IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 31, 2021, accepted September 14, 2021, date of publication September 20, 2021,
date of current version September 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2021.3113178

Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology

FERNANDO ROCHA MOREIRA[1], DEMÉTRIO ANTÔNIO DA SILVA FILHO[2], GEORGES DANIEL AMVAME NZE[1], (Member, IEEE), RAFAEL TIMÓTEO DE SOUSA JÚNIOR[1], (Senior Member, IEEE), AND RAFAEL RABELO NUNES[1,3]

[1]Electrical Engineering Department, University of Brasilia, Brasília, Federal District 70910-900, Brazil
[2]Institute of Physics, University of Brasilia, Brasília, Federal District 70919-970, Brazil
[3]UniAtenas University Center, Paracatu-MG 38602-002, Brazil

Corresponding author: Rafael Rabelo Nunes (rafaelrabelo@unb.br)

The authors gratefully acknowledge the financial support from CNPq - Brazilian National Research Council, CAPES - Brazilian Higher Education Personnel Improvement Coordination, FAP-DF - Brazilian Federal District Research Support Foundation, DPI-UnB - Decanate of Research and Innovation of the University of Brasília, and CENAPAD-SP - National Center for High-Performance Processing in São Paulo. F.R.M. acknowledges the financial support from DPI-UnB (Grant Edital 02/2021) and CENAPAD-SP for providing the computational facilities. D.A.S.F acknowledges the financial support from DPI-UnB (Grants Edital 04/2019 and Edital 02/2021), from CNPq (grants 305975/2019-6 and 420836/2018-7), and FAP-DF (Grants 193.001.596/2017 and 193.001.284/2016). G.D.A.Z. acknowledges CNPq (Grant 465741/2014-2 INCT in Cybersecurity). R.T.S.J. gratefully acknowledges CNPq (Grants 312180/2019-5 PQ-2 and 465741/2014-2 INCT on Cybersecurity), the Brazilian Ministry of the Economy (Grants 005/2016 and 083/2016), the Administrative Council for Economic Defense (Grant 08700.000047/2019-14), the General Attorney of the Union (Grant 697.935/2019), the National Auditing Department of the Brazilian Health System SUS (Grant 23106.118410/2020-85), and the General Attorney's Office for the National Treasure (Grant PGFN 23106.148934/2019-67). R.R.N. acknowledges the financial support from DPI-UnB (Grant Edital 01/2021) and the UniAtenas University Center.

ABSTRACT This paper aims to show how creating a risk plan can be solved with the help of the constructivist multicriteria method. A case study using Multicriteria Decision Aid Constructivist (MCDA-C) was applied, with cybersecurity framework's controls as a reference. The study was conducted in a large Brazilian bank in Brazil. The relevance of this work is the need to show that the application of multicriteria methods can be applied in the context of information security, which recommends the use of such methods to assist in risk analysis. The methodology used in this study was both quantitative and qualitative, obtaining primary data through brainstorming with decision-makers and forms answered by experts. The secondary data were obtained through the Framework for Improving Critical Infrastructure Cybersecurity, created by NIST - the National Institute of Standards and Technology of the United States. The problem was structured according to the constructivist method, and the data collected were processed and calculated. The study concluded that the category of Security Continuous Monitoring controls stood out compared to other categories. It also shows the importance of applying the constructivist method for the management of cyber risks by unravelling a problem and providing a basis for decision making. Our work contributes to a better understanding of risk management, encouraging the adoption of the constructivist method as a form of risk management best practice.

INDEX TERMS Cybersecurity, constructivist, MCDA-C, MCDM, multicriteria, NIST, risks, risk management, threats.

I. INTRODUCTION

The role played by technology has increased drastically in individuals' and companies' lives in recent decades. Large corporations have increasingly used technology to reduce costs and errors and to improve operational efficiency. Consequently, there has been an improvement in the ultimate customer service and profits for the organization [1].

The same happens in the world of technology in the financial branch. Competitiveness and the search for an increasingly digital operation has pushed banks to seek space on the Internet. In this way, these organizations can offer better products and applications, strengthening the customer competitiveness search. This competitiveness exposes critical data through the Internet, causing enterprises to worry about cybersecurity and avoid being victims of attacks [2], [3].

Some studies show that attacks of this nature on organizations are becoming increasingly common and have recently

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu.

more than doubled [1]. During the World Economic Forum in Davos, the ''2018 Global Risk Report'', cybercrime was placed second in the report, behind Extreme Climate Risk [4].

The same report states that organizations are increasingly vulnerable to this type of attack, with one happening every 39 seconds. These attacks show that organizations are increasingly exposed to this type of cybercrime risk, therefore increasingly demanding the implementation of security controls and risk analysis [4].

A risk analysis based on controls is usually a problem involving multiple criteria, so organizations can prioritize them by setting up a risk management methodology [5]. For example, NIST's ''Framework for Improving Critical Infrastructure Cybersecurity'' brings 108 controls to assist with cybersecurity risks, but does not say where to start a risk plan with these controls [6].

Some tools can collaborate to implement this risk plan, and International Organization for Standardization (ISO) 31.010:2012 has shown that multicriteria decision methods are applicable for identifying, analyzing, evaluating, and prioritizing risks. This standard displays multicriteria methods that result in an order of priorities through analyzing several criteria to be evaluated. In this way, the methods succeed in helping managers elaborate on an efficient and consistent risk plan [7].

These multicriteria methods are a table-based method of decision making. The values and weights of each alternative are determined by experts. These methods are capable of classifying, determining, and prioritizing the different alternatives, helping decision makers [5].

ISO 31.010:2012 also shows that in addition to multicriteria methods aiding in decision making, they make the problem more manageable. In this way, multicriteria methods can reduce the complexity and help in cost-benefit analysis. Another advantage of the methods is to find an optimal point of analysis when there is divergence among the stakeholders [7].

Hence, this paper sought to conduct a case study in a large Brazilian bank. The Multicriteria Decision Aid Constructivist (MCDA-C) method was used in the controls of the incident detection module of the NIST ''Framework for Improving Critical Infrastructure Cybersecurity''. This choice was made due to the corporation's need to review these controls within a more comprehensive process that deals with all risk management principles.

By using this approach, it was possible to show how much each control could collaborate in order to mitigate cyber risks, considering the organization scenario. It was possible to facilitate the information security manager's work to create a risk plan based on the collected data.

This article is structured as follows: Section 2 lists some related work in cybersecurity using multicriteria methods; Section 3 presents the risk management process; Section 4 describes MCDA-C, i.e., the multicriteria method used in the paper; Section 5 presents The Framework for Improving Critical Infrastructure Cybersecurity of NIST used as a reference risk management model; Section 6 describes and explains the operation of MyMCDA-C, the software used to assist this project; Section 7 presents the research design; Section 8 discusses the results obtained in the paper; and Section 9 presents the conclusions and future work.

II. RELATED WORK

Cybersecurity has been the focus of many studies, several of which have been conducted over the years for improvements in various sectors [8]. In this section, we will show some relevant studies being conducted in cybersecurity using multicriteria methods in various sectors.

Kinser *et al.* [8] in 2020 presented a method of performing a quantitative evaluation of services. This evaluation was based on the fundamental principles of cybersecurity: confidentiality, availability, and integrity. The authors considered the quantitative and qualitative assessments obtained through conformity, performance, and incident response assessments.

Tariq *et al.* [9] in 2020 conducted an application of weight-weight methods to blockchain. They attempted to use the empirical CyFEr paradigm that treats the reported problem in question as a multicriteria decision analysis (MCDA) problem. In this study, they used methods for weightings, such as a sum of classification, reciprocal classification, exponent of classification, and centroid of the classification order. The efficiency of these weights was tested in the blocking chain cybersecurity framework (BC2F), which was developed by NIST. As a result, this study brought about technical knowledge on applying methods that classify weights and assessments of security vulnerabilities; visions about BC2F; applications of weight classification methods to BC2F; and approach of the integration of CyFEr's weight classification methods.

Alenezi *et al.* [10] in 2020 proposed a methodology to prioritize security controls for daily home computing. The article showed how the use of multicriteria decision methods (MCDMs) could help solve this problem. The cybersecurity controls used by governments and industry were then identified. The controls were prioritized, and this methodology was applied in several examples to prove its effectiveness.

Ramadan and Ahmed [11] in 2020 described companies' complicated relationships between cybersecurity risk management and operational objectives. This factor becomes aggravating, especially regarding money. According to information security risk assessment models (ISRAs), the work describes and classifies incidents against blockchain cybersecurity vulnerabilities.

Fanelli and Waxler [12] in 2019 assessed the security performance of web applications using a decision-making approach. The authors performed a hybrid fuzzy AHP-TOPSIS methodology to perform this evaluation. They conducted a case study in which this approach was tested in a web application at the University of Lucknow, India. Other tests were also performed in order to validate their research. The authors demonstrated that the approach would help system architects create and use security tactics.

Gourisetti *et al.* [13] in 2019 used multicriteria methods to prioritize information security controls for cloud computing networks and wireless sensor networks. The authors used AHP fuzzy to establish priorities and select the most appropriate controls to satisfy the organization's cybersecurity requirements. The authors showed that prioritizing cybersecurity controls with this methodology improves the efficiency and cost-effectiveness. In this way, the organization chooses the most appropriate controls for its use.

Ganin *et al.* [14] in 2017 revealed that the existing approaches for risk management in cybersecurity do not include all the risk assessment components. These components are threat, vulnerability, consequence. The study shows a decision-analysis-based approach that quantifies the previously mentioned components through several criteria, which depicts a bridge between risk assessment and risk management, thus facilitating the decision-maker. This technique was used in a case study in a hypothetical HPC system (parallel system computing at an increased level of functionality).

From the review of recent literature, several articles have used multicriteria methods in various areas of cybersecurity. However, there is a need to develop a cyber risk management plan based on a framework that directs managers to best practices. There is also a need to use this framework along with a method that encompasses all risk management principles and can quantify the perception of all stakeholders, who are often subjective to decision making. Hence, in this paper the authors propose a multicriteria approach using MCDA-C based on the framework for improving critical infrastructure cybersecurity created by NIST to fill this gap.

III. RISK MANAGEMENT

The risk management process is iterative and aims to help organizations achieve their objectives and make decisions. This process is part of governance and leadership and should involve all organizational activities, including all stakeholders [15].

When performing risk management, several factors must be considered: internal and external context of the organization as well as human and cultural factors [15].

The risk management process is based on eight principles [15], [16]:

- **Integrated:** Risk management should involve all parts of the organization.
- **Structured and comprehensive:** The risk management process should have a structured approach contributing to consistent and comparable results.
- **Personalized:** This process must be personalized and can relate the external and internal contexts of the organization to the objectives.
- **Inclusive:** The risk management process should involve all stakeholders to consider points of view and perceptions.
- **Dynamics**: The risk management process must be dynamic because risks can arise, change or disappear as an organization's external and internal contexts change.
- **Best available information:** The data entries for the risk are based on historical and future expectations, considering any limitations and uncertainties associated with this information and expectations. It is important to emphasize that the information must be clear and available to all stakeholders.
- **Human and cultural factors:** Human and cultural factors must be considered because they influence all risks at each stage level.
- **Continuous improvement:** The risk management process must be improved according to the learning and experience acquired.

IV. MCDA-C–MULTI-CRITERIA DECISION AID CONSTRUCTIVIST

One way to help the risk management process and decision-making is to adopt a multicriteria method. Multicriteria methods aim to produce an order of preference among the available options. They involve a matrix of options and criteria ranked by obtaining a score for each option, fitting perfectly with the risk management process recommended by ISO 31.000:2018 [15].

The MCDA-C is a methodology to assist decision-making when multiple criteria are involved. This methodology is based on applying this method to complex decision-making problems and searching for a better solution that fits the needs of the decision-maker [17].

Starting from this point of view, the main characteristics of this methodology are [18]–[21]:

- Recognition of the limits of objectivity and acceptance of subjectivity.
- The implementation of a constructivist process aimed at the constant evolution of the decision-making process, which is opposed to a set of tools allowing unique and improved solutions to a problem.
- The non-separation of elements of an objective nature with those of a subjective nature.
- Improving proposal of the decision-making process, where the constructivist model faces the other methodologies.
- Presence of support in all stages of the decision process from the structuring phase thorough evaluation and recommendation.

Decision making is a process that is presented in an unstructured and problematic way [22]. By using a decision support methodology, the problem becomes structured and less chaotic, facilitating understanding of the problem [17].

In this way, MCDA-C collaborates in the decision-making process in the construction and elaboration of criteria and modeling preferences, presenting a result for the decision maker to make the final decision [17].

According to Ensslin *et al.* [23], the application of MCDA-C is divided into three phases: structure, evaluation, and recommendation. The structuring phase is where the decision-maker considers his significant concerns: identified, organized, and measured. The second phase is where

the scales and the replacement rates weights are elaborated, which assign value according to the decision-maker preferences. The last stage is called the recommendations phase, which seeks to understand the consequences of the decisions to be made.

All MCDA-C indicators are calculated through scales that contemplate the measurement theories and operation properties being built from the following steps [24]–[27]:

- Determine a hierarchical structure of values including the concerns of the decision-maker.
- Create and develop the descriptors, perform the ordinal scale and identify the references so that the decision-maker noted out the references of maximum and minimum points.
- Construct a cardinal scale through the incorporated data according to the levels declared by the decision-maker [30].

By analyzing all phases and how the MCDA-C is structured, it is possible to see how the MCDA-C's alignment with the risk management and analysis process and principles [15], [16]. Fig. 1 shows how these 3 phases are structured.

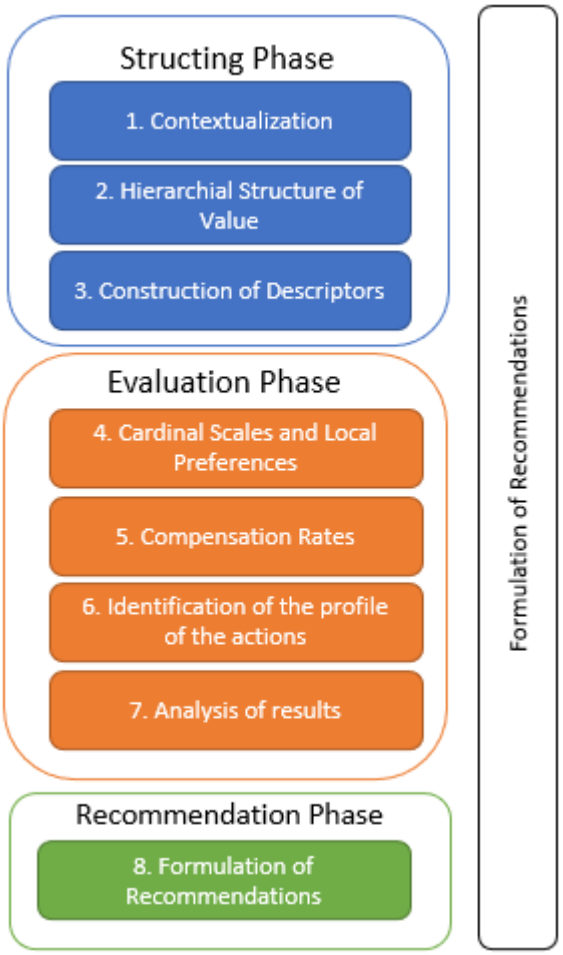


FIGURE 1. Stages of MCDA-C. Image adapted from [31].

Some multicriteria methods, such as the AHP used in some related works referenced in this paper, do not encompass all stakeholders in the organization [9], [10]. Thus, only decision makers participate in the process, which does not encompass the principles of integration, inclusion and human and cultural factors described in the risk management process [15], [16].

Hence, multicriteria method chosen in this paper is MCDA-C. The choice for this method is due to its structuring and comprehensiveness, as it involves all the risk management principles listed in ISO 31.000:2018 and ISO 31.004:2013 [15], [16].

V. FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

The Framework for Improving Critical Infrastructure Cybersecurity of NIST aims to assist critical infrastructure operators in identifying and developing cybersecurity risk guidelines.

This framework involves a set of assumptions, activities, results, and informative cybersecurity references presented in several critical infrastructure scenarios [6].

Critical infrastructure is defined in the US Patriot Act of 2001 as "systems and assets, whether physical or virtual, so vital to the United States that the inability or destruction of such systems and assets would have a debilitating impact. Whether that impact on national economic security, national health and public safety, or the combination of any of these areas".

This framework can be used by various public and private sectors that want to secure their organizations. The guide also explains that it does not replace the organization's security process, but instead complements it. For example, the organizations that use this framework are Microsoft, JP Morgan Chase, Intel, Boeing, Bank of England, and other US governmental entities [32].

The Guide has three parts: Basic Structure, Levels of Implementation, and Structure Evaluation.

The Basic Structure aims to present industry standards, guidelines, and practices. This makes it possible to communicate the activities and results of cybersecurity throughout the organization, from the executive level to the implementation or operational level [6].

This basic structure is composed of four elements: functions, categories, subcategories, and informative references. Functions organize basic cybersecurity activities at their highest level, followed by subdivisions called categories. The subcategories are the subdivisions of the categories being the specific result of the technical and management activities to be implemented [32].

- Identify - This function develops an organizational understanding to manage security risks. It seeks to cover systems, people, assets, and resources.
- Protect - This role is responsible for developing and implementing the necessary protections to ensure that

services continue to operate. It seeks to limit cybersecurity occurrences.
- Detect - This function aims to develop and implement the necessary controls to identify the occurrence of a cybersecurity event.
- Respond - This seeks and implements appropriate activities to perform some action when a cybersecurity incident is detected.
- Recover - This function seeks to perform activities and maintain resilience plans to restore any inoperative service due to a cybersecurity incident.

The guide emphasizes that each organization has its specific risks. Based on this premise, organizations can determine which activities need to prioritize investments, creating its profile according to its business and mission, using the categories and subcategories contained in the framework [6]. At that moment, the bank selected the Detection Function's categories and subcategories to review its cybersecurity incident detection processes.

The guide's levels of implementation provide an approach for assessing how the organization addresses cybersecurity risk. The levels range from Level 1, which is considered ''Partial'', to Level 4, ''Adaptable''. The levels are increasingly presented as the organization is mature in managing cybersecurity risks [32].

The Structure Evaluation seeks to evaluate the functions, categories, and subcategories of the guide regarding the organization's business requirements, indicating gaps to be filled to comply with a category or subcategory [6].

VI. MyMCDA-C

MyMCDA-C is a new software that assists managers seeking to use the multicriteria constructivist decision support model. MyMCDA-C is free software and allows the generation of graphs and tables charts and tables, taking constructivist multicriteria analysis into account [33].

This software has been widely used in Brazil in several research projects in the most varied sectors. In the literature, it is possible to find papers in which the software was used:
- Reverse Logistics [34], [35];
- Managerial Public Accounting [36];
- Usability analysis of websites [37], [38];
- Analysis of the influence of Instagram on consumers [33].

This tool can transform qualitative data into quantitative data inspired by mathematical calculation models using the MACBETH method [39].

It can calculate the maximum and minimum values of all criteria to the reference value found and then apply a weight to them [40]. The next step is to use the medians according to the evaluation scale and generate graphics maximizing and minimizing the actual values.

The calculations based on mathematical models that MyMCDA-C performs seek to associate managers' perceptions of the stakeholders of the criteria. The estimates of the values assigned to the sub-criteria at the last level for the negative values of the results scale used (1):

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

For positive cases above the ''Good level'' (2) was used:

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

To obtain the maximization value (3) was used:

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

where:
- NV - Negative value of an action on the scale of descriptors of a criterion;
- PV - Positive Value of an action on the scale of descriptors of a criterion;
- WN - Weight Number;
- N - Number of project criteria;
- PS - Position of the action on the Scale of descriptors. The order of effort.

By default, a value 0 is adopted for the neutral level, and 100 is adopted for the good level. To obtain the value of the other levels, a linear programming system is adopted according to (4) below [40].

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

Equation (5) was used to perform the upper criteria calculations for the tree's last level and results.

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

where:
- GV - Global Value of the potential performance 'a';
- RR - Replacement Rate corresponding to the criterion;

PV(a) - Partial Value of a potential action 'a' in the criterion

VII. RESEARCH DESIGN

In this section, the methodological procedures discussed during the planning, execution, and conclusion of this research will be described. These methods will describe their purposes, nature, data origin, approach, and methodology.

This study takes place in a large Brazilian bank located in Brazil and throughout the world, with more than 90,000 employees, being one of the 5 largest banks in the country. For this study, this bank's international area was selected, that is, the bank branches around the world that move more than US$ 150,000,000.00 per hour. The team size that participated in the research is 18 employees with diversified profiles and is responsible for the international IT management area of the bank. Therefore, the entire international IT management participated in this work, not just a sample.

This research proposes a model of evaluating and implementing cybersecurity controls for this Brazilian bank. Thus, this bank's new cybersecurity control would identify implementation priorities to improve information security management. Therefore, this research is an applied investigation.

The data from this research were collected primarily from the managers and employees of the company. The secondary data were obtained through documents such as the NIST framework [6].

The work presents a case study. Case studies are essential because they allow the transformation of the objectives into actions in which the organizations are inserted, allowing new discoveries [41].

By using MCDA-C, this work presented itself as a logic of mixed research. The structuring phase presented itself as inductive because the elements to be evaluated were taken from the NIST framework, and the scale values were performed. In the second phase of this method, the evaluation was deductive since it was a matter of conducting individual evaluations regarding the controls. Finally, the recommendations phase took a step as being inductive because it is based on the results presented during the method's application.

The research works with a double approach, both qualitative and quantitative. It is qualitative in the structuring phase, considering that we identify controls and their connections with the scales' values, and it is quantitative in the evaluation phase, considering the use of a mathematical model with metrics and compensation rates [27].

This study sought to apply the elements taken from the NIST framework to the MCDA-C, thus listening to experts and creating a cyber risk analysis plan and consequently complying with risk management principles and pillars. In this way, through the results generated by the MCDA-C, managers can assist in their decision-making.

Due to the size of the framework and context of this paper being aligned with the bank's needs, only the detect function was chosen for the analysis of this work. The financial institution was conducting a review of information security incident detection controls and chose to start with this particular category to review another's categories gradually in the future. Thus, together with MCDA-C, these were the intervention instruments used to develop the proposed work, providing information and perceptions to managers to improve their cybersecurity performance.

VIII. ANALYSIS OF RESULTS

In this section, the study results will be described. Several stakeholders were present in the process, as their perceptions were reflected in the MCDA-C final analysis results. According to MCDA-C, the first step is identifying the actors who will have a role in the research [21]. The actors are:

- Three decision-makers: Software Developer, IT Team Manager, IT Infrastructure Analyst.
- Facilitators: Researchers.
- Fifteen stakeholders: Management staff of the international IT area.
- Recipients: Clients

For this study, three experienced senior-level employees, who are references in their areas, were chosen as the decision-makers. They were responsible for modeling and analyzing the decision-making problem.

The fifteen stakeholders involved in the process are the rest of the international IT Management employees. They are employees with diverse profiles who work in this area. Fig. 2 shows the 15 stakeholders' profiles who participated in this process.

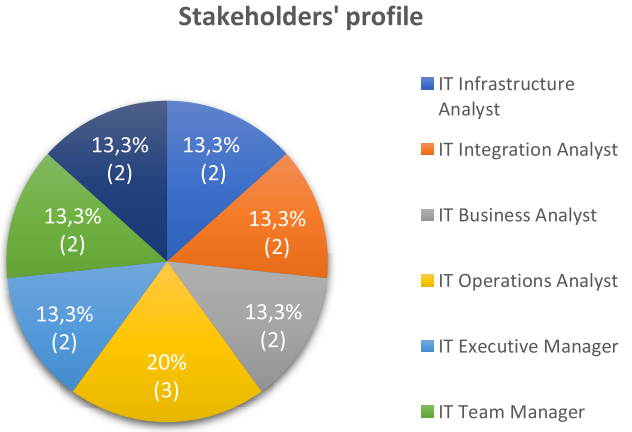


FIGURE 2. Stakeholders' profile.

It is important to emphasize that the decision choice of the three decision-makers and stakeholders with diversified profiles was intentional. The main reason is to reconcile and find a common term among them to facilitate communication and reduce biases.

The decision-makers were not included in the stakeholder's group, to avoid bias in the data collected and calculated according to the stakeholders' point of view. Thus, two distinct groups participated at different moments.

The decision-makers were not included in the stakeholder's group, to avoid bias in the data collected and calculated according to the stakeholders' point of view. Thus, two distinct groups participated at different moments.

The researchers in this work do not answer questions. They only have the role of applying the method, conducting it phase by phase and entering the data into the software.

Clients are the ultimate beneficiaries with cybersecurity improvement, so they do not participate in the process. First we needed to define a label for the research [27]. The decision-markers choosed the label: How much of the NIST Framework Detection Function controls could contribute to the bank's cybersecurity?

Next, it was necessary to define the weight number in the project, that is, the definition of the level of effort. MyMCDA-C requires these data to perform the calculations. Through this effort level, it is possible to perform an analysis of the criteria that require more effort to concentrate the resources. This value subsidizes the calculation of the effort that a security control must make to reach the maximization point. This means that with a heavier load, more effort is required to reach the top of maximization [33]. The decision makers opted for a weight number of 3, as it is the MyMCDA-C default value for this parameter.

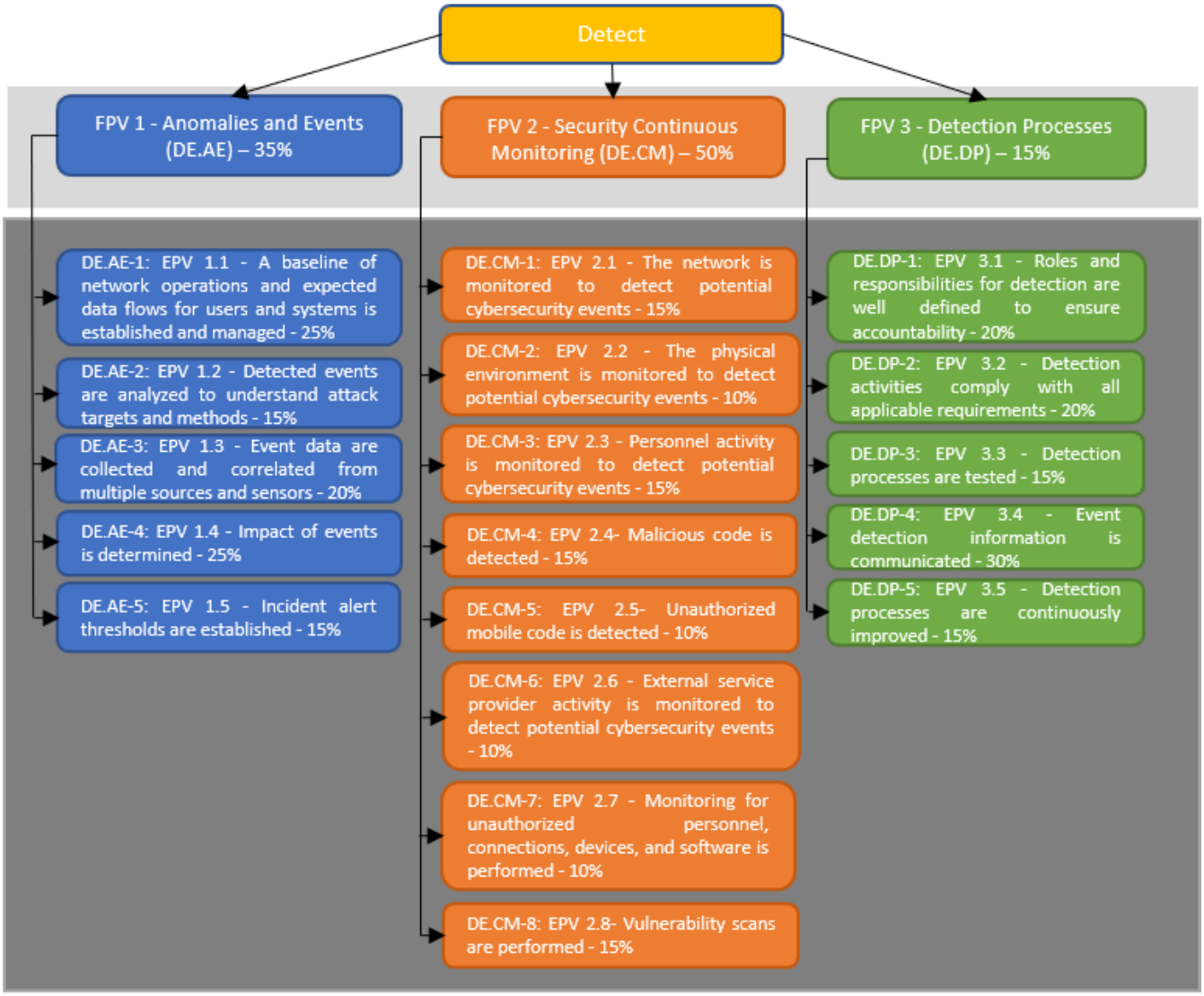


FIGURE 3. Structure of the detect function of the NIST framework, definition of EPV's and FPV's, and its respective compensation Rates.

The next step was to define a hierarchical structure with the controls to be evaluated. For this phase, the detection function of the NIST framework was selected [6]. This function was chosen because it has the objective of developing and implementing activities to identify cybersecurity occurrences. It is divided into 3 categories and 18 subcategories, i.e., the security controls to be evaluated [6].

For descriptor development, the same methodology was applied. Each of the Fundamental Points of View (FPV), and Elementary Points of View (EPV) were chosen according to the detection function of the NIST framework [6]. FPV's and EPV's are the terms used by MCDA-C to define first and second level respectively. In Fig. 3, inside the light gray diagram, there are the FPV's which are the NIST categories containing their respective grouped EPV's. The EPV's are the NIST cybersecurity controls that have been evaluated, these are inside the dark gray diagram. Here, we can see the MCDA-C addressing the personalized, structured, and comprehensive and dynamic principles of risk management. Fig. 3 illustrates the structure of the detection function according to [6]. This structure was replicated in MyMCDA-C so that it receives the data obtained in the next phases.

The next step was creating the Preferred Scale for the criteria according to the decision-makers. The decision-makers chose five evaluation levels: ''Neutral'' as the worst level, followed by ''Minimal collaboration'', ''Little collaboration'', and ''Good Collaboration'' with ''Excellent collaboration'' as the best level.

The reason for decision-makers to start in the ''Neutral'' level was that the implementation of Control would not negatively impact the bank; the worst-case scenario is not to affect the result. Thus, N1 ''neutral'' was defined as neutral, and N4 ''good collaboration'' was defined as good. Table 1 shows how the Scale of Preference was locally defined.

TABLE 1. Development of descriptors.

Level	Quantity	Neutral	Good
N1	Neutral	X	
N2	Minimal collaboration		
N3	Little collaboration		
N4	Good Collaboration		X
N5	Excellent collaboration		

TABLE 2. Cardinal scales and local preferences for EPV 2.5: unauthorized mobile code is detected.

Impact Level	Option Answer	Scale
N1	Neutral	0
N2	Minimal collaboration	33
N3	Little collaboration	67
N4	Good collaboration	100
N5	Excellent collaboration	154

Then, MyMCDA-C software converted the qualitative values into quantitative values. Thus, decision makers were able to use quantitative assessments to determine the level of each element. Table 2 shows an example of the scales converted from ordinal to cardinal for ''EPV 2.5: Unauthorized mobile code is detected''. Each EPV has its Cardinal scale calculated and rounded by MyMCDA-C. Below is a demonstration of the conversion of qualitative values from MyMCDA-C to the cardinal scale of EPV 2.5.

Adopting the default values for N1 ''Neutral'' as 0 and N4 ''Good'' as 100 [40]:

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

To obtain the values of N2 and N3, the linear programming method was adopted based on the values of N1 and N4.

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

Obtaining β by substituting α and using N4's equation:

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

Obtaining the value of α using N4's equation:

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

Obtaining the value of N2 and N3:

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

To obtain the value of N5, which is the maximization point of the EPV 2.5 performance scale, the following was used:

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

The compensation rates survey was conducted in a brainstorming meeting with three decision-makers for more than two hours. Fig. 3 shows the compensation rates defined by decision-makers for each control. Note that the rates were set from the lowest level of the hierarchy to the highest level. After the compensation rates were established by the decision-makers, they were inserted into MyMCDA-C.

TABLE 3. Order of effort.

Order	Control
1	EPV 2.5: Unauthorized mobile code is detected
2	EPV 2.4: Malicious code is detected
3	EPV 2.8: Vulnerability scans are performed
4	EPV 2.1: The network is monitored to detect potential cybersecurity events
5	EPV 3.1: Roles and responsibilities for detection are well defined to ensure accountability
6	EPV 2.3: Personnel activity is monitored to detect potential cybersecurity events
7	EPV 2.6: External service provider activity is monitored to detect potential cybersecurity events
8	EPV 2.7: Monitoring for unauthorized personnel, connections, devices, and software is performed
9	EPV 2.2: The physical environment is monitored to detect potential cybersecurity events
10	EPV 1.2: Detected events are analyzed to understand attack targets and methods
11	EPV 1.1: A baseline of network operations and expected data flows for users and systems is established and managed
12	EPV 1.3: Event data are collected and correlated from multiple sources and sensors
13	EPV 1.4: The impact of events is determined
14	EPV 1.5: Incident alert thresholds are established
15	EPV 3.2: Detection activities comply with all applicable requirements
16	EPV 3.4: Event detection information is communicated
17	EPV 3.5: Detection processes are continuously improved
18	EPV 3.3: Detection processes are tested

Then, the decision-makers determined the effort order of the controls. Table 3 shows the order of the improvement effort defined. This effort order, determined in Table 3, was entered into MyMCDA-C, with the control ''EPV 2.5: Unauthorized mobile code is detected'' receiving more effort, while the control ''EPV 3.3: Detection processes are tested'' received less effort.

TABLE 4. Evaluation of "EPV 2.5: Unauthorized mobile code is detected" by stakeholders.

Stakeholder	Selected descriptor	Corresponding N level
Stakeholder 1	I don't know	
Stakeholder 2	I don't know	
Stakeholder 3	Good collaboration	4
Stakeholder 4	I don't know	
Stakeholder 5	Good collaboration	4
Stakeholder 6	I don't know	
Stakeholder 7	Excellent collaboration	5
Stakeholder 8	Excellent collaboration	5
Stakeholder 9	Excellent collaboration	5
Stakeholder 10	Excellent collaboration	5
Stakeholder 11	Good collaboration	4
Stakeholder 12	I don't know	
Stakeholder 13	Good collaboration	4
Stakeholder 14	Good collaboration	4
Stakeholder 15	Excellent collaboration	5
Median of the levels		4,5

TABLE 5. Median of stakeholder responses on the impact of implementing nist security controls.

Control	Level	Descriptor	Correspondent Cardinal Scale
EPV 2.5: Unauthorized mobile code is detected	N5	Excellent collaboration	154
EPV 2.4: Malicious code is detected	N4	Good collaboration	100
EPV 2.8: Vulnerability scans are performed	N5	Excellent collaboration	148
EPV 2.1: The network is monitored to detect potential cybersecurity events	N5	Excellent collaboration	145
EPV 3.1: Roles and responsibilities for detection are well defined to ensure accountability	N4	Good collaboration	100
EPV 2.3: Personnel activity is monitored to detect potential cybersecurity events	N4	Good collaboration	100
EPV 2.6: External service provider activity is monitored to detect potential cybersecurity events	N4	Good collaboration	100
EPV 2.7: Monitoring for unauthorized personnel, connections, devices, and software is performed	N4	Good collaboration	100
EPV 2.2: The physical environment is monitored to detect potential cybersecurity events	N3	Little collaboration	67
EPV 1.2: Detected events are analyzed to understand attack targets and methods	N5	Excellent collaboration	127
EPV 1.1: A baseline of network operations and expected data flows for users and systems is established and managed	N4	Good collaboration	100
EPV 1.3: Event data are collected and correlated from multiple sources and sensors	N5	Excellent collaboration	121
EPV 1.4: Impact of events is determined	N5	Excellent collaboration	118
EPV 1.5: Incident alert thresholds are established	N3	Little collaboration	67
EPV 3.2: Detection activities comply with all applicable requirements	N4	Good collaboration	100
EPV 3.4: Event detection information is communicated	N5	Excellent collaboration	109
EPV 3.5: Detection processes are continuously improved	N5	Excellent collaboration	106
EPV 3.3: Detection processes are tested	N5	Excellent collaboration	103

When all scales and compensation rates were determined, stakeholders were asked about the label of the research: "How much of the NIST Framework Detection Function controls could contribute to the bank's cybersecurity?" A form was sent to each employee to respond according to their qualifications. Then, the responses for each EPV and FPV were collected, and the total median was calculated to be entered into MyMCDA-C. Medians that had a score of 0.5 were rounded up. All "I don't know" answers were discarded. Table 4 shows how this calculation process was done for "EPV 2.5: Unauthorized mobile code is detected". The final median value was rounded to 5 because MyMCDA-C works with rounded values. Hence, the corresponding final level for 5 is N5, "Excellent Collaboration" with the respective cardinal value 154 shown in Table 2.

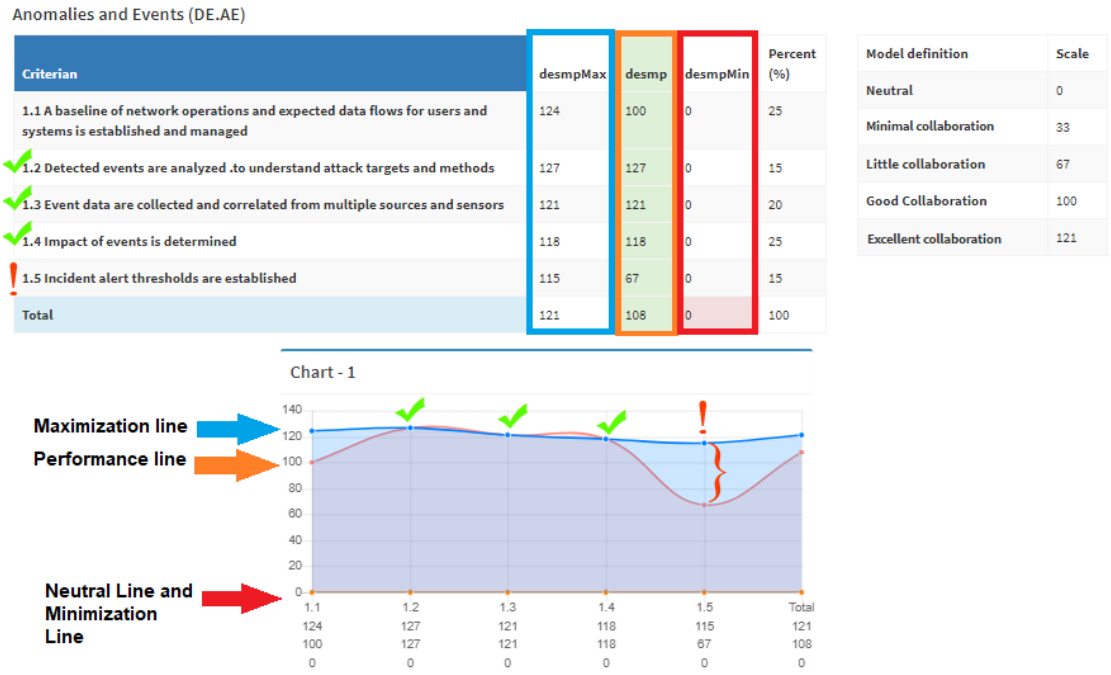


FIGURE 4. Anomaly and events - screenshot adapted from MyMCDA-C.

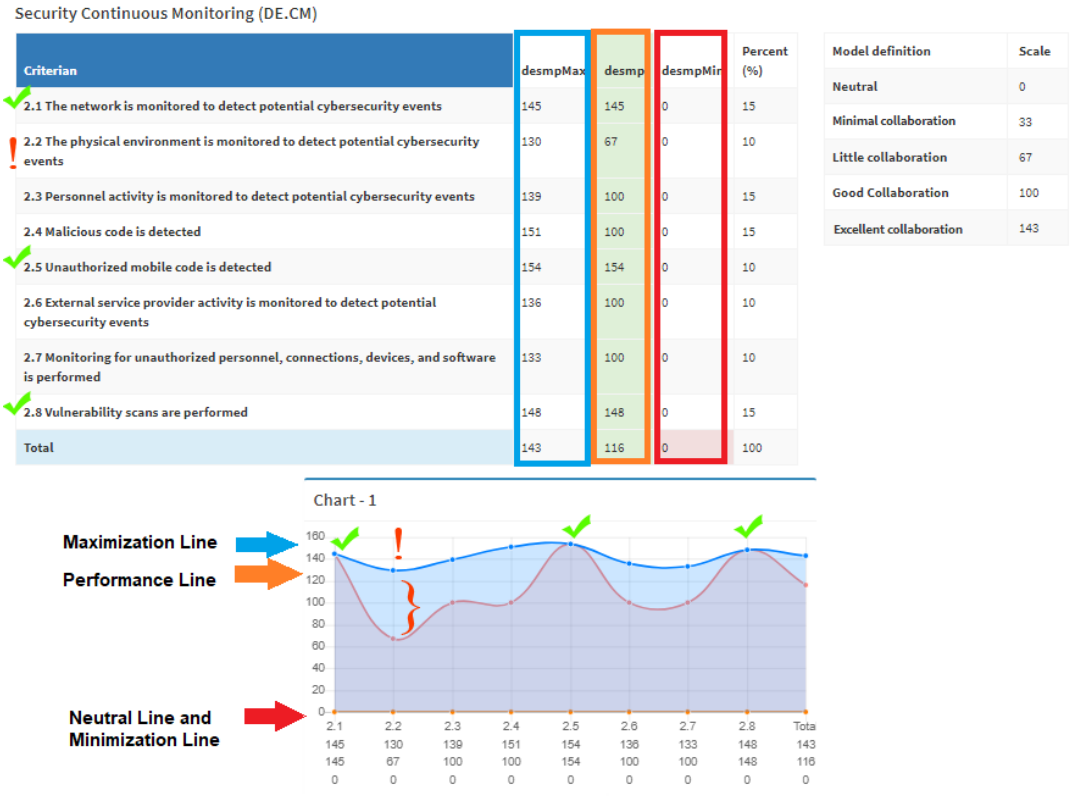


FIGURE 5. Security continuous monitoring - screenshot adapted from MyMCDA-C.

Table 5 shows the median responses from all stakeholders. Note that each row corresponds to a control with its respective median, level, and corresponding cardinal scale obtained according to the calculations performed by MyMCDA for each EPV.

Although the organization has a hierarchical structure, all answers have the same weight when calculating the median. Here we can see three more pillars of risk management. These are Integrated, Inclusive, Human, and cultural factors.

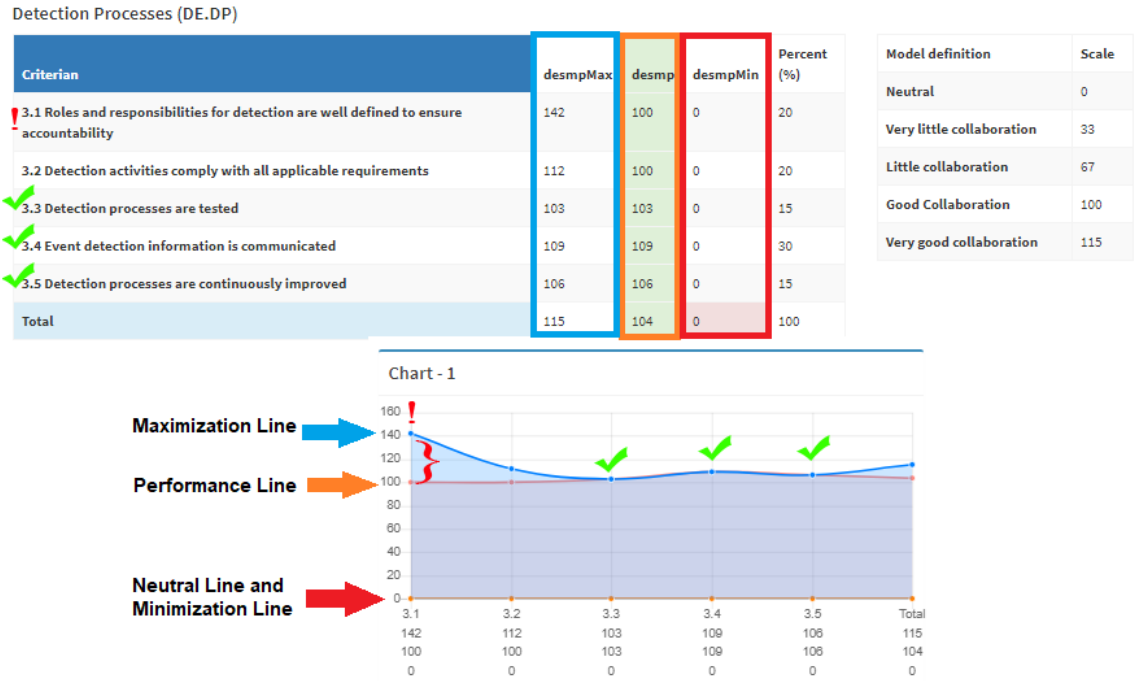


FIGURE 6. Detection processes - screenshot adapted from MyMCDA-C.

After processing the data in MyMCDA-C, several results were generated for decision making. All minimization points were equivalent to zero because N1 was zero and there were no negative values. At this point, we can see another principle of risk management being listed as the best available information.

In the next stage, the data entered into MyMCDA-C were processed. For "FPV - Anomalies and Events (DE. AE)", we could see that "EPV 1.2: Detected events are analyzed to understand attack targets and methods" had a better performance than the others, even with a lower compensation rate. This EPV was able to reach its maximum point, showing that it can contribute greatly to decision-makers' and stakeholders' vision. Fig. 4 illustrates this scenario.

However, "EPV 1.5: Incident alert thresholds are established" showed that it could contribute more compared to its maximum performance point, which makes it necessary for decision-makers to review this point.

Thus, opening a margin for improving this control, other EPVs have achieved an equivalent performance, showing that their implementation can significantly impact the bank's cybersecurity. Fig. 4 shows the EPVs with their compensation rates, the performance achieved, and the maximum performance to be obtained.

In Fig. 5, we can see that in the largest category of all "FPV 2 - Security Continuous Monitoring (DE.CM)", the compensation rates were well distributed. The "EPV 2.5: Unauthorized mobile code is detected" obtained a higher degree of performance, reaching its maximum point, showing that the implementation of this control contributes more to the bank's cybersecurity. Other controls also stood out in this way but with a slightly lower performance.

"EPV 2.2: The physical environment is monitored to detect potential cybersecurity events" was far from its maximization point with a difference of 63 steps. This means that decision-makers should look at this control differently, and could collaborate more. Other controls had a similar behavior, including the "EPV 2.4: Malicious code is detected". Fig. 5 illustrates this scenario.

For the category "FPV 3 - Detection Processes (DE. DP)", we have a scenario that shows the control "EPV 3.4: Event detection information is communicated" standing out. It reached the highest performance hitting its maximization point and showing that its implementation can obtain significant collaboration for banks' cybersecurity. It is essential to show that this control has a higher compensation rate, obtaining a more significant weight for decision-makers. Fig. 6 illustrates this scenario.

On the other hand, the "EPV 3.1: Roles and responsibilities for detection are well defined to ensure accountability" control did not achieve a greater performance than expected. Of all the controls, this is the one with the highest maximization point, that is, the one that would cause more collaboration in the decision-makers' vision. However, it was 42 steps away from its maximum performance. Therefore, this control should be analyzed with more attention by decision-makers. Fig. 6 illustrates the scenario described.

By performing an analysis of FPVs in general, we could see that "FPV 2 - Security Continuous Monitoring (DE. CM)" obtained the highest performance. However, it was more distant from its maximum degree, with a difference of 27 steps. The higher performance and higher maximization point show that the controls of this category collaborate more

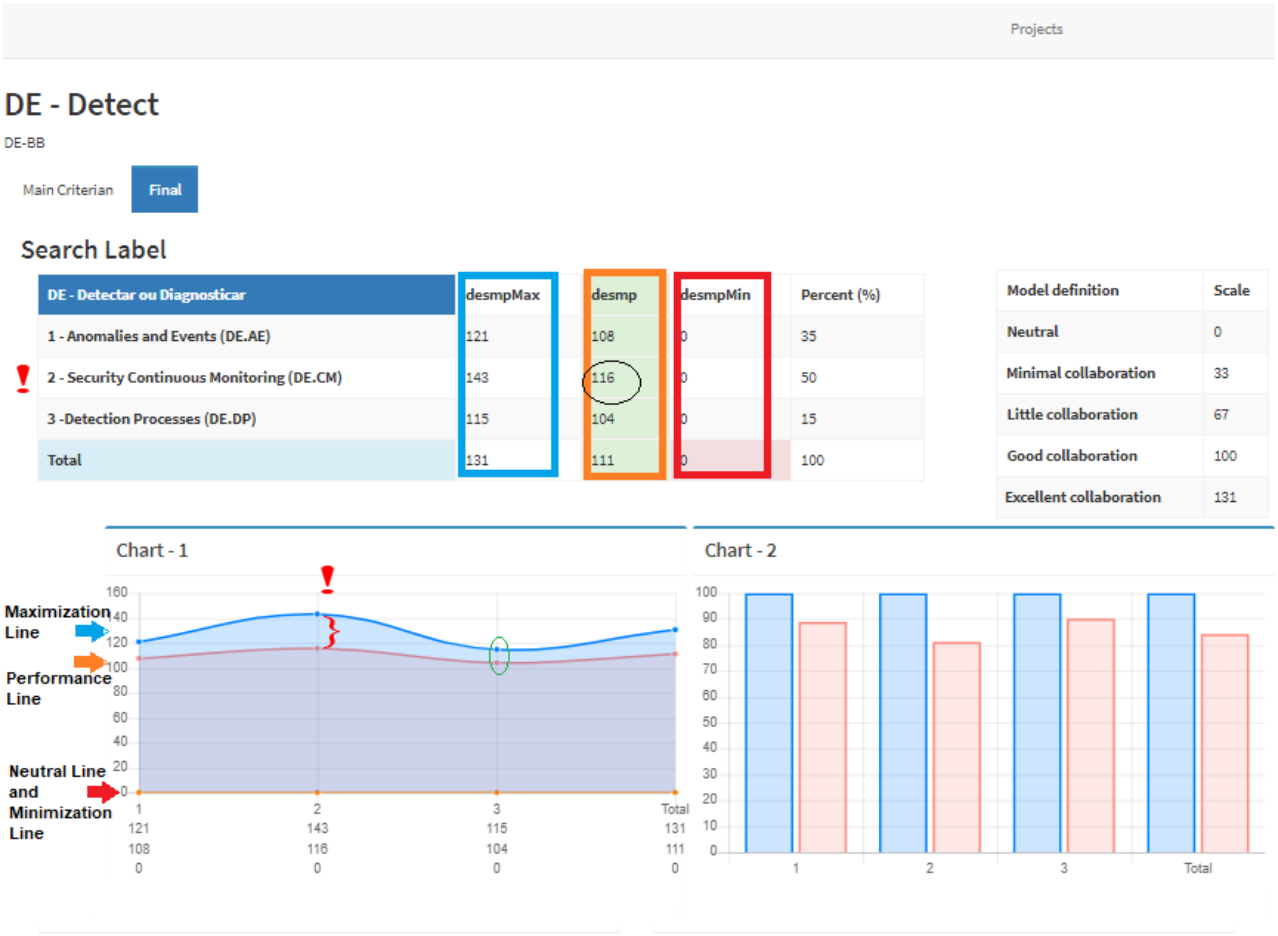


FIGURE 7. DE- detect - screenshot adapted from MyMCDA-C.

for the bank's security. According to the decision-makers, it is essential to note that this is the highest compensation rate. This means that some controls in this category should be reviewed.

When analyzing "FPV 3 - Detection Processes (DE. DP)", we see a more negligible difference between the performance and the degree of maximization. However, the compensation rate proved to be much lower than the others. Fig. 7 shows this scenario of maximization.

The other controls that did not receive positive or negative highlights must be evaluated if they can be implemented or reviewed. If an implementation is chosen, it does not need to be a priority like the ones that were highlighted. Notably, good risk management must be reviewed over time according to the experience gained. Thus, obeying the pillar of Continuous Improvement of Risk Management, the MCDA-C can be reapplied again.

IX. CONCLUSION

The article analyzed how cybersecurity controls for NIST's critical infrastructure would collaborate with a large Brazilian bank that moves millions of dollars per hour, specifically in the technology sector, which takes care of the international area. The data were collected through brainstorms conducted with decision-makers and forms sent to the project's stakeholders.

MCDA-C was used as an intervention tool due to its structuring form. It can identify and operate a criteria analysis of the decisions concerning the company situation.

The MCDA-C implementation covered all the pillars of risk management recommended by the ISO standards highlighted in the study.

The research objectives were achieved by obtaining all the performance points of how the implementation of information security controls could collaborate with the bank. All performance points were listed along with their maximization and minimization points, helping decision-makers make their decisions.

For this financial institution, the main controls to be implemented and prioritized are those of the "FPV 2 - Security Continuous Monitoring (DE. CM)" categories.

The primary collaboration of this work is to show that the constructivist model can also be used as a methodology to help create a cyber risk plan. This way shows that it can stand up to other methods, since most of the literature uses other multicriteria methods.

The limitation of this study was in only using the NIST Detect Function. It was due to the organization's need to improve its incident detection controls at that time.

Future projects must apply another multicriteria method to compare the results and use the best method in other functions of the "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1".

REFERENCES

[1] D. Pedriali, C. H. Arima, and F. J. Piacente, "Segurança da informação na Logística 4.0: Bibliométrico," *Res., Soc. Develop.*, vol. 9, no. 2, Jan. 2020, Art. no. e38921949, doi: 10.33448/rsd-v9i2.1949.

[2] F. B. Bancos, "Pesquisa febraban de tecnologia Bancária 2019," FEBRABAN-Federação Brasileira de Bancos, São Paulo, Brazil, Tech. Rep., 2019.

[3] F. R. Moreira, R. R. Nunes, W. F. Giozza, and G. A. Nze, "Optimization of the performance of an online payment application by the improvement of its infrastructure," in *Proc. 15th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Seville, Spain, 2020, pp. 1–2, doi: 10.23919/CISTI49556.2020.9140895.

[4] O. A. Klymenko, M. V. Gutsalyuk, and A. V. Savchenko, "Combating cybercrime as a prerequisite for the development of the digital society," *JANUS NET E-J. Int. Relation*, vol. 1, no. 11, pp. 19–29, 2020, doi: 10.26619/1647-7251.11.1.2.

[5] A. Shameli-Sendi, "Fuzzy multi-criteria decision-making for information security risk assessment," *Open Cybern. Syst. J.*, vol. 6, no. 1, pp. 26–37, Jun. 2012, doi: 10.2174/1874110X01206010026.

[6] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.

[7] *Risk Management–Risk Assessment Techniques*, Standard 31010 2012. 2012.

[8] S. Kinser, P. Graaf, M. Stein, F. Hughey, R. Roller, D. Voss, and A. Salmoriaghi, "Scoring trust across hybrid-space: A quantitative framework designed to calculate cybersecurity ratings, measures, and metrics to inform a trust score," in *Proc. Small Satellite Conf.*, Logan, UT, USA, 2020, pp. 1–10.

[9] M. I. Tariq, S. Ahmed, N. A. Memon, S. Tayyaba, M. W. Ashraf, M. Nazir, A. Hussain, V. E. Balas, and M. M. Balas, "Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks," *Sensors*, vol. 20, no. 5, p. 1310, Feb. 2020.

[10] M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective," *IEEE Access*, vol. 8, pp. 25543–25556, 2020, doi: 10.1109/ACCESS.2020.2970784.

[11] I. M., N. Ramadan, and H. Ahmed, "Cybersecurity risks of blockchain technology," *Int. J. Comput. Appl.*, vol. 177, no. 42, pp. 8–14, Mar. 2020.

[12] J. Fanelli and J. Waxler, "Prioritizing computer security controls for home users," *Peer J.*, vol. 7, Oct. 2019, Art. no. e27540v1, doi: 10.7287/peerj.preprints.27540v1.

[13] N. Gupta Gourisetti, M. Mylrea, and H. Patangia, "Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2019, pp. 206–213, doi: 10.1109/CCWC.2019.8666518.

[14] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Anal.*, vol. 40, no. 1, pp. 183–199, Jan. 2020, doi: 10.1111/risa.12891.

[15] *Risk Management—Guidelines International Organization for Standardization*, Standard ISO 31000, 2018.

[16] *Risk Management—Guidance For the Implementation*, Standard ISO 31004, 2013.

[17] A. Dutra, M. V. A. Lima, A. L. M. Lopes, and F. R. Serra, "O uso da metodologia multicritério de apoio decisão construtivista–MCDA-C para a incorporação da dimensão integrativa nos processos de avaliação de desempenho organizacional," in *Proc. Encontro Admin. Inf.*, Brazil, Floriand, 2007, pp. 1–15.

[18] C. A. E. Bana Costa, "Introdução geral às abordagens multicritério de apoio tomada de decisão," *Investion Oper.*, vol. 66, pp. 117–139, Jun. 1988.

[19] C. A. E. Bana Costa, "Três convicções fundamentais na prática do apoio decisão," *Pesquisa Oper.*, vol. 1, pp. 9–20, Jun. 1993.

[20] C. A. E. Bana Costa and P. H. Vincke, *Multiple Criteria Decision Aid: An Verview*, Berlim, Germany: Springer, 1990, pp. 101–118.

[21] B. Roy, "Decision science or decision-aid science?" *Eur. J. Oper. Res.*, vol. 66, no. 2, pp. 184–203, 1993, doi: 10.1016/0377-2217(93)90312-B.

[22] C. A. E. Bana Costa, "Processo de apoio decisão: Problemáticas, actores e acções apostila do curso metodologias multicritério de apoio decisão—ENE/UFSC," *Pesquisa Oper.*, vol. 13, no. 1, p. 15, Aug. 1995.

[23] L. Ensslin, E. Giffhorn, S. R. Ensslin, S. M. Petri, and W. B. Vianna, "Avaliação do desempenho de empresas terceirizadas com o uso da metodologia multicritério de apoio decisão—Construtivista," *Pesquisa Oper.*, vol. 30, no. 1, pp. 125–152, Apr. 2010, doi: 10.1590/S0101-74382010000100007.

[24] L. Ensslin, G. Montibeller, S. M. Noronha, *Apoio Decisão: Metodologias Para Estruturação de Problemas Avaliação Multicritério de Alternativas*. Brazil, Brasilia: Insular, 2001.

[25] J. Barzilai, "Notes on the analytic hierarchy process," in *Proc. NSF Design Manuf. Res. Conf.*, Tampa, FL, USA, 2001, pp. 1–6.

[26] F. Roberts, *Measurement Theory, in Encyclopaedia of Mathematics and its Applications*. London, U.K.: Addison-Wesley, 1979.

[27] A. A. Longaray, L. Ensslin, A. Dutra, S. Ensslin, R. Brasil, and P. Munhoz, "Using MCDA-C to assess the organizational performance of industries operating at Brazilian maritime port terminals," *Oper. Res. Perspect.*, vol. 6, 2019, Art. no. 100109.

[28] R. L. Keeney, *Value-Focused Thinking: A Path to Creative Decision Making*. London, U.K.: Harvard Univ. Press, 1992.

[29] C. A. Costa and E. Beinat, *Model-Structuring in Public Decisionaiding*. London, U.K.: London School of Economics, 2005.

[30] R. C. de Azevedo, R. T. de Oliveira Lacerda, L. Ensslin, A. E. Jungles, and S. R. Ensslin, "Performance measurement to aid decision making in the budgeting process for apartment-building construction: Case study using MCDA-C," *J. Construct. Eng. Manage.*, vol. 139, no. 2, pp. 225–235, Feb. 2013.

[31] L. Ensslin, A. Dutra, and S. R. Ensslin, "MCDA: A constructivist approach to the management of human resources at a governmental agency," *Int. Trans. Oper. Res.*, vol. 7, no. 1, pp. 79–100, Jan. 2000.

[32] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb Model," *J. Cybersecur.*, vol. 6, no. 1, Jan. 2020, Art. no. tyaa005, doi: 10.1093/cybsec/tyaa005.

[33] P. L. Braga, C. M. Lima, and E. C. C. Rodrigues, "A influência do Instagram no comportamento do consumidor online," in *Proc. Rev. Admin.*, Brazil, Belo Horizonte, vol. 19, 2020, pp. 15–28.

[34] G. L. Barros, E. C. C. Rodrigues, and C. M. Lima, "Logística reversa de pós-consumo: Análise das práticas em unidades escolares públicas do distrito federal," *Revista Negócios Em Projeção*, vol. 9, pp. 44–65, Oct. 2018.

[35] L. R. Barbalho, E. C. C. Rodrigues, and C. M. Lima, "Análise multicritério das lacunas entre logística reversa e processamento de bens," *Rea. Rev. Admin.*, vol. 19, no. 2, pp. 301–322, 2020.

[36] G. P. Cardoso and E. C. C. Rodrigues, "Contabilidade pública gerencial—Uma análise da informação de custos LUZ da percepção dos gestores públicos," in *Int. Conf. Manage. Accounting (ICMA/COGECONT)*, Blumenau/SC, Brazil, 2020, pp. 1–4.

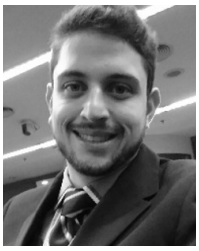
[37] A. S. Júnior, E. C. C. Rodrigues, C. M. Lima, R. R. Nunes, and G. L. Wielewski, "Análise da usabilidade do marketplace ifood pela ótica do consumidor," in *Proc. 30th. Enangrad*, Uberlândia, Brazil, 2019, pp. 1–17.

[38] E. R. Amaral, A. S. Júnior, G. L. Wielewski, E. C. C. Rodrigues, and C. M. Lima, "A usabilidade de site de compras vendas," in *Proc. 30th. Enangrad*, Uberlândia, Brazil, 2019, pp. 1–18.

[39] C. A. E. Bana Costa and J. C. Vansnick, "The MACBETH approach: Basic ideas, software and an application," in *Advances in Decision Analysis*, N. Meskens and M. Roubens, Eds. Dordrecht, The Netherlands: Kluwer, 1999, pp. 57–131.

[40] C. A. E. Bana Costa, J.-M. D. Corte, and J.-C. Vansnick, "Macbeth," *Int. J. Inf. Technol. Decis. Making*, vol. 11, no. 2, pp. 359–387, 2003.

[41] R. K. Yin, *Case Study Research: Design and Methods*, 4th ed. Thousand Oaks, CA, USA: Sage, 2009.



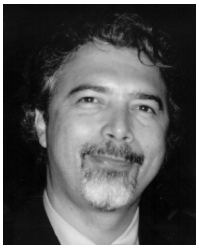
FERNANDO ROCHA MOREIRA born in Carmo do Paranaíba, Brazil. He received the bachelor's degree in information systems from the Federal University of Viçosa (UFV), Rio Paranaíba, Brazil, in 2013, the M.B.A. degree in project management from the University of São Paulo, Piracicaba, Brazil, in 2019, and the master's degree in information security from the University of Brasília (UnB), Brasília, Brazil, in 2021, with focus on cyber risk analysis.

DEMÉTRIO ANTÔNIO DA SILVA FILHO was born in Recife, Brazil. He received the bachelor's and master's degrees in physics from the Universidade Federal de Pernambuco (UFPE), Recife, in 1996 and 1998, respectively, and the Ph.D. degree from the Institute of Physics "Gleb Wataghin," State University of Campinas (UNICAMP), Brazil, in 2003.

During his doctorate, he participated in the doctoral program in Brazil with internship abroad (PDEE) of CAPES, spending a year at The University of Arizona, where he returned after defending his thesis to work as a Researcher. As a result of this internship, he published some relevant articles in this field of research, including an article in *Chemical Reviews* that has more than 4000 citations. He has been a CNPq Research Productivity Fellow, since 2011. He was the Coordinator of the Graduate Program in physics with UnB, from 2012 to 2014, and the Director of the Institutional Development and Innovation with the Pro-Rectorate of Research and Graduate Studies, University of Brasília. He is currently an Associate Professor with the University of Brasília. He has published more than 80 articles in international journals that have about 13,000 citations (Google Scholar). His H-factor is also equal to 31. He has experience in the assembly and administration of high-performance clusters and in information security.

GEORGES DANIEL AMVAME NZE (Member, IEEE) received the degree in electrical engineering from the University of Brasília (UnB), Brasília, Brazil, in 1999, the master's degree in electrical engineering from UnB, in 2002, and the Ph.D. degree, in Brasília, in 2006.

He is currently an Associate Professor with the University of Brasília. He has experience in the area of electrical engineering, with emphasis on telecommunication systems, working mainly on the following topics, such as network management and information security, information and communication technology, and health informatics. He has extensive experience in coordinating or participating in research and development projects, noting the recent projects linked to terms of decentralized implementation, specifically the projects such as, the "Technological innovations in governance management, in obtaining and generating information and in communications with State Enterprises under the aegis of the Secretariat of Coordination and Governance of State Enterprises of the Ministry of Planning, Development, and Management (SEST/MP)," as the Coordinator; the "Applied research in strategic planning, corporate risk management, and corporate information management within the competencies of the Directorate of Planning and Management of the Ministry of Planning, Budget, and Management (DIPLA/MP)," as a Participant; the "Cooperative project for research and development monitoring the development of the new system of people management of the Federal Executive Power of SIGEPE (MP-FUB)," as a Participant; the "Applied research of technological integration and systemic interoperation in the Federal Public Defender Office (DPU)," as the Substitute Coordinator; the "Integration of technologies and methods applied to the practice of virtual school of Federal Public Administration (ENAP)," as the Substitute Coordinator; the "Strategic management of information, and respective methods, instruments, and infrastructure, in the context of assisted implementation and validation of the PDTI of SOF," as a member; and the "Conception, instrumentation, and operationalization of advanced processes in IT Management (SLTI/MP)," as a member.



RAFAEL TIMÓTEO DE SOUSA JÚNIOR (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the Federal University of Paraíba (UFPB), Campina Grande, Brazil, in 1984, the master's/D.E.A. degree in information systems and computing from the Ecole Supérieure d'Electricité—Supélec, Rennes, France, in 1985, and the Ph.D. degree in telecommunications and signal processing from the University of Rennes 1, Rennes, France, in 1988.

He was a Visiting Researcher with the Network Security and Information Systems Group (SSIR), Ecole Supérieure d'Electricité—Supélec, from 2006 to 2007. He worked in the private sector, from 1988 to 1996. Since 1996, he has been an Associate Professor of engineering of communication networks with the Department of Electrical Engineering, University of Brasília, Brazil, where he is currently the Coordinator of the Professional Graduate Program in Electrical Engineering (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is also a Researcher with level 2 (PQ-2) productivity fellowship with the National Council for Scientific and Technological Development (CNPq). His professional experience includes research projects with Dell Computers, HP, IBM, Cisco, and Siemens. He is also the Coordinator of research, development, and technology transfer projects with the Ministries of Planning, Economy, and Justice of Brazil, the Institutional Security Cabinet of the Presidency of Brazil, the Administrative Council for Economic Defense, the Federal Attorney General, and the Federal Public Defender's Office. He has received research grants from Brazilian research and innovation agencies, such as CNPq, CAPES, FINEP, RNP, and FAPDF. He conducts research in cyber, information, and network security, distributed data services, machine learning for intrusion and fraud detection, and signal processing, energy harvesting, and physical layer security.

Dr. De Sousa Júnior was awarded the title of the 2019 Chapter of the Year by IEEE VTS. He is also the Leader of IEEE VTS Center-North Brazil Chapter and the IEEE Center-North Brazil Blockchain Study Group.

RAFAEL RABELO NUNES received the bachelor's degree in engineering of communication networks from the University of Brasília (UnB), Brasília, Brazil, in 2005, with some subjects studied at the University of Porto, Portugal, in 2005, the master's and Ph.D. degrees in electrical engineering from UnB, in 2009 and 2012, respectively, and the bachelor's degree in special teacher training program from the Universidade Católica de Brasília (UCB), Brasília, in 2014.

He is currently an Adjunct Professor with the University of Brasília on a partial basis, where he is dedicated to teaching and researching how IT can be used strategically by people and organizations, taking into account the risks involved. He also works in the structuring and maintenance of risk management in the Brazilian Supreme Court, and a Professor with UniAtenas University Center. He has more than 20 years of experience in information technology (IT), keeping his academic professional career inseparable. He has served as a special advisor to the Supreme Court president; an information security manager; a software development project manager; an infrastructure analyst; and a development analyst. In the private area, he was a Network Engineer at TIM and Claro, and a Professor with Estácio de Brasília University Center.