Cybersecurity Risk Assessment Through Analytic Hierarchy Process: Integrating Multicriteria and Sensitivity Analysis

Fernando Rocha Moreira[1][a], Edna Dias Canedo[1][b], Rafael Rabelo Nunes[2][c], André Luiz Marques Serrano[3][d], Cláudia Jacy Barenco Abbas[4][e], Marcelo Lopes Pereira Júnior[4][f] and Fábio Lúcio Lopes de Mendonça[4][g]

[1]*University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil*

[2]*UniAtenas University Center, Paracatu-MG, Brazil*

[3]*University of Brasília (UnB), Professional Postgraduate Program in Electrical Engineering - PPEE, Brasília–DF, Brazil*

[4]*University of Brasília (UnB), Department of Electrical Engineering, Brasília–DF, Brazil*

Keywords: Cybersecurity Risk Management, NIST Cybersecurity Framework, Analytic Hierarchy Process, Multicriteria Decision-Making, Public Sector Cybersecurity.

Abstract: Context: Cybersecurity is increasingly critical for public institutions, particularly as digital transformations expose them to a wide range of cybersecurity risks. Managing these risks effectively requires a structured approach that aligns with recognized standards and frameworks. Methods: This study presents the process of cybersecurity risk management within a Brazilian public agency, utilizing the cybersecurity incident detection controls proposed by the NIST Cybersecurity Framework (NIST-CSF). To assess and prioritize these controls, the Analytic Hierarchy Process (AHP) was applied as a multicriteria decision-making method. Expert judgments were collected and integrated into the AHP model to determine the relative importance of each control. Results: The application of the AHP method resulted in a prioritized list of cybersecurity controls. This list outlines the sequence in which controls should be implemented, enabling decision-makers to direct resources effectively and make informed choices in mitigating cybersecurity risks. Conclusion: The findings underscore the value of adopting multicriteria methods like AHP in cybersecurity risk management. This paper contributes to the literature by encouraging the use of such methods as best practices for improving cybersecurity risk assessment and management in public sector organizations.

1 INTRODUCTION

Technology has played a critical role in the daily lives of citizens and public services. It has facilitated and provided increasingly efficient services to the population. Moreover, technological evolution assumes great importance in achieving the strategic objectives of public agencies (Alves et al., 2023). However, along with the benefits brought by the use of technology, new risk factors also emerge (Canedo et al., 2021), among them, cybersecurity risk (Moreira et al., 2021).

Brazil has faced growing cyberattacks, with approximately 357,422 attacks reported in the second half of 2023 (CNN Brasil, 2023). A significant example of a cyberattack and data breach in the public sector occurred with the ConecteSUS Platform, the official application of the Ministry of Health. The platform was targeted in an invasion and hacked, resulting in its temporary shutdown. Approximately 50 terabytes of personal data were compromised, with some data being withheld and others altered in the system (Divino and Campos, 2024).

To improve the efficiency and effectiveness of public agencies, the Brazilian government created the Privacy and Information Security Program (PPSI) (BRASIL, 2023). The PPSI establishes privacy and

[a] https://orcid.org/0000-0003-3100-7128
[b] https://orcid.org/0000-0002-2159-339X
[c] https://orcid.org/0000-0002-1538-4276
[d] https://orcid.org/0000-0001-5182-0496
[e] https://orcid.org/0000-0002-6939-172X
[f] https://orcid.org/0000-0001-9058-510X
[g] https://orcid.org/0000-0001-7100-7304

Moreira, F. R., Canedo, E. D., Nunes, R. R., Serrano, A. L. M., Abbas, C. J. B., Pereira Júnior, M. L. and Lopes de Mendonça, F. L.
Cybersecurity Risk Assessment Through Analytic Hierarchy Process: Integrating Multicriteria and Sensitivity Analysis.
DOI: 10.5220/0013197300003929

In *Proceedings of the 27th International Conference on Enterprise Information Systems (ICEIS 2025) - Volume 2*, pages 117-128
ISBN: 978-989-758-749-8; ISSN: 2184-4992

information security controls to support best practices in mitigating cyberattacks and managing risks (BRASIL, 2023).

However, managing cybersecurity risks is no trivial task. Good risk management involves a well-defined process for assessing an institution's cybersecurity controls. Available security frameworks involve many controls that need to be assessed and prioritized (Moreira et al., 2021). For example, the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology includes 108 subcategories of cybersecurity, while ISO 27.001 includes 93 controls to be assessed and prioritized (NIST, 2018), (ISO/IEC, 2022).

Given this situation, information security managers face the problem of prioritizing security controls for risk management. ISO 31010 (ISO/IEC, 2018) presents several risk assessment and prioritization tools, which can help managers deal with the prioritization of security controls and risk management in their daily activities (ISO/IEC, 2018).

Among the tools proposed by ISO 31010 (ISO/IEC, 2018) are MCDM – Multi-Criteria Decision Methods. These methods are known to assist in decision-making processes and can produce a ranking of alternatives based on the selected criteria (ISO/IEC, 2019). One of the most widely used methods in the literature is the Analytic Hierarchy Process (AHP), which uses mathematical calculations to generate the final result (Saaty, 1980).

In this research, we applied the AHP multicriteria method within a federal public administration agency (APF), utilizing the Cybersecurity Framework (CSF) as a guide to prioritize the controls to be adopted. Due to confidentiality concerns surrounding the agency, we created a hypothetical scenario as the focus for the practical case study.

The study produced several findings, two of which we highlight here: 1) We evaluated the application of the AHP in the risk management process, ensuring that all its principles were addressed. 2) We analyzed and discussed the decisions made by managers and cybersecurity risk specialists, emphasizing the major concerns faced by professionals in this field today.

This study contributes to the existing literature by demonstrating the practical application of AHP in the context of cybersecurity risk management within public institutions, providing valuable insights into the decision-making process of risk prioritization. The study also discusses the main cybersecurity detection controls that should be prioritized by information security managers in the Brazilian public sector.

This paper is divided as follows: Section 2 contains the Related Work and the Background of the research, in which the similarities and differences in relation to the work in question will be presented and the concepts used to solve the problem in question are discussed; Section 3 will present the Study Settings; Section 4 will present the results obtained from solving this problem; Finally, section 5 discusses the conclusions of this study.

2 BACKGROUND AND RELATED WORK

2.1 Risk Management

The risk management process should be an interactive activity that supports organizations in developing strategies to achieve their objectives and in decision-making (ISO/IEC, 2018). This process is part of governance and leadership and should involve all organizational activities, including all stakeholders (Moreira et al., 2021). Furthermore, one of the objectives of a well-implemented Risk Management is the creation and protection of value, improved performance, encouragement of innovation, and support in achieving organizational goals (Canedo et al., 2021).

When it comes to cybersecurity risks, it is no different. This category of risks is crucial for the organization's objectives, considering that the impact of such failures on the business can lead to severe consequences, especially for organizations with high strategic dependence on ICT (Canedo et al., 2021).

To efficiently manage risks, it is essential to first establish the context and then proceed with the risk assessment process. The result of this process is then evaluated to verify whether the obtained information is adequate to define the necessary actions to reduce the risk to an acceptable level (ISO/IEC, 2018). A well-designed risk management process should involve eight principles (ISO/IEC, 2018):

- **Integrated.** Risk management should involve all parts of the organization.
- **Structured and Comprehensive.** The risk management process should be approached in a structured manner, contributing to consistent and comparable results.
- **Customized.** Risk management should be tailored to adjust to external and internal contexts and the organization's objectives.
- **Inclusive.** The risk management process should involve all stakeholders, ensuring that different viewpoints and perceptions are considered.

- **Dynamic.** New risks may arise, change, or disappear as the organization's external and internal contexts evolve; therefore, the risk management process must be dynamic.
- **Best Available Information.** The data entry process should be clear, based on both past and future considerations, and should account for limitations and uncertainties. All information should be clear and available to stakeholders.
- **Human and Cultural Factors.** This principle must be considered, as it directly influences all risks at every strategic level.
- **Continuous Improvement.** The risk management process should be continuously improved and reviewed based on the learning and experiences gained.

2.2 Analytic Hierarchy Process

One way to support the risk management process and decision-making is to use a Multi-Criteria Decision Making (MCDM). These methods aim to generate a preference ranking among the available options (Moreira et al., 2021). They use a matrix of options and criteria, rated based on a score for each option, ideally aligning with the risk management process recommended by ISO 31.000 (ISO/IEC, 2018).

The main objective is to establish a preference order among the available options. This involves an analysis that consists of constructing a matrix composed of options and criteria. These criteria are evaluated and ranked, and subsequently aggregated to generate a final score for each option (ISO/IEC, 2019).

(ISO/IEC, 2019) states that when applying an MCDA, the risk management process is followed, considering the steps: Risk Identification, Risk Analysis, and Risk Evaluation. It is classified as "Applicable" for the Risk Identification and Risk Evaluation phases. Regarding the Risk Evaluation phase, from the perspective of Consequences and Risk Levels, MCDA is considered "Strongly Applicable," while from the perspective of "Probability," it is deemed "Applicable."

The Analytic Hierarchy Process (AHP) is a multicriteria decision-making method derived from the American school, where the main objective is the precision of calculations and the result, producing a priority list of the alternatives being evaluated (Saaty, 1980). This method fits perfectly into the risk management process. The AHP has seven phases, as presented in Figure. 1 :

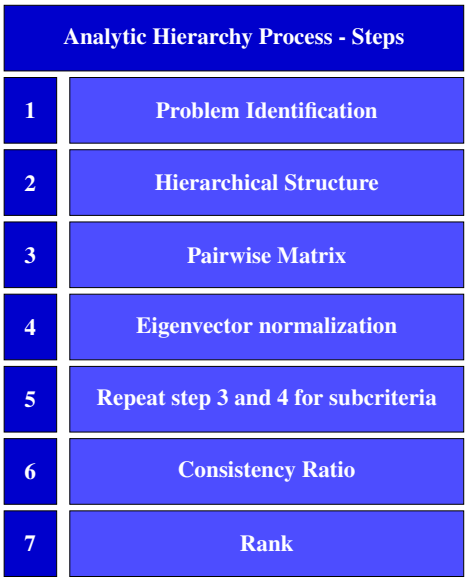

Figure 1: Steps of the Analytic Hierarchy Process (AHP).

1. **Problem Identification.** In this phase, it is necessary to identify the problem, understand it, as well as identify the real needs for its solution.
2. **Hierarchical Structure.** In this phase, the problem must be understood and transformed into a hierarchical tree. This tree should contain the criteria and alternatives to be judged, as indicated by the method's creator (Saaty, 1980).
3. **Pairwise Matrix.** This phase involves the evaluation and judgment of specialists involved in the decision-making process. The evaluation is conducted in a paired manner, where one alternative is evaluated against another concerning a specific criterion, using a scale proposed by the author (Saaty, 1980). Table 1 illustrates Saaty's scale.
4. **Eigenvector Normalization.** In this phase, the method normalizes the calculation vectors to enable the calculation of the consistency index, which will be done in phase 6.
5. **Repeat Step 3 and 4 for Subcriteria.** In this phase, steps 3 and 4 should be repeated for all alternatives and subcriteria concerning the criteria until all possible judgments within the hierarchical structure are completed (Siregar et al., 2024).
6. **Consistency Ratio.** In this phase, the consistency index is calculated. This index can indicate whether the judgments provided by the experts are meaningful and consistent. This is possible thanks to the pairwise comparison system using Saaty's scale. The index is calculated after the experts complete their evaluation of the alternatives against a criterion. If the consistency index exceeds 10

Table 1: Saaty's Scale. (Saaty, 1980).

Numerical Scale	Conceptual Scale	Description
1	Equal	The two elements contribute equally to the criterion
3	Moderate	The compared element is slightly more important than the other
5	Strong	Experience and judgment strongly favor the element over the other
7	Very Strong	The compared element is much stronger than the other, and such importance can be observed in practice
9	Absolute	The compared element presents the highest possible level of evidence in its favor
2,4,6,8	Intermediate values	When the evaluator has difficulty choosing between two levels of underlying importance

7. **Rank.** Finally, the method globally calculates the priority list, providing the contribution each element has concerning the objective. The AHP uses matrix calculations to obtain this result (Saaty, 1980).

Some software tools implement this process and facilitate the application of AHP. To address this problem, the Super Decision software was used to implement the project. This software, which implements the AHP method, was developed by the team of the method's creator, Thomas Saaty. Its development and maintenance are sponsored by the Creative Decisions Foundation. (Creative Decision Foundation, 2012).

2.3 NIST Cybersecurity Framework

The Cybersecurity Framework (CSF) is a cybersecurity framework that contains 108 controls called security subcategories, which companies and organizations can adopt for their internal cybersecurity risk management process. This guide was created in 2013 in the United States under Executive Order 13636, titled "Improving Critical Infrastructure Cybersecurity" (NIST, 2018).

Subsequently, the Cybersecurity Enhancement Act was created in 2014, assigning NIST the role of identifying and developing cybersecurity risk guidelines, encouraging critical infrastructure operators to voluntarily adopt the guide (NIST, 2018).

This guide was designed to combat and manage cybersecurity risks aimed at the economy, and it is also based on the business and organizational needs of companies. It has no regulatory nature for organizations. It provides guidance for organizations to incorporate cybersecurity risk management processes as part of the organization's overall risk management process (NIST, 2018).

The framework assists critical infrastructure managers in developing cybersecurity risk guidelines for their companies. Critical infrastructure refers to essential systems and assets whose disruption could cause severe impacts on economic security, health, and public safety. The CSF follows a tree structure, where the first level consists of functions, the second contains categories, the third includes subcategories representing cybersecurity controls, and the fourth comprises the references from which these controls were derived (NIST, 2018). The figure 2 illustrates the tree structure of the CSF for the Detect function.

The Detect function was utilized in this study. Its controls aim to develop and implement guidelines to identify the occurrence of cybersecurity events. This function includes the following categories: Anomalies and Events (DE.AE), Security Continuous Monitoring (DE.CM), and Detection Processes (DE.DP). Each category comprises specific activities relevant to cybersecurity detection.

In addition to the Detect function, the CSF includes other important functions that were not utilized in this paper. The controls of the Identify function are associated with the organizational understanding required to manage security risks. This function focuses on identifying systems, people, assets, and resources. The Protect function is responsible for developing and implementing the necessary protections to ensure the continued operation of services, aiming to limit cybersecurity incidents. The Respond function implements activities to take appropriate actions when a cybersecurity incident is detected. Finally, the Recover function aims to carry out activities and maintain plans to restore services that became inoperative due to a cybersecurity incident.

2.4 Related Work

There are some works in the literature that have used multicriteria methods to support risk management. (Brigido et al., 2022) used the AHP multicriteria method together with the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to create a risk mitigation model for the allocation of human resources in a law firm. The authors argued that AHP can validate human criteria judgments while TOPSIS prioritizes alternatives through risk similarity (Brigido et al., 2022).

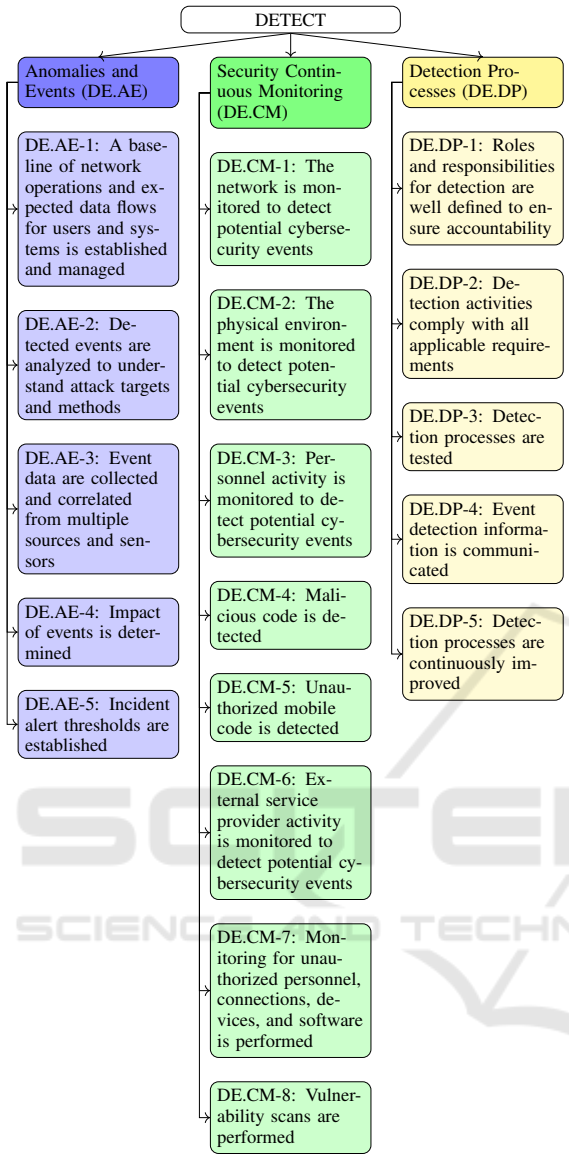

Figure 2: Hierarchical structure of the DETECT framework showing the three main categories.

(Ru et al., 2016) evaluated the influence of cyberattacks on the Electric Cyber-Physical System (ECPS). The authors created a model to perform a quantitative risk assessment, using AHP to model the problem as well as to quantify the impact of the attack on the ECPS. The authors conducted a practical case study, and the results indicated that applying the proposed method can support organizations in assessing risks in ECPS systems.

(Bitton et al., 2021) conducted an analysis of the threats to a Machine Learning (ML) system using AHP. As a reference, the authors used the NIST threat ontological model. Thus, the NIST model was used to assess the security risks of enterprise networks and ML-based systems. AHP was used to classify various attributes of cyberattacks through the judgment of security experts. As a result, the authors supported practitioners in the field of information security with a methodological and practical tool to assist in the execution of the cybersecurity risk quantification process in production systems using ML (Bitton et al., 2021).

(Moreira et al., 2021) used the Constructivist Multicriteria Decision Support Methodology (MCDA-C) to develop a cybersecurity risk assessment plan for a financial bank. The authors used the cybersecurity controls from the CSF as a reference. The controls were assessed, and unlike AHP, which produces a list of priorities, MCDA-C demonstrated the performance point of each cybersecurity control when compared to the points of maximization and minimization of each one. Through this approach, the authors contributed to a better understanding of risk management, using MCDA-C as a good practice in risk management (Moreira et al., 2021).

Multicriteria methods have been used to manage risks in various fields of knowledge, such as in the management of human resource allocation risks and in cybersecurity risk management. Unlike previous works, this study uses AHP with the CSF controls, aiming to support organizational managers in creating the risk management plan and developing a priority list of controls to be implemented to help risk managers mitigate cybersecurity risks. Thus, this work proposes a practical approach, using AHP based on the structure of the controls proposed by the CSF to improve the process of cybersecurity risk management.

This paper stands out for its innovative application of multicriteria methods in cybersecurity risk management, using CSF controls combined with the AHP method. Unlike previous studies that focused on areas such as human resource allocation multicriteria methods to support risk management. (Brigido et al., 2022), electric cyber-physical systems (Ru et al., 2016), and machine learning-based systems (Bitton et al., 2021), this work adopts a broad and practical approach, applicable to various organizations. Furthermore, in contrast to the MCDA-C-based approach used by (Moreira et al., 2021), which assessed the performance of cybersecurity controls in a financial bank, this study employs AHP to generate a prioritized list of CSF controls, facilitating decision-making and resource allocation. This unique integration of AHP with CSF controls provides a practical and structured tool for organizational managers, enabling efficient risk mitigation aligned with the current needs of cybersecurity.

3 STUDY SETTINGS

This research has an applied nature as it evaluates and prioritizes cybersecurity controls for an organization, a bank of the Brazilian Government. Based on this evaluation, the bank will identify gaps in its information security management process and will define measures to mitigate them.

Regarding data collection, it can be characterized as primary and secondary. The primary is justified as data was collected, raised, and analyzed through the judgment of decision-makers concerning the evaluation of cybersecurity controls. The secondary is justified as the cybersecurity controls were derived from the CSF along with its structure to be evaluated by the judges (NIST, 2018).

The work has a dual approach in terms of its methodology. It has quantitative characteristics considering the mathematical model with matrix calculations and consistency index used by AHP (Saaty, 1980). It also has a qualitative approach by utilizing the structure of Detection from the CSF being evaluated under the light of Saaty's scale, which has qualitative degrees of assessment.

The research presents itself in a mixed manner due to the phases of AHP application. The first phase is considered inductive because it adopted the structure and controls of the Detect function from the CSF (NIST, 2018). As the main concern of decision-makers is the processes for detecting cybersecurity incidents, the subcategories of the Detect function from the CSF were used. The second phase has a deductive character due to the paired judgments of each control concerning a criterion using Saaty's scale (Saaty, 1980). Finally, the phase of evaluating the cybersecurity controls presented itself inductively as it was based on the priority list of controls generated by AHP (Saaty, 1980).

In this paper, the structure of the Detect function from the CSF was used so that it could later be judged by decision-makers. As a result, a prioritized list of cybersecurity controls was generated, assisting in the creation of a cybersecurity risk assessment plan that complies with all risk management principles.

As the final priorities of the alternatives demonstrate a strong dependence on the weights assigned to the main criteria, small variations in the relative weights can result in significant changes in the final ranking, given that these weights are often derived from subjective judgments (Chang et al., 2007). Thus, it was essential to test the robustness of the priority list and the choices of experts by performing a sensitivity analysis against different weight assignments to the categories.

4 RESULTS

In this section, the results obtained through the evaluation of the cybersecurity controls contained in the CSF using AHP will be described. First, three research participants were selected, who are the decision-makers. These individuals hold representative positions in their respective areas within the organization, whose roles can be cited as shown in Table 2 :

The selection of a diverse profile among the judges was intentional, addressing human and cultural factors, integration, and inclusion, principles addressed by risk management. These specialists were chosen because they hold power and influence in the company's decision-making process.

Next, the controls from the Detect function of the CSF were selected, which, as required by the AHP application, already has a predefined tree structure. This structure is important because it addresses the principles of a comprehensive, customized, and dynamic framework outlined in the risk management process contained in ISO 31.000. In Figure 2, the structure is characterized such that the first level represents the main node, which is the Detect function of the CSF. The second level contains the categories that will be evaluated by AHP. The third level consists of the actual cybersecurity controls, which will be evaluated, prioritized, and where decision-makers or specialists should focus their efforts to implement risk mitigation solutions.

In the next phase, a brainstorming session was conducted with the specialists where the cybersecurity controls of the CSF were evaluated. For the evaluation, the Saaty scale, proposed by the method itself, was used. During this evaluation, each category/subcategory was subjected to a pairwise comparison with another category/subcategory. The question asked for the evaluation was as follows: In terms of importance criteria, how much could subcategory X contribute to the institution compared to category Y?

Table 3 presents the evaluation performed by specialists using the Saaty scale for the categories of the Detect function. For example, the category DE.CM - Security Continuous Monitoring received a score of 5, indicating strong importance compared to DE.AE - Anomalies and Events, predominantly shown in red. Scores of 1, in black, indicate categories considered "Equal" by specialists. The consistency index was 5%, below the 10% recommended by the method.

Table 2: Demographics Information of the Participants.

ID	Age group (in years old)	Highest Degree	Experience (in years)	Current Occupation	Team Size (people number)
P1	41-50	Postgraduate	15-20	Senior IT Development Analyst	<= 10
P2	31-40	Postgraduate	8-15	Senior IT Infrastructure Analyst	<= 10
P3	31-40	Postgraduate	8-15	IT Integration Manager	<= 10

Table 3: Judgment of the Categories of the Detect Function.

Controls	DE.AE	DE.CM	DE.DP
DE.AE	X	5	2
DE.CM	X	X	5
DE.DP	X	X	X

The results of the judgment of the categories, with DE.CM receiving 71%, DE.AE 18%, and DE.DP 11%, indicate that DE.CM (Security Continuous Monitoring) was considered the most critical priority for detecting cybersecurity threats. This focus on continuous monitoring reflects the importance of quickly detecting anomalous behaviors and malicious activities, ensuring a swift response to threats.

The DE.AE (Anomalies and Events) category, with a lower weight, is still relevant, highlighting the need to detect and respond to cybersecurity events. Meanwhile, DE.DP (Detection Processes), with 11%, although less prioritized, suggests that detection processes are in place and considered important but less critical than continuous monitoring and anomaly detection. When comparing the results obtained in this study with (Moreira et al., 2021) paper a similarity in findings is observed.

The Figure 3 illustrates the results of the experts evaluation of the categories using the AHP method.

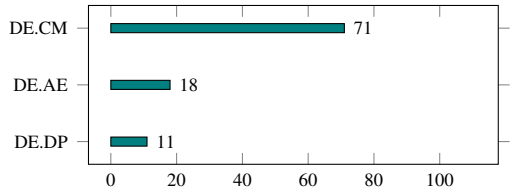

Figure 3: Detection - Categories.

Table 4 shows the evaluation performed by the specialists regarding the controls of Category 1: Anomalies and Incidents. The evaluation achieved a consistency index of 7.38%, which remained below the 10% threshold as indicated by Saaty.

Table 4: Table showing the judgment of specialists regarding the Anomalies and Events Subcategory (DE.AE).

Subcategories	DE.AE-1	DE.AE-2	DE.AE-3	DE.AE-4	DE.AE-5
DE.AE-1	X	1	2	2	3
DE.AE-2	X	X	1	4	7
DE.AE-3	X	X	X	2	5
DE.AE-4	X	X	X	X	4
DE.AE-5	X	X	X	X	X

The results presented under the Anomalies and Events criterion highlight DE.AE-2 as the highest priority, with 34 points, followed by DE.AE-3 with 28 points, DE.AE-4 with 17 points, DE.AE-1 with 16 points, and DE.AE-5 with 5 points. These values demonstrate a clear emphasis on the detection of anomalous behaviors and critical incidents.

These results suggest that proactive anomaly detection and event correlation are essential components of the organization's cybersecurity strategy, as shown in the Figure 4.

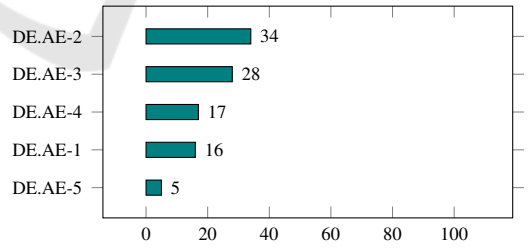

Figure 4: DE.AE - Anomalies and Events - Subcategories.

When comparing the results obtained in this study with those of other papers, a similarity in findings is observed. (Moreira et al., 2021) study presents the following order for the categories: DE.AE-2, DE.AE-1, DE.AE-3, DE.AE-4, and DE.AE-5. The common result highlights the concern for the DE.AE-2 subcategory, reinforcing the necessity and priority of detecting events to understand attack methods. However, it is evident that the DE.AE-5 subcategory is not considered significant by managers.

Table 5: Table containing the experts' evaluation regarding the Subcategory of Security Continuous Monitoring (DE.CM).

Controles	DE.CM-1	DE.CM-2	DE.CM-3	DE.CM-4	DE.CM-5	DE.CM-6	DE.CM-7	DE.CM-8
DE.CM-1	X	5	2	3	3	3	5	1
DE.CM-2	X	X	3	5	5	2	2	6
DE.CM-3	X	X	X	4	4	1	1	5
DE.CM-4	X	X	X	X	1	5	5	1
DE.CM-5	X	X	X	X	X	5	5	1
DE.CM-6	X	X	X	X	X	X	1	5
DE.CM-7	X	X	X	X	X	X	X	5
DE.CM-8	X	X	X	X	X	X	X	X

Regarding the evaluation of the other subcategories, differences are observed in the obtained priority order and their relative importance. These differences can be attributed to variations in judgments during the application process and the application protocols of MCDA-C compared to AHP. In MCDA-C, weights are determined through percentages agreed upon during a brainstorming session with decision-makers (Moreira et al., 2021), while in AHP, weights are derived using the Saaty scale, which, after application, generates percentage weights while ensuring a consistency index for the judgments (Saaty, 1980). Regarding the subcategories of the DE.CM - Security Continuous Monitoring category, the specialists performed the evaluation, as shown in Table 5. The evaluation achieved a consistency index of 2.738%, also below the 10% threshold as indicated by the method.

The evaluation result of the DE.CM - Security Continuous Monitoring category highlighted the subcategories DE.CM-4: Malicious code is detected and DE.CM-5: Unauthorized mobile code is detected as the most important and critical within this category. Figure 5 illustrates this scenario.

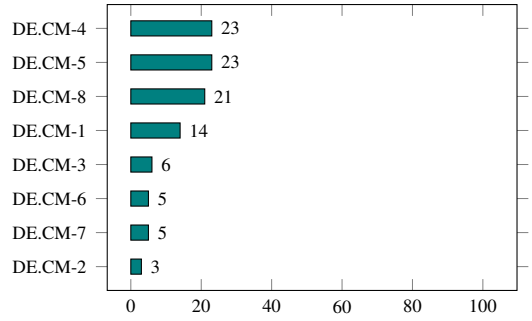

Figure 5: DE.CM - Security Continuous Monitoring - Subcategories.

When comparing the results obtained with those of other studies, a strong similarity is observed. (Moreira et al., 2021) presents the following priority order for the subcategories: DE.CM-5, DE.CM-4, DE.CM-8, DE.CM-1, DE.CM-3, DE.CM-6, DE.CM-7, and DE.CM-2. This order is almost identical to the results obtained in this paper, as there was a tie in priorities between DE.CM-5 and DE.CM-4. This indicates the concern of managers regarding the detection of malicious mobile code that can compromise an organization's outcomes.

In this scenario, it is possible to observe that in the category with the highest weight, the order of importance of the controls remained unchanged, unlike what occurred in the previous category. This indicates that, despite different methods of application, the results were consistent.

Table 6 illustrates the evaluation performed regarding the controls of the DE.DP - Detection Processes category. The evaluation achieved a consistency index of 3.096%, also below 10%.

Table 6: Table containing the experts' judgment regarding the Detection Processes Subcategory (DE.DP).

Controls	DE.DP-1	DE.DP-2	DE.DP-3	DE.DP-4	DE.DP-5
DE.DP-1	X	4	5	2	6
DE.DP-2	X	X	1	3	2
DE.DP-3	X	X	X	5	1
DE.DP-4	X	X	X	X	3
DE.DP-5	X	X	X	X	X

The judgments of the controls in the DE.DP - Detection Processes category highlighted DE.DP-1: DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability is communicated as the most important control in this category. Figure 6 shows this scenario.

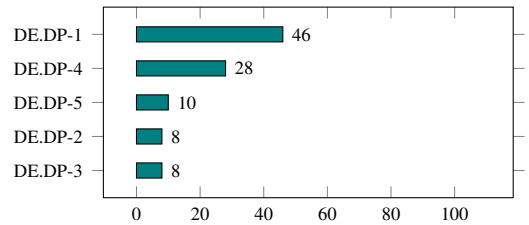

Figure 6: DE.DP - Detection Processes - Subcategories.

When comparing the evaluation of this study with other works on the DE.DP category, both similarities

and differences are observed. (Moreira et al., 2021) presents the following order of priorities: DE.DP-1, DE.DP-2, DE.DP-4, DE.DP-5, DE.DP-3.

This demonstrates that both the most prioritized subcategory, DE.DP-1, and the least important, DE.DP-3, held similar positions. However, the remaining subcategories appeared in different orders. This same phenomenon was also observed in the evaluation of the DE.AE category.

After completing all alternative evaluations by the experts, the global result was obtained through the AHP calculation, reflecting the prioritization of subcategories based on the assigned weights and evaluated criteria. This result was then analyzed in detail, enabling the identification of the most relevant subcategories within the Detect function of the CSF. The global analysis, calculated using the AHP method, consolidated the decisions made during the prioritization process, highlighting the critical controls that should be implemented to strengthen the organization's cybersecurity.

The global scale result provided a list prioritizing the cybersecurity controls for the organization. The list indicates which controls should be prioritized. Highlighted are controls DE.CM-4: Malicious code is detected and DE.CM-5: Unauthorized mobile code is detected. This suggests that the ability to detect threats involving malicious code and unauthorized mobile code is a critical priority for ensuring the early identification of potential attacks. This emphasis is crucial, as failures in these areas may compromise system security, allowing attacks to occur without timely detection.

Subsequently, the DE.CM-8 subcategory, "Vulnerability scans are performed," achieved a score of 15%. This result highlights that the detection of known vulnerabilities and potential system flaws is considered a critical area. The prioritization of actions aimed at conducting vulnerability scans underscores the importance of identifying and mitigating weaknesses before they can be exploited, reinforcing a proactive approach to cybersecurity.

Specifically for the categories DE.CM-1 (10%) and DE.AE-2 (6%), which ranked fourth and fifth respectively, provide important insights into their relative priorities in the context of threat detection. The 10% weight of DE.CM-1 indicates that continuous network monitoring to detect cybersecurity events is highly relevant, though not the top priority. This suggests that while network monitoring is crucial for identifying incidents, other controls, such as malicious code and vulnerability detection, are considered more critical for providing immediate defense against specific threats.

Conversely, the fifth position of DE.AE-2, accounting for 6%, highlights the importance of analyzing detected events not only to understand their potential impacts but also to identify the specific targets and methods employed in the attack. Such in-depth analysis is essential for the development of effective response and mitigation strategies. However, despite its critical role, this aspect is assigned a comparatively lower priority within the broader detection framework, relative to other mechanisms.

These rankings highlight that organizations may focus more on direct defensive actions against known or high-risk threats, while practices like network monitoring and behavioral analysis provide crucial support but are not the frontline of defense.

Among the controls with intermediate scores, DE.DP-1 (5%) and DE.AE-3 (5%) stand out. The control DE.DP-1, which addresses the definition of roles and responsibilities to ensure accountability in detection, indicates that the organization considers it essential to clearly establish responsibilities, although this is not a primary focus of action.

Similarly, DE.AE-3, related to the collection and correlation of event data from multiple sources and sensors, also scored 5%, reflecting the importance of consolidating information for security event analysis. Both controls are crucial for effective incident management, but their intermediate score suggests that the organization has prioritized other, more critical areas, such as the detection of malicious code.

Controls with slightly lower scores, such as DE.CM-3 (4%), DE.CM-6 (3%), DE.CM-7 (3%), DE.DP-4 (3%), DE.AE-4 (3%), and DE.AE-1 (3%), also represent relevant areas. DE.CM-3, which involves monitoring personnel activity, and DE.CM-6, which concerns monitoring external service providers' activity, indicate that the organization acknowledges the importance of overseeing human and third-party activities, though these areas received lower priority.

The control DE.CM-7, which relates to monitoring unauthorized connections, devices, and software, along with DE.AE-4, which determines the impact of events, were also rated at 3%. This reflects that while these activities are recognized, the organization may be focusing on actions more directly related to threat detection, such as those concerning malicious code and vulnerabilities. Figure 7 illustrates the prioritization of controls and provides a visual representation of the scenario previously described.

Sensitivity analysis is essential for verifying the robustness of the results obtained after applying the AHP method, ensuring that security control decisions are consistent and reliable. After obtaining the results,

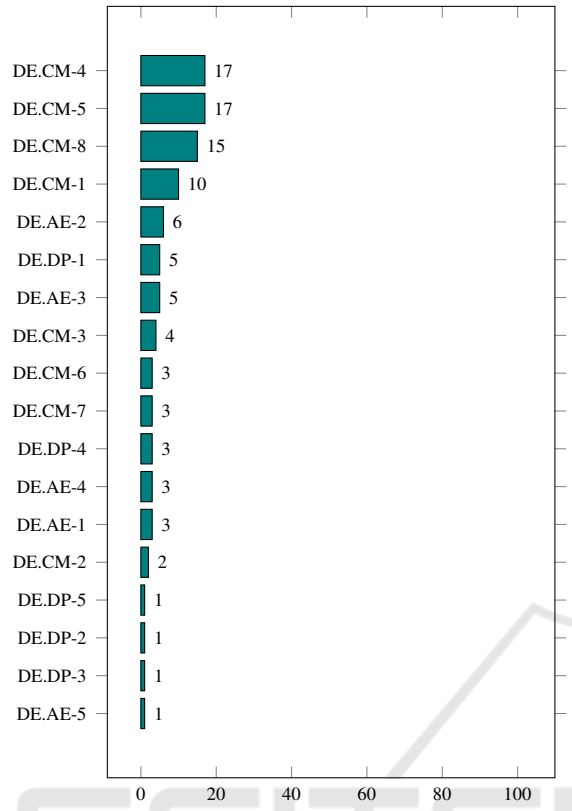

Figure 7: Scores obtained and preference order calculated by AHP at the global level of the subcategories within the Detect function of the NIST CSF, based on the previous weights and judgments provided by the decision-makers.

the researchers conducted a sensitivity analysis to assess how variations in the weightings of criteria could affect the prioritization of controls. This procedure is critical for identifying whether small changes in decision-makers' preferences could cause significant impacts on the order of control prioritization, which would indicate an excessive sensitivity in the model.

Figure 8 shows that the DE.CM subcategories begin to lose relevance when their weight is reduced to 50% of the total "Detect" function. For the DE.AE subcategories to become predominantly prioritized, their weight would need to reach 84%, as indicated by the dashed line in Figure. This contrasts with the 18% obtained in the assessment, demonstrating the consistency and reliability of the weights assigned by the experts. This result highlights the robustness of the analysis and the confidence in the decisions made during the prioritization process.

Figure 9 performs the sensitivity analysis of the weight of DE.CM - Security Continuous Monitoring against DE.DP - Detection Processes. The analysis shows a similar scenario, with a sharp decline in the DE.CM subcategories when the weight reaches

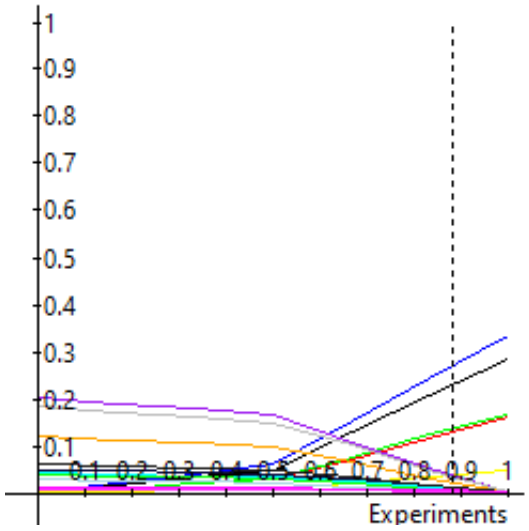

Figure 8: Sensitivity Analysis of the Subcategories of DE.AE - Anomalies and Events.

around 50%. For the DE.DP categories to gain prominence, their weight would need to reach around 88%, as indicated by the dashed line, compared to the 11% obtained. These values also demonstrate the certainty of the specialists' choices, as the weight would need to increase significantly for the subcategories to gain prominence.

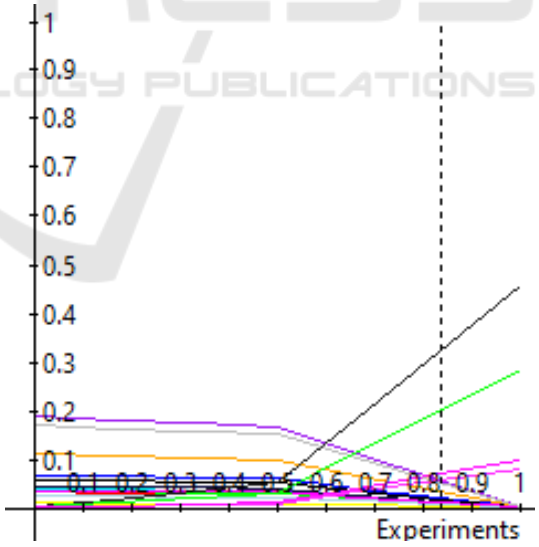

Figure 9: Sensitivity Analysis of the Subcategories of DE.DP - Detection Processes.

The sensitivity analyses of DE.CM against the other two categories, DE.AE and DE.DP, confirm the robustness and certainty of the experts' choices. Both analyses show a clear and consistent pattern, with DE.CM subcategories losing relevance only when their weight is significantly reduced, while DE.AE

and DE.DP would need a substantial increase in their weights—84% and 88%, respectively—to gain prominence. This demonstrates that the data and evaluations were consistent, providing a solid foundation for the prioritization process and reinforcing the reliability of the experts' judgments in the decision-making process.

All stages of the AHP methodology were successfully completed, from defining the problem and structuring the hierarchy of criteria to conducting the pairwise comparisons and synthesizing the results. The successful execution of each phase, supported by consistent and robust outcomes from the sensitivity analyses, confirms that the AHP approach was effectively implemented. This ensures a reliable framework for prioritizing cybersecurity controls, providing valuable guidance for decision-making in the management of cybersecurity risks.

The prioritized list of controls for the "Protect" function of the NIST Cybersecurity Framework, previously applied using the AHP method, adheres to the principle of Best Available Information in risk management. By employing AHP, the decisions regarding control prioritization are based on a thorough and systematic analysis of the most relevant and up-to-date information available concerning the organization's security environment.

It is essential to regularly perform the AHP application procedure to ensure effective management of cybersecurity risks and maintain adherence to the principle of Continuous Improvement. Cybersecurity threats, both internal and external, are constantly evolving, requiring ongoing adjustments to defense strategies. By periodically reapplying AHP, the organization can reassess and update its control priorities, ensuring they remain aligned with the current threat landscape. This process enables a swift and efficient response to emerging risks, optimizes resource allocation, and strengthens the organization's cybersecurity resilience in the face of evolving security challenges.

Through the information gathered and the created list, a new principle of risk management was also addressed, which is the principle of the best available information. It is important to emphasize that, for another principle to be addressed—the principle of Continuous Improvement—this process must always be repeated as the internal and external factors of the organization influence the company's objectives.

5 CONCLUSIONS

The proposed model effectively developed a risk assessment based on the cybersecurity controls outlined in the CSF. By applying the AHP method, a prioritized list was generated based on expert judgment, with the goal of supporting public managers in their decision-making processes. This list is crucial in determining the order in which cybersecurity controls should be implemented, optimizing resource allocation and ensuring that critical risks are addressed first.

The simulation using the AHP method revealed that the five most critical CSF subcategories for the organization are those related to the detection and monitoring of malicious codes and vulnerabilities. This highlights the major concerns of both experts and managers, indicating a clear focus on proactive threat detection and vulnerability management. These results demonstrate the alignment of the experts' priorities with the current cybersecurity landscape, where early threat detection and mitigation are essential for organizational resilience.

Moreover, the AHP method proved to be a powerful decision-making tool, allowing managers to confidently allocate resources and prioritize cybersecurity actions based on a structured, data-driven approach. The ability of AHP to reduce biases and provide a consistent framework for evaluating expert judgments reinforces its value in ensuring that decisions are made transparently and systematically. The application of AHP, as recommended by ISO 31000, adhered to the eight principles of risk management—ensuring a balanced, thorough, and reliable risk assessment process. These principles include context establishment, structured decision-making, stakeholder engagement, and continuous improvement, all of which were successfully addressed by the AHP model.

Additionally, AHP demonstrated that it is particularly valuable for public sector information security managers in Brazil. In conjunction with other security frameworks, such as PPSI, AHP can assist public administrators in prioritizing cybersecurity controls that are most relevant to their specific context. This capability makes AHP a versatile tool that can be tailored to fit various risk management frameworks, providing a strong foundation for effective cybersecurity risk management in government institutions. Thus, the continuous use of this approach can contribute to the development of more robust and dynamic security policies, capable of keeping up with the rapid changes in the technological and threat landscape. In this way, AHP can establish itself as an essential tool for the efficient management of cybersecurity risks in the public sector.

ACKNOWLEDGMENTS

The authors would like to thank the technical and computational support provided by the LATITUDE Laboratory of the University of Brasília, TED 01/2021 of the National Secretariat for Social Assistance – SNAS/DGSUAS/CGRS, TED 01/2021 of the General Coordination of Information Technology (CGTI) of the Attorney General's Office of the National Treasury – PGFN, the SISTER City Project – Secure and Real-Time Intelligent Systems for Smart Cities (Grant 625/2022), the Project Control and Unification System of Projects for the Federal District Government – Sispro-DF (Grant 497/2023), the Project Research, Development and Application – Methodology to Support the Elicitation of Ethical and Privacy Requirements (Grant 514/2023), the Dean's Office of Research and Innovation – DPI/UnB and FAP/DF.

REFERENCES

Alves, R. S., Georg, M. A. C., and Nunes, R. R. (2023). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E56):344–357.

Bitton, R., Maman, N., Elovici, Y., Shabtai, A., Singh, I., and Momiyama, S. (2021). Evaluating the cybersecurity risk of real-world, machine learning production systems. *ACM Computing Surveys (CSUR)*.

BRASIL (2023). PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023. Brazilian legislation.

Brigido, W. J. H., Miranda, J. P. C. T. D., and Monteiro, S. B. S. (2022). Risk-based resource allocation applying ahp-topsis. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6.

Canedo, E. D., do Vale, A. P. M., Gravina, R. M., Patrão, R. L., de Souza, L. C., dos Reis, V. E., de Mendonça, F. L. L., and de Sousa Jr., R. T. (2021). An applied risk identification approach in the ICT governance and management macroprocesses of a brazilian federal government agency. In Filipe, J., Smialek, M., Brodsky, A., and Hammoudi, S., editors, *Proceedings of the 23rd International Conference on Enterprise Information Systems, ICEIS 2021, Online Streaming, April 26-28, 2021, Volume 1*, pages 272–279, https://doi.org/10.5220/0010475902720279. SCITEPRESS.

Chang, C.-W., Wu, C.-R., Lin, C.-T., and Chen, H.-C. (2007). An application of ahp and sensitivity analysis for selecting the best slicing machine. *Computers & Industrial Engineering*, 52(2):296–307.

CNN Brasil (2023). Ataques hackers aumentam 88% no brasil, e país segue como 2º mais atacado do mundo. Accessed: August 17, 2024.

Creative Decision Foundation (2012). Super decision software for decision making. [Online]. Available: http://www.superdecisions.com.

Divino, S. B. S. and Campos, B. (2024). Comunicação de incidentes de segurança na lei geral de proteção de dados: A definição do prazo mediante análise de impacto regulatório como instrumento indispensável ao enforcement da autoridade nacional de proteção de dados. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)*, 12(1):84–104.

ISO/IEC (2018). ISO/IEC 31000:2018: Risk management — Guidelines.

ISO/IEC (2019). ISO 31010:2019 - Risk Management — Risk Assessment Techniques. Available at https://www.iso.org/standard/72140.html.

ISO/IEC (2022). Information Security, Cybersecurity and Privacy Protection (ISO/IEC 27002:2022).

Moreira, F. R., Filho, D. A. D. S., Nze, G. D. A., de Sousa Júnior, R. T., and Nunes, R. R. (2021). Evaluating the performance of nist's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access*, 9:129605–129618.

NIST (2018). Cybersecurity Framework V1.1 - Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Technical report, National Institute of Standards and Technology, Gaithersburg, MD, USA.

Ru, Y. et al. (2016). Risk assessment of cyber attacks in ecps based on attack tree and ahp. In *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, pages 465–470.

Saaty, T. L. (1980). *The Analytic Hierarchy Process*. McGraw-Hill, New York, NY, USA.

Siregar, I. M., Putri, L. W. B., and Sugihartono, T. (2024). Sensitivity analysis of various ahp process: A case study on consumption fish farming. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, 13(2):216–223.