INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

ASSESSING AND STRENGTHENING CYBERSECURITY MATURITY

A NIST-based index approach

Luís António Bernardo

Escola Superior de Tecnologia e Gestão

ESTG

2024 ASSESSING AND STRENGTHENING CYBERSECURITY MATURITY

Instituto Politécnico
de Viana do Castelo

Assessing and Strengthening Cybersecurity Maturity: A NIST-Based Index Approach

Autor

Luis Antonio Bernardo

Trabalho orientado por

Prof. João Paulo Magalhães and Prof. Silvestre Malta

Mestrado em Cibersegurança

07 de fevereiro de 2024

Mestrado em Cibersegurança
Master in Cybersecurity

Assessing and Strengthening Cybersecurity Maturity: A NIST-Based Index Approach

a master's thesis authored by

Luis Antonio Bernardo

and supervised by

João Paulo Magalhães

Professor Adjunto, Instituto Politécnico do Porto

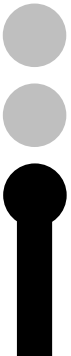
Silvestre Lomba Malta

Professor Assistente, IPVC

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

7 of February, 2024



Abstract

This master thesis focuses on the importance of the implementation of cybersecurity reinforcement measures and the evaluation of cybersecurity maturity within organizations. With the continuous evolution of cybersecurity threats, organizations face significant challenges in protecting their data and systems. The COVID-19 pandemic and the rise of remote work have further increased risks, making cybersecurity an even more essential aspect for organizations. The objective of this research is to evaluate and contribute to the growth of cybersecurity maturity in organizations, by adopting NIST Cybersecurity Framework (NIST CSF) as an auxiliary tool. This framework provides a comprehensive structure to manage cybersecurity risks and is widely adopted by organizations due to its flexibility and ease of implementation. The methodological approach of this research is based on the development of customized questionnaires aimed at different audiences, including cybersecurity experts and employees at different hierarchical levels in organizations. The objective of this method is to identify the level of cybersecurity maturity, providing a comprehensive analysis. The responses obtained from these questionnaires are analyzed to calculate a cybersecurity maturity index, which reflects the current state of the organization's cybersecurity practices. The findings of this research highlight the importance of prevention in cybersecurity as a fundamental approach to protect organizations against cyber threats. By identifying areas for improvement and implementing effective prevention strategies, organizations can improve their cybersecurity posture and mitigate risks. The research also emphasizes the importance of complying with data protection regulations, such as the General Data Protection Regulation (GDPR), to ensure the privacy and security of personal data. Overall, this research contributes to the advancement of knowledge and practices in cybersecurity by providing valuable information on cybersecurity maturity and the importance of prevention. By adopting preventive measures

and promoting a culture of cybersecurity awareness, organizations can strengthen their security defenses and safeguard their digital assets.

Keywords: Cybersecurity. COVID-19. Home Office. NIST CSF. Maturity. Cyber Security Maturity, Maturity Index, Cyber Resilience, Cyber Security Risk, Cyber Security Framework, Cyber Risk Quantification.

Resumo

Esta tese de mestrado concentra-se na importância da implementação de medidas de reforço e na avaliação da maturidade em cibersegurança dentro das organizações. Com a evolução contínua das ameaças em cibersegurança, as organizações enfrentam desafios significativos na proteção de seus dados e sistemas. A pandemia de COVID-19 e o aumento do trabalho remoto aumentaram ainda mais os riscos, tornando a cibersegurança um aspecto ainda mais essencial para as organizações. O objetivo desta pesquisa é avaliar e contribuir para o crescimento da maturidade em cibersegurança nas organizações, adotando o NIST CSF como ferramenta auxiliar. Este framework oferece uma estrutura abrangente para gerenciar os riscos em cibersegurança e é amplamente adotado pelas organizações devido à sua flexibilidade e facilidade de implementação. A abordagem metodológica desta pesquisa é baseada no desenvolvimento de questionários personalizados destinados a diferentes públicos, incluindo especialistas em cibersegurança e funcionários em diferentes níveis hierárquicos nas organizações. O objetivo deste método é identificar o nível de maturidade em cibersegurança, proporcionando uma análise abrangente. As respostas obtidas desses questionários são analisadas para calcular um índice de maturidade em cibersegurança, que reflete o estado atual das práticas de cibersegurança da organização. Os resultados desta pesquisa destacam a importância da prevenção em cibersegurança como uma abordagem fundamental para proteger as organizações contra ameaças cibernéticas. Ao identificar áreas para aprimoramento e implementar estratégias eficazes de prevenção, as organizações podem melhorar sua postura em cibersegurança e mitigar riscos. A pesquisa também enfatiza a importância da conformidade com regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR), para garantir a privacidade e segurança de dados pessoais. No geral, esta pesquisa contribui para o avanço do conhecimento e práticas em cibersegurança, fornecendo informações valiosas sobre matu-

ridade em cibersegurança e a importância da prevenção. Ao adotar medidas preventivas e promover uma cultura de conscientização em cibersegurança, as organizações podem fortalecer suas defesas de segurança e proteger seus ativos digitais.

Palavras-chave: Cibersegurança. COVID-19. Trabalho Remoto. NIST CSF. Maturidade. Maturidade em Cibersegurança, Índice de Maturidade, Resiliência Cibernética, Risco em Cibersegurança, Estrutura de Cibersegurança, Quantificação de Risco Cibernético.

Aknowledgements

The present master's dissertation has successfully reached its destination with the invaluable support of various individuals.

First and foremost, I extend my profound gratitude to my advisors, Professor João Paulo Magalhães and Professor Silvestre Malta, for their remarkable patience, dedicated commitment, and practical guidance throughout this work. I sincerely thank them for correcting and guiding me when necessary, never failing to inspire and motivate.

I would also like to express my thanks to all my colleagues in the Master's in Cybersecurity program, whose collaboration and exchange of ideas significantly enriched this academic journey.

A special acknowledgment goes to the staff at the Polytechnic Institute of Viana do Castelo, whose constant attention and availability contributed to an environment conducive to the development of this work.

Finally, I cannot overlook expressing my deep gratitude to my parents and my wife, Carla Adriana Dias Lucas, for their unwavering support throughout the elaboration of this work. Their words of encouragement and understanding were instrumental in overcoming challenges and achieving this academic milestone.

Contents

List of Figures

List of Tables

List of Abbreviations

B-ON Biblioteca do Conhecimento Online

BYOD Bring your own device

CIS Center for Internet Security

CLS Capability Levels

COBIT Control Objectives for Information and Related Technologies

COVID-19 Corona Virus Disease

CTI Cyber Trust Index

DPO Data Protection Officer

ESTG Escola Superior de Tecnologia e Gestão

GDPR General Data Protection Regulation

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IPVC Instituto Politécnico de Viana do Castelo

ISO International Organization for Standardization

IT Information Technology

MCyber Master in Cybersecurity

NIST CSF Cybersecurity Framework

NIST CSF NIST Cybersecurity Framework

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analysis

RGPD Regulamento Geral sobre a Proteção de Dados

VPN Virtual Private Network

WN Wireless Network

Chapter 1

Introduction

This chapter presents the context of this work in relation to the cybersecurity maturity present in companies. Section 1.1 describes how cybersecurity threats have intensified in the wake of COVID-19. Section 1.2 describes the importance of adopting frameworks that help maintain cybersecurity. Section 1.3 presents the objectives of this project. Section 1.4 describes how the help of experts in the field of cybersecurity can help in creating a new cybersecurity analysis tool. Finally, Section 1.5 presents the organization and chapters of this master thesis.

1.1 Context

Cybersecurity threats are continuously evolving and becoming increasingly complex and worrisome, posing a significant challenge to organizations around the world. Through data breaches, cyberattacks, and other ongoing malicious activities, it is essential that organizations adopt tools to improve cybersecurity in general.

The COVID-19 pandemic has made cybersecurity even more essential in organizations, accelerating a digital transformation process. Another contributing factor is the fact that remote work has become relevant and organizations have been forced to allow this new way of working, which further increases risks. These factors have led to significant increases in the number of cyberattacks that cybercriminals are exploiting that use the vulnerabilities left behind to break into systems and cause often irreparable damage.

There are various types of cyberattack that have various consequences and can be

severe. From financial losses and damage to the companies reputation, but also to legal liabilities, making the business unviable and permanently closing the business. Due to this, cybersecurity has become a top priority for organizations, regardless of the industry in which they operate.

1.2 Problem Statement and Motivation

As the challenge of protecting the organization is great, several have adopted cybersecurity frameworks to ensure the integrity of their operations, as well as to minimize the risks currently generated by these cyber threats. The NIST Cybersecurity Framework (NIST CSF) cybersecurity framework is one of the most widely used by companies because it provides a flexible framework to manage cyber risks and is relatively easy to implement.

However, despite the availability of these resources to manage cyber risks and keep the company secure, not all companies are able to adopt measures that minimize risks, as this requires resources, awareness of the risks involved, or lack of commitment from people in leadership positions who could change the direction of the company on this issue.

Therefore, assessing the maturity level of an organization's cybersecurity practices is critical, identifying gaps and weaknesses in its framework that encompasses cybersecurity. Through this, organizations can develop efficient and effective strategies to improve their cybersecurity performance and mitigate cyber risks.

1.3 Objectives

The central purpose of this master thesis lies in evaluating and improving cybersecurity maturity within an organization, through the design of a framework that enables the precise measurement of cybersecurity maturity. This effort aims to identify areas that can be improved, identifying possible changes in attitudes and behaviors, with the ultimate purpose of promoting continuous advancement in cybersecurity management practices.

1.4 Contributions

To achieve this objective, NIST CSF will be used as an auxiliary tool, where two surveys have been created aimed at different audiences. First, a comprehensive survey has been carried out at various levels of the organization, using online questionnaires as the main data collection tool. Second, the input of cybersecurity experts has been sought to refine and validate the conclusions, ultimately culminating in the development of a new methodology to assess cybersecurity maturity. Based on a consideration of experts surveys, it was possible to develop a new framework, which indicates the level of cybersecurity maturity the company is at, offering valuable information, highlighting potential vulnerabilities that could be exploited by malicious actors. Furthermore, these findings can serve as a basis for companies to improve their cybersecurity capabilities through technical improvements, promoting the creation of robust and effective cybersecurity policies and practices.

1.5 Organization

The remainder of this document is organized as follows. Chapter 2 presents related work in the area. Chapter 3 presents the methodology used to prepare the reports, based on the NIST CSF framework, the importance of data analysis, and finally the use of Regulamento Geral sobre a Proteção de Dados (RGPD), specifically on data protection. Chapter 4 presents the system model, as well as the analysis of the results, and in Chapter 5 the conclusions are made.

Chapter 2

State of the art

In this chapter is presented a literature review methodology, a comprehensive literature framework analysis, and data analysis of related work.

2.1 Literature Review Methodology

To advance current knowledge and refine the approach to cybersecurity-related topics, PRISMA tool has been used. The PRISMA model, as in the Figure 2.1 is used to prepare systematic reviews in scientific research. Its usefulness lies in its ability to provide a solid framework for reviews, which, in turn, promotes transparency in the presentation of evidence-based results. Therefore, PRISMA not only improves the quality and credibility of reviews in scientific research, but also increases the reliability of findings, contributing to a more solid and informed analysis.

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA [8]) is a set of guidelines used by various researchers and entities that was developed in 2009 and refined over time to ensure transparency and traceability of the research in question.

The PRISMA statement consists of a 27-item checklist and a flow chart, which allows a systematic review to be created in a structured way. The extensive checklist includes several items, which are described in the following: title, abstract, introduction, methods, results, discussion, and financing of the study. For ease and to give us an overall picture of the research, there is the flow chart that identifies the number of studies identified, included and excluded at each stage of the review process.

The main objective in adopting the PRISMA guidelines is to ensure a linear and coherent method, thus creating a systematic review and ensuring that the most important information is considered and made available in a clear and objective manner. By using this methodology, authors generally provide detailed information on the methods and procedures used and the criteria used to exclude articles.

PRISMA aims to increase the transparency and reproducibility of reviews, but not only this, it considerably improves the quality of reports. Other researchers can use the information provided to reproduce the research conducted step by step and thus verify the results.

In general, the PRISMA methodology is an important tool for researchers using systematic reviews, ensuring that the studies conducted are accurate, transparent, and the results found can be effectively reproduced by other researchers.

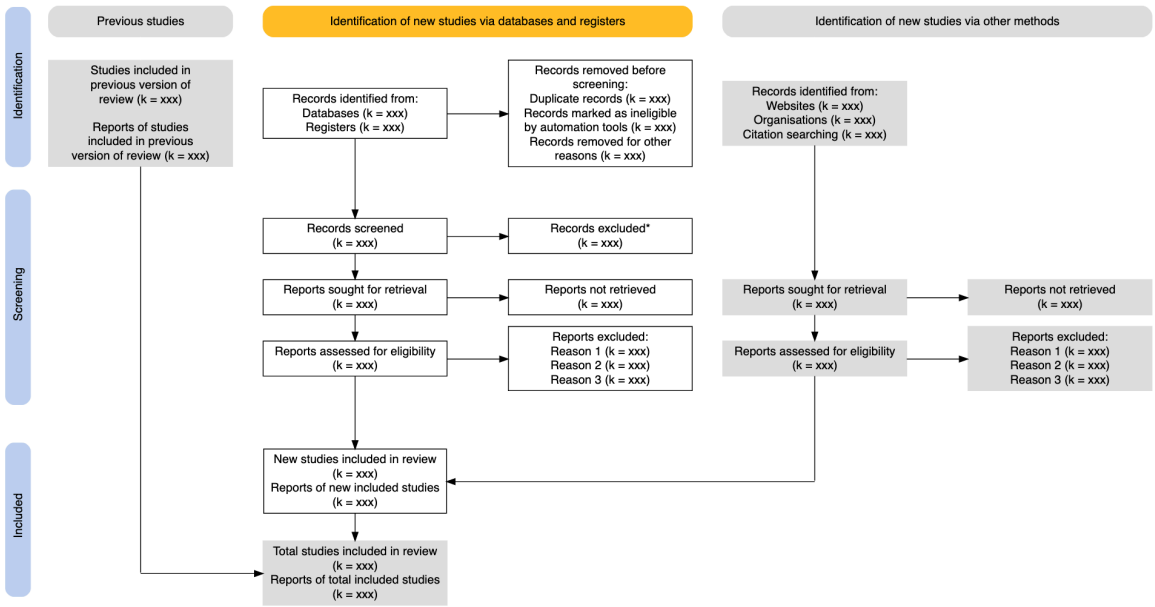


Figure 2.1: Prisma 2020

A detailed research was carried out to study the maturity of cybersecurity, and a total of 889 articles were identified, including 65 from Scopus [1], four from Institute of Electrical and Electronics Engineers (IEEE) [2], 730 from Biblioteca do Conhecimento Online (B-ON) [3]and 90 from Google Scholar [4]. In addition to these, three other individual research

[1] https://www.scopus.com/
[2] https://ieeexplore.ieee.org/
[3] https://www.b-on.pt/
[4] https://scholar.google.com/

articles were found on Google.

During the initial screening process, 703 articles were excluded. Among them, 19 were duplicates, 544 were not open access, and 140 had not been peer reviewed. This left us with 186 articles for the second screening.

In the second screening, another 178 articles were excluded. One of the articles was written in a language other than English or Portuguese. Of the remaining articles, 149 were excluded because they were not directly related to the topic of the master dissertation. In addition, four articles were excluded because they required the purchase of a book. As they did not correspond to the theme of the thesis, 24 articles were excluded after reading the abstract.

The primary purpose of the literature review is to identify instances in which the NIST CSF framework has been applied, either comprehensively or as a complementary tool to enhance cybersecurity maturity. The search for keywords, represented in Figures 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 to be used, was conducted using the VosViewer software, as indicated in table 2.1.

SEARCH	**FUNCTION**	**KEYWORDS**
1	General search	Cybersecurity, IOT, Security
2	Identify	Cybersecurity, cyberattack, security, risk assessment
3	Protect	Cybersecurity, iot, security, blockchain
4	Detect	Cybersecurity, machine learning, security, cyberattack, intrusion detection
5	Respond	Cybersecurity, iot
6	Recover	Cybersecurity, security operations, critical infrastructure, cyber resillience

Table 2.1: VosViewer Summary Table

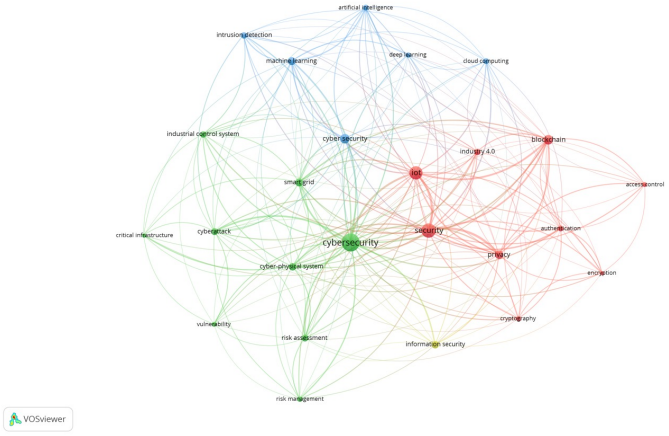


Figure 2.2: General Search

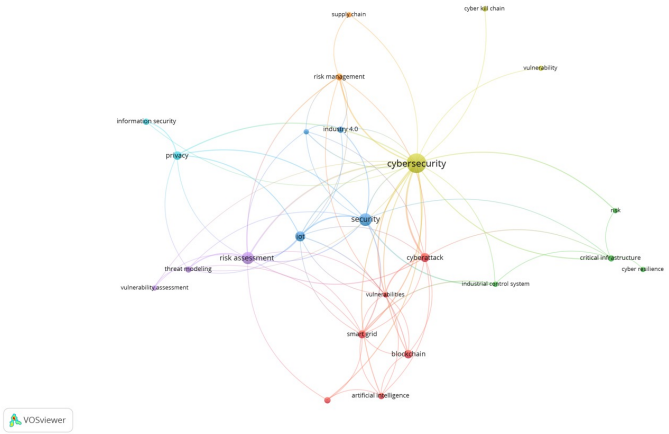


Figure 2.3: Identify

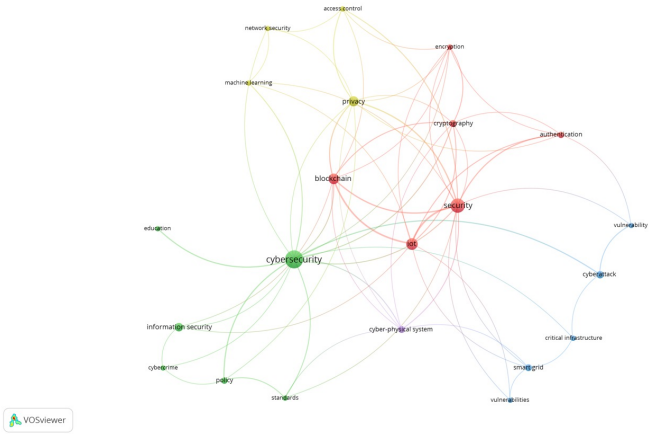


Figure 2.4: Protect

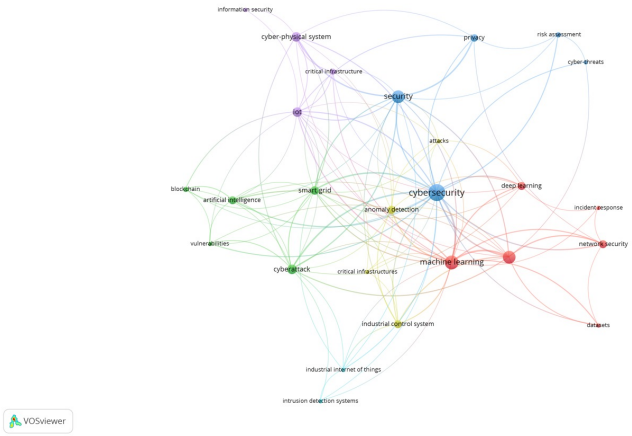


Figure 2.5: Detect

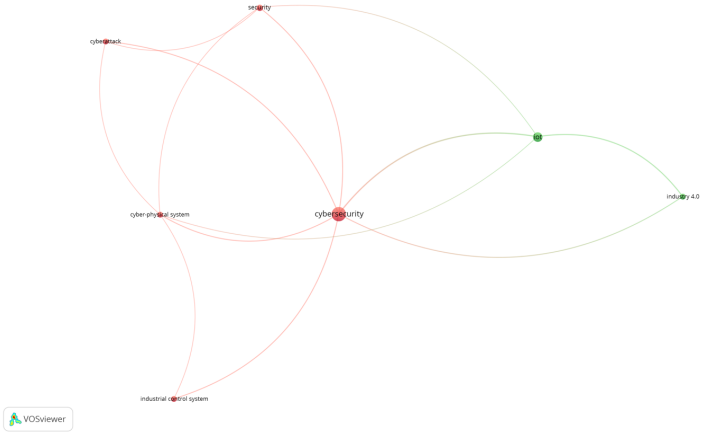


Figure 2.6: Respond

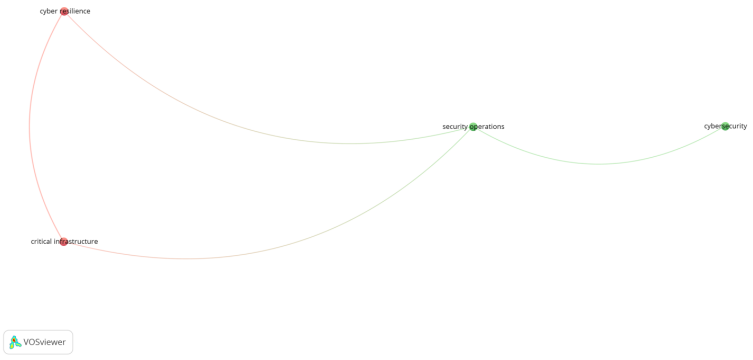


Figure 2.7: Recover

After the rigorous screening process, as shown in Figure 2.8, 11 articles remained

that would serve as the basis for the State of the Art in studying cybersecurity maturity. Using the preferred reporting item guidelines for systematic reviews and meta-analyses (PRISMA), we ensured that all relevant data were reported accurately and concisely. This approach increased the transparency and reproducibility of our research.

Through a criterion established by the PRISMA methodology, it was possible to select the most relevant articles that met the preestablished research conditions, making a reliable study for the proposed topic.

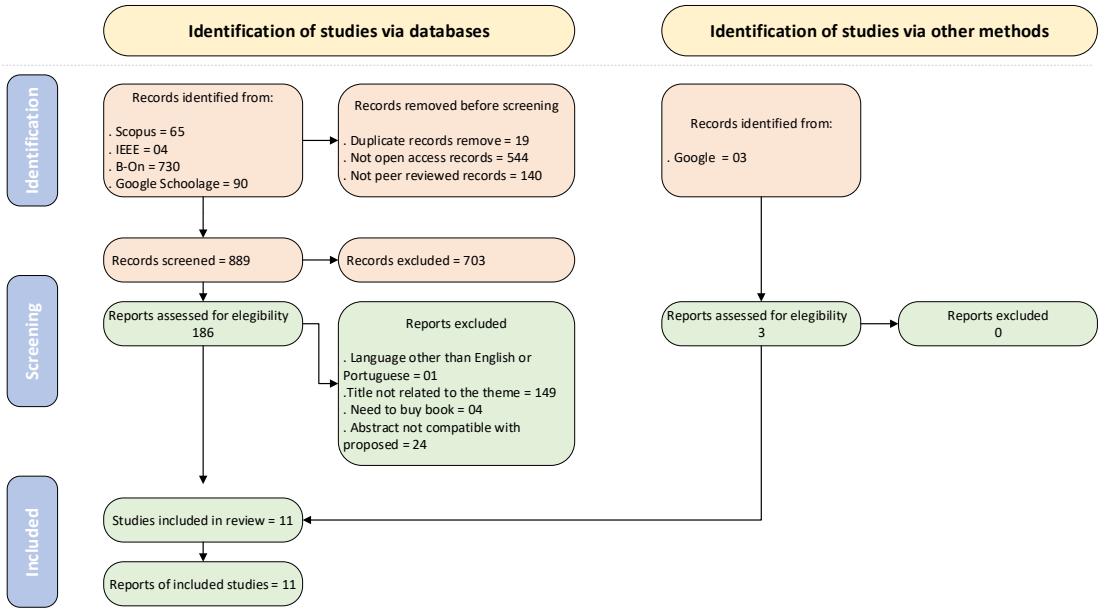


Figure 2.8: Prisma 2020 - Case

Through the literature review, it becomes clear that it is feasible to design a framework capable of playing a significant role in advancing cybersecurity maturity, providing a consistent contribution to this process.

2.2 Comprehensive Framework Analysis of the Literature

Today, cybersecurity is a fundamental part of personal, organizational, and national protection. Cybersecurity refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, use, disclosure, total or partial interruption, modification, or destruction. With the increasing number of cyber threats and attacks on individuals, organizations, and governments around the world, the importance

of efficient and powerful cybersecurity is highlighted. These threats can include different types of attacks, including phishing, malware, ransomware, data breaches, and denial-of-service attacks, among others.

An alternative to combating cyber threats are cybersecurity frameworks. Through these organized structures, they help in the organization and implementation of cyber best practices to later implement security best practices in the digital world, to later protect systems and networks against these same threats. There are several frameworks that work in this direction, the most popular being ISO/IEC 27001, NIST CSF Cybersecurity Framework, Center for Internet Security (CIS), and PCI DSS.

The NIST CSF is a US government agency responsible for developing and promoting cybersecurity and information security standards and guidelines. Among the various publications by NIST CSF, we can mention the Cybersecurity Framework, which provides a structure to improve the management of cybersecurity risks in different branches of activities. The NIST CSF Cybersecurity Framework is widely adopted and provides a common language and approach for organizations to manage and reduce cybersecurity risk. It is divided into five main functions: identify, protect, detect, respond, and recover. Using this framework by security-conscious companies can identify and prioritize cybersecurity risks and subsequently develop a strategy to manage those risks.

The authors of the article Understanding Cybersecurity Frameworks and Information Security Standards [11] define and aim to provide a broad overview of cybersecurity frameworks and information security standards in a world with increasing cyber threat. They thoroughly analyze some security structures and security standards, such as NIST CSF, International Organization for Standardization (ISO) and CIS, among others, in addition to comparing structures and standards, pointing out strengths and weaknesses. They came to the conclusion that, in the face of threats, there is no single solution for all organizations and that each should choose the structure or standard according to their needs, and this study can help decision making on which structure or standard to choose.

The authors of the article Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance [6] surveyed cybersecurity professionals and found that most organizations lack a formal security performance rating system, in addition to a lack of consistency in how security is measured. They used the results of this research to create a

prototype for a new framework, called Cyber Trust Index (CTI), which aims to assess and improve cybersecurity performance in organizations. They found that this new framework was effective in identifying gaps in security performance and providing actionable recommendations for improvement, providing a standardized ranking system and actionable recommendations, and could be used for benchmarking across different industries, but the Cyber Trust Index still needs further research and validation to determine its effectiveness and practicality.

The article Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS [10] analyzes and compares four widely used cybersecurity maturity assessment methodologies: the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF Cybersecurity Framework (NIST CSF)), Control Objectives for Information and Related Technology (Control Objectives for Information and Related Technologies (COBIT)), International Organization for Standardization/International Electrotechnical Commission 27002 (ISO/International Electrotechnical Commission (IEC) 27002), and Payment Card Industry Data Security Standard (PCI DSS). The study used a survey of cybersecurity experts to assess the strengths and weaknesses of each methodology and to determine which methodology was most suitable for specific types of organizations. Experts considered factors such as ease of use, level of detail, and effectiveness in identifying security risks. The results showed that NIST CSF NIST CSF was the most widely used and accepted methodology among experts. It was considered effective in identifying security risks and providing actionable recommendations. COBIT was also widely used, but was criticized for being too complex and difficult to use. ISO/IEC 27002 was seen as comprehensive but lacking practical guidance, while PCI DSS was considered useful for organizations handling payment card data but limited in its scope. In general, the study highlights the importance of selecting the appropriate cybersecurity maturity assessment methodology for the specific needs and requirements of each organization. It also underscores the need for ongoing evaluation and refinement of these methodologies to keep up with evolving cybersecurity threats and technologies.

The article What is the NIST Framework?[1] Framework for Improving Critical Infrastructure Cybersecurity was created to manage cybersecurity risks in a flexible way

according to the needs of organizations; it was first introduced in 2014. It aims to Identify, Protect, Detect, Respond, and Recover with a detailed approach to cybersecurity risk management, as well as providing guidance on how to implement the framework and measure your progress in a personalized way, according to your risks and needs. Further research demonstrated that companies that implemented this framework had high rates of improvement in risk management and best practices to promote cybersecurity.

Through machine learning techniques, the article NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements [12] verifies a generic model for assessing compliance and predicting requirements to achieve compliance, according to the National Institute of Standards and Technology (NIST CSF) Cybersecurity Framework (NIST CSF). A study was carried out with cybersecurity professionals from various organizations asking about the implementation of NIST CSF, NIST CSF and these data were used to train and validate the model to predict the controls needed to achieve compliance in new organizations. In this study, it was demonstrated that the model is a useful tool to verify the necessary controls for compliance with the NIST CSF NIST CSF, in addition to observing that the Protect function was the most difficult and the Respond was the easiest to implement, and when using machine learning techniques , the model can be useful for accuracies based on data collected in similar organizations.

In the article Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles [2] the use of Capability Levels (CLS) is explored to improve the implementation of the National Institute of Standards and Technology (NIST CSF) NIST CSF. The authors propose the use of CLS as a method for organizations to measure their cybersecurity maturity date and align their cybersecurity efforts with their business objectives. They suggested that this approach helps organizations shoehorn their implementation of NIST CSF to their unusual necessity and improve their overall cybersecurity posture. The authors conducted a survey of organizations that have enforced the NIST CSF using CLs to quantify their cybersecurity maturity. The following results showed that organizations that used CLs reported an improved alignment between their cybersecurity efforts and business objectives, as well as improved undefined and collaboration between different departments within the organization. The survey results also showed that the

organizations using CLs had a better understanding of their cybersecurity risks and were better equipped to prioritize their cybersecurity efforts. Additionally, organizations that used CLs were more likely to have a formalized cybersecurity program in place, which included policies and procedures, grooming and sentience programs, and habitue put on the lineassessments. In general, the article suggests that the use of CLs can be an operational approach for organizations to improve their cybersecurity posture and coordinate their cybersecurity efforts with their business objectives. The survey results provide evidence that organizations that use CLs have a better understanding of their cybersecurity risks, are better equipped to prioritize their cybersecurity efforts, and have a more formalized cybersecurity program in place.

The work presented in the article Analysis and evaluation of academic information system security using NIST SP 800-26 framework [7], from a university in Malaysia, collected data through questionnaires and interviews with IT employees to analyze and evaluate the security of academic information systems using NIST CSF SP 800-26. It was found that in the security level of the systems, although well established, there were gaps in implementation. User awareness of security policies was lacking, there were deficiencies in the technical controls used to protect systems, outdated software and hardware, weak passwords, and insecure wireless networks, leading to moderate security. The study recommended improving security measures, implementing stronger technical controls, increasing user awareness, training and education programs, and regular audits and reviews to ensure the effectiveness of security measures. With this, the importance of adopting and maintaining cybersecurity measures for the protection of information was highlighted and the use of NIST CSF SP 800-26 framework provides an adequate approach to evaluate and improve this security, in addition to this study providing useful data for other similar institutions that evaluate their own security measures.

The purpose of the study Measuring the State of Indiana's Cybersecurity [5] was to assess the cybersecurity posture of state agencies in Indiana using the framework developed by the NIST CSF. In the Identify, Protect, Detect, Respond, and Recover functions, there were varying levels of cybersecurity, in addition to the fact that compared to larger agencies, security levels were lower, and it was recommended to the Indiana Government to implement a cybersecurity program statewide, providing training, resources, and guidance

to agencies to improve cybersecurity levels.

The article The NIST cybersecurity framework: overview and potential impacts [9] provides an overview of the National Institute of Standards and Technology NIST CSF, which was improved in response to President Obama's Executive Order in 2013. The theoretical account is designed to provide organizations with a set of guidelines for managing cybersecurity risks and is intended to be flexible, scalable, and adaptable to different industries and organizations. The article describes the five core functions of NIST CSF: Identify, Protect, Detect, Respond, and Recover. Each of these functions is further broken down into specific categories and subcategories that organizations use to assess their cybersecurity posture and follow appropriate controls. The article also discusses the potential impacts of NIST CSF, including its ability to help undefined stakeholders and the collaboration between unusual stakeholders in an organization, its potential to improve the overall cybersecurity posture of organizations, and its ability to provide a common language for cybersecurity that is used in different industries. In general, the article suggests that NIST CSF Cybersecurity Framework has the potential to be a valuable tool for organizations looking to improve their cybersecurity posture, but its strength will depend on how well it is implemented and adopted by organizations. Additionally, the article notes that the model provides a useful set of guidelines, it is not a comprehensive solution to wholly cybersecurity risks and should be used in conjunction with unusual best practices and tools.

The article Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations [3] proposes the use of NIST CSF (NIST CSF) as a methodological analysis for cybersecurity management in political organizations. The NIST CSF NIST CSF is a widely accepted framework that provides guidance on how to finance and reduce cybersecurity risk. The authors conducted a case study in a government organization to assess the effectiveness of the proposed methodology. They adopted a mixed-method approach, which included interviews with employees, observations, and document analysis. The results showed that the use of NIST CSF NIST CSF was effective in increasing the organization's cybersecurity posture. The theoretical account provided a common language and an organized approach to cybersecurity management. It also helped the organization place and prioritize cybersecurity risks and

implement appropriate controls. The authors advocate the use of NIST CSF NIST CSF as a methodological analysis for cybersecurity management in government organizations. They also recommend that research be conducted to assess the potency of the framework in other types of organizations and to identify any potential limitations. In general, the clause provides utilitarian insight into the importance of an organized victimization methodology for the direction of cybersecurity and highlights the benefits of using the NIST CSF NIST CSF in government organizations.

The article Evolution of the Cybersecurity Framework [4] analyzes the history and evolution of the development of cybersecurity frameworks, highlighting the importance of ensuring security in the digital age. Focusing on NIST CSF, a recognized framework used to manage cyber risks, launched in 2014 and undergoing several reviews, they analyzed the changes and logic made in the reviews, in addition to the impact of the framework on organizations and the influence on the development of other structures for this purpose, concluding on the importance of these structures for the management of cyber risks, in addition to the continuous efforts to improve them.

Chapter 3

Work Methodology

In this chapter, the NIST CSF framework and the methodology for obtaining data are presented, which for this study will be the distribution of surveys. Next, a description of the data analysis is made and, finally, data protection based on RGPD is discussed.

The methodology adopted in this master thesis uses the NIST CSF framework as an additional tool to assess cybersecurity maturity. This approach aims to cover two distinct and essential audiences in the context of cybersecurity: the common user, who plays a crucial role in preventing threats, and cybersecurity experts, who have in-depth knowledge of the challenges and strategies in the area. To achieve this objective, personalized questionnaires will be developed for each group. Based on the analysis of the responses obtained, a cybersecurity maturity index will be calculated, using the weighting between the questionnaires, which will reflect the current state of the organization in relation to the security of its data and systems.

Furthermore, it is important to briefly mention the General Data Protection Regulation (GDPR), which is a comprehensive European legislation regarding the protection of personal data. The GDPR establishes strict guidelines for the collection, storage, and processing of personal data, aiming to guarantee the privacy and data security of European Union citizens. This highlights the relevance of cybersecurity not only as a data protection practice, but also as a fundamental legal requirement in an increasingly digitalized and interconnected environment.

3.1 About NIST CSF

National Institute of Standards and Technology is a tool to help organizations identify, protect against, detect, respond to, and recover from cyber threats. Below is a brief explanation of each part of the framework:

- **Core:** Core is the foundation of the framework and consists of five main functions:
  - **Identify:** This involves understanding the assets of the organization, assessing risks, and implementing measures to manage them. This includes identifying critical data, important systems, and potential vulnerabilities.
  - **Protect:** This role focuses on the development and implementation of measures to limit or mitigate the impact of cyber threats. This includes activities such as access control, security awareness, training, security policy, and preventive measures.
  - **Detect:** This feature aims to identify a cybersecurity breach as quickly as possible. This includes implementing intrusion detection systems, continuous monitoring, security analysis, and alerts to detect malicious activity.
  - **Respond:** When a cybersecurity breach occurs, having the right response plan is essential. This role includes activities aimed at rapid response, damage mitigation, incident investigation, notification of relevant parties, and restoration of normal operations.
  - **Recovery:** After an event, it is extremely important to return to normal work as soon as possible. This role includes activities such as damage assessment, data recovery, system repair, updating security controls, and learning from the incident to prevent it from happening again.
- **Profile:** The profile allows organizations to adapt the framework to their specific needs. This includes selecting and prioritizing key categories and subcategories, as well as setting cybersecurity goals and requirements. The profile helps organizations adapt the framework to their capabilities, regulatory and business requirements.

- **Action Plan:** An action plan is a part that helps organizations create a strategic planning framework for implementation. It provides guidance on setting continuous improvement goals, identifying specific activities, and allocating resources to achieve goals. The action plan helps organizations define a clear direction to implement and improve cybersecurity. In short, NIST CSF Cybersecurity Risk Management Framework provides a flexible and comprehensive framework to help organizations manage their cybersecurity risks. It provides guidance and best practices that can be tailored to an organization's specific needs, helping to promote agility and security in an increasingly complex and threatening digital environment.

3.2 Survey Design/Technologies

One approach to assessing cybersecurity maturity is to conduct surveys of system users, service routines, and specific aspects of cybersecurity. However, relying exclusively on the assessment of these individuals may result in conclusions that are not always accurate. For a more reliable assessment, it is essential to involve all organizational levels in the research, seeking the participation of as many employees as possible.

To carry out this study, the method chosen was by conducting online research by sending invitations to companies in Portugal and Brazil. The questionnaires were prepared using the LimeSurvey [1] online tool and stored on an AWS server that was prepared for this purpose, with an emphasis on protecting the privacy of the data from the research participants.

The questionnaires were based on NIST CSF, as shown in Figure 3.1, currently in version 1.1 of April 16, 2018.

[1] `https://www.limesurvey.org/`

FUNCTION	CATEGORY	SUBCATEGORY
Identify	Asset Management	6
	Business Environment	5
	Governance	4
	Risk Assessment	6
	Risk Management Strategy	3
	Supply Chain Risk Management	5
Protect	Identity Management and Access Control	7
	Awareness and Training	5
	Data Security	8
	Information Protection Processes and Procedure:	12
	Maintenance	2
	Protective Technology	5
Detect	Anomalies and Events	5
	Security Continuous Monitoring	8
	Detection Processes	5
Respond	Response Planning	1
	Communications	5
	Analysis	5
	Mitigation	3
	Improvements	2
Recover	Recovery Planning	1
	Improvements	2
	Communications	3

Figure 3.1: NIST Structure

The framework is subdivided into five functions (Identify, Protect, Detect, Respond, Recover), and each of them has its subdivisions, totaling 23. In addition, for each subdivision, there are subcategories which together total 108 topics related to cybersecurity. To carry out this study, two groups were created, the first, called Experts, aimed at people with experience in the area of cybersecurity, and the second, aimed at people and/or companies that will be assessed. The second group was divided into three subgroups, so that we could have a view of various sectors of the company. The first, called 'Management', for people in Administration positions such as Directors or Managers, the second 'Technical (IT)', for specific employees in the company's IT infrastructure area, and finally the third 'No Technical', intended for other collaborators.

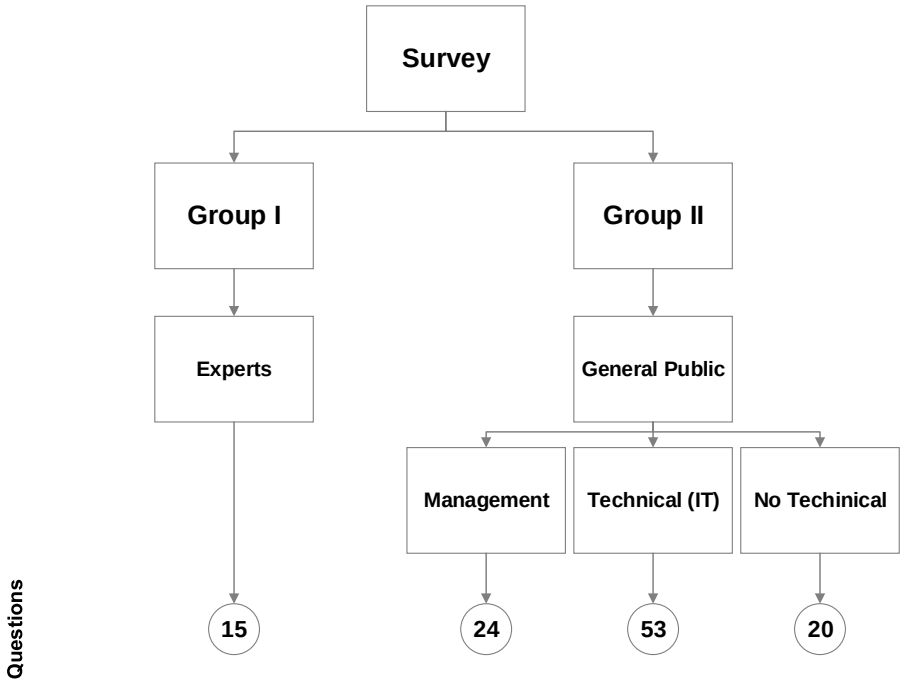


Figure 3.2: Survey Structure

As NIST CSF has a total of 108 reference points, it would not be feasible to promote questionnaires to evaluate each item of the framework. For this, a study was carried out in each category/subcategory, and more generic sentences were created. However, for each of the subgroups, there are issues that are not relevant to one group or another, with the main focus on people in the IT area. The structure of the questionnaires is represented in Figure 3.2, where the first group, aimed at company administrators, had 24 sentences, while the second group, aimed at the technical area, had 53 sentences. Finally, the third group, which was intended for other employees of the companies, with 20 sentences. It is important to point out that for the three groups, there were sentences from the five categories and with that, it allows a more global analysis. At all levels, participants could rate their degree of agreement with each statement using a five-point scale: Strongly Disagree / Disagree / Neither Agree nor Disagree / Agree / Strongly Agree. At the same time, another survey was carried out with 15 statements, also based on NIST CSF and

covering the five categories, which was distributed to cybersecurity specialists through individual invitations on LinkedIn. These specialists were divided into two distinct groups through a question. If the level of experience is less than five years, the answers will have a value 50% lower than the second group, which has five or more years of experience. The objective for this case is to identify what is most relevant and a priority for each of those who answered the questions, assigning a score to each sentence ranging from 1 to 10, with 1 being the least relevant and 10 being very relevant. This approach aims to gain a more comprehensive view of perceptions and knowledge related to cybersecurity. Data collection through multiple groups and with different experiences is expected to contribute to obtaining more robust and representative insights in the context of the study.

3.3 Data Analysis

The application of data analysis in several studies is justified because it guarantees the reproducibility and accuracy of the results. The technique follows pre-established rules defined by the researchers, facilitating the understanding of complex situations. Good data analysis is crucial in the case of complex data to facilitate interpretation. It is equally important in a master thesis because an incorrect analysis can distort the results and affect the final outcome. Thorough data analysis ensures unbiased research, free from external influences and preconceived notions. Ultimately, it contributes to a well-executed analysis and eliminates any possible biases or pre-existing opinions. Another important point is that the use of data analysis allows the results of a research to provide evidence, which in the end will serve as support for a hypothesis raised in the final thesis. With data extrapolation and based on consistent data analysis, we can conclude that when the database is extended, the results tend to be the same. Demonstration of results without good data analysis is a very difficult task for the researcher, putting in doubt its reliability and veracity. As explained above, data analysis allows the identification of patterns and similarities among the collected data, which often does not require exceptional data processing, but only the observation of what was collected. Exploring these patterns, when found, can lead researchers to even deeper analysis, leading them to make better decisions. Another point to be considered is that the use of data analysis supports the numerous

decision-making processes, always taking into account facts and patterns identified and not assumptions such as “I think that...” or decisions based on political favoritism or anything that will be used to benefit a small group and that often end up hindering a good decision. There is also the critical aspect of data analysis and its ability to contribute to knowledge in a particular field or research area. The identification of new patterns, relationships, or trends can help future research, contributing greatly to this knowledge and, consequently, being more assertive. In summary, we can consider that data analysis is a very important element in the process of a master thesis, providing a coherent, systematic, and rigorous direction for understanding the data that have been collected. These analyzes served to validate the proposed study, identifying patterns that are sometimes identified in a simple way, but in others require experience and specific knowledge, to support the decision-making process, increasing the credibility of the proposed study. Finally, it is very important that researchers use appropriate methods in data analysis, ensuring good research that is based on solid evidence and contributes to knowledge in general.

When conducting this master’s research, the analysis of the collected data followed a rigorous methodological process. As a starting point, the NIST CSF framework has been used as a basis for structuring the questionnaires. For a more comprehensive and in-depth approach, four different surveys were developed: one aimed at the management group, another aimed at the technical area team, a third survey aimed at other employees in the organization, and finally, a fourth survey designed specifically for specialists in cybersecurity. This last survey has been used as a balancing factor for the results, contributing to a more precise analysis. It is important to note that the entire process of analyzing the data found has been in full compliance with RGPD regulations, guaranteeing the privacy and security of the information collected.

3.4 RGPD - Data Protection

The RGPD, which is a set of data protection measures and aims to prepare the European Union for the digital age and entered into force on 5/24/2016 under the number 2016/679 and has been applicable since 5/25/2018, is comprehensive legislation. This legislation determines several measures and also requirements with the intention of guar-

anteeing the privacy and security of personal information.

The main GDPR topics aimed at data protection are briefly described below:

- **Data Protection Principles:** : The data protection principles that are defined in the RGPD are the correct, legal, and transparent processing of data, in addition to the importance of ensuring that the data are reliable, limiting them exclusively to their purpose when processing, retain personal data only for the time necessary, guaranteeing its integrity and confidentiality. Finally, there is a need to be responsible for compliance with legislation.

- **Consent:** According to the GDPR rules, the consent of people to process their personal data is extremely important. Companies, organizations, and anyone who, for whatever reason, collects personal data is required to have unequivocally consent to the collection and processing of these data. This consent must be given voluntarily and consciously; in addition, everyone has the right to withdraw the consent given initially at any time.

- **Rights of individuals:** Another point of reference for RGPD is the right that people have over their own data, that is, they have the right to access and have information about how their personal data are processed at any time. processed. Furthermore, if any personal data are incorrect, it is the right of people to be able to change it or even request its deletion from the database. Finally, the GDPR grants everyone the right to portability of data, allowing personal data to be migrated to another company or organization.

- **Security Measures:** The RGPD is exhaustive with regard to the technical and organizational security measures that companies or organizations are required to implement, with the intention of providing guarantees for the security of personal data. These measures can be the implementation of security policies and procedures, data encryption, monitoring of access to these data, carrying out and revalidating risk assessments, in addition to implementing measures aimed at preventing and detecting data breaches.

- **Data Protection Officer (DPO):** In certain cases, the GDPR requires organi-

zations and companies to designate a DPO. This person becomes responsible for supervising compliance with current data protection laws, thus ensuring that the rules are being complied with. This person also becomes the point of reference for any issue involving data protection.

- **Transfer of Data to Third Countries:** By the legislation contained in RGPD, there are restrictions on the transfer of personal data to countries that do not belong to the European Union. This measure aims to establish the minimum security of the personal data collected. There is the possibility of transferring personal data to countries outside the European Union, according to RGPD. These transfers, when carried out, must be supported by contractual clauses and/or corporate rules that respect current legislation.

- **Responsibility and Accountability:** Under the GDPR, organizations are fully responsible for complying with data protection laws. They must be able to demonstrate compliance with RGPD, that is, companies and organizations must keep all records organized about their activities regarding data processing; in addition, they must apply privacy policies to all processes and systems.

Creating a more closed data protection environment and providing guarantees that companies and organizations work with personal data in an adequate and secure way is one of the main objectives. By implementing the measures and requirements set out in the GDPR, companies can promote the privacy, trust, and security of anyone's personal data.

Chapter 4

Implementation and Analysis of Results

In this chapter, the methodology adopted to obtain the cybersecurity maturity index is descibed, as well as the analysis of the results and suggestions for improvements for the cybersecurity area.

4.1 General Survey

As mentioned above, the questionnaires used in this research were organized into three distinct parts: one for executives, another for IT professionals, and the last for other employees. Each questionnaire was structured to address NIST CSF five major functions, ensuring a comprehensive assessment of the cybersecurity posture of organizations.

To illustrate the methodology adopted in creating the questionnaires, let us take the"Identify" function in the "Governance" category as an example. In this specific category, a subdivision was identified that comprises four essential areas: Organizational Policy, Cybersecurity Roles and Responsibilities, Legal Requirements, and Risk Management.

The NIST CSF framework, which is demonstrated through the Figure 4.1, follows the organization logic in large groups that, as they unfold into more detailed levels, cover different layers. It is important to emphasize that this framework is constantly evolving, aiming to encompass all activities related to cybersecurity and ensure better alignment

with emerging demands.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 4.1: NIST Structure Expands

Extending the NIST CSF structure and focusing on the example of the "Identify" function in the "Governance" category, we originally have:

Identify function (ID)

1. **Governance Category (GV):** This category addresses the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements, understanding and informing cybersecurity risk management.

2. **Subcategories:** For the Governance category, four crucial subcategories were identified:

   (a) ID.GV-1: Establishment and communication of organizational cybersecurity policy.

   (b) ID.GV-2: Coordination and alignment of cybersecurity roles and responsibilities with internal roles and external partners.

   (c) ID.GV-3: Understanding and managing legal and regulatory requirements related to cybersecurity, including privacy and civil liberties obligations.

   (d) ID.GV-4: Addressing cybersecurity risks in governance and risk management processes.

To optimize the efficiency of the questionnaires and encourage greater participation from people, related statements were consolidated, reducing them from four to two, as shown:

- ID.GV-1 and ID.GV-2 The organizational cybersecurity policy (roles and responsibilities) is established and communicated, either to employees and/or partners.
- ID.GV-3 and ID.GV-4 Organization complies with industry and/or regional cybersecurity operational requirements, which is established and monitoring existing risks.

These two statements were incorporated into the three questionnaires sent to the companies, with the second included only in the questionnaires intended for the Management and IT areas.

This consolidation approach was applied to all functions and categories, resulting in simpler and more straightforward questionnaires, without compromising the integrity of cybersecurity assessments at participating organizations. The use of this optimized model seeks to facilitate the participation of the respondents and, at the same time, ensure a complete and in-depth analysis of the cybersecurity posture in the investigated companies.

The three questionnaires sent to companies are separated, where in the table 4.1 are the questionnaire questions for administrators, in the table 4.2 are the questionnaire questions for those responsible for the area of technology and finally in the table 4.3 are the questionnaire questions for other employees.

Management Survey

cod_survey	**Question**	**Function of NIST**
Manager001	Cybersecurity roles and responsibilities are established.	IDENTIFY
Manager002	There is a control of users, fixed devices, software platforms, and data flow that are connected to the network.	IDENTIFY
Manager003	The organization's mission and object are established and communicated.	IDENTIFY
Manager004	The organization's role and place has been established and communicated.	IDENTIFY
Manager005	To measure the organization's exposure to potential threats, a risk assessment is conducted periodically.	IDENTIFY
Manager006	Organizational cybersecurity policy (roles and responsibilities) is established and communicated, either to employees and/or partners.	IDENTIFY
Manager007	Cybersecurity operational requirements are met and existing risks are monitored in compliance with industry and/or regional guidelines.	IDENTIFY
Manager008	Internal and external threats and vulnerabilities are identified and documented.	IDENTIFY
Manager009	Risk responses are identified and prioritized.	IDENTIFY
Manager010	Threats, vulnerabilities, probabilities and impacts are used to determine risks.	IDENTIFY
Manager011	Any risk or occurrence of cybersecurity attacks, whether internal (employees) or external (business partners), is monitored and controlled, determining the organization's risk tolerance.	IDENTIFY

Table 4.1 continued from previous page

cod_survey	Question	Function of NIST
Manager012	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and the Cybersecurity Supply Chain Risk Management Plan.	IDENTIFY
Manager013	Suppliers, partners, risk management processes and supply chain information system are identified.	IDENTIFY
Manager014	There is constant training on cybersecurity and every employee, manager, and partners know how to avoid the main threats (Phishing, Ransomware techniques).	PROTECT
Manager015	An incident response and recovery plan is implemented and tested, and a vulnerability management plan is in place.	PROTECT
Manager016	Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening).	PROTECT
Manager017	Policies regarding the physical environment of assets are followed, as well as policies for destroying sensitive data.	PROTECT
Manager018	The results of every system audit are documented, implemented, and reviewed.	PROTECT
Manager019	The system that monitors cybersecurity is configured in such a way that occurrences are registered and easily accessible.	DETECT

Table 4.1 continued from previous page

cod_survey	**Question**	**Function of NIST**
Manager020	If a cybersecurity incident occurs, are the procedures for data recovery secure and well-coordinated with all parties involved, including users, customers, partners, and authorities?	RESPOND
Manager021	After a cybersecurity event, lessons learned are incorporated into the response policy and the strategy is updated.	RESPOND
Manager022	In the event of a cybersecurity event, are the processes for data recovery secured and coordinated with all stakeholders (users - customers - partners and authorities).	RECOVER
Manager023	After a cybersecurity event, lessons learned are incorporated into the response policy.	RECOVER
Manager024	Is the recovery plan periodically tested as to its ability to quickly recover data or services that may have been compromised by a cyber attack event.	RECOVER

Table 4.1: Management Survey

IT Survey

cod_survey	Question	Function of NIST
TI001	Cybersecurity roles and responsibilities are established.	IDENTIFY
TI002	Hardware, software, and personnel resources are prioritized according to classification and value to the business.	IDENTIFY
TI003	There is a control of users, fixed devices, software platforms, and data flow that are connected to the network.	IDENTIFY
TI004	There is a record of every external information system connected to the network.	IDENTIFY
TI005	There is a periodic risk assessment, to measure exposure to possible threats to the organization.	IDENTIFY
TI006	Organizational cybersecurity policy (roles and responsibilities) is established and communicated, either to employees and/or partners.	IDENTIFY
TI007	Currently, the organization meets industry and/or regional requirements for cybersecurity operations, which are being monitored.	IDENTIFY
TI008	Internal and external threats and vulnerabilities are identified and documented.	IDENTIFY
TI009	Risk responses are identified and prioritized.	IDENTIFY
TI010	Threats, vulnerabilities, probabilities and impacts are used to determine risks.	IDENTIFY
TI011	Any risk or occurrence of cybersecurity attacks, whether internal (employees) or external (business partners), is monitored and controlled, determining the organization's risk tolerance.	IDENTIFY

Table 4.2 continued from previous page

cod_survey	Question	Function of NIST
TI012	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and the Cybersecurity Supply Chain Risk Management Plan.	IDENTIFY
TI013	Suppliers and partners are evaluated periodically based on contractual obligations.	IDENTIFY
TI014	Suppliers, partners, risk management processes and supply chain information system are identified.	IDENTIFY
TI015	There is periodic response testing with providers and suppliers.	IDENTIFY
TI016	Access security best practices are adopted (authentication with complex, multi-factor passwords).	PROTECT
TI017	Physical network access to equipment is blocked when there is no permission.	PROTECT
TI018	There is constant monitoring of access to the company network.	PROTECT
TI019	There is control of network access (remote or otherwise), enforcing security policies.	PROTECT
TI020	There is monitoring of all user accounts, enforcing the network access policy.	PROTECT
TI021	There is network segregation/segmentation, with the goal of preserving integrity.	PROTECT
TI022	Cybersecurity officers are able to perform their duties.	PROTECT

Table 4.2 continued from previous page

cod_survey	Question	Function of NIST
TI023	There is constant training on cybersecurity and every employee, manager, and partners know how to avoid the main threats (Phishing, Ransomware techniques).	PROTECT
TI024	Production and test environments are separated.	PROTECT
TI025	Storage devices and media are encrypted and secured.	PROTECT
TI026	There is a tested and reliable data backup and restoration protocol.	PROTECT
TI027	There is control of all external devices connected to the network, avoiding possible data leaks.	PROTECT
TI028	There is encryption of all sensitive data.	PROTECT
TI029	There is encryption of network traffic.	PROTECT
TI030	An incident response and recovery plan is implemented and tested, and a vulnerability management plan is in place.	PROTECT
TI031	Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening).	PROTECT
TI032	Periodically, protection processes are evaluated and improved, sharing all new processes with all processed changes.	PROTECT
TI033	Policies regarding the physical environment of assets are followed, as well as policies for destroying sensitive data.	PROTECT

Table 4.2 continued from previous page

cod_survey	Question	Function of NIST
TI034	There is a basic configuration of systems and processes created, as well as verification that the life cycle of these systems are implemented.	PROTECT
TI035	There is a tested and reliable information backup and data restoration protocol.	PROTECT
TI036	There is periodic maintenance and documentation of assets in order to prevent unauthorized access.	PROTECT
TI037	Some mechanisms (e.g. fail-safe, load balancing, hot swap) are implemented to ensure resiliency requirements work in normal and adverse situations.	PROTECT
TI038	The default system configuration, adopts the principle of least functionality.	PROTECT
TI039	There is a record of every system audit, which is documented, implemented, and reviewed.	PROTECT
TI040	There is encryption of all removable media.	PROTECT
TI041	You have encryption and control of the communication network.	PROTECT
TI042	There is an automated system in place that can analyze and document anomalies and/or unwanted activity on the company's network, alerting the responsible parties.	DETECT
TI043	Periodically, there is a review of network activities, avoiding possible cyber incidents, being able to identify malicious code and performing vulnerability scans.	DETECT

Table 4.2 continued from previous page

cod_survey	Question	Function of NIST
TI044	Occurrences of cybersecurity attacks are logged, using current technologies such as backups, encryption.	DETECT
TI045	The system that monitors cybersecurity is configured in such a way that occurrences are registered and easily accessible.	DETECT
TI046	When there is a notification from the systems of a possible cybersecurity event, these are analyzed, there is an investigation, and the impact is understood. In addition, the incidents are classified according to the response plan.	RESPOND
TI047	If a cybersecurity incident occurs, are the procedures for data recovery secure and well-coordinated with all parties involved, including users, customers, partners, and authorities?	RESPOND
TI048	After a cybersecurity event, lessons learned are incorporated into the response policy and the strategy is updated.	RESPOND
TI049	Vulnerabilities once discovered are mitigated, contained and documented.	RESPOND
TI050	There is a cybersecurity event contingency plan.	RESPOND
TI051	In the event of a cybersecurity event, are the processes for data recovery secured and coordinated with all stakeholders (users - customers - partners and authorities).	RECOVER
TI052	After a cybersecurity event, lessons learned are incorporated into the response policy.	RECOVER

Table 4.2 continued from previous page

cod_survey	Question	Function of NIST
TI053	Is the recovery plan periodically tested as to its ability to quickly recover data or services that may have been compromised by a cyber attack event.	RECOVER

Table 4.2: TI Survey

Others Survey

cod_survey	Question	Function of NIST
General001	Cybersecurity roles and responsibilities are established.	IDENTIFY
General002	There is a periodic risk assessment, to measure exposure to possible threats to the organization.	IDENTIFY
General003	Organizational cybersecurity policy (roles and responsibilities) is established and communicated, either to employees and/or partners.	IDENTIFY
General004	Internal and external threats and vulnerabilities are identified and documented.	IDENTIFY
General005	Risk responses are identified and prioritized.	IDENTIFY
General006	Threats, vulnerabilities, probabilities and impacts are used to determine risks.	IDENTIFY
General007	Any risk or occurrence of cybersecurity attacks, whether internal (employees) or external (business partners), is monitored and controlled, determining the organization's risk tolerance.	IDENTIFY

Table 4.3 continued from previous page

cod_survey	Question	Function of NIST
General008	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and the Cybersecurity Supply Chain Risk Management Plan.	IDENTIFY
General009	Suppliers and partners are evaluated periodically based on contractual obligations.	IDENTIFY
General010	Suppliers, partners, risk management processes and supply chain information system are identified.	IDENTIFY
General011	There is periodic response testing with providers and suppliers.	IDENTIFY
General012	There is constant training on cybersecurity and every employee, manager, and partners know how to avoid the main threats (Phishing, Ransomware techniques).	PROTECT
General013	An incident response and recovery plan is implemented and tested, and a vulnerability management plan is in place.	PROTECT
General014	Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening).	PROTECT
General015	Policies regarding the physical environment of the assets are followed, as well as whether sensitive data is destroyed according to the policies.	PROTECT
General016	There is a record of every system audit, which is documented, implemented, and reviewed.	PROTECT

Table 4.3 continued from previous page

cod_survey	Question	Function of NIST
General017	The system that monitors cybersecurity is configured in such a way that occurrences are registered and easily accessible.	DETECT
General018	If a cybersecurity incident occurs, are the procedures for data recovery secure and well-coordinated with all parties involved, including users, customers, partners, and authorities?	RESPOND
General019	In the event of a cybersecurity event, are the processes for data recovery secured and coordinated with all stakeholders (users - customers - partners and authorities).	RECOVER
General020	After a cybersecurity event, lessons learned are incorporated into the response policy.	RECOVER

Table 4.3: Other Survey

4.2 Expert Survey

The objective of creating an auxiliary questionnaire, aimed at specialists in the field of cybersecurity, is to focus the research on a more comprehensive and objective approach, avoiding relying exclusively on people's feelings and personal experiences in relation to the subject. The experts questionnaire, referred to here as "Experts", is designed to differentiate this type of research, considering the vast experience and knowledge of these professionals in the sector.

The main function of the experts questionnaire is to calibrate the answers obtained in the other surveys, bringing a perspective based on the experiences of these experts. Through two distinct categories, participants are classified according to their time in the area: those with more than five years of experience and beginners.

The experts answers will serve to calibrate the results, as they live directly with the

cybersecurity environment and have the necessary expertise to discern the relevance of different aspects of the NIST CSF framework.

The experts questionnaire starts with the question about how long they have been working in the cybersecurity field, and this information will play a crucial role in the data analysis, as explained below:

- Experience $\geq$ five years: answers will be weighted with 100% of the score assigned to each question;
- Experience $<$ five years: the answers will have 50% of the score considered in the final evaluation.

The questionnaire continues with 14 carefully designed questions, covering aspects of the NIST CSF framework and encompassing the five major functions: Identify - Protect - Detect - Respond - Recover.

By considering the experts vast experience and knowledge, this research aims to obtain valuable insights into the relative importance of each aspect of cybersecurity, in order to complement and enrich the results obtained in the other researches. The analysis based on the experts contributions will allow a more solid and comprehensive approach in the evaluation of the cybersecurity posture, significantly contributing to the advancement of knowledge in this critical field of information security.

In the survey for Experts, which is detailed in table 4.4, the participation of Experts was extremely important, with 50% of the Experts who responded to the questionnaire having more than five years of experience in the area of cybersecurity. By considering the results obtained with the responses of the other participants, it was possible to identify the NIST CSF function that stands out with greater relevance in the general context: the Protection function.

Experts considered the relative importance of NIST CSF functions and, based on their experiences in the field of cybersecurity, the Protection function emerged as the most crucial in the current scenario. This finding is extremely important, as it demonstrates the emphasis placed by experts on implementing protective measures to mitigate threats and strengthen the security posture of organizations.

Expert Survey

Function NIST	cod_question_expert	Question
Protect	Experts005	Sharing an account is not allowed and cannot be done.
Recover	Experts013	Cyber-attack insurance is in place.
–	Experience001	Do you have more than 5 years of experience in Cybersecurity?
Protect	Experts007	Email filters are enabled.
Protect	Experts008	Periodically, there is security training for all employees.
Recover	Experts014	Security processes and procedures are continuously improved.
Detect	Experts009	Security software is installed on all devices and updated periodically.
Identity	Experts004	Updates for software and firmware on all devices.
Recover	Experts012	Both sensitive data and system configurations are backed up.
Detect	Experts010	There are periodic audits and their recommendations are followed up on.
Identity	Experts003	There is a change in the credentials used to access the system (factory credentials).
Respond	Experts011	There is a plan in place to contain a cybersecurity breach.
Identity	Experts001	There is access control to the company network.
Identity	Experts002	There is control of all devices that access the network.
Protect	Experts006	Two-factor authentication is enabled for all devices.

Table 4.4: Expert Survey

In Figure 4.2, is present a compilation of the importance assessments attributed by experts to each of the NIST CSF functions:

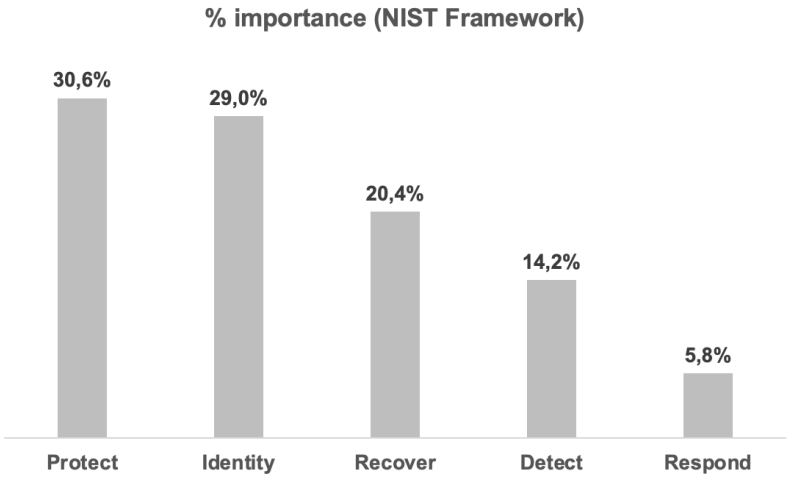


Figure 4.2: Degree of importance of NIST functions

Based on the results obtained and the degree of relevance attributed by the experts, it becomes evident that having the ability to identify cybersecurity problems and being aware of threats represents a crucial advantage for companies. The creation of robust and consistent security procedures can make a company less vulnerable and, at the same time, more protected and prepared to face the challenges of the information security scenario.

The Identification and Protection functions of NIST CSF play a central role in the effectiveness of security measures implemented by organizations. Knowing how to identify potential problems and threats is the first step to taking preventive and proactive actions, reducing the risk of security incidents. However, adopting effective protection strategies ensures greater resilience, detection, recovery and defense capacity in the face of constantly evolving cyber threats.

However, adopting effective protection strategies ensures greater resilience and defense capacity in the face of constantly evolving cyber threats.

By creating robust and consistent security procedures, companies establish a solid foundation of protection, making themselves less susceptible to attacks and security breaches. This approach also allows the company to remain agile and prepared to face the constant challenges of the cyber landscape.

For each of the 14 statements in the questionnaire, respondents assign a score between

1 and 10, here referred to as the total score, reflecting the importance that each aspect of cybersecurity has for them. However, the analysis is not limited to individual responses only, as we consider the participant's experience as a significant weighting factor.

Experts who have five years or more of experience in the field of cybersecurity have their answers weighted with 100% of the score assigned to each question. On the other hand, participants with less than five years of experience have their scores adjusted to 50%, reflecting the importance of their contributions despite having less experience in the area, here referred to as average experience.

The calculation of each NIST CSF function is demonstrated in Figure 4.1, which represents a weighted average of the responses obtained through surveys with cybersecurity professionals with different levels of experience.

$$\text{Degree of importance of NIST functions} : \frac{\text{Total Score}}{\text{Average Experience}} \tag{4.1}$$

The calculation shown in Figure 4.1 provides the initial importance of the NIST CSF functions, which is used to build the matrices necessary to determine the maturity level.

The flow described is represented by Figure 4.3, which illustrates how the information taken from the questionnaires aimed at experts was treated.

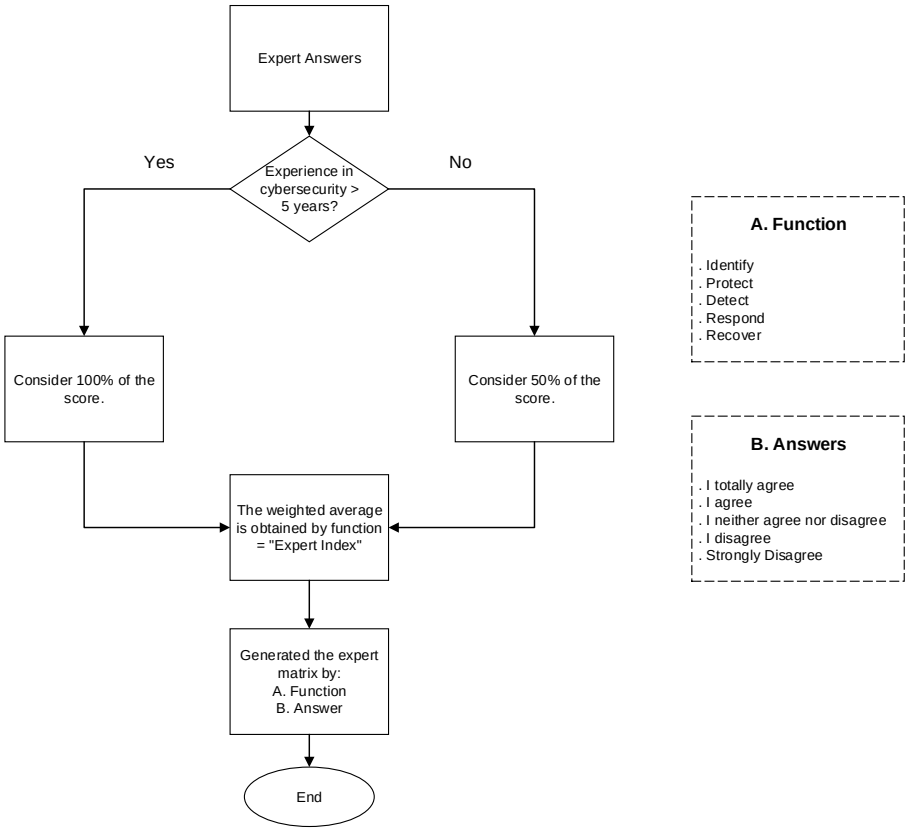


Figure 4.3: Flow of Experts

4.3 Cybersecurity Maturity Calculation

The calculation of cybersecurity maturity is the result of integrating two different matrices: one derived from responses collected through interviews, and the other consisting of contributions from cybersecurity specialists, bringing together both those with extensive experience, that is, more than five years of activity in the area, as well as newcomers in this field.

Methodology

To obtain the cybersecurity maturity index, the process must be divided into two stages.

4.3.1 Building the General Matrix

The process of building the general matrix involves research carried out with companies, through questionnaire responses, taking into account two factors:

- **Type of Researchs:** The surveys were directed to three professional groups: managerial, others, and IT. The number of questions varied between the groups, which led to different weights for the responses.
- **Types of Response:** For each question, five response alternatives were offered, each with a specific associated weight as presented in Table 4.5.

Answer	Weight
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

Table 4.5: Types of response

4.3.2 Calculation of the value of each question

In order to avoid an imbalance between NIST CSF functions, valuing or devaluing a certain issue or group (management, IT or others), the proportionality between questionnaire, NIST CSF function and number of questions was adopted as a premise, the value of each question is calculated by dividing one by the number of questions per NIST CSF function and by questionnaire type, as shown in Figure 4.2. For example, the value of each question for the NIST CSF Identify function in the managerial group is equal to 0.076, since one divided by 13 is equal to 0.076. The values of each question are shown in table 4.6.

$$\mathsf{Valueofeachquestion}: \frac{1}{\mathsf{Number\ of\ questions\ by\ type\ /\ function\ or\ group}} \tag{4.2}$$

	Number of Questions			Value of each question		
Function	**Management**	**Others**	**IT**	**Management**	**Others**	**IT**
Identify	13	11	15	0.076	0.090	0.066
Protect	5	5	26	0.200	0.200	0.038
Detect	1	1	4	1.000	1.000	0.250
Respond	2	1	5	0.500	1.000	0.200
Recover	3	2	3	0.333	0.500	0.333
Total	**24**	**20**	**53**			

Table 4.6: Value of each question

4.3.3 Building the matrix for each questionnaire

The construction of matrices by questionnaire type (managerial, other, and IT) requires the definition of weights for each response. These weights are established according to the relevance of the response to the research objective, as shown in table 4.7.

Response Type	**Weight**
SD - Strong Disagree	1
D - Disagree	2
N - Neutral	3
A - Agree	4
SA - Strong Agree	5

Table 4.7: Response Type and Weights

Example:

To illustrate the process, the managerial questionnaire type and the NIST CSF Identify function were used. The results are shown in table 4.8.

Based on table 4.8, the matrices by group type were created, as shown in tables 4.9 - matrix for the management group - 4.10 - matrix for the group of other employees, and finally 4.11 - matrix for those who work in the IT area.

	SD	**D**	**N**	**A**	**SA**
Factor	1	2	3	4	5
Individual Value	0.076				
Final Value	0.076	0.153	0.230	0.307	0.384

Table 4.8: Example distribution by response type

SD = Strongly disagree D = Disagree N = Neutral A = Agree AS = Strongly Agree

Management Group Matrix

	SD	D	N	A	SA
Identify	0.076	0.153	0.230	0.307	0.384
Protect	0.200	0.400	0.600	0.800	1.000
Detect	1.000	2.000	3.000	4.000	5.000
Respond	0.500	1.000	1.500	2.000	2.500
Recover	0.333	0.666	1.000	1.333	1.666

Table 4.9: Management Group Matrix

Other Group Matrix

	SD	D	N	A	SA
Identify	0.090	0.181	0.272	0.363	0.454
Protect	0.200	0.400	0.000	0.800	1.000
Detect	1.000	2.000	3.000	4.000	5.000
Respond	1.000	2.000	3.000	4.000	5.000
Recover	0.500	1.000	1.500	2.000	2.500

Table 4.10: Other Group Matrix

IT Group Matrix

	SD	D	N	A	SA
Identify	0.066	0.133	0.200	0.266	0.333
Protect	0.038	0.076	0.115	0.153	0.192
Detect	0.250	0.500	0.750	1.000	1.250
Respond	0.200	0.400	0.600	0.800	1.000
Recover	0.333	0.666	1.000	1.333	1.666

Table 4.11: TI Group Matrix

4.3.4 Building the Experts Matrix

The steps to calculate the matrix considering the importance of the NIST CSF functions assigned to experts are described below:

1. **Importance for experts**

   In Figure 4.2, the importance for specialists of each NIST CSF function had already been calculated. In table 4.12, there is a transcription of this data in the format that will be used to calculate the experts matrix.

Function	**% importance**
Identify	29.0

Table 4.12 continued from previous page

Function	% importance
Protect	14.2
Detect	30.6
Respond	5.8
Recover	20.4

Table 4.12: Importance in the view of the Experts

2. **Calculation of the value of each question**

   Due to the existence of three types of questionnaires, Management, Other employees and IT area, with different numbers of questions per NIST CSF function, it is necessary to calculate the value of each question separately. For this, the % importance of NIST CSF functions for experts is used, according to table 4.12. The calculated values are presented in table 4.13, which shows the value of each question by type of questionnaire and NIST CSF function.

Function	Importance	Number of questions			Value for each question		
		Management	Others	TI	Management	Others	TI
Identify	29.0	13	11	15	0.022	0.026	0.019
Protect	14.2	5	5	26	0.028	0.028	0.005
Detect	30.6	1	1	4	0.306	0.306	0.076
Respond	5.8	2	1	5	0.028	0.057	0.011
Recover	20.4	3	2	3	0.067	0.101	0.067
Total	**100.0**	**24**	**20**	**53**	**0.022**	**0.026**	**0.019**

Table 4.13: Calculation of the value of each NIST function

The formula used to calculate the value of each question is shown in Figure 4.3.

$$\text{Value of each question} : \frac{\%\text{importance} \times \text{NIST Function}}{\text{Number of questions by type}} \tag{4.3}$$

As an example, the value for each question of the management group and the NIST CSF Identify function is presented in Figure 4.4.

$$\text{Value of each question} = \frac{\left(\frac{29.0}{100}\right)}{13} \rightarrow 0.022 \tag{4.4}$$

The value of 0.022 for the management questionnaire and NIST CSF identify function is different from the other questionnaires (other employees and IT area), as each questionnaire presents a different number of questions per NIST CSF group, as shown in table 4.13.

3. **Calculation of the Expert Matrix by Type/Response**

   The last step is to calculate the value of each response, using the results obtained in the corresponding matrix. Possible answers are: totally disagree, disagree, neutral, agree and totally agree. For the "strongly agree" answer, the value is the same as that found in the corresponding matrix. This is the maximum value that the question could have if the respondent classified the question as "strongly agree". The other answers receive values according to the premise described in table 4.14.

Answer	**% Assigned**
Strongly disagree	0% of the value in matrix for each questionnaire. Table: 4.9/4.10/4.11
Disagree	25% of the value in matrix for each questionnaire. Table: 4.9/4.10/4.11
Neutral	50% of the value in matrix for each questionnaire. Table: 4.9/4.10/4.11
Agree	75% of the value in matrix for each questionnaire. Table: 4.9/4.10/4.11
Strongly Agree	100% of the value in matrix for each questionnaire. Table: 4.9/4.10/4.11

Table 4.14: Participation by type of response

Using the same example used previously, that is, Management Group and NIST CSF Identify Function, the result is 0.022. The possible values according to each answer are described in table 4.15.

Answer	%		**Value for the Response type**
Strongly disagree	0		0
Disagree	25		0.005
Neutral	50	**0.022**	0.011
Agree	75		0.016
Strongly Agree	100		0.022

Table 4.15: Example of distribution by response type

The Expert Matrix is built and ready to be used in conjunction with the participant matrix, through information crossing. The database includes three tables: Participant Responses, Participant Matrix, and Expert Matrix. Respondent responses provide insight into cybersecurity concerns. However, this study aims to present cybersecurity maturity based on the matrix created from experts responses. The new NIST CSF function scores, after profile recalibration based on the generated matrix, are assigned to the final result. The final result is established based on this methodology. The analysis of the numbers generated is carried out based on the maturity scale described in table 4.16, in which the results vary from 0 to 5.

Search Result	**Maturity**
≤ 1.99	Very poor
≤ 2.99	Poor
≤ 3.99	Fair
≤ 4.99	Good
$= 5.00$	Excelent

Table 4.16: Maturity Scale

After obtaining the result, whether individual or for groups of companies, considering different types of research (Management, IT and Others), it is possible to suggest, as long as the company has responded at all levels, in which subcategory of the NIST CSF function there is space for improvements or what are the main points of attention.

4.3.5 Calculations

After the construction of the matrices, as shown in tables 4.9 - matrix for the management group - 4.10 - matrix for the group of other employees, and finally 4.11 - matrix for those who work in the IT area, for the questionnaire types, and in table 4.13 for the expert matrix, which provided the values of the responses for each question, the calculation phase begins. The data presented below are a sample of the data received. The examples used to illustrate each step of the calculations refer to company B. The description of this phase is presented below.

1. **Consolidation of research results**

   The result is obtained by aggregating the matrices by questionnaire type (management, other, and IT). At this stage, only the results (calculated value per response) that each respondent answered in the questionnaires are considered. In table 4.17, there is an example of this step.

Function	Q1	Q2	...	...	Qn
Identify	3,73	3,45	...	...	...
Protect	4,40	4,20	...	...	...
Detect	3,00	3,00	...	...	...
Respond	3,00	3,00	...	...	...
Recover	3,00	3,00	...	...	...

Table 4.17: Consolidation of results

2. **Average search results**

   The simple average of all responses is calculated. In table 4.18, there is the simple average for company B.

Function	**Average**
Identify	3,60
Protect	4,44
Detect	3,50

Respond	3,40
Recover	3,42
Company	**3,67**

Table 4.18: Average

3. **Recalculation of the degree of importance of Experts**

   The importance score of experts is recalculated based on the obtained responses, using the expert matrix. In table 4.19, there is an example of this step.

Function	**Q1**	**Q2**	**...**	**...**	**Qn**
Identify	0,1978	0,1780	...	...	...
Protect	0,1208	0,1136	...	...	...
Detect	0,1531	0,1531	...	...	...
Respond	0,0289	0,0289	...	...	...
Recover	0,1018	0,1018	...	...	...

Table 4.19: Recalculation of the degree of importance of Experts

4. **Application of the degree of importance of Experts**

   The new importance score of experts is used to consolidate the research results. In table 4.20, there is an example of this step.

Function	**Q1**	**Q2**	**...**	**...**	**Qn**
Identify	0,3283	0,3092	...	...	...
Protect	0,2005	0,1975	...	...	...
Detect	0,2541	0,2660	...	...	...
Respond	0,0480	0,0502	...	...	...
Recover	0,1691	0,1771	...	...	...

Table 4.20: Application of the degree of importance of experts

5. **Average results considering the recalculated expert index**

The simple average of all responses is calculated, after the application of the recalculated expert index. In table 4.21, there is the average after recalculating the experts index.

Function	**Average**
Identify	29,4%
Protect	18,9%
Detect	28,3%
Respond	5,2%
Recover	18,3%

Table 4.21: Average after expert index recalculation

6. **Calculation of the maturity index considering the recalculated experts index**

With the expert index recalculated, it is possible to calculate the maturity index from the expert's perspective, as shown in table 4.22. This index is obtained by multiplying the new expert index by the total results of the initial research by NIST CSF function.

	Recalculated index	**Initial search**		**Initial survey with recalculated maturity index**	
		Q1	**Q2**	**Q1**	**Q2**
Identify	29,4%	3,73	3,45	5,00	4,90
Protect	18,9%	4,40	4,20	3,23	3,14
Detect	28,3%	3,00	3,00	4,84	4,71
Respond	5,2%	3,00	3,00	0,85	0,86
Recover	18,3%	3,00	3,00	3,13	3,05
Company	**100,0%**	**3,43**	**3,33**	**3,42**	**3,33**

Table 4.22: Calculation of the Cybersecurity Maturity Index

The formula used to calculate the maturity index considering the recalculated experts index is shown in Figure 4.5

$$\text{Maturity index with recalculated experts index : recalculated index} \times \text{sum of initial search} \tag{4.5}$$

As an example, in figures 4.6 and 4.7, there is a calculation to find the value of the identify and protect functions of Q1.

$$\text{Maturity} = \left(\frac{29.4}{100}\right) \times (3.73 + 4.40 + 3.00 + 3.00 + 3.00) \rightarrow 5.0 \tag{4.6}$$

$$\text{Maturity} = \left(\frac{18.9}{100}\right) \times (3.73 + 4.40 + 3.00 + 3.00 + 3.00) \rightarrow 3.23 \tag{4.7}$$

7. **Average results considering the recalculated expert index**

The simple average considering the recalculated experts index of all responses is recalculated. In the 4.23 table, you will find the simple average from the perspective of experts from company B.

Function	**Average**
Identify	4,97
Protect	3,47
Detect	4,84
Respond	0,95
Recover	3,36
Company	**3,52**

Table 4.23: Average considering the recalculated Expert Index

Once all calculations have been made, it is possible to compare the results of the responses obtained through the questionnaires with the results of the responses obtained through the questionnaires with the application of the experts importance grade. With

these numbers, it is possible to estimate the company's position on the cybersecurity maturity scale.

Example: Table 4.24 presents the cybersecurity maturity level by NIST CSF function and the company as a whole, obtained in company B.

	Company		**Company with the Expert Index**	
	Maturity Index	**Maturity**	**Maturity Index**	**Maturity**
Identify	3,60	Fair	4,97	Good
Protect	4,44	Good	3,47	Fair
Detect	3,50	Fair	4,84	Good
Respond	3,40	Fair	0,95	Very Poor
Recovery	3,42	Fair	3,36	Fair
Company	**3,67**	**Fair**	**3,52**	**Fair**

Table 4.24: Result Comparison

4.4 Analysis of Results

Over a period of approximately 40 days, the surveys were available for completion. After this interval, the surveys were closed and the collection of responses began. In total, four companies in Portugal were available to respond to questionnaires at different levels. It is important to note that not all companies responded at all levels; however, for this study, this does not represent an obstacle. Similarly, research involving experts was also completed, and data was collected to begin analyzes related to cybersecurity maturity. As no sensitive data was collected, the companies and people who responded will not be identified. Likewise, cybersecurity experts will also remain anonymous. Companies will be referred to as Company A, Company B, Company C and Company D, while cybersecurity experts will be addressed as Experts.

Company A

Company A has a very low level of cybersecurity maturity, whether for the company's employees or experts. Across all NIST CSF roles, there is a clear tendency for low grades. The Respond index, which measures a company's ability to respond to cybersecurity

incidents, is the lowest among companies participating in the surveys. This means that company A is very poorly prepared to deal with cyber attacks, as identified in Figure 4.4. These results are worrying as they point to a high risk that the company will be the target of cyber attacks. Furthermore, they can lead to financial losses, damage to reputation, and even the interruption of the company's operations.

Figure 4.4: Company A

Company B

Company B has a satisfactory level of cybersecurity maturity, but one that can improve. Functions such as Identify and Detect are very close to the maximum level of maturity, but, like Company A, the Respond function has the biggest difference, being rated as Very Poor when applied to weighting with the experts perception, this fact can be seen in Figure 4.5. Analysis of the results of the study shows that company B has a good level of maturity in terms of identifying and detecting threats. This means that the company is able to identify and detect cyber threats with a high degree of accuracy. However, company B has a very low level of maturity in terms of incident response. This means that the company is not well prepared to deal with cyber attacks.

Figure 4.5: Company B

Company C

Company C presents a higher level of cybersecurity maturity, both in terms of employee perception and when applied to experts perception. Like Company B, it presents even better results in the Identify and Detect functions, and also has a good result in the Recover function. Analysis of the study results shows that company C has a good level of maturity in terms of identifying and detecting threats, as well as in terms of incident recovery. This means that the company is able to identify and detect cyber threats with a high degree of accuracy and is also able to restore its systems and data after a cyber attack. However, company C can still improve its level of maturity in terms of incident response, being able to deal with cyber attacks effectively, as shown in Figure 4.6. These results are positive as they point to a lower risk that the company will be the target of cyber attacks. However, there is still room for improvement, which can help the company further reduce its risk.

Figure 4.6: Company C

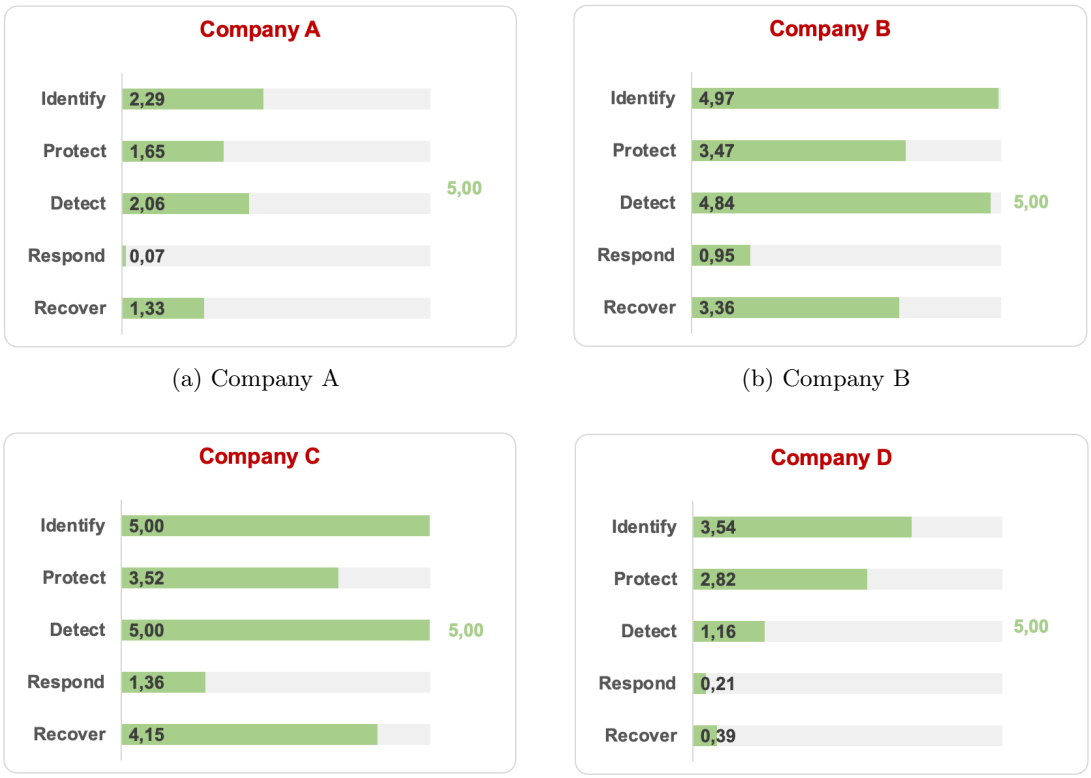
Company D

Company D has a very low level of cybersecurity maturity, both in terms of employee perception and when applied to experts perception. Like Company A, it presents poor results in practically all aspects of the NIST CSF framework, mainly in the Respond and Recover functions, as shown in Figure 4.7. Analysis of the study results shows that company D has a very low level of maturity in terms of threat identification and detection, incident response, and incident recovery. This means that the company is not well prepared to deal with cyber attacks. As seen previously, the results obtained are worrying with regard to possible cyber attacks, putting the company at risk of losing credibility or even having financial losses.

Figure 4.7: Company D

In the comparative analysis of the indices, shown in Figure 4.8, it is possible to observe that companies C and D have greater cybersecurity maturity compared to the other two. Furthermore, these two companies are the only ones that exceed the averages of this group in all five functions defined by NIST CSF. In the context of NIST's five functions, it is interesting to note that the Identify function presents the most positive indicators for all companies, followed by the Detect indicator. Another worrying fact is the Respond function, which is considerably inferior to other functions in all companies. This function records the lowest indicators, with the best result being 1.36 in Company C, classified as "very low". Based on the data collected, limitations that require attention were identified. Such limitations were classified according to the functions outlined by NIST CSF. In certain cases, these limitations are shared between the companies under analysis. Cybersecurity improvement proposals are structured according to the NIST CSF, following its hierarchy, and covering the categories that represent the main pillars of each area. As illustrated in the tables below, which present the thoughtful evaluations of experts, it is clear that the areas with the greatest need are "Respond" and "Recover". Additionally,

it appears that there is room for improvement in all organizations, with the continuous objective of creating a more prepared corporate environment. This is necessary to better face the numerous threats that arise, which bring with them a considerable potential for damage, whether financial, reputational, or even the company's operational continuity.



(a) Company A

(b) Company B

(c) Company C

(d) Company D

Figure 4.8: Comparison between companies

The suggestions for improvements in the cybersecurity area for the companies analyzed are detailed in Appendix **??**, divided according to the NIST CSF framework. Table A.1 presents the suggestions for the Identify function, Table B.1 presents the suggestions for the Protect function, Table C.1 presents the suggestions for the Detect function, Table D.1 presents the suggestions for the Respond function, and Table E.1 presents the suggestions for the Recover function.

Figure 4.9: NIST Framework Subgroup

The suggestions for improvement are based on the NIST CSF framework subgroups, which were identified as areas with potential for improvement. In this thesis, the suggestions were concentrated in the subgroups with the worst results, as presented in Figure 4.9, which presents the results of Company B, encompassing all the functions of the NIST CSF framework.

Chapter 5

Conclusions and Future Work

This master thesis research has contributed to the assessment and improvement of cybersecurity maturity in evaluated organizations, resulting in the creation of a maturity index based on NIST CSF. This index provides a comprehensive view of the security posture of organizations, revealing that, overall, they have an intermediate level of cybersecurity maturity, with significant differences among them.

It is crucial to emphasize the importance of prevention in cybersecurity. The creation of the index is just one step in strengthening organizational security, and it is essential to adopt proactive measures, such as the implementation of robust policies, employee awareness, and regular system updates. The results highlight the need for investment in preventive measures to enhance cybersecurity posture, along with providing specific recommendations to improve maturity in this context.

The findings of this study enable organizations to identify their strengths and weaknesses in cybersecurity, allowing the development of action plans to enhance their maturity. However, it is crucial to consider the study's limitations, such as the small sample size of four companies and the exclusive application of the NIST CSF. Future research could explore issues such as the impact of the maturity index on security posture, comparing organizations that adopt it as an indicator of cyber attacks with those that do not. Additionally, assessing the effectiveness of different preventive measures in various types of organizations and investigating future trends in cybersecurity maturity based on historical data and pattern identification.

References

[1] Steven Cockcroft. "What is the NIST Framework?" In: (2020). DOI: 10.1093/itnow/bwaa116. URL: https://doi.org/10.1093/itnow/bwaa116.

[2] Adenekan Dedeke. "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles". In: *IEEE Security Privacy* 15.5 (2017), pp. 47–54. DOI: 10.1109/MSP.2017.3681063.

[3] Juarez Frayssinet Esenarro. "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations." In: *Cuadernos de desarrollo aplicados a las TIC* (2021), pp. 123–141. DOI: 10.17993/3ctic.2021.102.123-141.

[4] Alex Grohmann. "Evolution of the Cybersecurity Framework". In: *ISSA Fellow* (2018).

[5] James E. Lerums. "Measuring the State of Indiana's Cybersecurity". In: *Purdue University Graduate School* (2019). DOI: 10.25394/PGS.7449230.v1.

[6] Sasawat Malaivongs, Supaporn Kiattisin, and Pattanaporn Chatjuthamard. "Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance". In: *Applied Sciences* 12.21 (2022). ISSN: 2076-3417. DOI: 10.3390/app122111174. URL: https://www.mdpi.com/2076-3417/12/21/11174.

[7] Poningsih Poningsih and Muhammad Ridwan Lubis. "ANALYSIS AND EVALUATION OF ACADEMIC INFORMATION SYSTEM SECURITY USING NIST SP 800-26 FRAMEWORK". In: *Sinkron : jurnal dan penelitian teknik informatika* 7.1 (Feb. 2022), pp. 267–273. DOI: 10.33395/sinkron.v7i1.11205. URL: https://jurnal.polgan.ac.id/index.php/sinkron/article/view/11205.

[8] "PRISMA". In: PRISMA - Transparent reporting of Systematic Reviews and Meta-Analyses. URL: http://prisma-statement.org.

[9] Lei Shen. "THE NIST CYBERSECURITY FRAMEWORK: OVERVIEW AND POTENTIAL IMPACTS". In: *Aspen Publishers, Inc.* (2014), pp. 3–6. ISSN: 10942904.

[10] Diah Sulistyowati, Fitri Handayani, and Yohan Suryanto. "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS". In: *JOIV : International Journal on Informatics Visualization* 4 (Dec. 2020). DOI: 10.30630/joiv.4.4.482.

[11] Hamed Taherdoost. "Understanding Cybersecurity Frameworks and Information Security Standardsmdash;A Review and Comprehensive Overview". In: *Electronics* 11.14 (2022). ISSN: 2079-9292. DOI: 10.3390/electronics11142181. URL: https://www.mdpi.com/2079-9292/11/14/2181.

[12] Nuno Teodoro, Luís Gonçalves, and Carlos Serrão. "NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements". In: *2015 IEEE Trustcom/BigDataSE/ISPA*. Vol. 1. 2015, pp. 418–425. DOI: 10.1109/Trustcom.2015.402.

Appendices

Appendix A

Improvement Suggestions - Function: Identify

Function: Identify

Companies	Category	Improvement Suggestions
A - D	Risk Management Strategy	1. Comprehensive Risk Assessment: Expand the scope of risk assessment, considering not only immediate threats, but also possible future scenarios.
		2. Classification of Critical Assets: Improve the process of classifying critical assets, identifying those that, if compromised, could result in substantial losses for the organization.
		3. Impact Assessment: Improve the assessment of the impact that the realization of different risks would have on business continuity and system integrity.
		4. Definition of Risk Metrics: Establish clear and measurable metrics for assessing identified risks. This will facilitate comparison over time and provide a solid basis for decision making.

Table A.1 continued from previous page

Companies	Category	Improvement Suggestions
		5. Integration of Stakeholders: Include different stakeholders in the risk management process, such as members of senior management, technical, and legal teams. Multidisciplinary collaboration will improve understanding of the risks and feasibility of mitigation strategies.
		6. Culture of Awareness: Foster an organizational culture focused on cyber risk awareness. Ongoing employee education and training on security best practices will contribute to a proactive posture in the face of threats.
A	Risk Assessment	1. Contextualization of Risks: Expand risk analysis, considering the specific operational context of each organization. By incorporating elements such as the mission, objectives, and regulatory environment, it will be possible to assess risks in a more accurate and personalized way.
		2. Scenario Analysis: Introduce the practice of analyzing risk scenarios, exploring different hypothetical situations that could result in exposure to threats.
		3. Risk Quantification: Incorporate quantitative approaches to risk assessment, assigning numerical values to threats and potential impacts.
		4. Vulnerability Assessment: Strengthen vulnerability analysis by carefully mapping systems and assets weaknesses.

Table A.1 continued from previous page

Companies	Category	Improvement Suggestions
		5. Business Impact Assessment: Expand the impact assessment to cover not only technical aspects but also operational, financial, and reputational impacts.
		6. Ongoing Assessment: Establish an ongoing risk assessment process rather than viewing it as a one-off event. Cybernetic dynamics demands an ever-evolving analysis, ensuring the adaptability of security strategies.
		Multidisciplinary Collaboration: Foster collaboration between technical, legal, and management teams, seeking an interdisciplinary analysis of risks. Different perspectives will contribute to a more comprehensive and grounded view.
D	Supply Chain Risk Management	1. Multidimensional Evaluation of Suppliers: Expand the evaluation of suppliers beyond the purely financial aspects, also incorporating cybersecurity criteria. This will ensure a more careful selection of business partners, minimizing exposure to possible risks.
		2. Resilience Analysis: Introduce a resilience analysis in vendor evaluation, assessing the ability to recover from cyber incidents.
		3. Ongoing Monitoring: Implement an ongoing monitoring system to track vendor activities and security posture over time.

Table A.1 continued from previous page

Companies	Category	Improvement Suggestions
		4. Third Party Assessment: Expand the risk assessment to include third parties with access to the supply chain.
		5. Diversification of Suppliers: Encourage the diversification of suppliers, reducing the concentration of dependence on a single provider.
		6. Emerging Risk Assessment: Incorporate emerging risk analysis into supply chain assessment, considering evolving threat scenarios.
		7. Interdepartmental Collaboration: Foster collaboration between procurement, information security and risk management departments. This multidisciplinary approach will enrich the risk analysis and facilitate the implementation of preventive measures.

Table A.1: Suggestions: Identify Function

Appendix B

Improvement Suggestions - Function: Protect

Function: Protect

Companies	Category	Improvement Suggestions
A	Maintenance	1. Update Policies: Establish clear and comprehensive policies for the continuous updating of systems and software.
		2. Patch Management: Implement an efficient patch management system with automated processes for identifying, testing, and deploying critical updates. This will reduce the window of exposure to potential attacks.
		3. Remote Maintenance Security: Strengthen security measures for remote maintenance activities, requiring multi-factor authentication, strong encryption, and real-time supervision of remote access sessions.

Table B.1 continued from previous page

Companies	Category	Improvement Suggestions
		4. Change Monitoring: Implement a real-time change monitoring system to detect unauthorized changes to systems during or after maintenance.
		5. Role-Based Access: Adopt a role-based access approach to maintenance activities, ensuring that only authorized personnel have access to critical systems.
		6. Post-Maintenance Penetration Testing: Perform regular penetration tests after maintenance activities to assess the resiliency of upgraded systems.
		7. Education and Awareness: Foster education and awareness among maintenance staff on cybersecurity best practices.
A - B - C - D	Data Security	1. Data Classification: Implement an effective data classification system, assigning sensitivity and restriction levels to each type of information.
		2. End-to-End Encryption: Adopt end-to-end encryption to protect data in transit and at rest.
		3. Granular Access Control: Implement an access control system with levels of granularity that allow only authorized personnel to have access to data relevant to their functions. This will minimize the risk of information being leaked or misused.

Table B.1 continued from previous page

Companies	Category	Improvement Suggestions
		4. Ongoing Monitoring: Establish an ongoing monitoring system to identify unusual behavior or suspicious activity in relation to data.
		5. Data Retention Policies: Define clear data retention policies, determining how long different types of information will be kept.
		6. Anonymization and Pseudonymization: Explore anonymization and pseudonymization techniques to reduce the identifiability of personal data while maintaining its usefulness for analysis and internal operations.
		7. Vulnerability Tests: Conduct regular vulnerability tests on the systems that house the data, identifying possible security breaches and correcting them promptly.
		8. Awareness Training: Promote regular training on data security awareness for all employees, ensuring that they understand the importance of protecting information and know how to do it properly.
B	Identity Management and Access Control	1. Multi-Factor Authentication (MFA): Expand the adoption of multi-factor authentication across all critical systems and resources. MFA provides an additional layer of security by requiring users to provide multiple authentication factors before gaining access.

Table B.1 continued from previous page

Companies	Category	Improvement Suggestions
		2. Strong Password Policies: Implement strict password creation and update policies, promoting strong and complex passwords. Also, encourage the use of password managers to prevent unsafe practices.
		3. Principle of Least Privilege: Adopt the principle of least privilege when granting access to resources and systems. Ensuring that users only have the permissions they need to perform their roles, thereby reducing the potential attack surface.
		4. Access Monitoring: Establish a real-time access monitoring system to detect unusual patterns or suspicious activity. This will allow for the early detection of unauthorized access attempts.
		5. Regular Access Review: Perform regular access permission reviews, ensuring that only active and authorized users have access to resources. This will minimize the risk of unauthorized access by former employees or inactive users.
		6. Identity Management Tools: Implement identity management tools that facilitate efficient and secure user provisioning and deprovisioning.

Table B.1 continued from previous page

Companies	Category	Improvement Suggestions
		7. Segregation of Duties: Ensure that users have distinct role assignments, preventing overlapping of permissions and minimizing the risk of internal abuse.
		8. Awareness Training: Promote regular awareness training on secure identity management and access control practices. This will ensure that employees understand the importance of protecting access credentials.

Table B.1: Suggestions: Protect Function

Appendix C

Improvement Suggestions - Function: Detect

Function: Detect

Companies	Category	Improvement Suggestions
A - D	Security Continuous Monitoring	1. Monitoring Automation: Implement monitoring automation tools to analyze logs and events in real time.
		2. Behavioral Analysis: Integrate behavioral analysis into systems and networks to identify deviations from normal patterns of activity. This will allow detection of threats that evade signature-based detection.
		3. Threat Intelligence: Integrate threat intelligence feeds to enrich monitoring context.
		4. Event Correlation: Implement event correlation systems to identify relationships between different events that may indicate an attack in progress.

Table C.1 continued from previous page

Companies	Category	Improvement Suggestions
		5. Malware Detection: Use advanced malware detection solutions that can identify malicious behavior and code patterns, even unknown variants.
		6. Prioritized Alerts: Configure monitoring systems to generate priority alerts based on the severity and potential impact of detected events.
		7. Post-Incident Analysis: Integrate post-incident analysis after the detection of a security event to assess the scope and potential harm of the incident.
		8. Monitoring Performance Assessment: Undertake regular assessments of monitoring performance, identifying areas where effectiveness can be improved.
		9. Training and Awareness: Promote regular training for security staff on best practices for continuous monitoring and how to interpret and respond to generated alerts.
A - D	Anomalies and Events	1. Defining Behavior Profiles: Develop normal behavior profiles for systems, users, and networks.
		2. Malicious Behavior Detection: Incorporate malicious behavior detection algorithms that can identify patterns of activity that are indicative of threats.

Table C.1 continued from previous page

Companies	Category	Improvement Suggestions
		3. Data Correlation: Implement data correlation systems that can analyze information from multiple sources to identify complex patterns of activity.
		4. Threat Intelligence: Integrate threat intelligence to enrich analysis of anomalies and events, enabling detection of known and emerging attacks.
		5. Contextualized Alerts: Configure detection systems to generate alerts that contain meaningful contextual information to facilitate effective response.
		6. Machine Learning and AI: Using machine learning and artificial intelligence techniques to improve the detection of subtle and unknown anomalies.
		7. Behavior Tests: Conduct regular simulation tests of anomalous behavior to assess the effectiveness of detection systems.
		8. Data Integration: Integrate data from multiple sources, such as system logs, network information and security events, for a comprehensive view of activities.
		9. Team Training: Invest in ongoing training for the security team to improve their skills in identifying and analyzing anomalies and events.

Table C.1: Suggestions: Detect Function

Appendix D

Improvement Suggestions - Function: Respond

Function: Respond

Companies	Category	Improvement Suggestions
A - B - C - D	Response Planning	1. Incident Response Team (IRT): Strengthen the structure and capacity of the incident response team, including defining clear roles and responsibilities, as well as ongoing training to keep skills up to date.
		2. Updated Response Plan: Keep an incident response plan up-to-date and accessible to all team members. This will ensure that everyone knows their roles and knows how to act in different scenarios.
		3. Training Scenarios: Conduct regular incident simulations to train staff and test the response plan in controlled situations.

Table D.1 continued from previous page

Companies	Category	Improvement Suggestions
		4. Effective Communication: Define clear internal and external communication procedures during an incident, ensuring that all relevant parties are informed in a timely manner.
		5. Recovery and Mitigation: Integrate recovery and mitigation measures into a comprehensive response plan to restore operational normality and minimize damage.
		6. Impact Assessment: Incorporate a detailed assessment of the potential impact of incidents, considering operational, financial and reputational aspects.
		7. Post-Incident Communication Strategy: Define a post-incident communication strategy to manage information disclosure and mitigate the impact on the organization's reputation.
		8. External Collaboration: Establish collaboration protocols with external entities, such as suppliers, partners and regulatory authorities, for a coordinated response.
		9. Ongoing Review: Conduct periodic reviews of the response plan to identify areas for improvement and adjust strategies based on lessons learned.

Table D.1 continued from previous page

Companies	Category	Improvement Suggestions
A - D	Analysis	1. Comprehensive Data Collection: Establish procedures for the comprehensive collection of relevant data during an incident, including system logs, network flows and other pertinent sources.
		2. Digital Forensics Techniques: Train the incident response team in advanced digital forensics techniques for in-depth analysis of compromised systems and identification of attack vectors.
		3. Data Correlation: Use tools and methods to correlate collected data and identify patterns that may indicate the origin and extent of the incident.
		4. Root Cause Analysis: Perform root cause analysis to identify the failures that allowed the incident to occur and implement appropriate corrective measures.
		5. Impact Assessment: Assess the incident's impact on different areas of the organization, including operations, finance, and reputation.
		6. Trend Analysis: Use trend analysis to identify recurring incident patterns and take proactive steps to prevent future recurrences.
		7. Intelligence Sharing: Integrate threat intelligence feeds to get up-to-date information on known and emerging threats.

Table D.1 continued from previous page

Companies	Category	Improvement Suggestions
		8. Detailed Documentation: Keep detailed records of all incident analysis steps, including results, conclusions and actions taken.
		9. Continuous Improvement: Conduct periodic reviews of past incident reviews to identify areas for improvement and adjust review processes as needed.
B	Improvements	1. Structured Post-Incident Assessment: Institute a structured post-incident assessment, involving all relevant parties, to identify strengths and weaknesses of the response and identify opportunities for improvement.
		2. Clear Corrective Actions: Define specific and measurable corrective actions based on lessons learned from previous incidents.
		3. Action Tracking: Implement a corrective action tracking system to ensure that they are effectively implemented and produce the desired results.
		4. Best Practice Standards: Incorporate best practice standards, such as NIST CSF recommendations, to consistently and comprehensively drive improvements.
		5. Innovation and Technology: Explore the use of emerging technologies, such as artificial intelligence and automation, to optimize post-incident response and analysis processes.

Table D.1 continued from previous page

Companies	Category	Improvement Suggestions
		6. Ongoing Training: Provide regular training to the incident response team, incorporating lessons learned and best practices identified.
		7. Periodic Reviews: Conduct periodic reviews of implemented improvements to assess their effectiveness and make adjustments as necessary.
		8. Knowledge Sharing: Foster a culture of knowledge sharing, allowing security teams to learn from incidents collaboratively.
		9. Transparent Communication: Maintain transparent communication about the improvements implemented and the results achieved, promoting trust between the interested parties.
D	Mitigation	1. Pre-Defined Action Plan: Develop predefined action plans for different types of cyber incidents, allowing for a quick and targeted response.
		2. Response Automation: Use automation tools to speed response to incidents, such as isolating compromised systems and blocking malicious activity.
		3. Network Isolation: Develop clear procedures to isolate compromised network segments, preventing the spread of threats.
		4. Rapid Security Updates: Ensure that critical security updates and patches are implemented quickly to reduce the risk of exploiting vulnerabilities.

Table D.1 continued from previous page

Companies	Category	Improvement Suggestions
		5. Backups and Restore: Create and maintain regular backups of systems and data, allowing quick restoration in case of incidents.
		6. Post-Mitigation Monitoring: Implement continuous post-mitigation monitoring to verify the effectiveness of the actions taken.
		7. Response Testing: Perform regular incident response testing to validate the effectiveness of mitigation plans.
		8. Post-incident Review: Conduct post-incident reviews to assess the effectiveness of mitigation actions and identify opportunities for improvement.
		External Collaboration: Establish collaboration protocols with vendors, partners, and external security organizations for coordinated mitigation.

Table D.1: Suggestions: Respond Function

Appendix E

Improvement Suggestions - Function: Recover

Function: Recover

Companies	Category	Improvement Suggestions
A - D	Recovery Planning	1. Setting Recovery Objectives: Establish clear recovery objectives for systems, data, and operations, defining acceptable recovery times and availability targets.
		2. Assigned Recovery Team: Designate a recovery team responsible for coordinating recovery activities in the event of an incident.
		3. Detailed Recovery Plan: Develop a detailed recovery plan with step-by-step procedures for restoring critical systems and operations.
		4. Prioritization of Recovery: Identify critical systems and resources that require priority recovery and ensure these are the first to be restored.

Table E.1 continued from previous page

Companies	Category	Improvement Suggestions
		5. Recovery Tests: Conduct regular recovery tests to validate the plan's effectiveness and identify potential gaps.
		6. Backups and Storage: Ensure backups are up-to-date and securely stored, allowing critical data recovery.
		7. Recovery Communication: Establish internal and external communication protocols during recovery to keep all interested parties informed.
		8. Post-Recovery Monitoring: Implement continuous post-recovery monitoring to verify the stability of restored systems.
		9. Detailed Documentation: Keep detailed records of all recovery steps, including decisions made and results achieved.
		10. Continuous Update: Keep the recovery plan updated as the technology infrastructure and organizational processes evolve.
A - D	Improvements	1. Structured Post-Recovery Assessment: Institute a structured post-recovery assessment, involving all stakeholders, to identify recovery strengths and weaknesses and identify opportunities for improvement.
		2. Clear Corrective Actions: Define specific and measurable corrective actions based on lessons learned from previous incidents.

Table E.1 continued from previous page

Companies	Category	Improvement Suggestions
		3. Action Tracking: Implement a corrective action tracking system to ensure that they are effectively implemented and produce the desired results.
		4. Best Practice Standards: Incorporate best practice standards, such as NIST CSF recommendations, to consistently and comprehensively drive improvements.
		5. Innovation and Technology: Explore the use of emerging technologies to streamline recovery processes and accelerate service restoration.
		6. Ongoing Training: Provide regular training to the recovery team, incorporating lessons learned and best practices identified.
		7. Periodic Reviews: Conduct periodic reviews of implemented improvements to assess their effectiveness and make adjustments as necessary.
		8. Knowledge Sharing: Foster a culture of knowledge sharing, allowing recovery teams to learn from past experiences.
		9. Transparent Communication: Maintain transparent communication about the improvements implemented and the results achieved, promoting trust between the interested parties.

Table E.1 continued from previous page

Companies	Category	Improvement Suggestions
B - D	Communications	1. Pre-Defined Communication Plan: Develop a pre-defined communication plan that covers the different recovery scenarios, identifying the interested parties, the communication channels and the messages to be transmitted.
		2. Assigned Communications Team: Designate a team responsible for coordinating communication during the recovery process, ensuring that information is transmitted in a clear and coordinated manner.
		3. Internal and External Communication: Establish protocols for communication both internally, with the teams involved in the recovery, and externally, with partners, suppliers, customers and regulatory authorities.
		4. Consistent Messages: Ensure that the messages transmitted are consistent and aligned with the current situation, avoiding conflicting information.
		5. Transparency and Regular Updates: Maintain transparent communication by providing regular updates on recovery progress, even if it means no significant updates.
		6. Diverse Communication Channels: Utilize a variety of communication channels, such as email, instant messaging, and collaboration platforms, to effectively reach stakeholders.

Table E.1 continued from previous page

Companies	Category	Improvement Suggestions
		7. Feedback and Questions: Provide channels to receive feedback from stakeholders and respond to questions, demonstrating accountability and commitment to resolution.
		8. Communication of Completion: Communicate clearly when the recovery process is complete and normal operations are restored.
		9. Post-Recovery Assessment: Conduct post-recovery assessments to review communication effectiveness, identify areas for improvement, and adjust processes as needed.

Table E.1: Suggestions: Recover Function