 MUJIB, M.; SARI, R. F. Performance evaluation of data center network with network micro-segmentation. *ICITEE 2020 - Proceedings of the 12th International Conference on Information Technology and Electrical Engineering*, p. 27–32, 2020.

53 ZAHEER, Z.; CHANG, H.; MUKHERJEE, S.; MERWE, J. V. D. Eztrust: Network-independent zero-trust perimeterization for microservices. *SOSR 2019 - Proceedings of the 2019 ACM Symposium on SDN Research*, p. 49–61, 2019.

54 OLECHOWSKI, A.; OEHMEN, J.; SEERING, W.; BEN-DAYA, M. The professionalization of risk management: What role can the iso 31000 risk management principles play? *International Journal of Project Management*, v. 34, n. 8, p. 1568–1578, 2016. ISSN 0263-7863. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0263786316300631>.

55 DUTRA, A. *Elaboração de um Sistema de Avaliação de Desempenho de Recursos Humanos da Secretaria de Estado da Administração à Luz da Metodologia Multicritério de Apoio à Decisão*. Tese (Doutorado) — Universidade de Santa Catarina, 1998.

56 JÚNIOR, A. L. N.; MACHADO, C. M.; SILUK, J. C. M.; SOLIMAN, M.; HUPFER, N. T.; PARIS, S. R. de. Comparativo entre as metodologias MCDA-C, DEA e AHP. *Revista da FAE*, v. 18, n. 1, p. 6–19, 2015. ISSN 2447-2735. Disponível em: <https://revistafae.fae.edu/revistafae/article/view/27/27>.

57 MUNIER, N. A new approach to the rank reversal phenomenon in mcdm with the simus method. *Multiple criteria decision making*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, v. 11, p. 137–152, 2016.

58 ZLAUGOTNE, B.; ZIHARE, L.; BALODE, L.; KALNBALKITE, A.; KHABDULLIN, A.; BLUMBERGA, D. Multi-Criteria Decision Analysis Methods Comparison. *Environmental and Climate Technologies*, v. 24, n. 1, p. 454–471, 2020. ISSN 22558837.

59 CUNHA, D. A.; ANDRADE, M.; PRADO, L. A.; SANTANA, L. O.; Gonçalves da Silv, M. P. RISK assessment in airport maintenance runway condition using MCDA-C. *Journal of Air Transport Management*, Elsevier Ltd, v. 90, n. August 2020, 2021.

60 COSTA, I. P. d. A.; CORRIÇA, J. V. d. P.; PEREIRA, P. D. D. A. d. M.; GOMES, P. D. C. F. S.; SANTOS, P. D. M. dos. Análise Multicritério Para Composição De Portfólio De Cursos De Tecnologia Da Informação: Uma Aplicação Do Método Electre-Mor. *Revista SIMEP*, v. 1, 2021.

61 MOREIRA, F. R.; Da Silva Filho, D. A.; NZE, G. D. A.; de Sousa Junior, R. T.; NUNES, R. R. Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access*, v. 9, 2021. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9540950/>.

62 STOILOVA, S.; MUNIER, N. A Novel Fuzzy SIMUS Multicriteria Decision-Making Method. An Application in Railway Passenger Transport Planning. *Symmetry*, v. 13, n. 3, p. 483, mar 2021. ISSN 2073-8994.

63 STOILOVA, S. D. A multi-criteria approach for evaluating the urban transport technologies by using simus method. In: IOP PUBLISHING. *IOP Conference Series: Materials Science and Engineering*. [S.l.], 2019. v. 618, n. 1, p. 012059.

64 SAATY, T. L. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, v. 48, n. 1, p. 9–26, 1990. ISSN 03772217.

65 SALABUN, W. The characteristic objects method: A new distance-based approach to multicriteria decision-making problems. *Journal of Multi-Criteria Decision Analysis*, v. 22, n. 1-2, p. 37–50, 2015. ISSN 10991360.

66 SAŁABUN, W.; PIEGAT, A. Comparative analysis of MCDM methods for the assessment of mortality in patients with acute coronary syndrome. *Artificial Intelligence Review*, Springer Netherlands, v. 48, n. 4, p. 557–571, dec 2017. ISSN 0269-2821.

67 ENSSLIN, S. R.; CARVALHO, F. N. de; GALLON, A. V.; ENSSLIN, L. Uma metodologia multicritério (MCDA-C) para apoiar o gerenciamento do capital intelectual organizacional. *Revista de Administração Mackenzie*, v. 9, n. 7, p. 136–162, 2008.

68 ENSSLIN, L.; GIFFHORN, E.; ENSSLIN, S. R.; PETRI, S. M.; VIANNA, W. B. Avaliação do desempenho de empresas terceirizadas com o uso da metodologia multicritério de apoio à decisão - construtivista. *Pesquisa Operacional*, v. 30, n. 1, p. 125–152, apr 2010. ISSN 0101-7438.

69 Bana E Costa, C. A.; ENSSLIN, L.; CORRÊA, É. C.; VANSNICK, J. C. Decision Support Systems in action: Integrated application in a multicriteria decision aid process. *European Journal of Operational Research*, v. 113, n. 2, p. 315–335, 1999. ISSN 03772217.

70 ENSSLIN, L.; DUTRA, A.; ENSSLIN, S. MCDA: a constructivist approach to the management of human resources at a governmental agency. *International Transactions in Operational Research*, v. 7, n. 1, p. 79–100, jan 2000. ISSN 0969-6016.

71 MUNIER, N.; CARIGNANO, C. E.; ALBERTO, C. L. SIMUS. Un método de programación multiobjetivo. *Revista de la Escuela de Perfeccionamiento en Investigación Operativa*, v. 24, n. 39, p. 44–54, 2016.

72 DEZERT, J.; TCHAMOVA, A.; HAN, D.; TACNET, J.-M. The spotis rank reversal free method for multi-criteria decision-making support. In: *2020 IEEE 23rd International Conference on Information Fusion (FUSION)*. [S.l.]: IEEE, 2020. p. 1–8.

73 BACZKIEWICZ, A.; KIZIELEWICZ, B.; SHEKHOVTSOV, A.; WATROBSKI, J.; WIECKOWSKI, J.; SALABUN, W. Towards an e-commerce recommendation system based on MCDM methods. In: *2021 International Conference on Decision Aid Sciences and Application (DASA)*. IEEE, 2021. p. 991–996. ISBN 978-1-6654-1634-4. Disponível em: <https://ieeexplore.ieee.org/document/9682356/>.

74 AGHAMOHAMMADPOUR, A.; MAHDIPOUR, E.; ATTARZADEH, I. Architecting threat hunting system based on the dodaf framework. *J. Supercomput.*, Kluwer Academic Publishers, USA, v. 79, n. 4, p. 4215–4242, sep 2022. ISSN 0920-8542.

75 HP3C '22: Proceedings of the 6th International Conference on High Performance Compilation, Computing and Communications. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396295.

76 ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450396707.

77 CSSE '22: Proceedings of the 5th International Conference on Computer Science and Software Engineering. New York, NY, USA: Association for Computing Machinery, 2022. ISBN 9781450397780.

78 KUMAR, P.; MANGLA, S. K.; KAZANCOGLU, Y.; EMROUZNEJAD, A. A decision framework for incorporating the coordination and behavioural issues in sustainable supply chains in digital economy. *Annals of Operations Research*, 2022.

79 AZADNIA, A. H.; GERANSAYEH, M.; ONOFREI, G.; GHADIMI, P. A weighted fuzzy approach for green marketing risk assessment: Empirical evidence from dairy industry. *Journal of Cleaner Production*, v. 327, 2021.

80 KHORUZHY, L.; BULYGA, R. P.; VORONKOVA, O. Y.; VASYUTKINA, L.; SAENKO, N. R.; POLTARYKHIN, A. L.; ARAVINDHAN, S. A new trust management framework based on the experience of users in industrial cloud computing using multi-criteria decision making. *Kybernetes*, v. 51, n. 6, p. 1949–1966, 2022.

81 PAPAKONSTANTINOU, N.; BOSSUYT, D. V.; LINNOSMAA, J.; O'HALLORAN, B.; HALE, B. A zero trust hybrid security and safety risk analysis method. *Journal of Computing and Information Science in Engineering*, v. 21, n. 5, 2021.

82 PAPAKONSTANTINOU, N.; BOSSUYT, D. van; LINNOSMAA, J.; HALE, B.; O'HALLORAN, B. Towards a zero trust hybrid security and safety risk analysis method. In: . [S.l.: s.n.], 2020. v. 9.

83 SANDBORN, P.; LUCYSHYN, W. *System sustainment: Acquisition and engineering processes for the sustainment of critical and legacy systems*. [S.l.: s.n.], 2022. 1 – 374 p.

84 WANG, W.; CHEN, X.; GAN, W.; YANG, Y.; ZHANG, W.; ZHANG, X.; WU, F. Research on network security situation assessment model based on double ahp. *Communications in Computer and Information Science*, v. 1588 CCIS, p. 489 – 506, 2022.

85 ANDRADE, R. O.; YOO, S. G.; ORTIZ-GARCES, I.; BARRIGA, J. Security risk analysis in iot systems through factor identification over iot devices. *Applied Sciences (Switzerland)*, v. 12, n. 6, 2022.

86 SU, X.; ZHONG, M. Supply chain risk prevention and control based on fuzzy influence diagram and discrete hopfield neural network. *Discrete Dynamics in Nature and Society*, v. 2021, 2021.

87 MEHRAJ, S.; BANDAY, M. T. A dynamic weighted averaging technique for trust assessment in cloud computing. *International Journal of Cloud Applications and Computing*, v. 12, n. 1, 2022.

88 GOMES, M.; PEREIRA, R.; SILVA, M.; VACONCELOS, J. B. de; ROCHA, A. Kpis for evaluation of devops teams. *Lecture Notes in Networks and Systems*, v. 470 LNNS, p. 142 – 156, 2022.

89 BUI, H. T.; HUSSAIN, O. K.; PRIOR, D.; HUSSAIN, F. K.; SABERI, M. Proof by earnestness (poe) to determine the authenticity of subjective information in blockchains - application in supply chain risk management. *Knowledge-Based Systems*, v. 250, 2022.

90 JABAR, T.; SINGH, M. M. Exploration of mobile device behavior for mitigating advanced persistent threats (apt): A systematic literature review and conceptual framework. *Sensors*, v. 22, n. 13, 2022.

91 SILVA, E. L. da; MENEZES, E. M. Metodologia Da Pesquisa E Do Trabalho. *UFSC*, n. January 2005, p. 138, 2005.

92 GIL, A. C. *Métodos e técnicas de pesquisa social*. 7. ed. São Paulo: Editora Atlas, 2019. 230 p. ISBN 9788597020984.

93 GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 7. ed. São Paulo: Editora Atlas, 2022. 186 p. ISBN 9786559771646.