O MÉTODO MULTICRITÉRIO NO APOIO À PRIORIZAÇÃO NA IMPLEMENTAÇÃO DO ZERO TRUST

Luiz Guilherme Schiefler de Arruda[1], William Ferreira Giozza[1] e Rafael Rabelo Nunes[1,2,3]
[1]*Departamento de Engenharia Elétrica – Universidade de Brasília (UnB)*
Campus Universitário Darcy Ribeiro, UnB – Brasília, DF, 70910-900 - Brasil
[2]*Departamento de Administração – Universidade de Brasília (UnB)*
Campus Universitário Darcy Ribeiro, UnB – Brasília, DF, 70910-900 - Brasil
[3]*Centro Universitário Atenas*
Rua Euridamas Avelino de Barros, nº 1400, Prado – Paracatu, MG, 38602-002 - Brasil

RESUMO

Este trabalho propõe diretrizes para priorizar a implementação das dimensões do modelo Zero Trust (ZT) desenvolvida pela Microsoft utilizando um método multicritério construtivista. No artigo é apresentado a sequência de elaboração da árvore de Pontos de Vista (PV) até o nível dos descritores e os procedimentos necessários até a tomada de decisão por parte dos gestores. O trabalho apresenta relevância, visto que o conceito ZT é relativamente recente e, com o apoio do método multicritério, demonstra uma maneira de auxiliar na tomada de decisão na priorização de sua implementação.

PALAVRAS-CHAVE

MCDA-C, Segurança Cibernética, *Zero Trust Architecture* (ZTA), Apoio à Decisão

1. INTRODUÇÃO

Desde o início das infraestruturas de Tecnologia da Informação (TI) sua proteção foi baseada no perímetro, ou seja, algo semelhante a um castelo, onde há altos muros na proteção e apenas uma maneira de entrada e saída. Assim tudo que se encontra dentro do castelo é considerado seguro e aquilo que está fora é considerado perigo (Ward & Beyer, 2014). Entretanto, esta arquitetura de segurança de rede, baseada na proteção de bordas apresenta dois grandes riscos: ausência de defesa contra ataques oriundos internamente a rede; e uma dependência dos dispositivos de segurança existentes nas bordas (Chuan et al., 2020).

Com este pensamento, grandes empresas estão considerando imperativo a adoção de uma nova abordagem na segurança, devendo começar com a implementação de uma estratégia *Zero Trust* (ZT) (Microsoft, 2021a). Considerando esse ponto, a Microsoft publicou de adoção de um framework ZT composto por seis dimensões, a saber: Identidades, Dispositivos, Aplicações, Dados, Infraestrutura e Rede (Microsoft, 2021b).

Desta maneira, este artigo apresenta uma proposta para priorizar as dimensões que devem ser consideradas no intuito de ampliar a segurança cibernética com a implementação da ZTA com a utilização da Metodologia Multicritério de Apoio à Decisão Construtivista (MCDA-C). Assim, o trabalho apresenta em sua seção 2 uma explicação sobre o ZT e a *Zero Trust Architecture* (ZTA), bem como implementações desta arquitetura realizada pela Microsoft; na seção 3 será explicitado como o Método Multicritério de Apoio a Decisão (MCDA) pode ser utilizado na priorização de implementação da ZTA; e finalizando na seção 4 são discorridas as conclusões da utilização desta metodologia.

2. O *ZERO TRUST* (ZT)

O crescimento da computação na nuvem e IoT, bem como de pessoas trabalhando de maneira remota, trouxe um aumento na complexidade relacionada a proteção dos recursos de uma corporação. Baseado nesta concepção, segundo Kerman et al. (2020) o conceito conhecido como ZT é um conjunto de princípios de segurança cibernética com foco na mudança de uma segurança estática e baseada em perímetros para uma focado nos sujeitos, ativos corporativos, indivíduos e pequenos grupos de recursos.

Com isso, algumas empresas, como a Google (Ward & Beyer, 2014) e a Microsoft (Microsoft, 2021a), desenvolveram sua própria ZTA que seria um *framework* de implementação deste conceito de segurança. No mesmo sentido, o *National Institute of Standards and Technology* (NIST), apresentou em 2020 seu padrão para a implementação da ZTA (Kerman et al., 2020).

A Microsoft observou uma necessidade na mudança da forma na qual empregava a segurança de seus ativos aliado ao crescimento do trabalho híbrido. Desta maneira, surgiu a necessidade de uma nova abordagem na proteção de identidades, validação da integridade dos dispositivos, aplicação de privilégios mínimos, entre outros (Microsoft, 2021a). Este modelo foi desenvolvido para prover uma experiência de usuário simplificada, habilitando-os a gerenciar e encontrar conteúdos com facilidade e segurança (Deshpande, 2021).

A ZTA da Microsoft desenvolve sua implementação abordando seis dimensões, apresentando, desta maneira, um nível de maturidade para medir a implementação e prontidão do ZT focado na utilização das ferramentas desenvolvidas por eles (Bobbert, 2020; Microsoft, 2021b).

3. MÉTODO MULTICRITÉRIO DE APOIO A DECISÃO (MCDA)

Conforme a ISO (2012), é necessária uma abordagem sistemática de gestão de riscos de segurança da informação para identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um Sistema de Gestão de Segurança da Informação (SGSI) eficaz. O MCDA é uma da ferramentas que pode ser utilizada para identificar, analisar e avaliar riscos (ABNT 2012).

Além disso, o MCDA auxilia na solução de problemas, com aspectos qualitativos ou quantitativos complexos. Ela facilita a decisão ao apresentar as opções a serem escolhidas conforme a importância do problema e o critério escolhido (Hamzane & Abdessamad, 2019). Moreira et al. (2021) utilizaram esse método para priorizar controles da função Detectar do *framework* NIST CSF.

Desta maneira, o MCDA-C, uma ramificação do MCDA, adota o paradigma construtivista para auxiliar no processo decisório, apresentando recomendações e linhas de ação com o propósito de construir o conhecimento em cenários complexos. Com isso, podemos compreender que o MCDA-C atua como um facilitador do processo decisório (Júnior et al., 2015).

Segundo apresentado por Bana e Costa et al. (1999); L. Ensslin et al. (2000) o processo de construção dos critérios utilizados no MCDA-C apresenta uma sequência lógica, que de certa forma pode ser cíclica, descrita em três etapas: i) Estruturação do problema; ii) Avaliação; e iii) Criação das orientações de ação. Além disso, Ensslin et al. (2008) complementam que a primeira etapa apresenta uma fundamental importância pois é durante esta fase que ocorre o entendimento do problema e onde ele está inserido.

Considerando as três etapas lógicas, L. Ensslin et al., (2010) descrevem que a primeira etapa apresenta uma metodologia qualitativa, na medida em que se desenvolve a estruturação dos objetivos. Por outro lado, os mesmos autores observam uma abordagem metodológica quantitativa na segunda etapa, visto que, transforma as escalas cardinais em ordinais.

3.1 Estruturação do Problema

Esta etapa do processo consiste na produção de um entendimento do problema e todo o contexto no qual ele está inserido. É constituída das seguintes subetapas: i) caracterização do contexto e identificação dos atores; ii) identificação dos Elementos Primários de Avaliação (EPA); iii) agrupamento dos EPA por afinidades; iv) construção da árvore de pontos de vista e mapas de relação meios-fins; e v) construção dos descritores dos objetivos (L. Ensslin et al., 2010).

O Ponto de Vista (PV) inicial, a partir do qual o estudo foi desenvolvido, é a implementação da ZTA. Considerando as dimensões utilizadas pela Microsoft, este PV apresenta seis Pontos de Vistas Fundamentais (PVF): Identidade, Dispositivo, Rede, Dados, Infraestrutura e Aplicações. A partir disso, considerando os controles apresentados pela Microsoft (2021b) foi possível construir as ramificações dos PVF, chamados de Ponto de Vista Elementar (PVE).

Com os PVE definidos, a cada um deles foi atribuído um conjunto de cinco descritores que servirão, no decorrer da pesquisa, como uma maneira de definir, na visão da pessoa que responde, o nível de implementação para este PVE. Assim, com a árvore estabelecida e os descritores definidos é possível construir escalas ordinais e posteriormente, níveis hierárquicos, partindo de não implementado até completamente implementado e cada um destes níveis correspondendo a uma escala numérica, onde o mais alto deles corresponde ao que seria a meta para implementação e um nível médio, como o aceitável. Desta maneira, uma escala de um a cinco foi definida, sendo considerado o nível dois (N2) e quatro (N4) os pontos mínimos e ideal para cada PVE, respectivamente.

3.2 Avaliação do Problema

Etapa com objetivo de construir um modelo matemático, no qual as alternativas serão avaliadas, baseado no resultado da realização das seguintes etapas: i) construção das funções de valor; ii) identificação das taxas de compensação/substituição entre objetivos; iii) identificação do perfil de desempenho; e iv) avaliação global (L. Ensslin et al., 2010) .

A partir dos níveis estabelecidos na etapa anterior, o próximo passo é elaborar um modelo matemático que será utilizado no processo para definir-se o nível de esforço necessário à implementação de cada dimensão, visto que as escalas obtidas anteriormente podem não representar números reais. Com isso, juntamente com os decisores da corporação, foi definido os pesos, em percentual, considerando o esforço para a implementação do ZTA, considerando, inicialmente apenas os seis PVF. Na sequência, da mesma maneira, os PVE foram avaliados, sendo considerado apenas os PVE dentro de cada PVF. Ao término desta etapa, foi possível ter uma sequência, dos PVE em relação ao nível de dificuldade para a implementação de cada um deles.

Segundo Moreira et al. (2021) a cada descritor é atribuída uma escala cardinal obtida, utilizando uma equação linear, descrita na equação (1) entre o nível considerado mínimo (valor 0) e bom (valor 100), neste caso, N1 e N4 respectivamente. Para o valor ótimo, é considerado a posição (PS) na ordem de prioridade dos descritores (N) e um peso (P), conforme podemos observar na equação (2).

$$N(x) = 33{,}33 * (x - 1) \quad (1) \qquad N_M(x) = 100 + P * \big(N - (PS - 1)\big) \quad (2)$$

Na sequência, um questionário é enviado aos *stakeholders*, de maneira que seja respondido, na sua opinião, como está a implementação de cada PVE, considerando a escala de descritores (N1 a N5) definidas anteriormente. O *stakeholder* poderá, também, escolher a opção não sei responder. Após as respostas são tabuladas sendo calculada a mediana dos descritores para cada PVE, sendo desconsiderado, nesse caso, as respostas não sei responder. Com isso, torna-se possível verificar qual o nível de implementação atual de cada um dos controles em cada situação.

3.3 Criação das Orientações de Ação

Finalmente, com a realização das duas etapas anteriores, é possível fornecer subsídios aos decisores/organizações, para que estes tenham condições de aperfeiçoar cada alternativa e de analisar o conjunto de alternativas que mais contribui para a organização (L. Ensslin et al., 2010).

A última etapa é realizada a partir dos dados tabulados dos questionários respondidos pelos *stakeholder*s. Esta tabulação é ordenada em um gráfico para cada PVF, onde são apresentados: o nível mínimo considerado para a implementação, no caso 0, visto que não é possível uma implementação negativa; o nível considerado excelente; e a performance obtida das respostas dos *stakeholder*s. Com isso, é possível visualizar, graficamente, conforme a Figura 1, aqueles pontos que precisam de um maior cuidado e implementação por parte da empresa.

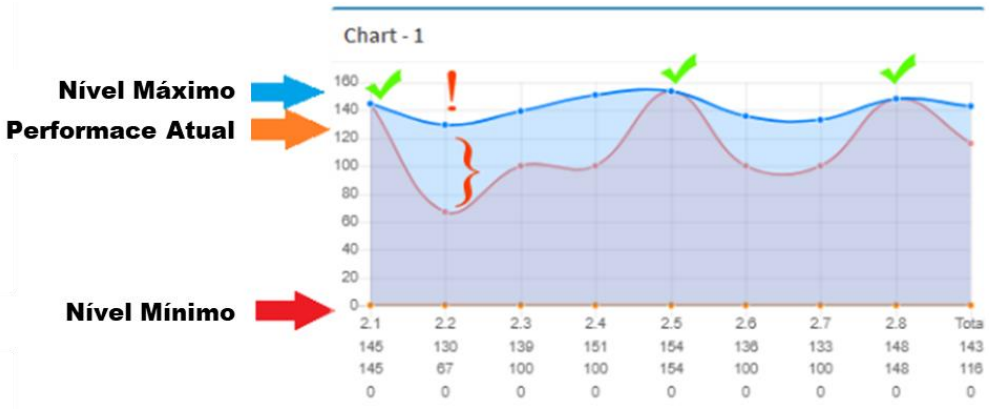

Figura 1. Gráfico obtido com a aplicação do MCDA-C (Moreira et al. 2021)

Baseado no estudo de Moreira et al. (2021), será possível analisar os controles onde os esforços devem ser priorizados para melhorar a segurança da corporação. Isso ocorre analisando o gráfico, quando a linha laranja (Performance Atual) se encontra o mais afastado da linha azul (Nível Máximo).

Assim, verificando aqueles pontos de atenção, sugestões sobre o que fazer para melhorar estes descritores para atingir um nível adequado em cada PVE, são apresentadas aos decisores para que, no caso de aceitação e consideração dos pontos observados, a empresa possa saber como proceder para melhorar sua implementação da ZTA.

4. CONCLUSÃO

No decorrer do estudo, mostrou-se a importância que duas empresas mundialmente conhecidas estão dando no quesito relacionado a segurança. Isto ocorre com seus trabalhos de implementação da ZTA. Entretanto, não foi possível observar na leitura das implementações nem da padronização elaborada pelo NIST, uma sequência ou priorização no desenvolvimento das dimensões.

Neste diapasão, o MCDA-C surge como uma ferramenta com capacidade de auxiliar as corporações no processo de tomada de decisão. Assim, utilizou-se dela como suporte na elaboração de uma priorização. Isto porque, com o apoio dos *stakeholders* da empresa, é possível repassar aos decisores e gestores informações sobre a situação interna de modo a criar uma reflexão e melhor entender como está a organização no tocante a segurança das informações.

Ao final da aplicação do MCDA-C proposta neste estudo, será possível apresentar graficamente aos decisores, como está o nível de implementação dos controles, além daqueles que necessitam de uma maior atenção por estarem com uma baixa implementação dentro da corporação.

O objetivo da pesquisa foi apresentar uma maneira de apresentar uma priorização de implementação das dimensões utilizadas pela Microsoft em sua ZTA. Esta priorização será possível com a realização das etapas apresentadas pelo MCDA-C.

AGRADECIMENTOS

Os autores agradecem o suporte da ABIN TED 08/2019. O autor Rafael Rabelo Nunes agradece o suporte do Centro Universitário Atenas e da Universidade de Brasília, por meio do Edital PI/DPG 02/2022.

REFERÊNCIAS

Ameer, S., Gupta, M., Bhatt, S., & Sandhu, R. (2022). BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems. *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, 235–244. https://doi.org/10.1145/3532105.3535020

Associação Brasileira de Normas Técnicas. (2012). Gestão de riscos – Técnicas para o processo de avaliação de riscos (ABNT NBR ISO/IEC 31010:2012).

Bana E Costa, C. A., Ensslin, L., Corrêa, É. C., & Vansnick, J. C. (1999). Decision Support Systems in action: Integrated application in a multicriteria decision aid process. *European Journal of Operational Research*, *113*(2), 315–335. https://doi.org/10.1016/S0377-2217(98)00219-7

Bobbert, Y. (2020). Zero Trust Validation: From Practical Approaches to Theory. *Scientific Journal of Research & Reviews*, *2*(5), 1–13. https://doi.org/10.33552/sjrr.2020.02.000546

Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (2020). An Implementation Method of Zero-trust Architecture. *Journal of Physics: Conference Series*, *1651*(1). https://doi.org/10.1088/1742-6596/1651/1/012010

Deshpande, A. (2021). A Study on Rapid Adoption of Zero Trust Network Architectures by Global Organizations Due to COVID-19 Pandemic. In *New Visions in Science and Technology Vol. 1* (pp. 26–33). Book Publisher International (a part of SCIENCEDOMAIN International). https://doi.org/10.9734/bpi/nvst/v1/3640F

Ensslin, L., Dutra, A., & Ensslin, S. R. (2000). MCDA: a constructivist approach to the management of human resources at a governmental agency. *International Transactions in Operational Research*, *7*(1), 79–100. https://doi.org/10.1111/j.1475-3995.2000.tb00186.x

Ensslin, L., Giffhorn, E., Ensslin, S. R., Petri, S. M., & Vianna, W. B. (2010). Avaliação do desempenho de empresas terceirizadas com o uso da metodologia multicritério de apoio à decisão - construtivista. *Pesquisa Operacional*, *30*(1), 125–152. https://doi.org/10.1590/S0101-74382010000100007

Ensslin, S. R., Carvalho, F. N. de, Gallon, A. V., & Ensslin, L. (2008). Uma metodologia multicritério (MCDA-C) para apoiar o gerenciamento do capital intelectual organizacional. *Revista de Administração Mackenzie*, *9*(7), 136–162.

Hamzane, I., & Abdessamad, B. (2019). A built-in criteria analysis for best IT governance framework. *International Journal of Advanced Computer Science and Applications*, *10*(10), 185–190. https://doi.org/10.14569/ijacsa.2019.0101026

International Organization for Standardization. (2012). Information technology – Security techniques – Information security risk management (ISO Standard No. 27005:2012). https://www.iso.org/standard/75281.html

Júnior, A. L. N., Machado, C. M., Siluk, J. C. M., Soliman, M., Hupfer, N. T., & Paris, S. R. de. (2015). Comparativo entre as metodologias MCDA-C, DEA e AHP. *Revista Da FAE*, *18*(1), 6–19. https://revistafae.fae.edu/revistafae/article/view/27/27

Kerman, A., Borchert, O., Rose, S., Division, E., & Tan, A. (2020). Implementing a Zero Trust Architecture. *Nist*, *October*.

Microsoft. (2021a). *Evolving Zero Trust: How real-world deployments and attacks are shaping the future of Zero Trust strategies*. https://www.microsoft.com/pt-br/security/business/zero-trust

Microsoft. (2021b). *The Comprehensive Playbook for Implementing Zero Trust Security*. https://clouddamcdnprodep.azureedge.net/gdc/gdctT4SO0/original

Moreira, F. R., da Silva Filho, D. A., Nze, G. D. A., de Sousa Junior, R. T., & Nunes, R. R. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access*, *9*, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. ;;*Login:*, *39*(6), 6–11. https://www.usenix.org/publications/login/dec14/ward

Zlaugotne, B., Zihare, L., Balode, L., Kalnbalkite, A., Khabdullin, A., & Blumberga, D. (2020). Multi-Criteria Decision Analysis Methods Comparison. *Environmental and Climate Technologies*, *24*(1), 454–471. https://doi.org/10.2478/rtuect-2020-0028