REVISTA DE GESTÃO E SECRETARIADO
MANAGEMENT AND ADMINISTRATIVE PROFESSIONAL REVIEW
ISSN: 2178-9010

Revista GeSec
São Paulo, SP, Brasil v. 14, n. 1, p. 1158-1169,2023

DOI: http://dx.doi.org/10.7769/gesec.v14i1.1581

Threat modeling: a study on its application in digital transformation from the perspective of risk

Modelagem de ameaças: um estudo sobre sua aplicação na transformação digital a partir da perspectiva do risco

Abinel Santiago Cerqueira Junior[1]
Carlos Hideo Arima [2]

Abstract

Information security is a topic that has been increasingly discussed nowadays after the beginning of the pandemic and its understanding has been fundamental to protect information in several organizations. The present study aims to identify and analyze the application of threat modeling in digital transformation from the perspective of information security risks. For the development of the research, a systematic review of the literature was conducted with the adoption of a protocol based on PRISMA-P to identify which threat modeling techniques have been applied in digital transformation and which information security risk approaches are used in the application of the threat modeling. The result of this study suggests that threat modeling applied in digital transformation uses customized models by means of unspecified techniques and that qualitative risk approaches have been adopted more frequently in digital transformation.

Keywords: Information Security. Threat Modeling. Digital Transformation. Risk Management. Cyber Risk.

[1] Master in Management and Technology in Productive Systems. Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS). R. Alcântara, 113, Vila Guilherme, São Paulo – SP, CEP: 02110-010.
E-mail: abinel.cerqueira@cpspos.sp.gov.br Orcid: https://orcid.org/0000-0003-2256-941X
[2] PhD in Controllership and Accounting. Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS). R. Alcântara, 113, Vila Guilherme, São Paulo - SP, CEP: 02110-010. E-mail: charima@uol.com.br
Orcid: https://orcid.org/0000-0001-7922-0943

Resumo

A segurança da informação é um tema que tem sido cada vez mais discutido hoje em dia após o início da pandemia e seu entendimento tem sido fundamental para proteger a informação em várias organizações. O presente estudo visa identificar e analisar a aplicação do modelo de ameaça na transformação digital a partir da perspectiva dos riscos de segurança da informação. Para o desenvolvimento da pesquisa, foi realizada uma revisão sistemática da literatura com a adoção de um protocolo baseado no PRISMA-P para identificar quais técnicas de modelagem de ameaças foram aplicadas na transformação digital e quais abordagens de risco de segurança da informação são utilizadas na aplicação da modelagem de ameaças. O resultado deste estudo sugere que a modelagem de ameaças aplicada na transformação digital usa modelos personalizados por meio de técnicas não especificadas e que abordagens de risco qualitativo foram adotadas com mais freqüência na transformação digital.

Palavras-chave: Segurança da Informação. Modelagem de Ameaças. Transformação Digital. Gerenciamento de Riscos. Risco Cibernético.

Introduction

The digital transformation brings new perspective for organizations because its fast growing around the world permits new digital services that can be available to users. To control cybersecurity risk existent in this context, threat prevention can help to manage and control this type of risk.

For this, threat modeling is a technique that aims to continuously improve a digital environment in various contexts, such as, in the construction or maintenance of software, implementation, maintenance or adoption of new technologies and solutions, assisting in topics related to information security (YOKOYAMA; ARIMA, 2022).

Ucedavélez and Morana (2015) affirm that threat modeling is a strategic process, which aims to consider possible scenarios of attack and vulnerabilities in a system with the objective of identifying different levels of risk and impact of a threat. In view of this presentation, the research questions that the present study seeks to verify is:

1. What threat modeling techniques are applied in the context of digital transformation?

2. What risk approaches in information security are mentioned and applied in threat modeling?

To answer the above questions, the present study has as general objective to identify and analyze the techniques of threat modeling applied in digital transformation from the perspective of risk management.

This study was structured as follows: Background section describes the foundations of information security based on ISO 27001:2022, digital transformation and cyber risk management process. The Methodology section presents the method used to apply the systematic review of the literature. Results section describes the analysis of results found in review and Conclusion section presents the final considerations about this review.

Background

Information security can be defined as preserving the confidentiality, integrity, and availability of information. For this reason, information can take several forms, including its storage on electronic media or its printing and writing on paper (ISO, 2022).

To ensure that information security controls are applied, it is necessary to map the key threats that can exploit existing vulnerabilities in an environment. In this context, threat modeling enables to assess and manage the risks attributed to threats that can affect information security.

As a support tool in meeting business objectives, threat modeling aims to identify the risks associated with the consequences of a constantly evolving threat environment, composed of vulnerabilities in software, networks and motivated by interests in business information. As an example, the attack surface and STRIDE (acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) are well-known techniques in the application of threat modeling (UCEDAVÉLEZ; MORANA, 2015).

The attack surface is a technique that studies software components that can lead to potential vulnerabilities, including data entry and exit points and the STRIDE model, created by Microsoft to model threats, considers six attributes that can be related to any threat: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (MANADHATA et al.,2011; SCANDARIATO et al., 2015).

In the context of information security, the term risk serves as an object of interest for threat modeling. From existing processes for risk assessment, it can be affirmed that threat modeling is a process directly related to risk management (UCEDAVÉLEZ; MORANA, 2015; YOKOYAMA; ARIMA, 2022).

The information security risk management process suggested by ISO/IEC 27005:2022, a technical standard for information security risk management, allows greater effectiveness in the assessment and classification of risks in information security. From the context in which the information to be protected is inserted, the risk assessment process is initiated so that the treatment or acceptance of the risk is defined according to the impact and probability of the risk assessed. The Figure 1 shows the information security risk management process available in ISO/IEC 27005:2022 (ISO, 2022).

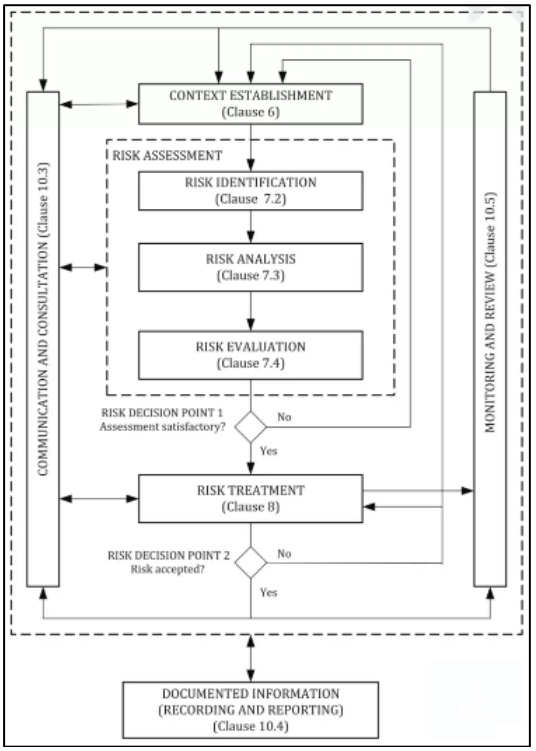

Figure 1 – Flowchart for information security risk management process
Source: ISO/IEC 27005:2022 (2022)

During the risk management process, it is essential that stakeholders are informed about the controls to be applied, as well as the acceptance of risks. It is noteworthy that, in view of the recent changes caused by the digitization of services, it is important to highlight the role of digital transformation in organizations and society.

Kaltum et al. (2016) defines that digital transformation is a profound change that accelerates business activities, processes, competencies, and models to fully explore the changes and opportunities of digital technologies and their impacts on society in a strategic and prioritized way. Terms such as digital, digitization, digitization, and digital business models are used to refer to digital transformation (BICAN; BREM, 2020).

In a scenario where digital transformation has enabled facilities, changes in technological processes and experiences for organizations, the application of threat modeling allows institutions, of various sizes and sectors, to have greater effectiveness in identifying and analyzing threats that can exploit vulnerabilities present in technologies and systems. For example, a study presented by Islan et al. (2016) shows how a threat model can be applied in IoT (Internet of Things) devices, that receives and transmits personal data, to minimize cyber risk in a healthcare infrastructure.

To support decision-making on which technical, organizational, or administrative measure should be applied to manage different levels of risk, the perspective of risk

management based on known technical standards, such as ISO/IEC 27005:2022, allows to ensure data protection and information security.

Methodology

For the development of this study, a systematic literature review was applied with the adoption of a protocol based on PRISMA-P with the objective of obtaining a qualitative and quantitative analysis of the selected publications, according to the flowchart presented in Figure 1.

The PRISMA-P protocol was developed as a roadmap to support researchers in conducting systematic reviews that return a minimum set of important items to be considered in the research protocol (MOHER et al., 2015).

The adoption of the protocol based on PRISMA-P allows the researcher to follow the steps suggested in the flowchart, which are: identification, screening, eligibility and documents included for qualitative and quantitative analysis.

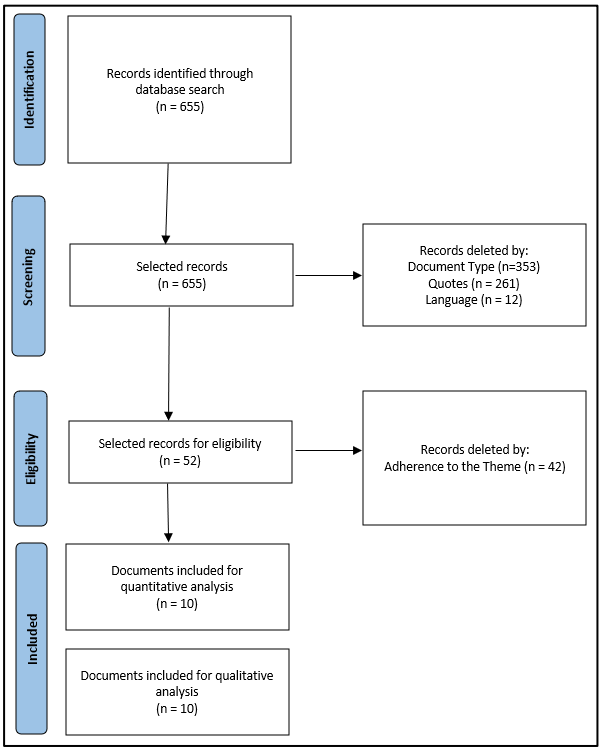

Figure 2 – Flowchart for systematic literature review
Source: Research results (2022)

In June 2022, bibliographic research was conducted on the subject in the Web of Science and Scopus databases, considering the keywords "threat modeling", "digital transformation"

and "information security risk". The research period was defined from 2011 to 2021 to highlight the evolution of the theme over the years.

The record identification step in the databases was performed according to inclusion criteria, where the results found in the Web of Science and Scopus databases were consolidated in table 1, totaling 655 records. It should be noted that most of the results found are available in the Scopus database.

Databases	Number of Results
Scopus	372
Web of Science	283

Table 1 - Number of Results per Database
Source: Research results (2022)

With the support of Excel for data recording and execution of the screening and organization of results, considering the exclusion criteria adopted, 603 records were removed, which are: "publications other than articles" (353), "publication with less than 20 citations" (238) and "publications that are not in English" (12).

To meet the objectives of the present study, after the eligibility stage, the 52 selected publications were analyzed based on the title and abstract. In all, considering adherence to the research theme, the inclusion phase of documents was completed with the selection of 10 publications for analysis.

Results

After the application of the methodology, the results found were consolidated in graphs and tables for better interpretation and analysis. Bibliometrics was produced with the support of Excel and the Bibliometrix, which allows quantitative and statistical analysis of publications (ARIA; CUCCURULLO, 2015). Figure 2 shows the number of publications in the period 2011 to 2021.

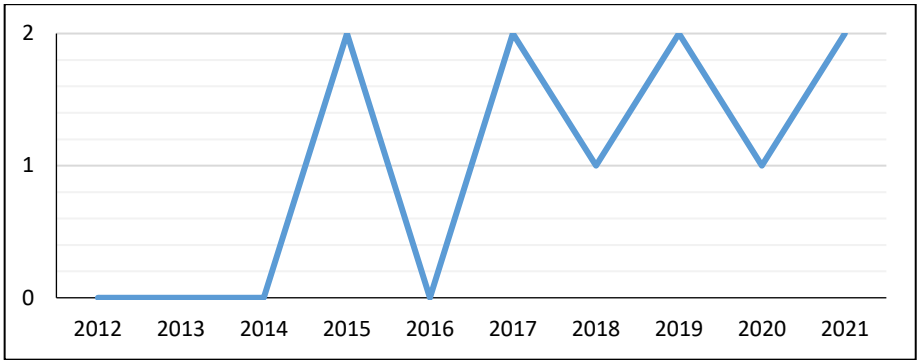

Figure 3 - Distribution of selected studies by year
Source: Research results (2022)

By analyzing the graph presented, based on the exclusion criteria adopted, it is possible to visualize that the largest number of studies is concentrated in 2015, 2017, 2019 and 2021, with two articles in total. In 2018 and 2020, only one article was published. From 2012 to 2014 and 2016, there were no publications. To identify the journals that published the selected studies in this analysis, Figure 3 lists the journals that disclosed the selected studies.

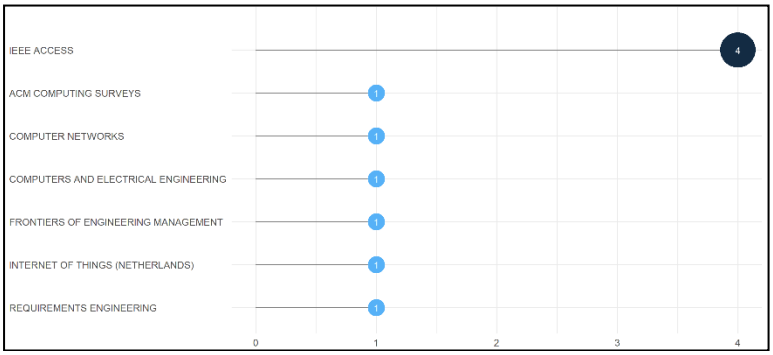

Figure 4 - Journals of selected publications
Source: Research results (2022)

Considering the sample selected after systematic review, IEEE Access is the journal with the highest number of publications with four in total, followed by ACM Computer Surveys, Computer Networks, Computers and Electrical Engineering, Frontiers of Engineering Management, Internet of Things (Netherlands) and Requirements Engineering with only one publication. To analyze the application of threat modeling in digital transformation, Figure 4 lists the studies selected by themes, whose objective is to identify the technologies and themes addressed.

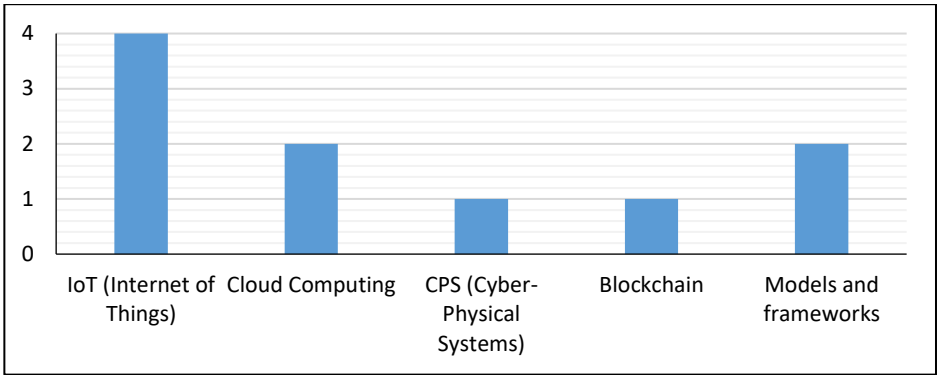

Figure 5 - Number of studies per theme
Source: Research results (2022)

It is observed that the number of studies related to the theme IoT is the one that appears most prominently, with four publications. Then, the themes cloud computing (cloud) and frameworks and models (TEAM and STRIDE, respectively), appear with two articles each and Blockchain and Cyber-Physical Systems (CPS) present in only one paper. Figure 5 shows the word cloud generated with the use of Bibliometrix software from the keywords and abstract of the ten selected studies.

Figure 6 – Word cloud
Source: Research results (2022)

When performing the text analysis based on the created word cloud, it is noted that the words challenges, internet, security, and simulation are the terms that appear prominently in the word cloud. Table 2 presents the relationship of studies with the techniques of threat modeling applied and the risk management approach adopted with its references, such as STRIDE and ISO/IEC 27005.

Authors	Title	Year	Threat Modeling Techniques	Risk Management approach (references)
Islam et al.	The internet of things for health care: A comprehensive survey	2015	Attack surface	Unspecified
Scandariato et al.	A descriptive study of Microsoft threat modeling technique	2015	STRIDE	Qualitative (STRIDE)
Shin et. al	Survey of secure data deduplication schemes for cloud storage systems	2017	Custom model (techniques not specified)	Unspecified
Ahmad et al.	TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks	2018	Custom model (techniques not specified)	Qualitative (ISO/IEC 27005)
Mohsin et al.	IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things	2017	Custom model (techniques not specified)	Qualitative
Casola et al.	Toward the automation of threat modeling and risk assessment in IoT systems	2019	STRIDE, per-asset threat modeling	Qualitative (STRIDE, NIST, ISO/IEC 27005)
Hong et al.	Systematic identification of threats in the cloud: A Survey	2019	STRIDE	Qualitative (STRIDE)
Zografopoulos et al.	Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies	2021	MITTRE ATT&CK (attack model e adversary model)	Qualitative and Quantitative
Khan et al.	When social objects collaborate: Concepts, processing elements, attacks and challenges	2021	Custom model (techniques not specified)	Unspecified
Shemov et al.	Blockchain applied to the construction supply chain: A case study with threat model	2020	Custom model (techniques not specified)	Unspecified

Table 2 – Relationship of threat modeling techniques and risk management approaches
Source: Research results (2022)

It is possible to note that qualitative approaches and customized models, without specifying modeling techniques, are applied in the most frequently selected studies. On the threat modeling techniques applied in digital transformation, Figure 6 shows the techniques adopted in these studies.

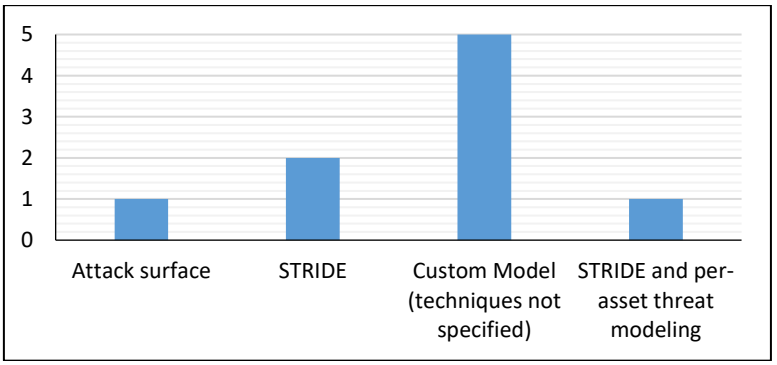

Figure 7 - Threat modeling techniques applied in selected studies
Source: Research results (2022)

It is possible to highlight that the use of customized models with unspecified techniques contains five studies in this sample. Two articles explore the STRIDE model, only one study addresses the attack surface technique and the STRIDE applied in conjunction with per-asset threat modeling.

Figure 9 shows the information security risk management approaches identified in these studies. For better visualization of the data, the references of the applied approaches, such as ISO/IEC 27005 and STRIDE, were omitted in this graph.

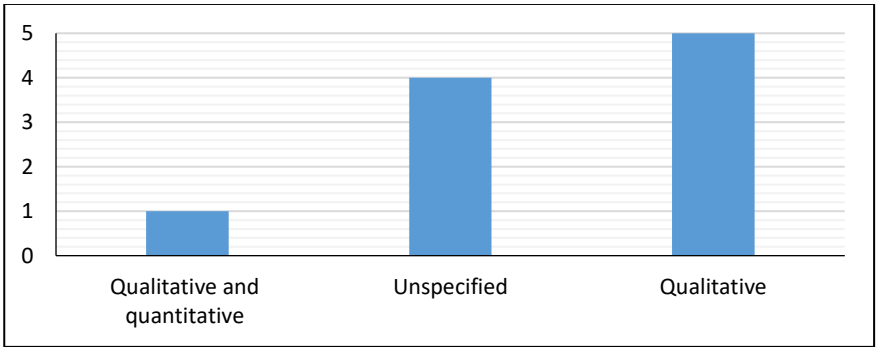

Figure 8 - Information Security Risk Management Approaches
Source: Research results (2022)

It is noted that qualitative are the approach most frequently used in digital transformation, with five studies in total. Four studies did not specify which approach in cyber risk management was applied and only one study indicates the application of a qualitative and quantitative approaches to information security risk management.

Conclusions

The results of this research show that threat modeling has been studied in digital transformation, especially in IoT, cloud computing, cyber-physical systems and blockchain technologies. Of the ten studies selected for analysis, the number of theoretical studies is more frequent.

About the threat modeling techniques identified, custom models using unspecified techniques and the STRIDE model have been applied in digital transformation for information security. The information security risk management approach and threat modeling techniques applied in the studies that have been presented indicate that the threat modeling process lacks greater integration with the risk management process. With the analysis of the results, this study brings three contributions:

- Threat modeling can be applied to support the information security risk management process, considering the use of different techniques to create a customized model for different technologies and systems.
- Qualitative risk management approaches are used more frequently than quantitative approaches.
- Threat modeling can be applied in different contexts, both in software development and information technology infrastructures.

The study presents limitations regarding the number of studies selected for qualitative and quantitative analysis. In view of the short time to perform the research, it was necessary to consider the results only for the selected studies and period cited in the methodology section.

For future studies, it is suggested that practical studies on threat modeling, preferably in real environments, be conducted in critical infrastructures and operational security processes, such as vulnerability management and penetration testing. Another point that can be addressed is the proposition of approaches for quantitative risk assessment in conjunction with threat modeling models.

References

ARIA, M.; CUCCURULLO, C. Bibliometrix: An R-tool for comprehensive science mapping analysis. **Journal of informetrics**, v. 11, n. 4, p. 959-975, 2017.

BICAN, P.M.; BREM, A. Digital business model, digital transformation, digital entrepreneurship: Is there a sustainable “digital”? **Sustainability**, v.12, n.13, p.5239, 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2022**

Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO/IEC, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27005:2022**

Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva: ISO/IEC, 2022.

ISLAM, S.M.R. et al. The internet of things for health care: a comprehensive survey. **IEEE access**, v. 3, p. 678-708, 2015.

KALTUM, U.; WIDODO, A.; YANUARDI, A.W. Local TV goes to global market through digital transformation. **Academy of Strategic Management Journal**, v. 15, p. 221-229, 2016.

MANADHATA, P.K.; WING, J.M. A formal model for a system's attack surface. In: Moving Target Defense. **Springer**, New York, NY, 2011. p. 1-28.

MOHER, D. et al. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. **Systematic reviews**, v. 4, n. 1, p. 1-9, 2015.

SCANDARIATO, R.; WUYTS, K.; JOOSEN, W. A descriptive study of Microsoft's threat modeling technique. **Requirements Engineering**, v. 20, n. 2, p. 163-180, 2015.

UCEDAVELEZ, T.; MORANA, M.M. **Risk Centric Threat Modeling: process for attack simulation and threat analysis**. John Wiley & Sons, 2015.

YOKOYAMA, R.; ARIMA, C.H. Análise textual e bibliométrica sobre modelagem de ameaça. **Brazilian Journal of Development**, v. 8, n. 1, p. 7678-7690, 2022.

YOKOYAMA, Rodrigo; ARIMA, Carlos Hideo. Modelagem de ameaça, análise de risco e suas aplicações na literatura, **International Journal of Development Research**, 12, (04), 55049-55055. 2022.

Submetido em: 23.12.2022
Aceito em: 23.01.2023