INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Assessment of Iscte's Cybersecurity Capabilities

João Miguel Jorge Manuelito Faria

Master’s degree in Computer Engineering

Supervisor:
PhD Carlos Serrão, Associate Professor,
Iscte - Instituto Universitário de Lisboa

Co- Supervisor:
PhD João Pedro Oliveira, Assistant Professor,
Iscte - Instituto Universitário de Lisboa

November, 2022

TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Assessment of Iscte's Cybersecurity Capabilities

João Miguel Jorge Manuelito Faria

Master’s degree in Computer Engineering

Supervisor:
PhD Carlos Serrão, Associate Professor,
Iscte - Instituto Universitário de Lisboa

Co- Supervisor:
PhD João Pedro Oliveira, Assistant Professor,
Iscte - Instituto Universitário de Lisboa

November, 2022

Acknowledgements

To my family and girlfriend, for their friendship, encouragement and caring all these years, for always providing everything I needed to face all challenges and without who this work would not be possible.

To Professors Carlos Serrão and João Oliveira, for all their insight, suggestions, and contributions to this work, as for their availability and readiness to solve the issues found.

To all my friends and colleagues for their friendship and support.

To Iscte – Instituto Universitário de Lisboa and all its personnel for providing the opportunity.

To everyone, my sincere gratitude.

Resumo

À medida que o mundo avança para um ambiente mais digitalizado, a cibersegurança é cada vez mais crucial para o sucesso de cada organização. Além disso, tem havido um aumento do número de ciberataques. Por esta razão, foi criada legislação para mitigar estas questões e para elevar os níveis de cibersegurança. Foram criados quadros para aumentar este nível, de modo a cumprir as legislações. Contudo, para a maioria das organizações é difícil avaliar as suas capacidades de cibersegurança e saber onde melhorar. Para abordar este problema, esta dissertação visa responder à questão de investigação "Será possível conceber um sistema para facilitar a Avaliação das Capacidades de Cibersegurança?", desenvolvendo um sistema que permita às organizações autoavaliarem as suas capacidades de cibersegurança com facilidade. A solução proposta permite aos supervisores de cibersegurança distribuir responsabilidades de resposta entre outros membros da organização, alcançando melhores interpretações. Isto facilita uma resposta fácil e atempada, permitindo que a organização avalie corretamente as suas capacidades atuais. Aplicando o questionário e o sistema proposto, é possível conseguir uma avaliação mais assertiva.

Palavras-Chave: Cibersegurança, Avaliação, Administração, Conformidade.

Abstract

As the world moves toward a more digitalised environment, cybersecurity is increasingly crucial for every organization's success. Furthermore, there has been an increase to the number of cyber-attacks. For this reason, legislation was created to mitigate these issues and to raise cybersecurity levels. Frameworks have been created to increase this level as to comply with legislations. However, for most organizations it is difficult to assess their cybersecurity capabilities and to know where to improve. To address this problem, this dissertation aims to answer the research question “Is it possible to design a system to facilitate Cybersecurity Capabilities Assessment?” by developing a system to enable organizations to self-assess their cybersecurity capabilities with ease. The proposed solution allows cybersecurity supervisors to distribute answering responsibilities between other organization members, reaching better interpretations. This facilitates an easy and timely response, allowing the organization to correctly assess their current capabilities. Applying the questionnaire and the system proposed a more assertive assessment can be achieved.

Keywords: Cybersecurity, Assessment, Governance, Compliance.

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

CIA	Confidentiality, integrity, and availability
CNCS	Centro Nacional de Cibersegurança
CSF	Cybersecurity Framework
DSRM	Design Science Research Methodology
ENISA	European Union Agency for Cybersecurity
EU	European Union
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IS	Information Security
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
QACCS	Quadro de Avaliação de Capacidades de Cibersegurança
QNRCS	Quadro Nacional de Referência para a Cibersegurança

Chapter 1 - Introduction

This chapter makes an introduction to the topic, explaining the context and motivation that led to the choice and elaboration of the research developed, as well as the proposed objectives and the methodology used, and presents the five chapters that structure this work.

1.1 Context and Motivation

Nowadays, given the digital nature of most business movements, organisations need to feel the security necessary for the compliance of their success. From this point of view, cybersecurity is critical to the protection of data, networks, systems, and programs. As cyberattacks against organizations increase and improve [1], [2], the need for cybersecurity is ever-growing.

New Portuguese Legislation 46/2018[1] establishes Cyberspace Security Legal Regime, transposing the Network Information System (NIS) directive 2016/1148[2], relating to measures dedicated to ensuring a high common level of security in networks and data in all European Union. Moreover, the decree-law 65/2021[3] Regulates the Cyberspace Security Legal Regime and sets some deadlines for the implementation of measures.

Organizations, when not applying these measures, are subject to reputational, digital, economic, physical, and social impacts [2]. According to [2] the most targeted sector is public administration and government.

ISCTE – Instituto Universitário de Lisboa, Iscte, is a public institution and must comply with the specified Cybersecurity Regulations.

To address the need to comply with regulations across the country, the Portuguese National Cybersecurity Centre (CNCS – Centro Nacional de Cibersegurança) issued a document called the "National Cybersecurity Framework" (QNRCS - Quadro Nacional de Referência para a Cibersegurança) [3], as well as the "Cybersecurity Assessment Framework" (QACCS - Quadro de Avaliação de Capacidades de Cibersegurança) [4]. This Framework allows organizations to easily identify their current Cybersecurity capabilities and, consequently, possible deviations from an ideal situation.

[1] https://dre.pt/dre/detalhe/lei/46-2018-116029384
[2] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[3] https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988

The Framework describes a set of processes for identification of this capability (Identify, Protect, Detect, Respond and Recover) and three levels of capability (Basic, Intermediate, and Advanced) duly aligned with the sector's best practices.

The Cybersecurity Assessment Framework, QACCS, is a document that, due to its specificity, contains a set of features that are difficult to interpret and apply. Moreover, the knowledge necessary to interpret QACCS isn't gathered in a single person, so the ability to spread across multiple members of the organization according to their expertise is essential to success.

To expedite the implementation of the Framework aforementioned, this work aims to develop a system to be used as a self-assessment tool for an organization's cybersecurity capabilities.

1.2 Goals and Research Question

The main goals of this dissertation are:

- Study QACCS and QNRCS proposed by CNCS, as well as other international references in this field.
- Apply QACCS to Iscte – Instituto Universitário de Lisboa, with the purpose of identifying and assessing Iscte's Cybersecurity Capabilities.
- Identify existing deviations that could lead to improvements in the Cybersecurity Capabilities.
- Study and design a system that allows to register and control the Cybersecurity Capabilities, as well as recording evidence that corroborates the level of Cybersecurity Capabilities at any given moment of the organization.

  The study focuses on the following research question:

  "Is it possible to design a system to facilitate Cybersecurity Capabilities Assessment?"

1.3 Methodology

This dissertation has followed Design Science Research Methodology (DSRM), which defines a six-stage process, problem identification and motivation, objectives, design and development, demonstration, evaluation, and communication. [5]

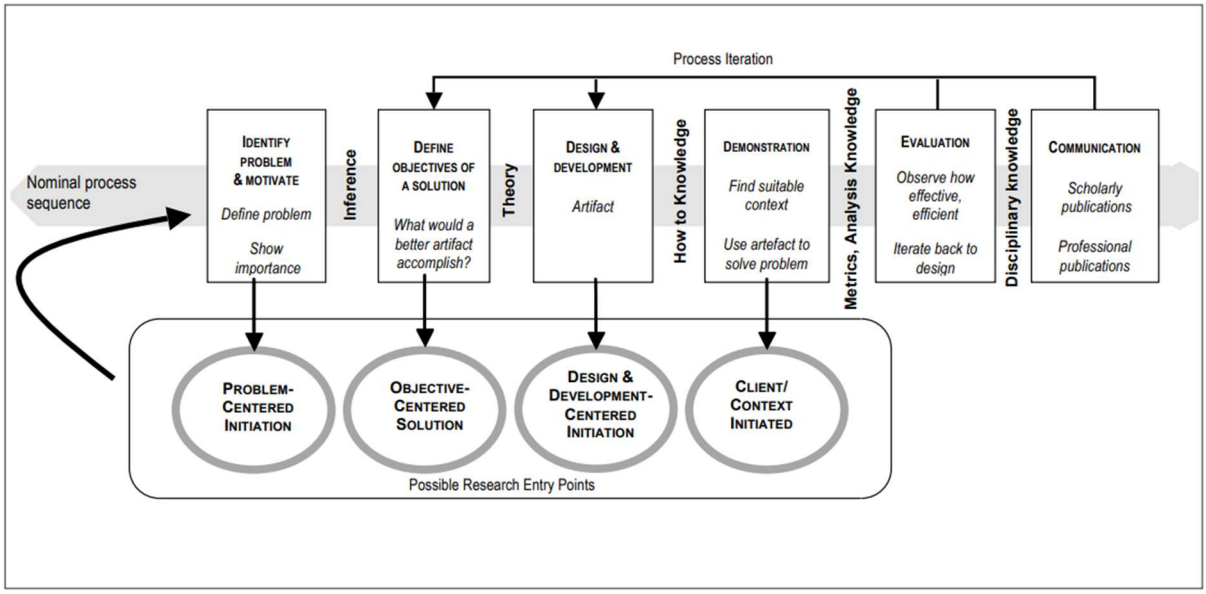


Figure 1: Design Science Research Methodology (DSRM) Process Model [5]

1. Problem identification and motivation

The problem was identified and explained in Chapter 1. There is a critical need to assess Cybersecurity capabilities and identify weaknesses. This is becoming a priority in almost any environment, given the importance of Cybersecurity in every business.

2. Objectives

The solution objectives are to develop a tool capable of assessing Cybersecurity Capabilities.

3. Design and development

The design and development of this tool are presented in Chapter 3.

4. Demonstration

Application and experimenting with the framework will be its demonstration.

5. Evaluation

Critical thinking and objective validation will be the evaluation.

6. Communication

This dissertation, and its public presentation, are the communication to the audience.

1.4 Structure

This document is structured into five different chapters.

The first chapter introduces the topic, specifies its objectives, gives context and motivation, as well as presents the methodology used.

The second chapter develops the importance of the topic, provides important concepts, and explores current solutions.

The third chapter describes the work developed, the options taken, and the choices made.

The fourth chapter presents the validation and evaluation process.

The fifth, and final chapter concludes this dissertation, describing the results obtained, the limitations encountered and suggestions for future work.

Chapter 2 - State of the Art

This chapter provides additional context, elaborates how the literature review was performed, introduces important concepts, and examines the existing related work.

2.1 Introduction

Given the evolving characteristics of the organisational era, cybersecurity was developed as a natural response to the increase in the importance of computers and computerized systems, and its purpose is to protect networks, data, and devices from attacks. There have been concerns about protecting information since 1967 [6] and it is still an object of reflection and analysis [7]. In this view, cybersecurity is critical to the protection of data, networks, systems, and programs. As cyberattacks become more and more effective and frequent [1], [8], the demand for cybersecurity keeps increasing.

Given the constant progress of systems and techniques, there is a recurrent insurgence of new threats. At the same time, motivated by the continuous increase in digitalisation, the possible impact of these threats escalates.

The most prominent threats can be classified, according to the European Union Agency for Cybersecurity (ENISA), into eight prime threat groups: ransomware, malware, social engineering, threats against data, threats against availability – denial of service (DoS), threats against availability – internet threats, disinformation – misinformation, and supply chain attacks [2].

As has been the case in previous years, 2021 registered an increase in attacks targeting the data of organizations [8], [9].

Humans played a part in 82% of breaches in the past year [10]. Said breaches are security events that compromise the integrity, confidentiality, or availability of an information asset, with confirmed disclosure of data [10].

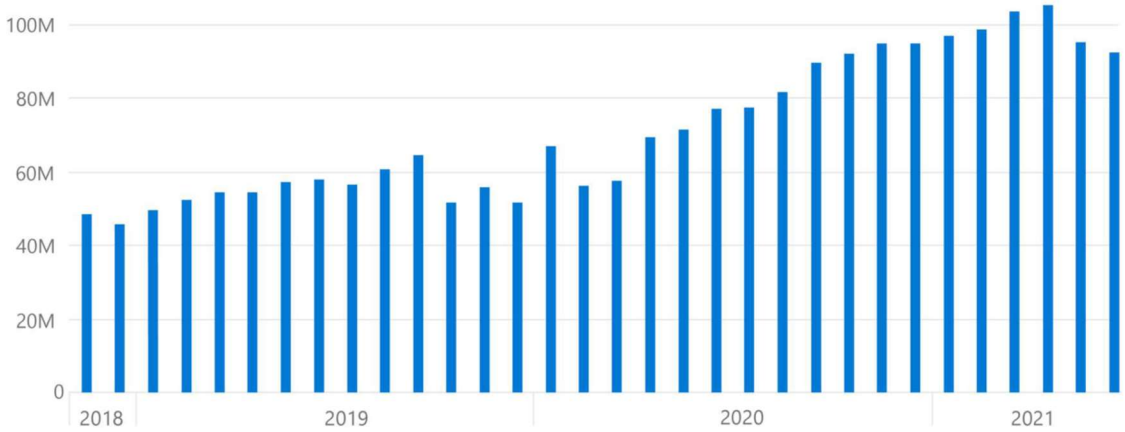


Figure 2: Microsoft's Defender - Ransomware encounter rate (machine count): Enterprise customers [8]

Ranking at the top between July 2021 and July 2022 are ransomware and threats against availability [2].

The count of ransomware is ever-increasing [8], impacting 37% of organizations in 2021 [9], which was an increase of 93% in a year [11]. This increase in cybersecurity attacks ultimately decreases companies' stock market value [12], which in turn negatively impacts the organizations.

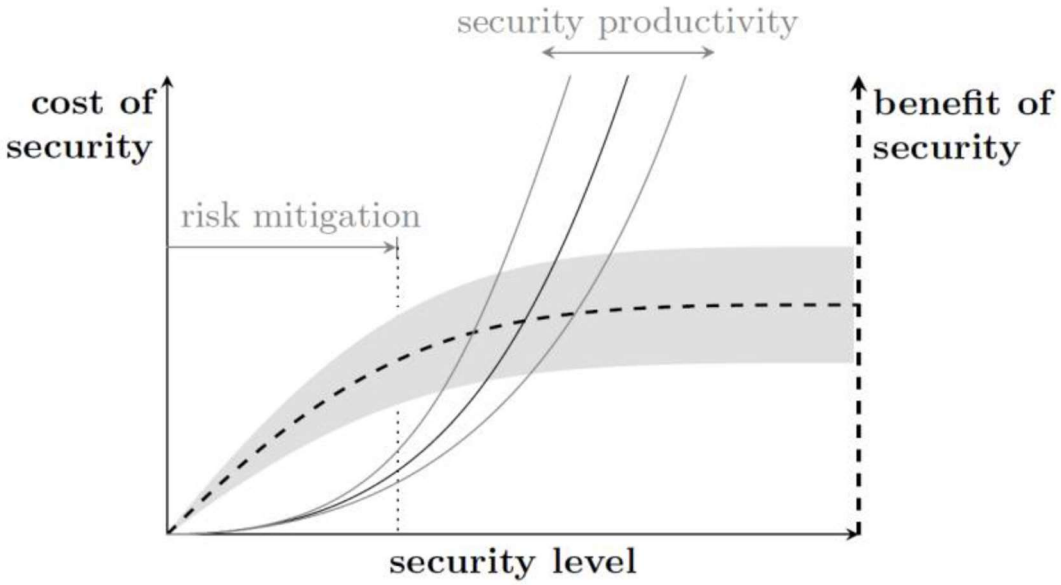


Figure 3: Decomposition of the security production function into two steps [13]

To increase the security level of a corporation, money must be invested. However, the cost of security increases at a far greater pace than the benefit collected, and thus care must be applied to achieve adequate balance.

However, there is an urge to increase cybersecurity, and, while every user is important, the lead must come from managers and be aligned throughout the organization [14].

2.2 Systematic Literature Review

The systematic literature review was performed by following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [15]. This approach allowed for a methodical step-by-step process.

Figure 4, based on [15], provides a schematic of the process.

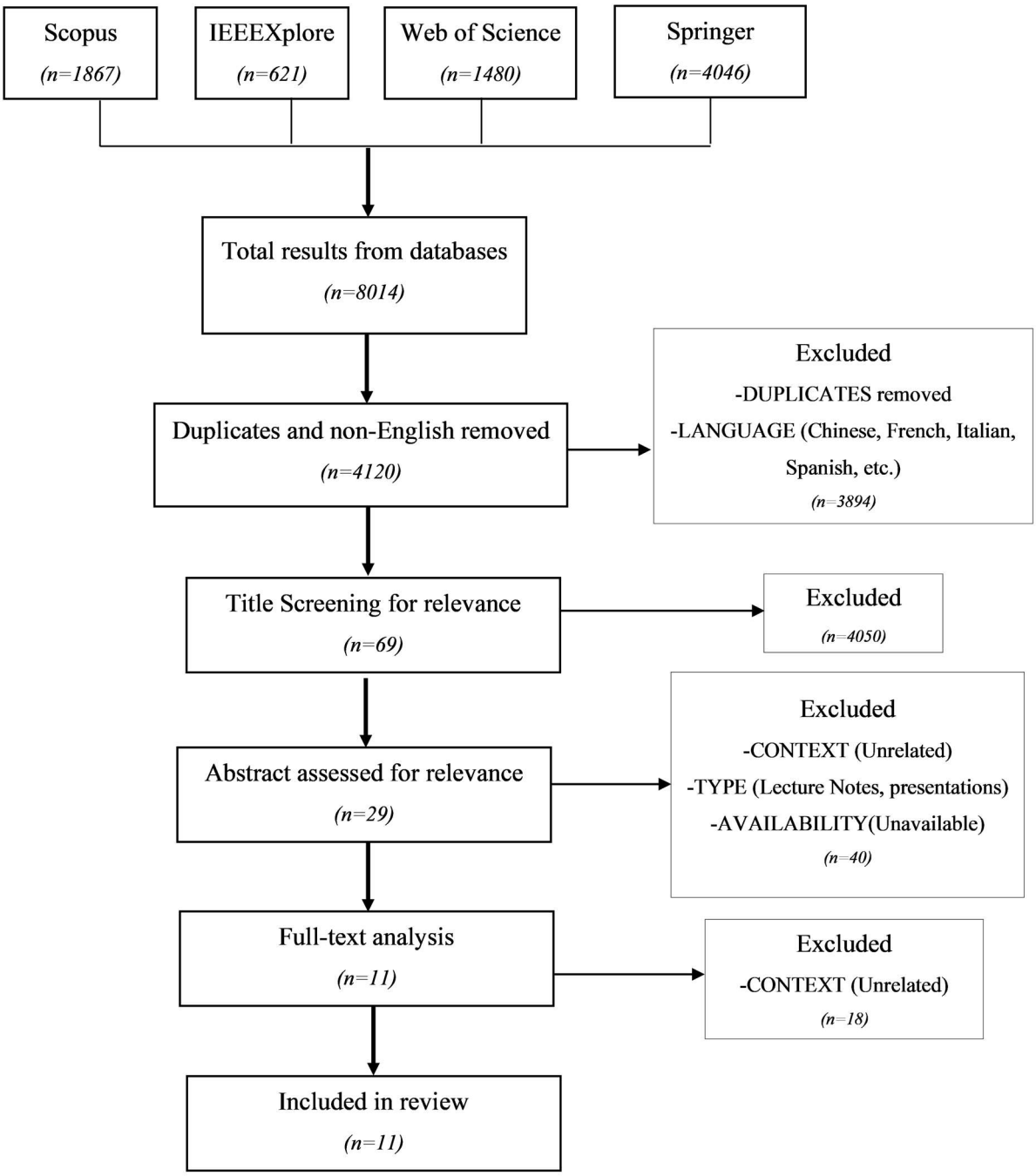


Figure 4: PRISMA Chart for the review process

The keywords chosen revolved around the word *cybersecur**, using a wildcard to increase the number of hits. Along with it, several other words were chosen to specify the topic. *Compliance* and *governance* refer closely to the assessment of capabilities. *Framework* and *application* were used to include results that specify a more practical approach, but together with *risk* to ensure that only results of interest would be considered.

cybersecur AND compliance; cybersecur* AND governance; cybersecur* AND risk AND application; cybersecur* AND risk AND framework*

The searches were performed on 4 databases, Scopus, IEEE Xplore, Web of Science, and Springer, chosen for their relevance in the field, during the month of January 2022. The date range searched was January 2012 – January 2022. Table 1 discriminates the results returned per each database for each of the search terms used.

Table 1: Search terms and count of results by database

Search terms vs database	Scopus	IEEE Xplore	Web of Science	Springer
cybersecur* AND compliance	318	103	265	853
cybersecur* AND governance	388	71	343	522
cybersecur* AND risk AND application	512	246	367	1434
cybersecur* AND risk AND framework	649	201	505	1237
Total with duplicates	1867	621	1480	4046

This search returned a total of 8014 results from all databases. After de-duplicating and the removal of non-English documents from the results 4120 remained. Screening the title for relevance left 69 results of interest, and further inspection using the abstract, document type, as well as availability, converged to 29 results. These were fully read and analysed and 18, while insightful, were excluded for relevance. The remaining 11 were included in the review and are listed in Table 2.

Table 2: Papers included in review

Authors	Title	Year
Govender S.G., Kritzinger E., Loock M.	A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture	2021
Maleh Y., Sahid A., Belaissaoui M.	A MATURITY FRAMEWORK FOR CYBERSECURITY GOVERNANCE IN ORGANIZATIONS	2021
Ibrahim A., Valli C., McAteer I., Chaudhry J.	A security review of local government using NIST CSF: a case study	2018
von Solms B., von Solms R.	Cybersecurity and information security - what goes where?	2018
Chmielecki T., Cholda P., Pacyna P., Potrawka P.,	Enterprise-oriented cybersecurity management	2014

Rapacz N., Stankiewicz R., Wydrych P.		
Sterbenz J.P.G., Çetinkaya E.K., Hameed M.A., Jabbar A., Qian S., Rohrer J.P.	Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation	2013
Garfinkel S.L.	Inside risks the cybersecurity risk	2012
Williams K.L.	Management Wake-Up and Govern: The Era of the Cyber Security Governance	2014
Teodoro N., Goncalves L., Serrao C.	NIST CyberSecurity Framework Compliance A Generic Model for Dynamic Assessment and Predictive Requirements	2015
Kohler C.	The EU Cybersecurity Act and European standards: an introduction to the role of European standardization	2020
Markopoulou D., Papakonstantinou V., de Hert P.	The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation	2019

An additional Google search was conducted for important definitions, concepts, and regulations. All data was selected from credible sources such as government entities, and professional standard organizations.

2.3 Definitions

2.3.1. Cybersecurity

The International Organization for Standardization (ISO) defines, in ISO/IEC 27000:2018, *Information Security* (IS) as the preservation of Confidentiality, Integrity, and Availability (CIA) of information [16]. The first aspect, confidentiality, is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes [16], which is of uttermost importance when it comes to important information. The second aspect, integrity, is the property of accuracy and completeness [16], such as the information being ready and correct for usage. The final aspect, availability, is the property of being accessible and usable upon demand by an authorized entity [16], keeping everything ready for use when necessary.

According to ENISA, cybersecurity opposes to cyber incidents, covering all aspects of preventing, forecasting, tolerating, mitigating, removing, analysing, and investigating said incidents. Cybersecurity should, considering the multiple components of cyberspace, also cover

multiple attributes, Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability, Robustness, Survivability, Resilience, Accountability, Authenticity and Non-repudiation. [17]

Cybersecurity, according to the National Institute of Standards and Technology (NIST), is the ability to protect or defend the use of cyberspace from cyberattacks [18]. Cyberspace is defined, in the same document, as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cybersecurity is defined as part of Information Security, that specifically focuses on protecting the CIA of digital information assets against any threats [19]. Its aim is to protect against the risks that arise as most organizations utilize cyberspace for critical business processes [19].

2.3.2. Risk

ISO always defines Risk as an effect of uncertainty on objectives [16], with an effect being a deviation from the expected, and objective being the result to achieve. Furthermore, a Threat is the potential cause of an unwanted incident, which can result in harm to a system or organization [16]. The purpose of cybersecurity is to defend the organization against these threats.

As risks increase [19], there is a need for organizations to implement machine-assisted decision-making tools to minimize said risks [20].

2.3.3. Resilience

As stated, there is a rising risk that challenges the normal operation of organizations and, despite the increase in focus towards cybersecurity, systems are not becoming more cyber secure [21], [22].

The answer to this problem is resilience [22]. Cyber resilience is defined by NIST as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources [23]. A resilient organization can still fulfil their objectives even when being attacked [23].

2.4 Organizations

2.4.1. National Institute of Standards and Technology (NIST)

NIST published, in February 2014, the NIST Cybersecurity Framework (CSF), which was revised in 2018 [24]. This framework serves as guidance for assessing, managing, and reducing cybersecurity risk.

The NIST CSF is organized into five functions, Identify, Detect, Protect, Respond, and Recover. These functions are divided into 23 total categories, which in turn define multiple subcategories, adding up to 108 total subcategories in all categories [24].

2.4.2. European Union Agency for Cybersecurity (ENISA)

The European Commission founded, by Regulation (EC) No 460/2004[4], the European Network and Information Security Agency to lead the way in responding to information security problems and issues. ENISA has since changed its name to European Union Agency for Cybersecurity and keeps dedicated to achieving and maintaining a high level of cybersecurity across Europe.

The NIS directive provides legal measures to raise the level of cybersecurity in the European Union (EU), being the first EU-wide legislation on cybersecurity. While being a late response [25], this directive aims to increase trust throughout the EU, despite the intense cooperation required across the Union [26].

2.5 National Cybersecurity Framework (QNRCS)

Portuguese decree-law 46/2018 transposes the NIS directive, implementing the EU-required measures for a high level of common security in network and information security. This law assigns to CNCS the status of National Cybersecurity Authority.

CNCS established QNRCS as a tool to support the timely and systematic response to all threats and incidents that undermine the benefits of networks and information systems [3], to increase the general level of cybersecurity across organizations.

This Framework was created with the same cybersecurity functions as NIST's framework, Identify, Protect, Detect, Respond, and Recover, as well as following the same structure with categories and subcategories.

[4] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

The Framework has 23 total categories spread between the five functions and 102 subcategories. Each of these subcategories have, where applicable, a Technical Implementation, as well as a Process Implementation and Evidence [3].

The mentioned topics enable organizations to evolve step by step towards a more cyber-secure environment. However, the guidelines provided are broad, representing key objectives, rather than a checklist of actions.

The Framework is also adaptable and should be used by each organization combined with critical thinking, as the demands of some recommendations might not be proportional to the size and scope of the organization.

2.5.1. Cybersecurity Assessment Framework (QACCS)

The Cybersecurity Assessment Framework [4] is a supplement to the National Cybersecurity Framework, and it presents, for each cybersecurity measure in QNRCS, three levels of capability to enable organizations to fulfil the defined objectives, according to their context and size. Table 3 describes the three proposed levels.

Table 3: Cybersecurity Capability Levels, adapted from [4]

Capability Level	Description	Evidence
1 – Initial	Basic security measures that could be implemented to achieve the security goal, namely in *ad-hoc*, isolated and non-formal initiatives.	Evidence of implementation of Initial level measures.
2 – Intermediate	Security measures that meet most cases and needs to achieve information security objectives. The measures are formally achieved.	Evidence of implementation of the Intermediate level measures.
3 - Advanced	Advanced security measures involving continuous monitoring of controls, recurrent assessment, and review, considering changes, incidents, tests, and exercises, for proactive improvement.	Evidence of implementation of Advanced level measures.

These levels of capability are cumulative, meaning that for an organization to position, in a specific objective at level 3 – Advanced, they will have to implement the security measures of levels 1 – Initial, and 2 – Intermediate.

2.6 Frameworks for Cybersecurity maturity analysis

The NIST CSF [24] is being deployed in various locations [27], and with high levels of influence and success [27]–[29]. This makes a great case for the importance of cybersecurity maturity analysis.

Maleh et al. [30] propose a cybersecurity maturity framework to evaluate the organization divided into different categories. They also present a use case using a questionnaire with explicit answers, that, when combined with the framework, provide a numerical result that represents the level of cybersecurity maturity [30].

Aliyu et al. [31] present a maturity model integrating several regulations focused on Higher Education Institutes. The proposed maturity assessment model has 15 requirements divided into 3 groups, Identify, Protect & Detect, and Respond & Recover [31]. The maturity model proposed has 6 levels of maturity, from 0 to 5, which build on each other, meaning a certain level can only be assigned if all the lower levels are completed first [31].

Govender et al. [32] propose a tool structured into three features, assessment of information security risk, reduction of information security cost and sustainability of information security culture. Each feature has a set of questions divided into evaluation areas, accumulating 83 questions in 21 areas across all three features [32]. The questions follow a simple scoring mechanism of one point for “yes” and zero points for “no” [32].

2.7 Conclusions

This chapter outlines the related work found as well as provides important definitions and concepts required.

The literature reviewed performed showed that, while there are multiple frameworks proposed and being applied in multiple contexts, there is a distinct lack of easy-to-use or practical implementations, despite some of the related work proposing a questionnaire-based approach. Nevertheless, these works still have a degree of difficulty in applicability.

CNCS, however, proposes a cybersecurity check-up[5] aimed for easier interpretation and with a question-based approach. This tool, while interesting, still requires a single user to answer all questions, which makes applicability for big organizations difficult. Nonetheless it is still a step in the right direction.

[5] https://cibercheckup.cncs.gov.pt/

Chapter 3 - Proposed Solution

This chapter presents the developed solution to fulfil the goals outlined in section 1.2, which comprises two parts, a questionnaire, and a web-based system.

3.1 Introduction

The first part of the proposed solution, the questionnaire was created in accordance with CNCS' assessment framework QACCS, and for each of the cybersecurity functions, Identify, Protect, Detect, Respond, and Recover questions were created from each subcategory of the framework. In total there are 102 questions divided according to Table 4.

Table 4: Distribution of questions

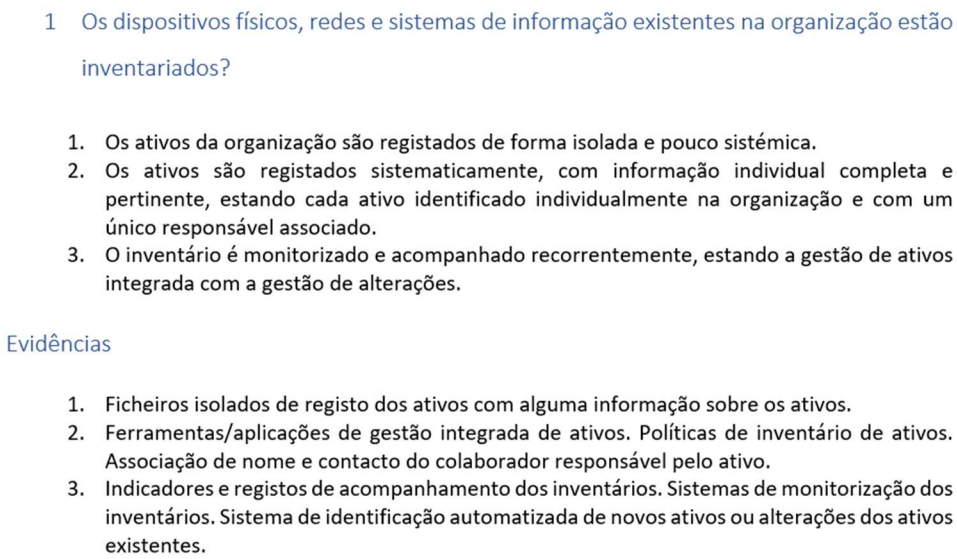
Identify	25 questions
Protect	38 questions
Detect	18 questions
Respond	16 questions
Recover	5 questions
Total	102 questions

The developed system has two types of users, a basic user, and a more advanced user - a supervisor with more permissions. Both user types work together to assess the organization's cybersecurity capabilities. The supervisors can upload questions to the database and distribute them among all the personnel as well as view the status of the organization's cybersecurity. All personnel can answer the questions attributed to them, along with supplying evidence to support the answers provided.

3.2 Questionnaire

For each one of the 102 subcategories in QACCS a question was created, modelled after the cybersecurity measure proposed by CNCS. Then three answering options were created, one for each level of maturity, basic, intermediate, and advanced, corresponding to a value of 1, 2 and 3, respectively. The text for each option was shaped by the measures proposed for each level of capacity. Moreover, the evidence required to prove the achievement of said level of capability were registered, according to the same assessment framework.

Each question was structured like the example in Figure 5 indicates.



1 Os dispositivos físicos, redes e sistemas de informação existentes na organização estão inventariados?

1. Os ativos da organização são registados de forma isolada e pouco sistémica.
2. Os ativos são registados sistematicamente, com informação individual completa e pertinente, estando cada ativo identificado individualmente na organização e com um único responsável associado.
3. O inventário é monitorizado e acompanhado recorrentemente, estando a gestão de ativos integrada com a gestão de alterações.

Evidências

1. Ficheiros isolados de registo dos ativos com alguma informação sobre os ativos.
2. Ferramentas/aplicações de gestão integrada de ativos. Políticas de inventário de ativos. Associação de nome e contacto do colaborador responsável pelo ativo.
3. Indicadores e registos de acompanhamento dos inventários. Sistemas de monitorização dos inventários. Sistema de identificação automatizada de novos ativos ou alterações dos ativos existentes.

Figure 5: Example of Question in Questionnaire

Moreover, the same 102 questions were structured into a JSON [33] file to uniform and simplify their display. An example of a question in the JSON format is Figure 6.

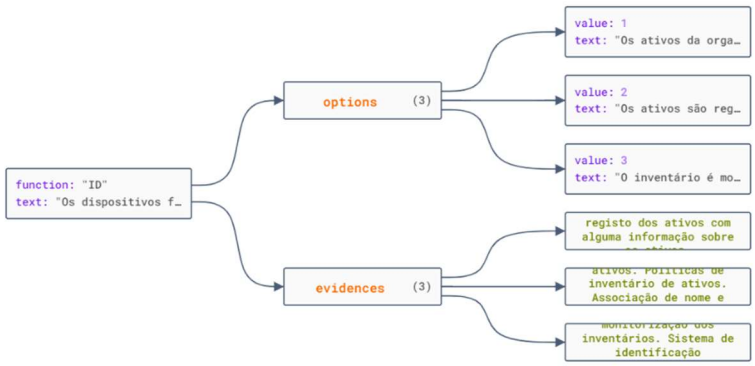


Figure 6: JSON Example of a Question object

The full Questionnaire is available in Appendix A for a more thorough analysis.

This Questionnaire provides an easier interpretation of QACCS, modelled through each cybersecurity measure presented, enabling ease of use without sacrificing meticulousness. These questions present a more definitive view of each measure and enable definitive answers for each of the maturity levels present in each subcategory of QACCS.

3.3 User Stories

User Stories were adopted to better plan which steps to take to develop the system. User Stories describe functionalities that will be available in a product [34]. This approach focuses the development on the user's valued features.

One of the earliest formulations of a user story is the Connextra template, incorporating roles into the stories [34]. Moreover, this template is the most popular one [35]. Therefore, this was the template chosen to be applied.

As a (role), I want to (capability), so that (benefit).

The following table describes the user stories created.

Table 5: User Stories

#ID	**As a…**	**I want to…**	**So that…**
US01	New User	create an account	I can access the system and be registered in it
US02	Admin	import questions	load the framework with the necessary questions to evaluate the cybersecurity capabilities
US03	Supervisor	attribute questions to a user	delegate answering to the qualified personnel
US04	User	answer questions	provide information to assess cybersecurity capabilities
US05	User	upload evidence files	support statements
US06	Supervisor	view the current report	understand the organization's cybersecurity capability status at a given time
US07	Supervisor	view the detailed report by function	view which questions haven't been answered

The acceptance criteria for each of the user stories presented is in Table 6, where the user story validation is performed, in section 4.1.

3.4 Technologies used

To fasten the development of the tool, a web development framework was employed. The chosen framework was Django [36] because it is free and open source, is very well documented and has a large community, which in turn means there is plenty of support available, as well as multiple libraries to solve most common problems. The version of Django used was 4.0.6, built on top of Python version 3.10.4 [37].

For more front-end interaction, Vue.js version 5.0.8 [38] was used. This was integrated with Django using Django-webpack-loader version 1.6.0 [39].

As a database, MongoDB version 6.0.1 [40] was used. This allowed for the recording of documents being used as evidence in the system.

Bootstrap version 4.6.2[6] was used to increase front-end customization with ease and speed.

Finally, JSON [33] objects were used to import the questions from the questionnaire into the developed system. Figure 7 provides a different visualization of this structure than Figure 6.

```
{
    "function" : "XX",
    "text" : "question_text",
    "options" : [
        {
            "value" : 1,
            "text" : "option_1"
        },
        {
            "value" : 2,
            "text" : "option_2"
        },
        {
            "value" : 3,
            "text" : "option_3"
        }
    ],
    "evidences" : [
        "evidence_1",
        "evidence_2",
        "evidence_3"
    ]
}
```

Figure 7: JSON skeleton structure of Question

[6] https://getbootstrap.com/docs/4.6/getting-started/introduction/

All the technologies used are free and open source, which was a focus of the development.

3.5 Models

Django structures and manages data through Python objects referred to as Models. Each model is, in this case, tied to a single document in the MongoDB database, and contains all the information about the data being stored. The models have fields, which are the attributes of the objects and are mapped to a field of the document in the database.

All the Models have an _id, which is autogenerated, and serves as the main identifier of a Model.

The main Model is the Question Model, which has a link to one and only one user, the user that has been attributed with the said question and is responsible for answering it. It also has a *function* Slug Field, with the options ID, PR, DE, RS, and RC, for the cybersecurity function associated with the question, and an *identifier* Slug Field which is generated from the function and with a number automatically iterating to unequivocally identify the question, for example, *ID-5*. The remaining Fields include *text*, which holds the question's text, *chosen_option*, an Integer to hold which of the options is currently selected, and *order*, an auxiliary Field to customize the ordering of the models.

The Option Model has a reference to the Question it belongs to, a *text* field that contains the option's text to be displayed, a *value* field that represents the option's value (1, 2, or 3) according to the QACCS framework level of maturity, and an *evidence* field with the text regarding evidence providing.

The Evidence Model has a reference to the Question it concerns, a file Field to store the file provided, and a *question_identifier* field to maintain a way to identify the question in case of question deletion.

On the topic of deletion, Django provides a few options to deal with the deletion of a model. The ones used for these models are *cascade* on the relationship between a question and options, which means that when a question gets deleted all the options associated with it are also deleted; and *set_null*, which is being used on the relationships between question and evidence, setting the question reference to *null* but preserving the evidence, as well as between question and user, setting the user reference to *null* but maintaining the question model.

The following figure provides a visualization of the created models and their relationships.

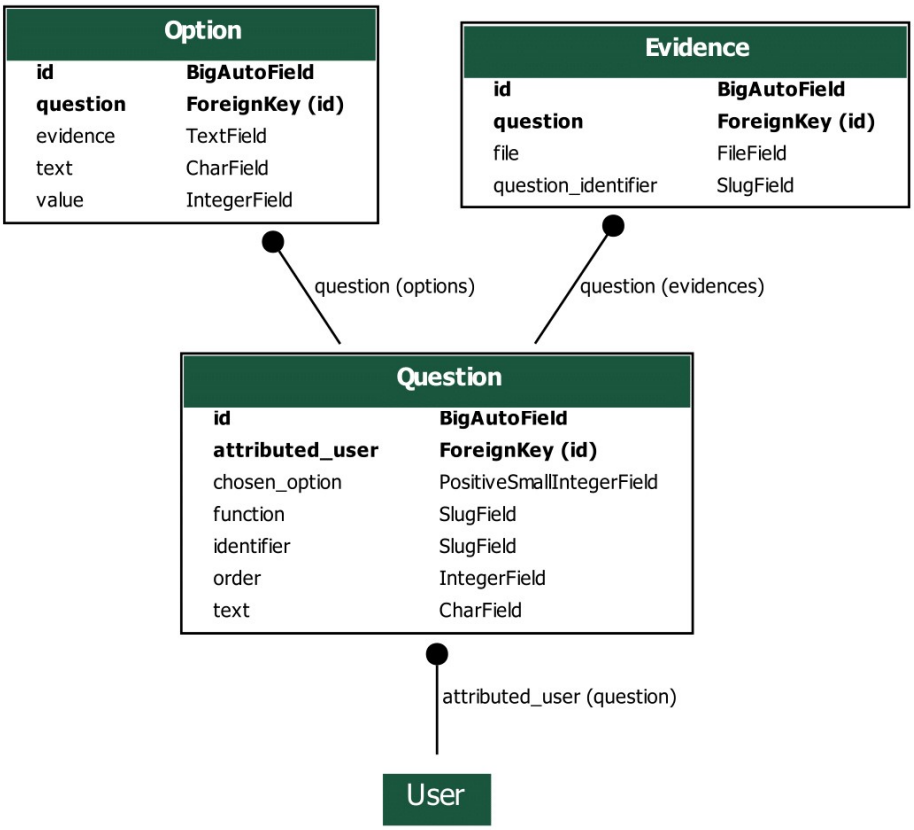


Figure 8: Django Models

3.6 System Structure

The Django project was structured into two different applications, a User one, tasked with allowing for user logins and sign-ups, and another one, Questions, that contains all the relevant work regarding question creation, handling, presentation, evidence providing as well as reports regarding the cybersecurity maturity.

Each question in the database followed a model from Django's Object Relational Mapper (ORM) as stated before in section 3.5.

To facilitate the creation of questions in bulk, a form was set up that accepted JSON files and created questions according to the data provided.

The following subsections further detail the work developed in each of these applications.

3.6.1. User application

The User application manages everything related to the users, account creation, login, and sign-out.

The primary features of this application are the login form, illustrated in Figure 9, and the account creation form, illustrated in Figure 10.

Everything in this application was developed using Django's [36] authentication system[7]. This allowed for a secure implementation of logins and account creation. Moreover, Django enforces minimum length and complexity requirements on passwords, as seen in Figure 10.

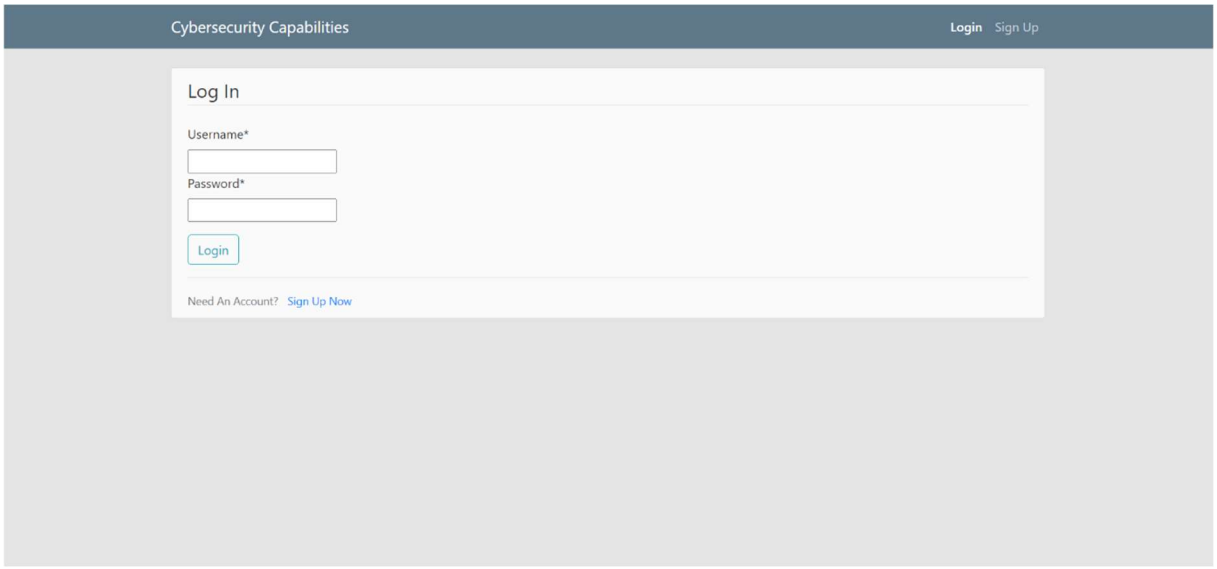


Figure 9: User Login Screen

[7] https://docs.djangoproject.com/en/4.0/topics/auth/default/

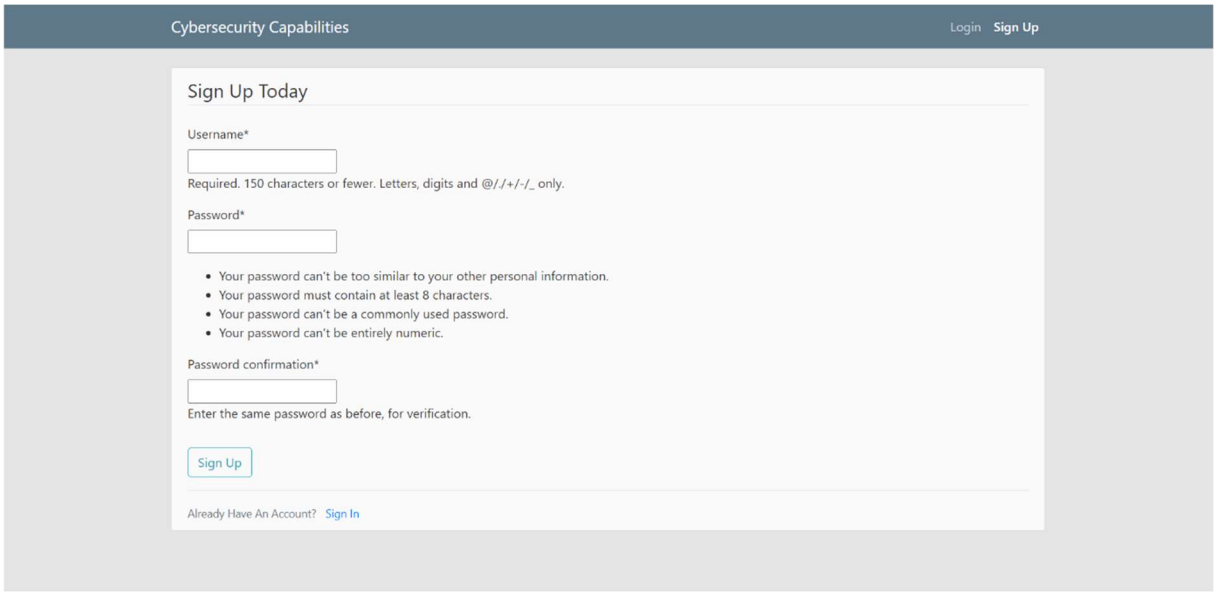


Figure 10: Account Creation Screen

3.6.2. Questions application

The Questions application is responsible for all the question-related aspects of the tool, including uploading, answering, and everything related to evidence providing.

The main feature of the Questions application is the question viewing and answer submission. This was developed using Vue.js, as stated in section 3.4, to increase interaction without the need for a page reload. The page comprises of a list of questions and a panel to answer the question being viewed in detailed, as well as a submit button. The user clicks on the question's text in the list to select a question to view in detail. Figure 11 illustrates the question screen of a logged-in user.

Figure 11: Question Answering Screen

When the page loads, the first question shows in the detailed panel by default. To answer any question, the user clicks on a radio button or on an option's text to change the selected option in the front-end. If the user desires to unselect the option, clicking the same radio button or option's text removes the selection. After answering all the questions, the user clicks the submit button to send to the back-end the answers he provided, which update the question models, namely the *chosen_option* field.

Following the submission of the question's answers, the website redirects the user to the evidence-providing screen, where the user selects a question from a list that contains only the already answered questions, and provide the files required to demonstrate the reached levels of cybersecurity capability.

On the supervisor side, a supervisor follows the workflow shown in Figure 12. After uploading the questionnaire to the system, the supervisor attributes question to the user most qualified to answer it. Then, after users have answered the questions, the supervisor views the report and analyses the current capabilities. After this the supervisor is empowered to make better decisions.

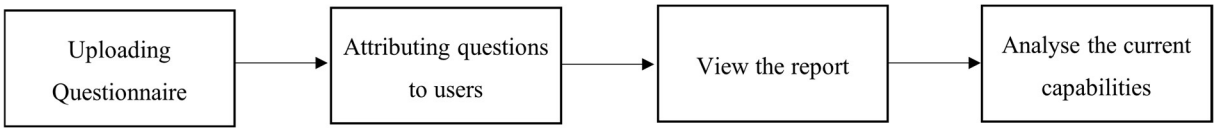


Figure 12: Supervisor Workflow

Another important feature of the Questions application is the calculation of cybersecurity maturity to be shown in the report. These calculations take place each time the Report Screen is loaded by a supervisor and examine each of the questions in the database, adding up the total cybersecurity capability that has been reached, according to the value of the selected option, and the ideal scenario, where the requirements for the most advanced level in each question have been met. Then the current scenario value is divided by the ideal scenario value, multiplied by one hundred (100) and rounded, to get a percentage of maturity. This process occurs in two separate ways, with the questions divided in the five cybersecurity functions, and with all the questions at once. This calculation does not take into account the submission, or lack of submission, of evidence of each question.

Figure 13 shows a supervisor's report screen where all the cybersecurity functions are at 0% maturity, because no questions have been answered yet. As the answers are submitted, this report evolves towards 100%, which would signify a fully capable organization in terms of cybersecurity, according to the questionnaire that has been uploaded.

Figure 13: Empty Report Screen

3.7 Website Design

The website was developed based on ease of access, so a navigation bar was employed, on the top of the screen, with all the relevant links to facilitate use. This navigation bar changes for users, supervisors, and logged-out users. A user has Questions and Evidence options on the left, and a Logout option on the right. A supervisor has, additionally, Report, Upload Questions and

Attribute Questions, all of these on the left side. A logged-out user only has options to Login and Sign Up, on the right of the bar. The following figures provide visualizations of these navigation bars.

Figure 14: User Navigation Bar

Figure 15: Supervisor Navigation Bar

Figure 16: Logged-Out User Navigation Bar

Developing the website, the colours used in QNRCS were employed in various scenarios to better illustrate which cybersecurity function the question belonged to. Figure 17 illustrates the colours used.

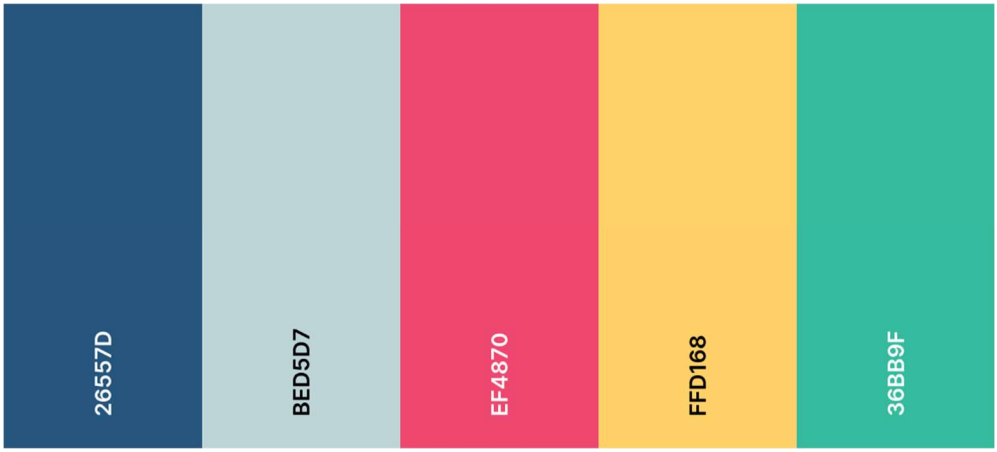


Figure 17: Colours used for each Cybersecurity Function

In the most significant screens, namely the Question Answering, the Evidence Providing and the Question Attribution, explanations were introduced to improve clarity and increase usability. Figure 18 exemplifies one of these explanations.

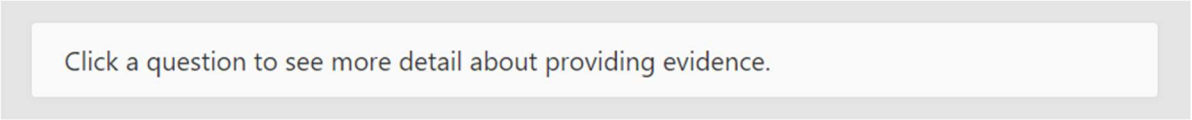


Figure 18: Explanation of evidence

A Django tool, messages, was employed to increase user feedback on certain actions, like the success of a question's file upload, or the erroneous attempt to attribute questions when there are no questions loaded. Figure 19 and Figure 20 presents two examples of these messages.

Figure 19: Success Message

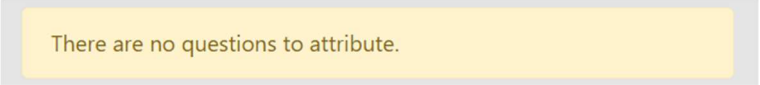


Figure 20: Warning Message

3.8 Conclusions

The result of the work developed, the questionnaire and the web-based application, provide a tool to enable organization's supervisor to gain insight about the current cybersecurity capabilities.

Chapter 4 - Solution Validation

This chapter presents the validation of the proposed solution, as well as compares the developed system with the QACCS proposed by CNCS.

4.1 User Stories Acceptance Criteria

The validation of the proposed solution was making sure all the acceptance criteria for each of the user stories were met.

Table 6: User Stories Acceptance Criteria

#ID	**Acceptance criteria**
US01	Ensure the user can: - Create an account - Login to the app
US02	Ensure the supervisor can: - Login to the app - Upload a file with questions
US03	Ensure the supervisor can: - Login to the app - View the questions available - Attribute questions to a user
US04	Ensure the user can: - Login to the app - View the questions attributed to them - Answer the questions - Submit the answers
US05	Ensure the user can: - Login to the app - View the questions in need of evidence providing - Select a question - Submit evidence files
US06	Ensure the supervisor can: - Login to the app

	- View the report
US07	Ensure the supervisor can: - Login to the app - View the detailed report of a specific function - Tell which user has been attributed to each question. - Tell which questions haven't been answered

4.1.1. User Story 01

The acceptance criteria for User Story 01 are a new user being able to create an account and log in.

As shown in Figure 21, a new user can create an account by filling out the sign-up form with a username and a password and submitting the form by clicking the "Sign Up" button at the bottom of the page.

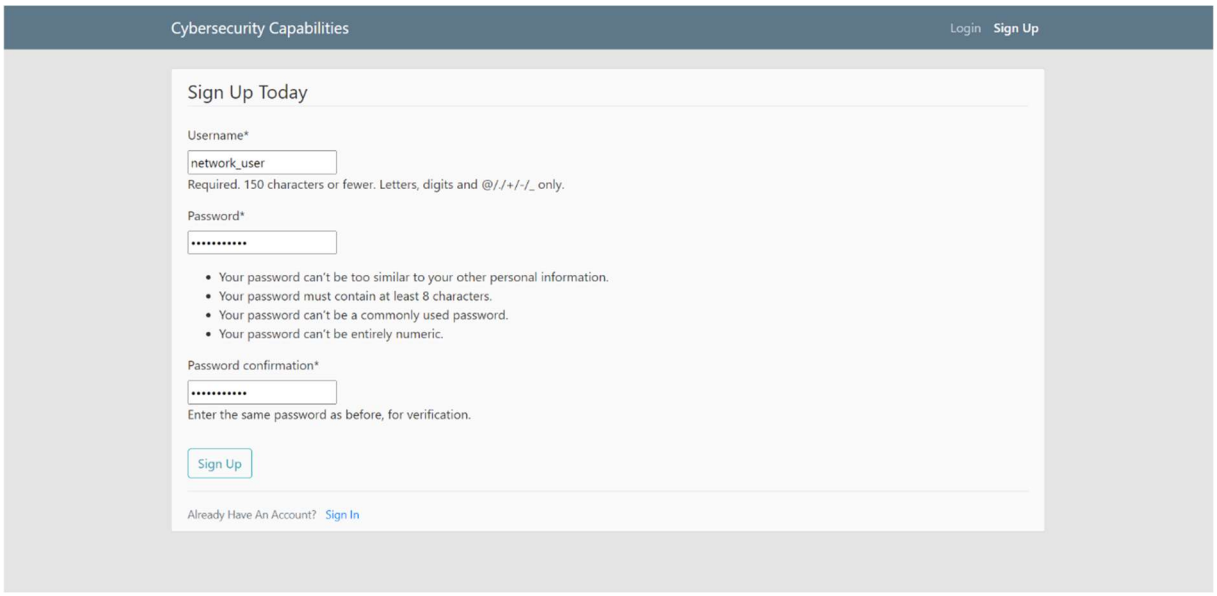


Figure 21: US01 - Sign Up Page

As it shows in Figure 22, the user can log in by filling out the login form with an existing username and password and pressing the "Log In" button at the bottom of the page.

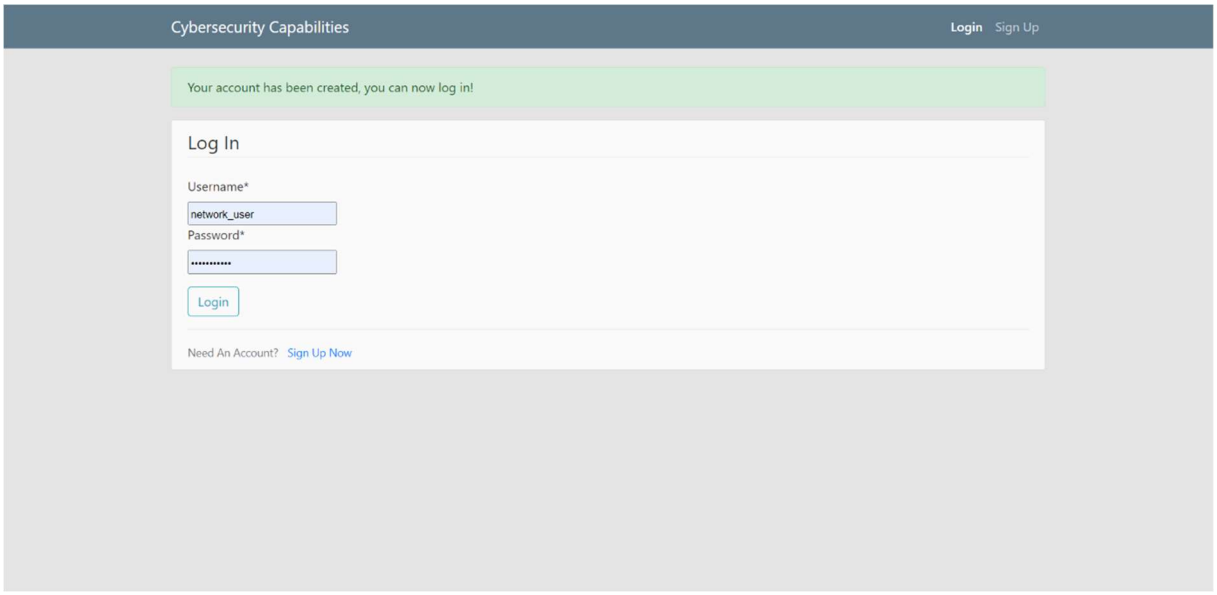


Figure 22: US01 - Login Page

After the login, the user is redirected to the home page and can use the application. This fulfils User Story 01.

4.1.2. User Story 02

The acceptance criteria for User Story 02 are a supervisor login to the app and uploading a JSON file with questions.

As seen in Figure 23, the supervisor can log in by completing the form with a username and password.

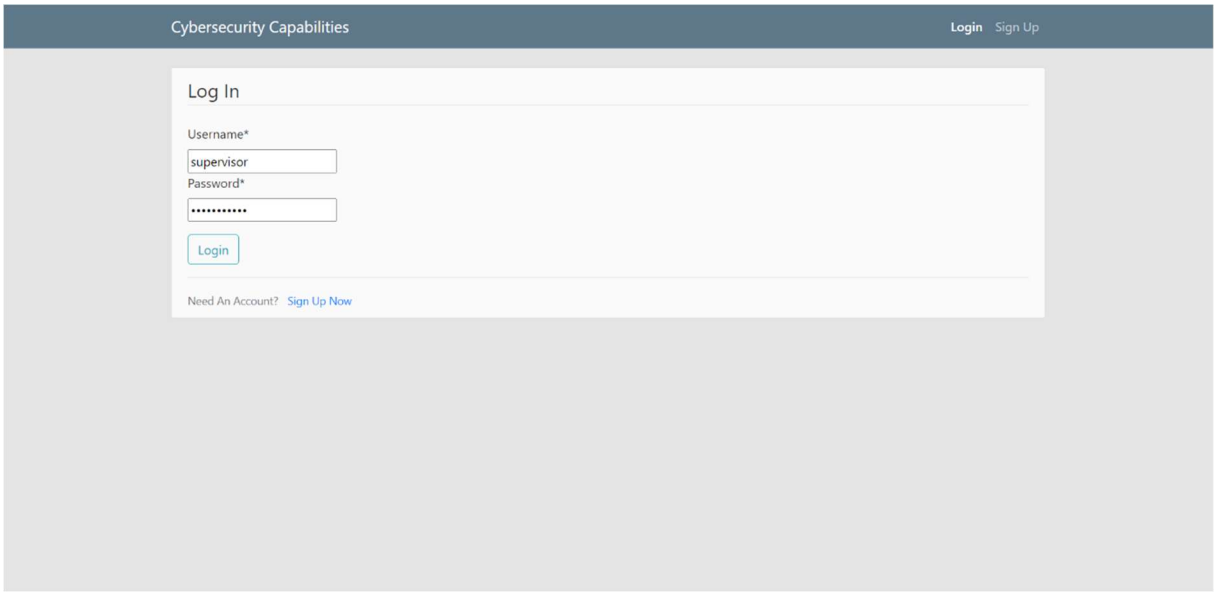


Figure 23: US02 - Supervisor Login Page

In the Question Upload screen, Figure 24, the supervisor can choose a JSON file by browsing his file system and submit it by clicking the “Submit” button.

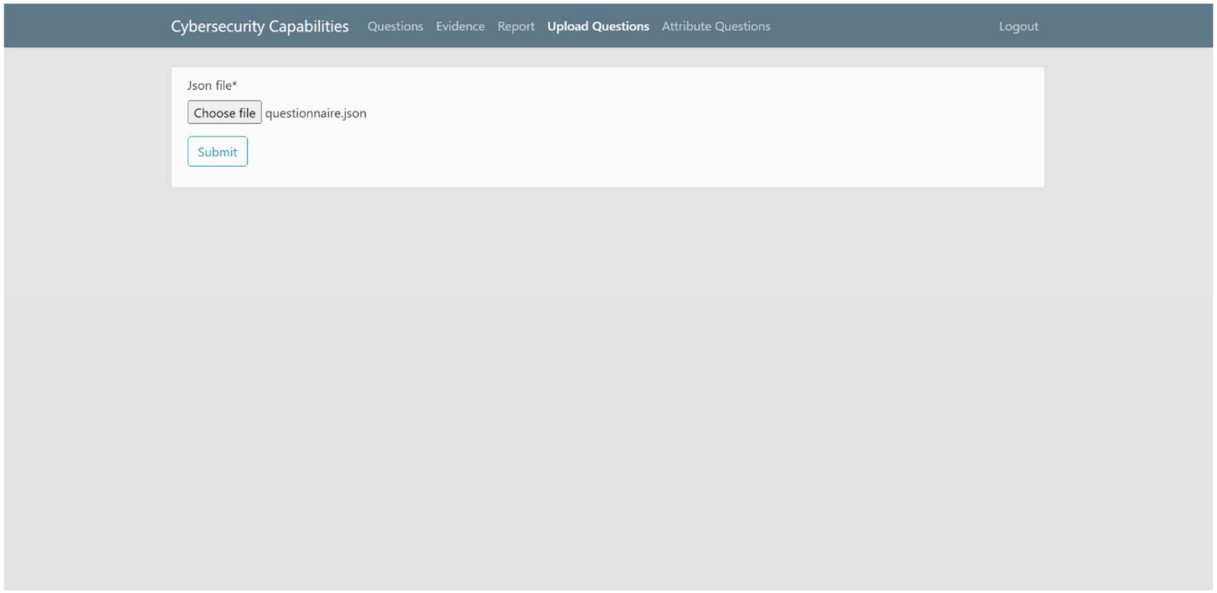


Figure 24: US02 - Question Upload Page

4.1.3. User Story 03

The acceptance criteria for User Story 03 are a supervisor login to the app, viewing the questions to be attributed and attributing them to a user.

As shown in Figure 23 the supervisor can log in, then, in Figure 25, the supervisor can select questions from a list, and finally, at the bottom of the page, select a user from a drop-down menu to attribute the selected questions to them by clicking the “Attribute questions” button.

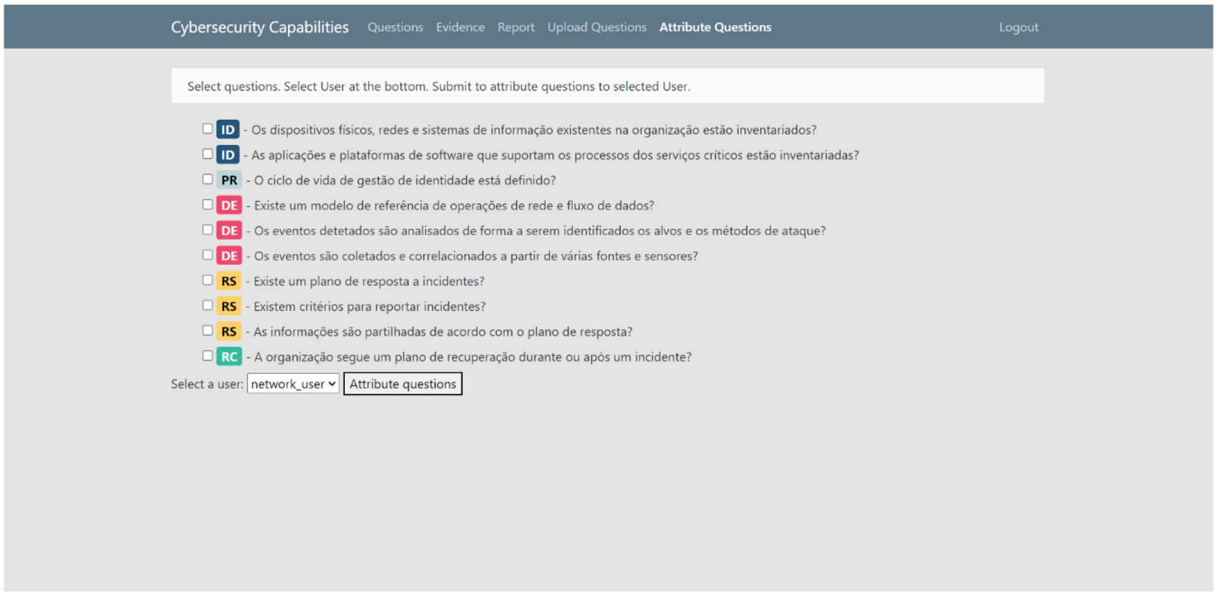


Figure 25: US03 - Question Attribution Page

4.1.4. User Story 04

The acceptance criteria for User Story 04 are a user can log in to the app, view the question attributed to them, answer the questions, and then submit the answers.

Firstly, the user can log in, as shown in Figure 22. The user can select questions on the left panel of the page shown in Figure 26, and answer them on the coloured panel. When all questions are answered, the user can submit the answers by pressing the green “Submit” button on the bottom of the page, as displayed in Figure 27.

Figure 26: US04 - Question Answering Page

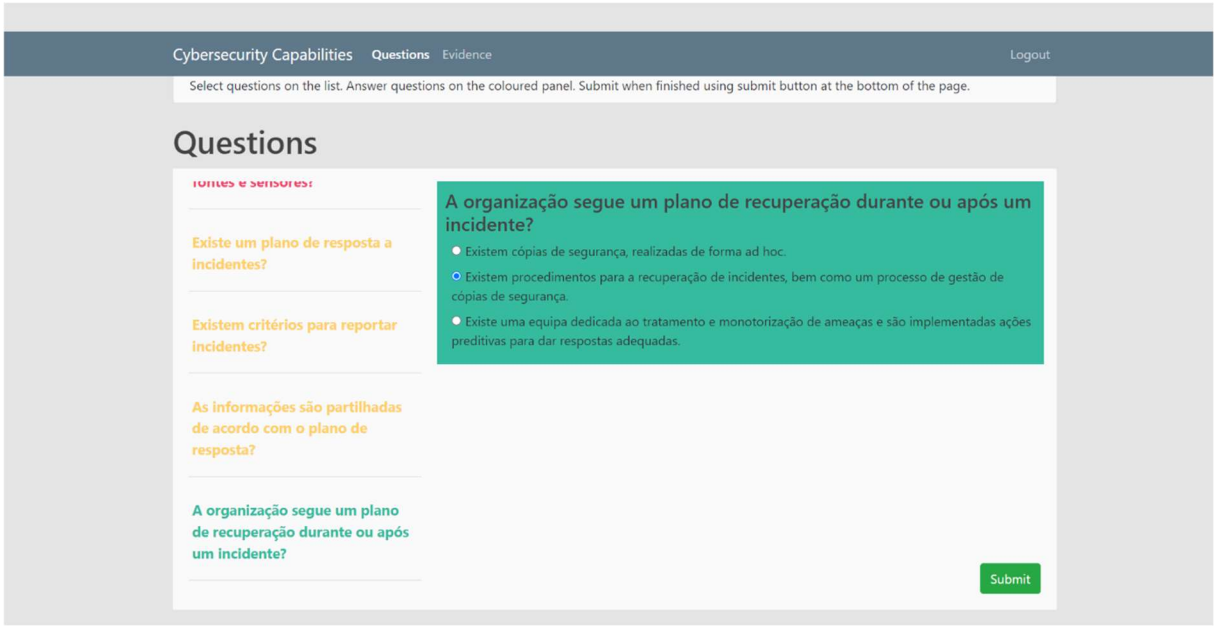


Figure 27: US04 - Question Answering Page submission

4.1.5. User Story 05

The acceptance criteria for User Story 05 are a user can log in to the app, view the questions in need of evidence providing, select a question and submit the pertinent evidence files.

The user can log in, as previously seen and illustrated in Figure 22. Then, by selecting the Evidence tab in the navigation bar at the top of the screen, navigate to the main evidence page, as demonstrated by Figure 28. In this screen, the user selects a question from the list provided by clicking on its text.

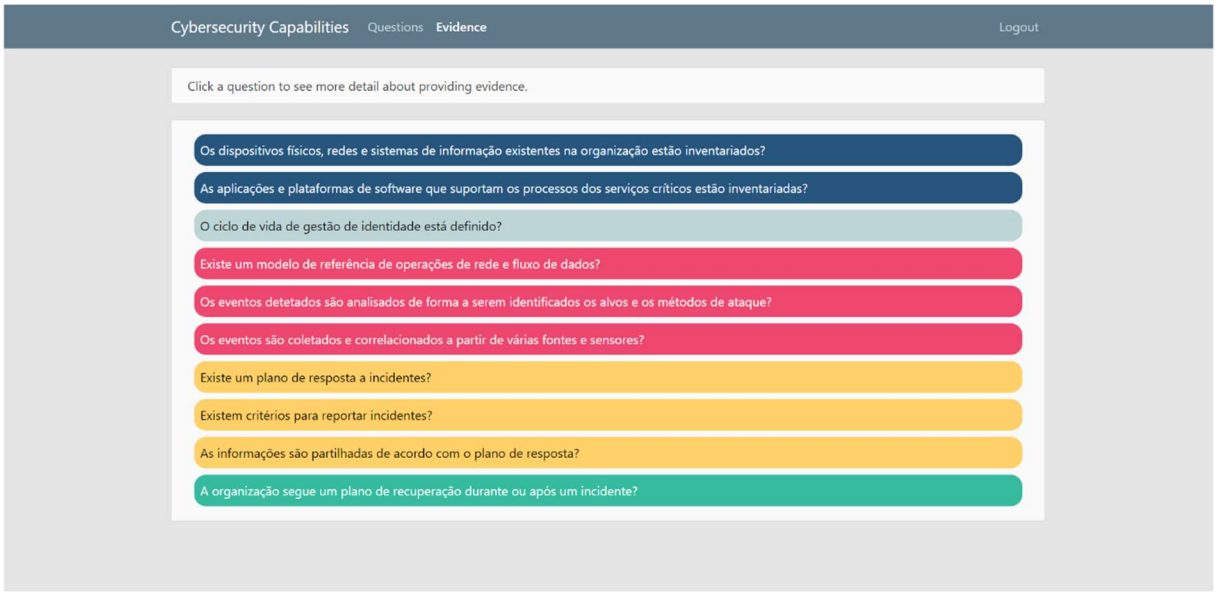


Figure 28: US05 - Main Evidence Page

After selecting a question, a specific page for evidence providing of the selected question is shown, exemplified in Figure 29. On this page the user can read the text of the question, the option selected and the evidence in need of submission. Finally, the user can select files from the file system to provide the necessary evidence and submit these files by pressing the “Submit” button below.

Figure 29: US05 - Question Evidence Page

4.1.6. User Story 06

The acceptance criteria for User Story 06 are a supervisor can log in to the app and view the report concerning the cybersecurity capabilities at the given time.

The supervisor can log in, as demonstrated in Figure 23. By clicking the Report button in the navigation bar, the report page is opened, as shown in Figure 30.

Figure 30: US06 - Report Page

4.1.7. User Story 07

The acceptance criteria for User Story 07 are a supervisor can log in to the app and view the detailed report for a given cybersecurity function. Then identify which user, if any, has been attributed to each of the questions, as well as examine which questions have not been answered yet.

As indicated before, and as is shown in Figure 23, the supervisor can log in. Then, when on the report page (Figure 30), clicking on any of the five function badges brings up a more detailed page about that specific function.

Figure 31 presents the Detailed Report Page for the identify function. In this example, there are three questions shown, the first one is yet to be answered, the second one has been answered, so its answer is presented, and the third and final one has not been attributed to any user yet.

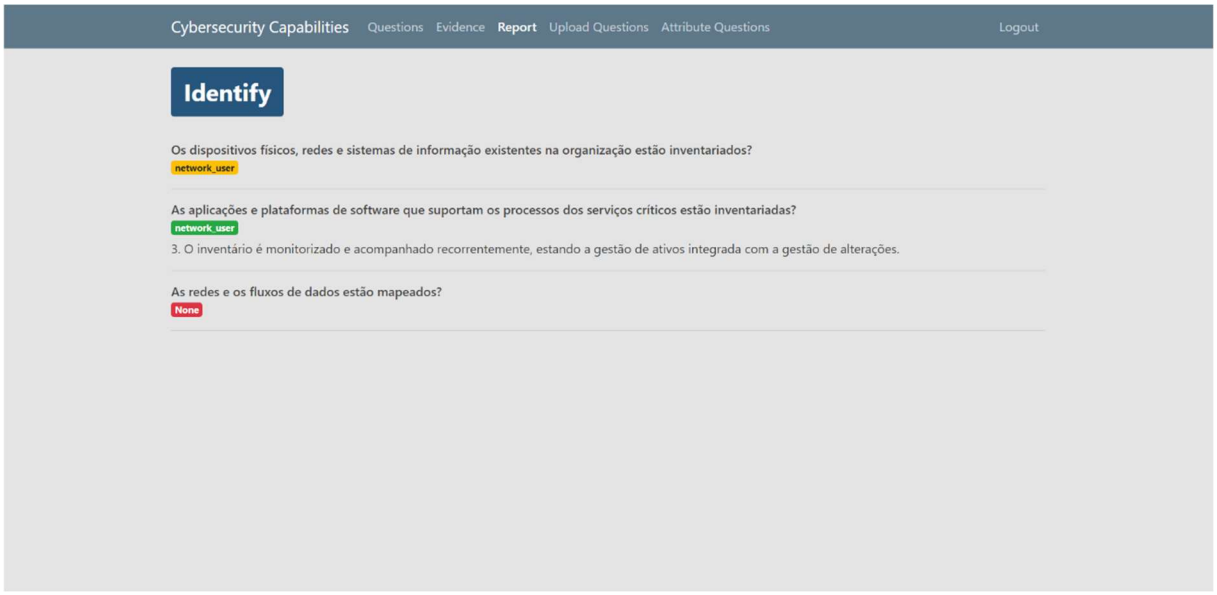


Figure 31: US07 - Detailed Report Page

4.2 Conclusion

The previous section, section 4.1, proves how the system developed can be used to fulfil all the user stories defined in section 3.3, which demonstrate that the system is a valid solution to reach the goals proposed.

The artifact proposed improves on the existing solutions by enabling the spreading of answering responsibility to the more qualified users in the organization, as demonstrated by user story three. Furthermore, the ability to record evidence, as proved in user story 05, offer an important addition to the existing tools.

Due to limitations, further validations with experts or the application of the system in a real-life use case were not possible.

Chapter 5 - Conclusions and Future Work

In this chapter, a summary conclusion is presented, as well as the limitations of the work developed and the respective proposals for improvement in future work.

5.1 Conclusions

The main objective of this dissertation was to create an easier way to self-access cybersecurity capabilities, developing a system that empowers supervisors to be up to date about the multiple components of cybersecurity, addressing and diminishing possible dangers.

For the development of the application, a review was carried out to ascertain whether any similar tools already existed. From the analysis of the research, it is concluded that there is no system with similar capacities and depth available. A few questionnaires were identified that propose the recollection of information about cybersecurity capabilities but are still cumbersome to employ.

After the research work, the first part of the solution was developed, comprising a questionnaire based on the QACCS subcategories. The second part of the solution was to develop a web application capable of storing questions and their respective answers, calculating the distance from an ideal situation based on the answers provided.

The questionnaire, which aims to be easy to use and interpret, can be imported to the web application to provide supervisors with questions that they can direct towards the qualified personnel to answer them. Once filled in, the application records the answers and presents a set of data in the form of a report, enabling the supervisor to make informed cybersecurity decisions.

Finally, the solution was validated using evidence of the acceptance criteria for each of the user stories, as well as compared with existing tools.

All in all, this works answers positively the proposed research question “Is it possible to design a system to facilitate Cybersecurity Capabilities Assessment?”.

5.2 Limitations

The goal of applying QACCS to Iscte with the purpose of identifying and assessing Iscte’s Cybersecurity Capabilities, as well as the goal of identifying potential deviations from the ideal that could lead to improvements were not fulfilled.

The developed system was not implemented and tested with organizations, which would be a validation method.

5.3 Future Work

Despite the results achieved there are some improvements to be made in future work.

Preparing the front-end to perform editions on questions. Providing more user context and help.

Developing and implementing a feature allowing for next-step suggestions based on the status of the responses, enabling users to better locate efficient next steps to progress their organization's cybersecurity.

Addition of an evidence document explorer for supervisors to better visualize the state of the evidence provided.

Deploying the system in a container to be used in a real-life scenario, testing, and implementing it with multiple organizations to determine the impact of the proposed system in increasing the organization's cybersecurity capabilities.

References

[1] Check Point Research, 'Cyber Security Report 2022', 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.checkpoint.com/downloads/resources/cyber-security-report-2022.pdf

[2] European Union Agency for Cybersecurity, 'ENISA THREAT LANDSCAPE 2022', 2022, doi: 10.2824/764318.

[3] Centro Nacional de Cibersegurança, 'Quadro Nacional de Referência para a Cibersegurança', Lisboa, 2019. Accessed: Nov. 30, 2022. [Online]. Available: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[4] Centro Nacional de Cibersegurança, 'Quadro de Avaliação Capacidades Cibersegurança', Jan. 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf

[5] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, 'A design science research methodology for information systems research', *Journal of Management Information Systems*, vol. 24, no. 3, 2007, doi: 10.2753/MIS0742-1222240302.

[6] W. H. Ware, 'Security and privacy in computer systems', in *Proceedings of the April 18-20, 1967, spring joint computer conference on - AFIPS '67 (Spring)*, 1967, p. 279. doi: 10.1145/1465482.1465523.

[7] H. S. Lallie *et al.*, 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Comput Secur*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[8] Microsoft, 'Microsoft Digital Defense Report', Oct. 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[9] SOPHOS, 'The State of Ransomware 2021', 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

[10] Verizon, 'Data Breach Investigations Report', 2022. Accessed: Nov. 30, 2022. [Online]. Available: verizon.com/dbir/

[11] Check Point Research, 'Cyber Attack Trends Mid Year Report 2021', 2021.

[12] maria cristina Arcuri, M. Brogi, and G. Gandolfi, 'How does cyber crime affect firms? The effect of information security breaches on stock returns', Nov. 2017.

[13] R. Böhme, ‘Security Metrics and Security Investment Models’, in *Advances in Information and Computer Security*, 2010, pp. 10–24.

[14] K. L. Williams, ‘Management Wake-Up and Govern: The Era of the Cyber Security Governance’, in *2014 Annual Global Online Conference on Information and Computer Technology*, Dec. 2014, pp. 50–52. doi: 10.1109/GOCICT.2014.20.

[15] M. J. Page *et al.*, ‘The PRISMA 2020 statement: an updated guideline for reporting systematic reviews’, *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[16] ‘Information technology — Security techniques — Information security management systems — Overview and vocabulary’, *ISO/IEC 27000:2018*, 2018.

[17] European Union Agency for Cybersecurity, ‘ENISA overview of cybersecurity and related terminology’, 2017. Accessed: Nov. 30, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[18] ‘Guide for conducting risk assessments’, Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

[19] B. von Solms and R. von Solms, ‘Cybersecurity and information security – what goes where?’, *Information & Computer Security*, vol. 26, no. 1, pp. 2–9, Mar. 2018, doi: 10.1108/ICS-04-2017-0025.

[20] T. Chmielecki *et al.*, ‘Enterprise-oriented Cybersecurity Management’, Sep. 2014, pp. 863–870. doi: 10.15439/2014F38.

[21] S. L. Garfinkel, ‘The cybersecurity risk’, *Commun ACM*, vol. 55, no. 6, pp. 29–32, Jun. 2012, doi: 10.1145/2184319.2184330.

[22] J. P. G. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, ‘Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation’, *Telecommun Syst*, Dec. 2011, doi: 10.1007/s11235-011-9573-6.

[23] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, ‘Developing Cyber-Resilient Systems’:, Gaithersburg, MD, Dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[24] ‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’, Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[25] D. Markopoulou, V. Papakonstantinou, and P. de Hert, ‘The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection

Regulation', *Computer Law & Security Review*, vol. 35, no. 6, p. 105336, Nov. 2019, doi: 10.1016/j.clsr.2019.06.007.

[26] C. Kohler, 'The EU Cybersecurity Act and European standards: an introduction to the role of European standardization', *International Cybersecurity Law Review*, vol. 1, no. 1–2, pp. 7–12, Oct. 2020, doi: 10.1365/s43439-020-00008-1.

[27] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, 'A security review of local government using NIST CSF: a case study', *J Supercomput*, vol. 74, no. 10, pp. 5171–5186, Oct. 2018, doi: 10.1007/s11227-018-2479-2.

[28] Juan Eduardo Catril Opazo, 'NIST CYBERSECURITY FRAMEWORK IN SOUTH AMERICA', UNIVERSIDAD DE CHILE, Santiago, 2020.

[29] N. Teodoro, L. Goncalves, and C. Serrao, 'NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements', in *2015 IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 418–425. doi: 10.1109/Trustcom.2015.402.

[30] Y. Maleh, A. Sahid, and M. Belaissaoui, 'A MATURITY FRAMEWORK FOR CYBERSECURITY GOVERNANCE IN ORGANIZATIONS', *EDPACS*, vol. 63, no. 6, pp. 1–22, Jun. 2021, doi: 10.1080/07366981.2020.1815354.

[31] A. Aliyu *et al.*, 'A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom', *Applied Sciences*, vol. 10, no. 10, p. 3660, May 2020, doi: 10.3390/app10103660.

[32] S. G. Govender, E. Kritzinger, and M. Loock, 'A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture', *Pers Ubiquitous Comput*, vol. 25, no. 5, pp. 927–940, Oct. 2021, doi: 10.1007/s00779-021-01549-w.

[33] F. Pezoa, J. L. Reutter, F. Suarez, M. Ugarte, and D. Vrgoč, 'Foundations of JSON schema', in *Proceedings of the 25th International Conference on World Wide Web*, 2016, pp. 263–273.

[34] M. Cohn, *User Stories Applied: For Agile Software Development*. USA: Addison Wesley Longman Publishing Co., Inc., 2004.

[35] G. Lucassen, F. Dalpiaz, J. M. E. M. van der Werf, and S. Brinkkemper, 'The Use and Effectiveness of User Stories in Practice', 2016, pp. 205–222. doi: 10.1007/978-3-319-30282-9_14.

[36] Django Software Foundation, 'Django (Version 4.0.6)'. 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.djangoproject.com/

[37] Python Software Foundation, ‘Python (Version 3.10.4)’. 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.python.org/

[38] ‘Vue.js (Version 5.0.8)’, 2022, Accessed: Nov. 30, 2022. [Online]. Available: https://vuejs.org/

[39] ‘Django Webpack Loader (Version 1.6.0)’, 2022, Accessed: Nov. 30, 2022. [Online]. Available: https://github.com/django-webpack/django-webpack-loader/

[40] MongoDB Inc., ‘MongoDB (Version 6.0.1)’. 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.mongodb.com/

Appendix A

Identificar

ID.GA-1

1 Os dispositivos físicos, redes e sistemas de informação existentes na organização estão inventariados?

1. Os ativos da organização são registados de forma isolada e pouco sistémica.
2. Os ativos são registados sistematicamente, com informação individual completa e pertinente, estando cada ativo identificado individualmente na organização e com um único responsável associado.
3. O inventário é monitorizado e acompanhado recorrentemente, estando a gestão de ativos integrada com a gestão de alterações.

Evidências

1. Ficheiros isolados de registo dos ativos com alguma informação sobre os ativos.
2. Ferramentas/aplicações de gestão integrada de ativos. Políticas de inventário de ativos. Associação de nome e contacto do colaborador responsável pelo ativo.
3. Indicadores e registos de acompanhamento dos inventários. Sistemas de monitorização dos inventários. Sistema de identificação automatizada de novos ativos ou alterações dos ativos existentes.

ID.GA-2

2 As aplicações e plataformas de software que suportam os processos dos serviços críticos estão inventariadas?

1. Os sistemas da organização são registados de forma isolada e pouco sistémica.
2. As aplicações e plataformas são registadas sistematicamente com informação completa e pertinente, estando cada sistema identificado individualmente na organização e com um único responsável associado.
3. O inventário é monitorizado e acompanhado recorrentemente, estando a gestão de ativos integrada com a gestão de alterações.

Evidências

1. Ficheiros isolados de registo dos sistemas com alguma informação sobre os sistemas. Tabela de identificação de responsáveis pelos sistemas utilizados.
2. Ferramentas/aplicações de gestão integrada de sistemas. Políticas de inventário de ativos. Associação de nome e contacto do colaborador responsável pelo sistema.
3. Indicadores e registos de acompanhamento dos inventários. Sistemas de monitorização dos inventários. Sistema de identificação automatizada de novos sistemas ou alterações dos sistemas existentes.

ID.GA-3

3 As redes e os fluxos de dados estão mapeados?

1. Os ativos de redes de comunicações são identificados, existindo perceção sobre a topologia de rede.
2. Os ativos de redes de comunicações são identificados e inventariados, existindo registos de zonas, endereços IP e identificação de alvos críticos.
3. O inventário de rede de comunicação é mantido com ferramentas de descoberta automática e revisto periodicamente.

Evidências

1. Registo dos ativos de redes.
2. Mapa de endereços IP. Mapa de topologia da rede. Mapa do fluxo de comunicações.
3. Uso de ferramentas ou aplicações automatizadas de descoberta de ativos de rede. Relatórios de avaliação e acompanhamento dos fluxos dos dados.

ID.GA-4

4 As redes e sistemas de informação externos estão identificados e catalogados?

1. Os ativos de rede externos são identificados de forma *ad hoc*.
2. Os ativos de rede externos possuem dados completos de identificação, existindo um registo georeferencial da localização dos equipamentos.
3. Os ativos são monitorizados e geridos remotamente, sendo vistoriados periodicamente e a performance avaliada, para fins preventivos.

Evidências

1. Identificação dos ativos de rede em ambiente externos.
2. Registo do ativo com endereço IP, inventário, tipologia, responsável e geolocalização. Política de segurança para ativos em ambientes externos.
3. Inventário automatizado dos ativos de rede externos. Relatório de acompanhamento dos indicadores de performance. Evidências de vistorias (relatórios, registo de manutenção).

ID.GA-5

5 Os ativos necessários para a prestação de bens e serviços são classificados?

1. Os ativos são classificados de forma *ad hoc*.
2. Estão definidos métodos de classificação dos ativos por criticidade e valor percebido.
3. A classificação dos ativos é revista em períodos regulares, e influencia na seleção dos controlos de segurança aplicados.

Evidências

1. Registos possivelmente incompletos com classificação de ativos.
2. Política de classificação de ativos. Formalização do processo de classificação.
3. Registo atualizado da classificação dos ativos. Mapa de tipos de controlos de segurança por níveis de classificação dos ativos. Relatórios de avaliação dos critérios de classificação.

ID.AO-1

6 O papel da organização na cadeia logística está identificado e é comunicado?

1. Os fornecedores de cada subgrupo da organização encontram-se identificados, ainda que de forma isolada.
2. O governo, no relacionamento entre organização e fornecedores, está estabelecido e documentado, existindo registos integrados de tipificação dos fornecedores.
3. Os contratos são revistos em intervalos regulares e os fornecedores de serviços críticos têm os seus controlos de segurança validados.

Evidências

1. Registo formal de fornecedores por subgrupo da organização.
2. Política e procedimentos para a relação com fornecedores. Sistema de cadastro integrado dos fornecedores.
3. Relatórios de análise e avaliação de risco na cadeia de fornecedores. Resultados de auditorias à cadeia crítica de fornecedores da organização.

ID.AO-2

7 O posicionamento da organização no seu setor de atividade está identificado e é comunicado?

1. A organização tem a sua missão e objetivo definidos, conseguindo identificar partes internas e externas interessadas.
2. A política de segurança da informação faz referência à missão, aos objetivos da organização e às suas partes interessadas, sendo divulgada por todas as partes interessadas.
3. As políticas e os relacionamentos com as partes interessadas são revistos em intervalos regulares.

Evidências

1. Contrato ou estatuto de formação da organização. Relação de fornecedores, parceiros e demais interessados.
2. Referência à missão e objetivos da organização na política de segurança. Registos comprovativos da divulgação da política de segurança pelas partes interessadas.
3. Registos de revisão das relações com partes interessadas.

ID.AO-3

8 A missão, visão, valores, estratégias e objetivos da organização são definidas e comunicadas?

1. A organização tem a sua missão, visão, valores e objetivos estratégicos definidos e consegue identificar partes interessadas, internas e externas, para o efeito.
2. A política de segurança da informação faz referência à missão, visão, objetivos e valores da organização e às suas partes interessadas, sendo divulgada por todas as partes interessadas.
3. As políticas, os relacionamentos com as partes interessadas e o plano de negócio são revistos em intervalos regulares e conforme a estratégia da organização.

Evidências

1. Contrato ou estatuto de formação da organização. Relação de fornecedores, parceiros e demais interessados.
2. Referência à missão e objetivos da organização na política de segurança. Registos comprovativos da divulgação da política de segurança pelas partes interessadas.
3. Registos de revisão das relações com partes interessadas.

ID.AO-4

9 Os ativos críticos estão identificados e registados?

1. Os ativos críticos são identificados de forma *ad hoc*.
2. Os ativos que suportam os processos críticos são identificados em sistema de gestão de ativos consolidado, sendo utilizada uma ferramenta/aplicação para a gestão integrada dos ativos da organização.
3. Os registos dos ativos são atualizados dinamicamente conforme as alterações realizadas nos ambientes existentes, sendo realizadas manutenções preventivas planeadas e revistas as capacidades de cada ativo.

Evidências

1. Registo possivelmente incompleto dos ativos críticos.
2. Registo em ferramenta de gestão dos ativos críticos de infraestrutura, redes e sistemas da organização. Política de classificação de ativos conforme criticidade.
3. Sistema de descoberta automática de ativos. Registo de manutenções preventivas aos equipamentos de infraestrutura.

ID.AO-5

10 Os requisitos de resiliência necessários para suportar a prestação de serviços críticos estão definidos?

1. Existem notas *ad hoc* sobre os requisitos mínimos para prestação de serviços críticos.
2. Existe um plano de continuidade registado e testado com estratégias de recuperação, sendo mantidos contratos com fornecedores para manutenção de serviços críticos.
3. O plano de continuidade é revisto regularmente, sendo os agentes externos em cadeia crítica auditados quanto às capacidades de resiliência.

Evidências

1. Documentação com os requisitos mínimos de infraestrutura para suportar os serviços críticos. Fornecedores críticos identificados.
2. Documentação do Plano de Continuidade de Negócio (PCN) e registo de testes efetivos realizados. Registo nos contratos com fornecedores críticos de cláusulas de continuidade.
3. Resultados de simulacros/testes em ambientes de produção. Registo de ações de sensibilização de colaboradores. Relatórios de auditorias a fornecedores e parceiros.

ID.GV-1

11 A política de segurança da informação está definida e é comunicada?

1. Existe uma política de segurança estabelecida e divulgada internamente.
2. Os colaboradores são informados e participam em ações de sensibilização sobre a existência da política e os seus termos.
3. A política de segurança está relacionada com outras políticas ligadas à segurança da informação dentro da organização, mantida num sistema de Gestão Eletrónica de Documentação e é revista com regularidade mínima anual.

Evidências

1. Documento com a política da informação. Comunicação interna para disseminação da política de informação.
2. Publicação oficial da política de segurança da informação pela gestão de topo. Armazenamento da política em local de fácil acesso aos colaboradores.
3. Acompanhamento de documentos de segurança. Sistema eletrónico de registo e armazenamento das políticas.

ID.GV-2

12 Os requisitos legais e regulamentares para a cibersegurança são cumpridos?

1. Os colaboradores têm conhecimento informal das leis e regulamentações aplicáveis à organização.
2. As leis e regulamentações aplicáveis à organização estão identificadas nas políticas de segurança.
3. Está estabelecida uma equipa específica para cumprimento das leis e regulamentações aplicáveis à organização, responsável pela revisão regular de publicações de novos diplomas legais, bem como por realizar auditorias.

Evidências

1. N/A.
2. Secção, na política de segurança, que faz referência a leis e regulamentações pertinentes. Divulgação e consciencialização sobre a política de privacidade.
3. Criação de equipa de conformidade interna ou contrato com fornecedor externo para o efeito. Registo da execução de procedimentos e/ou sistema de monitorização/ clipping das publicações de leis pertinentes. Relatórios de auditorias internas e/ou de parceiros, quanto ao cumprimento das leis pertinentes.

ID.AR-1

13 As vulnerabilidades dos ativos são identificadas e documentadas?

1. As vulnerabilidades são identificadas, mas não existe processo formal de tratamento.
2. As vulnerabilidades são identificadas e tipificadas nos ativos de informação, existindo um processo de gestão de vulnerabilidades que monitoriza os ativos e uma equipa dedicada ao acompanhamento de publicações de novas vulnerabilidades.
3. Existe um processo formal de revisão e análise recorrente das vulnerabilidades identificadas, bem como sistemas de pesquisa de vulnerabilidades dedicados, para identificar vulnerabilidades de forma automática.

Evidências

1. N/A.
2. Relatórios de pesquisa de vulnerabilidades. Classificação das vulnerabilidades pelos critérios definidos.
3. Relatórios de avaliação e revisão dos processos de análises de vulnerabilidades. Sistema automatizado de deteção de vulnerabilidades. Sistema de novos ativos na infraestrutura.

ID.AR-2

14 A organização partilha informações sobre ameaças de cibersegurança com grupos de interesse da especialidade?

1. São estabelecidos contactos informais com grupos de interesse.
2. Existem canais de comunicação estabelecidos com grupos de interesse, sobre ameaças e temas de segurança da informação, identificando os responsáveis pela comunicação.
3. Os canais de comunicação são otimizados de forma a garantir controlos e métricas de acompanhamento, estando todas as comunicações possíveis sistematizadas em processos automáticos, ocorrendo revisão periódica das comunicações para avaliar a sua efetividade.

Evidências

1. N/A.
2. Secção na política de segurança que faz referência a leis e regulamentações pertinentes. Divulgação e consciencialização sobre a política de privacidade.
3. Registos das comunicações feitas e dos resultados obtidos. Sistema de coleta e tratamento de comunicações de vulnerabilidades integrado com os processos de gestão das vulnerabilidades. Registo de avaliação das comunicações e dos meios utilizados para o efeito.

ID.AR-3

15 As ameaças internas e externas estão identificadas e documentadas na metodologia de gestão do risco?

1. Existe uma lista genérica de ameaças, sem mapeamento ou documentação na metodologia de gestão do risco.
2. Existe um mapa de ameaças conhecidas, associado a cada tipo de ativo, e uma indicação de tratamento para cada ameaça mapeada.
3. Existe suporte de um sistema de gestão de riscos que permite uma melhor eficiência do processo de gestão de riscos, englobando a revisão e avaliação periódicas das estratégias de tratamento.

Evidências

1. Documento com lista de ameaças.
2. Mapa de ameaças por vulnerabilidade, por ativo. Estratégias de tratamento dos riscos estabelecidas.
3. Registos da análise e avaliação de riscos nos ambientes e ativos da organização. Registo da participação da gestão de topo nas tomadas de decisão sobre o tratamento dos riscos. Relatórios de avaliação do processo de gestão de riscos.

ID.AR-4

16 A gestão do risco é efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos?

1. Existe uma metodologia de gestão do risco estabelecida.
2. As vulnerabilidades e ameaças são categorizadas conforme os critérios de probabilidade e impacto formalmente definidos.
3. Os ativos têm a sua relevância associada ao grau de importância para o negócio ou têm um valor monetário associado, sendo as avaliações de risco suportadas por sistemas específicos.

Evidências

1. Documento com a metodologia de gestão do risco.
2. Procedimentos que descrevem as metodologias de análise de riscos. Catálogo das ameaças e vulnerabilidades identificadas na estrutura da organização. Categorização dos ativos quanto à sua relevância para a organização.
3. Relatórios de avaliação quantitativa de riscos. Sistema de suporte à avaliação de riscos.

ID.AR-5

17 A organização garante que as respostas aos riscos são identificadas e priorizadas?

1. Os riscos são tratados, mas de forma não sistematizada.
2. A metodologia de riscos estabelece formalmente estratégias para o tratamento dos riscos identificados, de acordo com o apetite ao risco da organização.
3. Os riscos são categorizados numa escala de importância para a priorização dos tratamentos, e o seu tratamento tem em conta os custos financeiros e o potencial dano.

Evidências

1. N/A.
2. Formalização em documentação interna de riscos sobre a metodologia de tratamento de riscos. Critérios formais e aceites pela gestão de topo para definição dos critérios de tratamento dos riscos, conforme a importância dos ativos para a organização.
3. Revisão periódica das classificações dos riscos e dos critérios de classificação. Avaliação operacional e financeira da relação custo-benefício.

ID.GR-1

18 A organização define um processo de gestão de risco?

1. As estratégias para a gestão de riscos não estão definidas ou não são consistentes em toda a organização.
2. Existem estratégias definidas para a gestão de riscos e são consistentes em toda a organização, estando definidos os responsáveis pela gestão do processo e pelo tratamento dos riscos identificados.
3. Existe uma cultura de risco na organização, percebida em diversos níveis, sendo a gestão de riscos suportada por um sistema dedicado e os riscos revistos periodicamente.

Evidências

1. N/A.
2. Política de gestão de riscos. Exercício de análise e avaliação de riscos transversais à organização. Nomeação formal, através de e-mail ou de descritivo de função, do responsável pela coordenação da gestão de riscos. Identificação de responsáveis pelo tratamento dos riscos nos resultados das análises.
3. Evidências de cultura de risco, com estratégias e dinâmicas consistentes em toda a organização e identificadas de forma não ambígua entre os colaboradores. Software ou plataforma de suporte à gestão de riscos em pleno uso. Registo de avaliações dos riscos identificados e reavaliações de controlos implementados.

ID.GR-2

19 A organização determina e identifica a sua tolerância ao risco?

1. A tolerância ao risco é decidida arbitrariamente e/ou de forma *ad hoc*.
2. As estratégias de tratamento de riscos são relacionadas ao nível de risco aceite pela organização, sendo os processos de aprovação dos riscos definidos e aprovados pela gestão de topo.
3. Nas revisões das estratégias de riscos, os indicadores de tolerância ao risco são atualizados.

Evidências

1. N/A.
2. Registo formal na documentação da gestão de riscos da tolerância ao risco aceite; da estratégia de tratamento de riscos conforme o nível do risco percebido; dos riscos aceites pela gestão de topo.
3. Evidências da revisão das estratégias de risco, em simultâneo com os seus indicadores de tolerância.

ID.GR-3

20 A organização define a sua estratégia de tratamento do risco?

1. O tratamento dos riscos é feito de forma *ad hoc* e não sistematizada.
2. É identificada a estratégia de resposta aos riscos associados aos ativos críticos observados.
3. São consideradas orientações e boas práticas de tratamento de riscos no setor de atuação para a seleção da estratégia de tratamento.

Evidências

1. N/A.
2. Existem registos de riscos indicados, pelo menos para uma das quatro estratégias clássicas (negar, mitigar, transferir ou aceitar).
3. Resultados de *benchmarks* de mercado, regulações e orientações do governo ou do mercado para a seleção da estratégia de tratamento do risco.

ID.GL-1

21 A organização define, avalia e gere processos de gestão do risco da cadeia logística?

1. A cadeia de logística está identificada.
2. A organização aplica a gestão de riscos na sua cadeia logística.
3. Os fornecedores e parceiros são categorizados de acordo com o nível de risco atribuído após avaliação, e os controlos de segurança dos fornecedores críticos são avaliados regularmente.

Evidências

1. Documento com a identificação dos diferentes fornecedores e parceiros da cadeia logística.
2. A política de gestão de fornecedores indica a necessidade de tratamento da gestão de riscos nas atividades da organização e dos seus responsáveis, e uma periodicidade de análise.
3. Mapa de riscos que indica o risco dos fornecedores. Registos de avaliações de riscos dos fornecedores e dos seus impactos.

ID.GL-2

22 A organização avalia o risco da cadeia logística de cibersegurança?

1. Os fornecedores da organização, que fazem parte da cadeia de logística de cibersegurança, são identificados.
2. A política de fornecedores indica controlos específicos para a cadeia logística crítica da organização, bem como classifica-os quanto à sua criticidade.
3. Existe capacidade de, proativamente, definir controlos de segurança para novos fornecedores, encarregando-se a organização que o impacto na cadeia logística seja evitado.

Evidências

1. Documento com listagem de fornecedores envolvidos na cadeia de logística de cibersegurança.
2. Os fornecedores são categorizados conforme indicado nos critérios da política de gestão de fornecedores. Os fornecedores críticos e de cibersegurança são categorizados quanto à criticidade que têm para o negócio.
3. Critérios de classificação proativa de risco dos seus fornecedores. Formulário de registo de fornecedores integrado com a avaliação de riscos.

ID.GL-3

23 Os contratos com fornecedores respeitam o plano de gestão do risco para a cadeia logística?

1. Existe um processo formal de contratação de fornecedores.
2. A organização garante que o tema da segurança da informação é incluído nos contratos da cadeia logística.
3. A organização avalia os controlos de segurança dos seus fornecedores, em intervalos regulares.

Evidências

1. Contratos formais com os fornecedores relevantes para a cadeia de logística.
2. Cláusulas sobre confidencialidade e privacidade nos contratos e termos de contratação da organização. Registos da tomada de conhecimento e aceitação das políticas de segurança da parte dos parceiros e fornecedores.
3. Indicadores de acompanhamento dos controlos de segurança que dão visibilidade sobre a forma como a cadeia logística atende à gestão de riscos. Registos de validação de conhecimento e aceitação das políticas.

ID.GL-4

24 Os fornecedores são periodicamente avaliados?

1. A avaliação dos fornecedores é feita de forma não sistematizada.
2. As políticas internas da organização preveem a possibilidade de os seus fornecedores serem avaliados no âmbito da segurança da informação, existindo planos de auditoria orientados pela perceção do risco, que incluem os fornecedores.
3. Existem mecanismos de acompanhamento e monitorização dos controlos de riscos na cadeia logística.

Evidências

1. N/A.
2. Referência nas políticas e contratos com fornecedores à possibilidade de auditorias por parte da organização. Plano anual de auditoria de segurança da informação com a cadeia de fornecedores no âmbito, listados pelo nível de exposição ao risco.
3. Procedimentos e ferramentas de monitorização dos indicadores de segurança na cadeia logística. Revisões das auditorias realizadas e acompanhamento dos pontos identificados.

ID.GL-5

25 O plano de resposta e recuperação de desastre é exercitado com o acompanhamento de fornecedores?

1. Estão identificados os fornecedores que suportam os processos críticos da organização.
2. Os planos de resposta e recuperação de desastres definidos consideram a cadeia de fornecedores.
3. Validação dos planos de resposta e recuperação de desastres da organização, com a participação ativa de fornecedores críticos envolvidos no âmbito.

Evidências

1. Registos de fornecedores críticos à organização.
2. Registo de dependências a fornecedores externos na cadeia crítica da organização. Referência aos fornecedores nos planos de resposta a incidentes e recuperação de desastres.
3. Tratamento dos resultados de testes de recuperação e resposta a incidentes com o envolvimento dos fornecedores. Registos de testes realizados nos procedimentos de resposta e recuperação de desastres, com o envolvimento da cadeia de fornecedores críticos.

Proteger

PR.GA-1

1 O ciclo de vida de gestão de identidade está definido?

1. A associação de acessos de identidades é feita com base nos acessos atribuídos no passado.
2. Existem políticas de gestão de identidades e acessos, estando as etapas dos ciclos de acesso bem definidas e existe uma base única de identidades e regras de acesso.
3. Os acessos são estabelecidos e limitados de acordo com perfis funcionais, sendo revistos em intervalos regulares.

Evidências

1. Registo da associação de acessos atribuídos a identidades.
2. Políticas destinadas à gestão das identidades e dos acessos nos sistemas e acessos em geral. Procedimentos relativos à gestão de acessos. Documentação de um diretório centralizado, pelo qual as identidades e os acessos são geridos.
3. Perfis funcionais para cada tipo de acesso. Controlos que evitam acessos excessivos sem a justificação pelo descritivo funcional. Relatórios de revisão de acessos.

PR.GA-2

2 Existem controlos de acesso físico às redes e sistemas de informação?

1. Existem controlos que restringem o acesso físico e os acessos são registados permitindo a identificação individual.
2. Os acessos físicos são integrados com um sistema transversal de gestão de identidades e acessos.
3. Os acessos de pessoas externas são monitorizados e os acessos são avaliados regularmente.

Evidências

1. Evidências de instalação de controlos de acesso físico (portas, barreiras, torniquetes). Registos de entrada e saída dos ambientes físicos.
2. Registos de acessos físicos associados a um sistema integrado de identidades e acessos.
3. Registos de acompanhamento de pessoas externas por colaboradores com autorização de acesso a zonas seguras. Registo de revisão dos acessos físicos, de acordo com os perfis de acesso. Registo das avaliações regulares dos procedimentos para acessos físicos.

PR.GA-3

3 A organização gere os seus acessos remotos?

1. A organização suporta acessos remotos, mas não controla nem monitoriza os acessos.
2. Existem políticas internas que tratam de acessos remotos, controlados de maneira centralizada e integrada nos sistemas internos por soluções tecnológicas que aplicam a segurança específica para o efeito.
3. Autenticação federada aos demais sistemas da organização, com multi-fatores para acessos remotos, sendo estes acessos monitorizados e revistos regularmente.

Evidências

1. Documentação da solução de acesso remoto (VPN, *jumpserver*).
2. Registo de aceitação da política de acesso remoto através de VPN. Registo de aceitação da política de teletrabalho pelos colaboradores beneficiados. Documentação de sistema de VPN implementado com uso da criptografia adequada na autenticação e no tráfego.
3. Documentação de tecnologias de acesso com bloqueio proativo pelas regras de *logon* interativo, tempo de sessão e/ou origem das ligações. Documentação da integração da autenticação externa aos perfis de acessos definidos internamente. Registos de utilização de duplo fator de autenticação para acessos remotos. Registo de monitorização específica dos acessos remotos. Registo de revisões e revalidações dos acessos remotos.

PR.GA-4

4 A organização aplica, na gestão de acessos, os princípios do menor privilégio e da segregação de funções?

1. São atribuídos acessos de forma nominal e não são partilhados entre múltiplos colaboradores ou entidades, concedidos copiando os acessos anteriores de colaboradores com perfis similares.
2. Os acessos são concedidos conforme o perfil funcional, sendo perfis de acessos elevados atribuídos com critérios de restrição e segundo o princípio do menor privilégio.
3. A definição de funções e níveis de acessos é revista regularmente, bem como os acessos com privilégios elevados, havendo lugar a controlos complementares como férias obrigatórias e *job rotation*.

Evidências

1. N/A.
2. Registos de pedidos de acesso por perfil funcional. Registos de pedidos e aprovações apropriadas para acessos privilegiados.
3. Registos da execução da revisão de acessos. Listagem de acessos removidos, alterados e criados na última revisão. Registos correspondentes aos acessos disponíveis. Alertas de segurança sobre acessos privilegiados.

PR.GA-5

5 A organização protege a integridade das redes de comunicação?

1. As redes internas encontram-se segregadas conforme a sua finalidade.
2. A rede tem a sua topologia documentada e regras de acessos definidas e documentadas, bem como qualquer alteração nas regras de conexão é registada.
3. As regras de conexão são revistas, os equipamentos de redes de comunicação são monitorizados e as alterações são efetuadas após resultados de validação.

Evidências

1. Lista de *routers*, *firewalls* e demais tecnologias de redes de comunicações, que possibilitem a segmentação da rede.
2. Documentação que identifique as regras permitidas de conexão entre cada segmento da rede. Registos de eventos de operação e de auditoria produzidos pelos equipamentos de segurança de redes. Registos de pedidos de alteração de regras de *firewalls* ou outros equipamentos para segurança de redes de comunicações.
3. Registos de monitorização de eventos dos equipamentos de redes. Relatórios de testes de intrusão no âmbito da infraestrutura da rede de comunicação.

PR.GA-6

6 A organização verifica a identidade dos colaboradores e vinculá-las às respetivas credenciais?

1. Os colaboradores têm as suas credenciais e identidades registadas e vinculadas.
2. Os procedimentos de validação das identidades são registados em políticas, existindo um processo de gestão de identidades e acessos, com base na identificação dos colaboradores.
3. A gestão de acessos é revista e avaliada com recorrência e os resultados são utilizados para a melhoria do processo, bem como os antecedentes são revistos periodicamente.

Evidências

1. Registo da atribuição de credenciais nominais aos colaboradores.
2. Documentos com a política e procedimentos que suportam o processo de gestão de identidades e acessos.
3. Registos de revisão dos procedimentos de concessão de acessos, suportados pela verificação de antecedentes.

PR.GA-7

7 Estão definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação?

1. Os mecanismos de autenticação foram definidos de acordo com os sistemas.
2. Existe um sistema de gestão de identidades e acessos estabelecido e que abrange utilizadores, dispositivos e outros ativos de sistemas, bem como uma política de acessos.
3. As autenticações são realizadas de forma integrada e transversal entre sistemas e são reforçadas para evitar fraudes e/ou falhas em pontos únicos de validação.

Evidências

1. Conjunto de soluções de autenticação com palavras-passe, estabelecido consoante o sistema.
2. Registo de acessos concedidos conforme o sistema de autenticação, transversal aos sistemas. Registos de autenticação de acessos consoante a identificação e a autorização, independente de utilizadores e dispositivos.
3. Documentação de implementação de serviços de autenticação federada entre sistemas diversos. Observação de múltiplos fatores de autenticação em sistemas críticos.

PR.FC-1

8 Os colaboradores têm alguma formação em segurança da informação?

1. Os colaboradores apresentam alguma consciência sobre os temas de segurança da informação e como a organização os trata, sendo realizadas intervenções de consciencialização para o tema de segurança da informação.
2. As ações de formação e consciencialização são registadas em planos, procedimentos e metas da organização, bem como são planeadas consoante a audiência.
3. Realizam-se periodicamente ações de formação, e medem-se os resultados das ações de formação e consciencialização.

Evidências

1. Observação do comportamento dos colaboradores perante a temática da segurança da informação. Registos de sessões de formação e consciencialização dos colaboradores sobre o tema.
2. Formalização de um plano com calendarização de ações de formação estabelecida. Registo das ações de formação às partes interessadas.
3. Registos de avaliação do conhecimento e da absorção das formações e consciencializações. Utilização de meios de comunicação distintos para a otimização e ampliação das comunicações de segurança da informação.

PR.FC-2

9 Os utilizadores com acesso privilegiado compreendem quais são os seus papéis e responsabilidades?

1. Os utilizadores com acessos privilegiados são informalmente notificados das responsabilidades acrescidas, relativas aos acessos providenciados.
2. Os utilizadores de acessos privilegiados têm formação específica sobre segurança da informação e existem procedimentos de registo da aceitação de condições especiais de acessos para os utilizadores de acessos privilegiados.
3. São medidos os resultados das ações de formação e consciencialização aos utilizadores com acessos privilegiados, bem como existe uma garantia da atualidade da aceitação das condições especiais de acessos com privilégios elevados.

Evidências

1. N/A.
2. Plano de formação específico para os utilizadores com acessos privilegiados. Conteúdo programático da formação específica para utilizadores com acessos privilegiados. Registo das presenças de utilizadores com acessos privilegiados em ações de formação. Registo do termo de responsabilização sobre a utilização de sistemas com acessos privilegiados.
3. Registos de avaliação do conhecimento e da absorção das formações e consciencializações. Registo da renovação regular dos termos de responsabilidade sobre os sistemas. Evidências da recorrência de ações de formação ou consciencialização específicas, com os utilizadores de acessos privilegiados. Procedimento de ações de consciencialização aquando do encerramento do contrato do colaborador com acessos privilegiados.

PR.FC-3

10 As partes interessadas externas compreendem quais são os seus papéis e responsabilidades?

1. Estão estabelecidos requisitos mínimos de segurança da informação para a sua cadeia de clientes e fornecedores.
2. Existe formação e sensibilização sobre os requisitos de segurança que os clientes, parceiros e fornecedores devem seguir.
3. Os clientes, parceiros e fornecedores têm como dever cumprir os requisitos de segurança definidos, estando envolvidos no processo de melhoria contínua.

Evidências

1. Registo dos requisitos mínimos de segurança, no âmbito do relacionamento com fornecedores, parceiros e clientes.
2. Registo de formação para os agentes externos. Material de divulgação dos requisitos de segurança a serem seguidos.
3. Registos de termos de compromisso com os requisitos de segurança da organização. Registos correspondentes aos acessos disponíveis. Registos de auditorias aos clientes e fornecedores sobre o cumprimento dos requisitos de segurança estipulados.

PR.FC-4

11 A gestão de topo compreende as suas funções e responsabilidades?

1. A gestão de topo tem as suas funções e responsabilidades definidas de forma informal.
2. Os papéis e responsabilidades da gestão de topo no âmbito da segurança da informação estão estabelecidos.
3. Estão estabelecidos o envolvimento e a consciencialização da gestão de topo em temas de segurança da informação.

Evidências

1. N/A.
2. Matriz "RACI" da segurança da informação, onde se inclua a gestão de topo. Registo de papéis e responsabilidades dos membros da gestão de topo no tema da segurança da informação.
3. Registo da participação da gestão de topo em ações de consciencialização. Registo de políticas e documentos de segurança da informação aceites e "endossados" pela gestão de topo.

PR.SD-1

12 A organização protege os dados armazenados?

1. Estão estabelecidas regras de proteção da confidencialidade, integridade e disponibilidade dos ficheiros, documentos e dados.
2. Está estabelecida a classificação da informação consoante a sua sensibilidade e relevância.
3. Os dados são armazenados consoante os seus níveis de classificação, incluindo os dados *offline* (p. ex. cópias de segurança).

Evidências

1. Políticas de cifras. Evidências de regras para a salvaguarda de ficheiros, consoante o nível de segurança necessário.
2. Política, procedimentos e documentos complementares relativos à classificação da informação. Evidência de controlos de proteção da informação ajustados à classificação da mesma.
3. Gestão de controlos e sistemas criptográficos. Evidência de armazenamentos adequados consoante o local e tipo de informação armazenada e controlos implementados.

PR.SD-2

13 A organização protege os dados em circulação?

1. Existe perceção de riscos sobre os dados em circulação e são adotados controlos genéricos de proteção de dados em circulação.
2. As políticas e os procedimentos que tratem da proteção de dados em circulação são registados formalmente e são adotadas soluções criptográficas adequadas a cada situação.
3. É adotada a utilização de tecnologias de cifra dedicadas, consoante a classificação da informação, bem como os controlos compensatórios para situações adversas.

Evidências

1. Evidências de que existe uma perceção de risco sobre alguns tipos de dados mais críticos ao negócio. Utilização da criptografia em casos comuns.
2. Políticas e procedimentos que enderecem a proteção de dados em circulação. Utilização estruturada de serviços de criptografia para dados em circulação.
3. Procedimentos para definição da tecnologia de cifra consoante a classificação da informação. Registo de análise e avaliação de riscos para os casos adversos (p. ex. controlos compensatórios, registo da aceitação do risco, etc.).

PR.SD-3

14 A organização gere formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos?

1. Existe o registo informal ou *ad hoc* dos dados que entram e saem por meio de armazenamento físico e os dados em suporte amovível são protegidos de forma não sistematizada.
2. Existe o registo formal dos controlos de dados que entram e saem por meio de armazenamento físico.
3. Existe a garantia de que a destruição dos dispositivos amovíveis não exporá dados sigilosos, e é realizada uma revisão periódica dos procedimentos de descarte de dispositivos de armazenamento amovíveis e destruição definitiva de dados.

Evidências

1. Utilização de software de cifra para componentes amovíveis de forma não padronizada (por exemplo, departamentos diferentes usam ferramentas diferentes).
2. Políticas, normas e procedimentos que enderecem o ciclo de vida da informação, armazenada em ativos físicos amovíveis. Registos de responsáveis atribuídos em dispositivos amovíveis que possam conter dados. Adoção de software de cifra para componentes amovíveis.
3. Procedimentos de destruição de dispositivos amovíveis. Adoção de software para destruição definitiva de dados. Registo de testes de eficácia dos procedimentos de destruição de dispositivos de armazenamento e de destruição definitiva de dados.

PR.SD-4

15 A organização providencia a capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação?

1. A gestão da capacidade é efetuada sem ter em conta métricas bem definidas, não existindo nenhum processo formal para garantir a disponibilidade das redes e sistemas de informação.
2. As capacidades dos sistemas de informação são monitorizadas.
3. A disponibilidade dos recursos de redes e sistemas é garantida, existindo capacidades de gestão pró-ativa permitindo agir com base na previsão fundamentada.

Evidências

1. N/A.
2. Procedimentos e documentos de suporte à gestão de capacidades. Sistemas de monitorização das capacidades primárias.
3. Alarmística estabelecida para indicadores fora do esperado. Redundâncias dos recursos de redes e sistemas. Registos das ações de avaliação da gestão de capacidade.

PR.SD-5

16 A organização implementa proteções que evitam exfiltração de informação?

1. Estão formalizados os procedimentos de salvaguarda da informação contra meios de exfiltração.
2. Os controlos de proteção da informação que mitigue o risco de exfiltração de dados estão implementados, baseados na avaliação de risco.
3. Estão implementados processos e mecanismos de prevenção contra a perda de informação, e estes são revistos periodicamente.

Evidências

1. Implementação de procedimentos de salvaguarda e prevenção contra exfiltração (p. ex. definição de protocolos e formas de comunicação, restrição de uso de interfaces de extração de informação, etc.).
2. Classificação de informação em sistemas de mensagens e troca de emails. Bloqueios preventivos a sistemas não autorizados de partilha de ficheiros.
3. Implementação de soluções de Data Loss Protection (DLP). Registo de auditorias e avaliação dos controlos implementados.

PR.SD-6

17 A organização utiliza mecanismos de verificação para confirmar a integridade de software, firmware e dados?

1. Existe verificação manual ou não sistematizada da verificação de integridade dos sistemas de informação, *firmware* e dados.
2. Estão estabelecidas as ações que avaliem e atestem a integridade dos sistemas, sendo também avaliada a integridade de bibliotecas desenvolvidas por terceiros que estejam envolvidas no funcionamento dos sistemas de informação.
3. É avaliada, de forma transversal e regular, a integridade dos sistemas e dados e dependências de bibliotecas desenvolvidas por terceiros.

Evidências

1. N/A.
2. Documentos de suporte a processos/ procedimentos de verificação da integridade. Resultados dos testes estáticos, dinâmicos e interativos de segurança dos sistemas e infraestrutura.
3. Sistema de ferramentas centralizadas de verificação de integridade. Relatórios de integridade dos diferentes sistemas.

PR.SD-7

18 Os ambientes de desenvolvimento e de teste estão separados de ambientes de produção?

1. A segregação de ambientes é efetuada de forma *ad hoc* e não sistematizada.
2. Estão estabelecidas zonas distintas para desenvolvimento e produção, bem como normativos internos sobre desenvolvimento seguro.
3. É garantido o controlo do acompanhamento da evolução do software em ambiente de produção, bem como é protegido de eventos não planeados. Estão, também, implementadas soluções tecnológicas para a proteção dos dados de teste.

Evidências

1. Registo de alguns sistemas com ambientes de desenvolvimento segregados dos ambientes de produção.
2. Documentos de suporte ao desenvolvimento seguro de software. Registo da segregação de todos os diferentes ambientes.
3. Registos de execução dos processos de gestão de alterações e versões. Soluções para anonimizar dados de produção para fins de testes. Controlo de versionamento de software.

PR.SD-8

19 A organização implementa mecanismos de validação e verificação da integridade do hardware?

1. Existe verificação manual ou não sistematizada da verificação de integridade do hardware.
2. A integridade do hardware é gerida.
3. A manutenção preventiva e preditiva é realizada.

Evidências

1. N/A.
2. Registo de contrato de manutenção dos equipamentos pelo fabricante ou fornecedor certificado.
3. Registo de plano de manutenção periódica. Sistemas de monitorização e alarmística para a integridade do hardware.

PR.PI-1

20 Existe uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança?

1. Apenas de forma informal e não sistematizada.
2. Existem regras que definem a configuração base de redes e sistemas, e estas estão estabelecidas para cada tipo de sistema.
3. As configurações base dos sistemas são monitorizadas, estando garantidas as atualizações de seguranças, bem como a integração das regras base em processos de entrega contínua.

Evidências

1. N/A.
2. Políticas que definam as configurações base. Procedimentos de configuração dos equipamentos conforme requisitos base. Registo da especificação de configurações base para as tecnologias utilizadas.
3. Registo de monitorização contra alterações das configurações base dos sistemas. Sistema de gestão de atualizações de segurança. Sistema de integração/entrega contínua (CI/CD).

PR.PI-2

21 Está implementado um ciclo de vida de desenvolvimento seguro de software?

1. Está definido um conjunto rudimentar de requisitos de segurança mínimos para os projetos de desenvolvimento.
2. Existe a definição exaustiva dos requisitos de segurança a seguir nos projetos de desenvolvimento, bem como regras internas para o desenvolvimento seguro.
3. Os controlos dinâmicos de segurança nos ciclos de desenvolvimento estão implementados e o código fonte é monitorizado e gerido de maneira segura.

Evidências

1. Conjunto rudimentar de medidas de segurança a aplicar para projetos de desenvolvimento.
2. Registos de análise de riscos de projetos e indicação de requisitos de segurança. Conjunto de políticas, procedimentos e requisitos de segurança para o desenvolvimento seguro.
3. Processos de testes e validações de segurança estabelecidos no ciclo de desenvolvimento. Uso de ferramentas de integração contínua (CI). Evidências da gestão de códigos-fonte e controlo de versão.

PR.PI-3

22 Está implementado um processo de gestão de alterações?

1. Existe um processo informal para a gestão de alterações.
2. Estão estabelecidas regras internas para a gestão de alterações, e os processos de avaliação e aprovação de alterações estão definidos.
3. Os mecanismos técnicos para acompanhar as alterações estão estabelecidos, e é realizada a revisão periódica dos procedimentos e registos de alterações.

Evidências

1. Evidências *ad hoc* de alterações passadas.
2. Documentação de procedimentos de gestão de alterações. Evidências de análise e avaliação prévia às alterações.
3. Adoção de sistema de integração e entrega contínua (CI/CD). Evidência de avaliação dos registos e procedimentos de alterações, conforme procedimentos e aprovações.

PR.PI-4

23 São realizadas, mantidas e testadas cópias de segurança dos dados da organização?

1. São realizadas cópias de segurança de sistemas e ficheiros de forma não sistematizada.
2. Estão estabelecidas regras internas formais para a realização das cópias de segurança, sendo a integridade das cópias verificada de forma independente.
3. A confidencialidade, integridade e disponibilidade da informação armazenada das cópias de segurança são garantidas. Os procedimentos realizados para as cópias de segurança são verificados.

Evidências

1. Evidência da cópia de segurança de sistemas e ficheiros importantes.
2. Documentos de suporte às cópias de segurança (políticas, procedimentos, registos, padrões, etc.). Registo da realização de testes de restauro das cópias de segurança em ambiente isolado.
3. Utilização de sistemas criptográficos de dados, cuja confidencialidade seja necessária. Estabelecer ciclos de diferentes tipos de restauro e uso das cópias de segurança. Emprego de soluções automatizadas para a validação da integridade das cópias de segurança. Evidências de avaliação regular dos sistemas, ficheiros e procedimentos de cópias de segurança.

PR.PI-5

24 As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização são seguidas?

1. A proteção de infraestruturas é feita de forma não sistematizada (por exemplo, apenas alguns sistemas são protegidos por UPS).
2. As infraestruturas estão protegidas contra alterações elétricas que causem danos, e as alterações no ambiente que possam afetar os sistemas são monitorizadas e detetadas.
3. A prevenção contra alterações elétricas que possam causar danos é feita de forma proativa, existindo mecanismos que garantem a constância no fornecimento de energia. A eficácia dos controlos para manter a organização funcional é auditada.

Evidências

1. N/A.
2. Aplicação de sistemas de proteção contra variações na corrente elétrica, que possam danificar os sistemas. Utilização de sensores de fumo, humidade e temperatura.
3. Existência de sistemas de gestão automática do fornecimento de eletricidade. Utilização de fontes alternativas de eletricidade (ex.: geradores). Registo de testes do plano de continuidade, considerando controlos físicos.

PR.PI-6

25 Os dados são destruídos de acordo com a política definida?

1. Os dados são destruídos de forma *ad hoc*.
2. A informação sensível é destruída apropriadamente, estando documentados procedimentos de destruição de informação sigilosa.
3. É realizada a avaliação da eficácia da destruição da informação em meio físico e digital.

Evidências

1. N/A.
2. Procedimentos e políticas que tratem da higienização de ficheiros. Sistemas de higienização de ficheiros.
3. Registo de revisão dos mecanismos utilizados para a higienização de ficheiros, tanto físicos quanto digitais. Evidência do comprometimento de parceiros e prestadores de serviços com a higienização de ficheiros compartilhados ou de responsabilidade da organização. Registo das eliminações realizadas.

PR.PI-7

26 Os processos de proteção são continuamente melhorados?

1. Os processos de proteção são efetuados de forma não sistematizada.
2. Estão estabelecidos procedimentos e controlos de monitorização e melhoria continua.
3. Os procedimentos e controlos são revistos regularmente, sendo realizadas auditorias internas recorrentes, aos controlos de segurança.

Evidências

1. N/A.
2. Procedimentos de controlo e monitorização.
3. Registos de atualizações dos procedimentos e controlos. Planeamento de auditoria interna. Registo de auditorias internas, realizadas no âmbito da segurança da informação. Planos de ação para tratamento de resultados de auditoria.

PR.PI-8

27 A efetividade das tecnologias de proteção é tida em conta na melhoria dos processos de proteção?

1. Os processos de proteção são melhorados de forma não sistematizada.
2. A eficácia das tecnologias de proteção é medida e avaliada, e existe um processo estabelecido de evolução através de lições aprendidas.
3. Os processos de tratamento de incidentes são revistos regularmente, sendo as lições aprendidas comunicadas às partes relevantes.

Evidências

1. N/A.
2. Registos de melhorias aos processos de proteção. KPIs (indicadores de performance) das tecnologias de proteção.
3. Registo de lições aprendidas com eventos de segurança. Registo de revisões e/ou auditorias nos processos de tratamento de incidentes.

PR.PI-9

28 Os planos de resposta a incidentes, da continuidade de negócio, de recuperação de incidentes e de recuperação de desastres são atualizados?

1. Os planos de resposta são atualizados de forma *ad hoc*.
2. Existem processos, formalmente definidos, para as atividades relativas a resposta a incidentes e garantia da resiliência da organização, sendo os planos de resposta medidos e avaliados quando executados.
3. As estratégias e ações para a resposta a incidentes e para a garantia da continuidade da organização são avaliadas regularmente.

Evidências

1. N/A.
2. Registo formal de processos e políticas para a resposta a incidentes. Registo formal de processos e políticas para a continuidade de negócio. Registo de sessões de consciencialização ou outras formas de divulgação dos planos de continuidade.
3. Registo de revisão dos planos de continuidade de negócio. Registo de ações para o tratamento de incidentes.

PR.PI-10

29 Os planos de resposta e recuperação são testados e exercitados?

1. Os planos de resposta são exercitados de forma não sistematizada.
2. Os planos de continuidade são registados e testados quanto ao âmbito definido.
3. O plano de continuidade é testado pela sua eficiência em âmbito realista.

Evidências

1. Registo de exercícios pontuais e isolados.
2. Registo de exercícios sistematizado (ex.: restauro de ambientes, “table top”, etc.).
3. Registo de simulacros de casos reais em departamentos da organização ou transversais. Registo de revisão das estratégias de continuidade e garantia da sua atualização.

PR.PI-11

30 A cibersegurança é contemplada nos processos de gestão de recursos humanos?

1. O registo dos colaboradores é realizado.
2. Estão estabelecidas regras para a seleção, recrutamento e contratação, bem como para a cessação da contratação.
3. Existem perfis funcionais com competências em cibersegurança e segurança da informação, para as contratações, estando definidas ações para o tratamento do não cumprimento das normas internas de segurança da informação.

Evidências

1. Dossier dos colaboradores com dados cadastrais identificativos.
2. Procedimentos e políticas de contratação, mobilidade e cessação de funções de colaboradores.
3. Perfis funcionais com competências em cibersegurança e segurança da informação. Ações disciplinares para casos de infração contra a segurança da informação.

PR.PI-12

31 Está definido e implementado um processo de gestão de vulnerabilidades?

1. A pesquisa de vulnerabilidades é executada em intervalos regulares.
2. A análise de vulnerabilidades é regular e sistemática. As vulnerabilidades são identificadas com equipas de tratamento adequadas e são exploradas, para atestar o seu nível de risco real.
3. É avaliado regularmente o processo de análise de vulnerabilidades, estando estabelecidos planos de ação formais para o tratamento das vulnerabilidades, onde as partes interessadas, externas, são envolvidas.

Evidências

1. Plano de avaliação das vulnerabilidades. Relatório de ferramentas automáticas de pesquisa de vulnerabilidades.
2. Registo de submissão de vulnerabilidades para serem tratadas por partes interessadas. Registo de análise de vulnerabilidades, realizado regularmente, e do seu devido tratamento. Documentação de adoção de ferramenta de pesquisa de vulnerabilidades. Relatório recente (<= 1 ano) de testes de intrusão nos sistemas e infraestrutura.
3. Registo da revisão regular do processo de análise de vulnerabilidades e tratamento de dados. Evidência do apoio de fornecedores, parceiros e entidades competentes no tratamento das vulnerabilidades. Planos de ação para o tratamento de vulnerabilidades.

PR.MA-1

32 As atividades de manutenção e reparação dos ativos da organização são realizadas e registadas em programas e planos aprovados e controlados?

1. As atividades de manutenção são realizadas sem seguir um processo formal e sem registo controlado.
2. Os processos de manutenção são realizados formalmente e envolvem as pessoas adequadas.
3. As manutenções realizadas por pessoas externas são acompanhadas adequadamente. O fluxo de trabalho de requisições de manutenção e reparação está automatizado, bem como estão estabelecidos períodos de manutenção preventiva aos ativos da organização.

Evidências

1. Registos ocasionais de manutenções efetuadas.
2. Políticas e procedimentos de manutenções. Evidências da consciencialização e formação de colaboradores para realizar as manutenções necessárias. Registo de autorizações de perfis de acessos para fins de manutenção.
3. Registo de manutenções preventivas planeadas. Documentação de ferramenta de gestão de pedidos para acompanhar as manutenções. Implementação de controlo e registo de acesso em áreas seguras.

PR.MA-2

33 As operações de manutenção remota das redes são revistas, aprovadas, executadas e registadas?

1. As manutenções remotas são realizadas sem um processo formal de aprovação.
2. As manutenções remotas são realizadas conforme aprovação prévia, estando estabelecidos meios seguros.
3. Os controlos de acompanhamento do fluxo de solicitações e aprovações para as manutenções remotas estão automatizados, existindo a garantia de que a conexão é encerrada sempre que não for necessária à sua manutenção. Estão estabelecidas métricas de acompanhamento e garantia das manutenções.

Evidências

1. Registos ocasionais de manutenções remotas.
2. Registo dos fluxos de avaliação e aprovação das manutenções remotas, conforme procedimentos definidos. Infraestrutura de conexão e autenticação forte com agentes externos para as manutenções.
3. Uso de sistema de gestão de *workflow* para pedidos e fluxos de aprovação das manutenções. Contratos, SLAs e demais registos que atestem a garantia das manutenções. Registos tecnológicos que indiquem a terminação das conexões sempre que não seja necessário estarem ativas.

PR.TP-1

34 Os registos de auditoria e de histórico são documentados, implementados e revistos de acordo com as políticas?

1. Os registos de auditoria não seguem um processo de gestão formal.
2. Os registos de eventos para auditorias são geridos de maneira sistémica, com formatos e taxonomias definidos. Estão estabelecidos critérios formais para a auditoria de sistemas.
3. Os registos de auditorias transversais aos sistemas da organização são geridos centralmente, e a integridade dos registos de eventos para fins de auditorias é garantida.

Evidências

1. Registos ocasionais de auditoria.
2. Políticas e normas relativas à coleta e análise de registos de eventos. Procedimentos documentados sobre a coleta e tratamento dos registos de eventos para a análise. Documentação de sistema de coleta, tratamento e análise dos registos de eventos.
3. Armazenamento, tratamento e correlação de registos de eventos em sistema centralizado de análise para fins de auditorias. Existência de controlos técnicos de integridade dos registos, tais como validação por função *hash*, sincronização dos relógios e garantia do *timestamping*.

PR.TP-2

35 Os suportes de dados amovíveis são protegidos e a sua utilização é restrita, de acordo com a política definida?

1. Existe uma implementação básica e *ad hoc* de medidas de proteção aos suportes de dados amovíveis.
2. Estão estabelecidas regras de uso e boas práticas sobre dispositivos amovíveis, bem como mecanismos técnicos para a proteção de dados em dispositivos amovíveis. É feita a promoção de ações de sensibilização dos utilizadores sobre os riscos associados aos dispositivos amovíveis.
3. A utilização de dispositivos amovíveis é bloqueada e é garantida a higienização dos dispositivos amovíveis no momento da sua destruição.

Evidências

1. Evidência de *Bitlocker* ativo em discos amovíveis. Políticas de domínio aplicadas para restrição de acesso a discos amovíveis.
2. Registar políticas, padrões, normas e boas práticas sobre a utilização de dispositivos amovíveis. Documentação da utilização de soluções criptográficas para dispositivos amovíveis. Registos de ações de sensibilização sobre a utilização aceitável de dispositivos amovíveis.
3. Emprego de bloqueios físicos ou lógicos para o uso de dispositivos amovíveis de armazenamento. Procedimentos de descarte seguro de dispositivos amovíveis. Utilização de sistemas de destruição segura de dados em dispositivos amovíveis.

PR.TP-3

36 O princípio da minimização de funcionalidades é incorporado na configuração de sistemas, de modo a fornecer apenas os recursos essenciais?

1. Os sistemas são configurados com os recursos necessários de forma não sistematizada.
2. Os acessos concedidos são os mínimos necessários e são estabelecidas funcionalidades mínimas para cada necessidade de operação.
3. Os acessos são condizentes com as necessidades mínimas para as funções, e os requisitos mínimos são revistos e atualizados periodicamente.

Evidências

1. Registos ocasionais e isolados de sistemas configurados apenas com as funcionalidades mínimas necessárias.
2. Integração com gestão de identidades e acessos. Registo formal de políticas e padrões de configurações de recursos mínimos por defeito.
3. Registo de revisões periódicas aos padrões e procedimentos de configurações de sistemas. Registo da revisão dos acessos concedidos. Revisão das definições de perfis funcionais por necessidades de acessos.

PR.TP-4

37 As redes de comunicações e de controlo são protegidas?

1. As zonas de rede são segregadas de forma não sistematizada e a tecnologia de encriptação é aplicada de forma *ad hoc*.
2. As zonas de rede são segmentadas conforme a finalidade e são utilizadas soluções tecnológicas de filtro de fluxo de dados.
3. São revistas periodicamente as configurações dos sistemas de filtro das conexões. As alterações na rede obedecem a processos de validação sistematizados.

Evidências

1. Registo de sistemas protegidos com SSL/TLS. Registos da impossibilidade de chegar a qualquer ponto da rede a partir dos postos de trabalho dos colaboradores.
2. Diagrama de redes a indicar a segmentação por zonas. Registo da utilização de IDS/IPS, *firewalls*, *proxies*, WAFs e outras soluções tecnológicas para filtro e bloqueio de dados em transmissão.
3. Registo de revisões regulares das definições e dos sistemas de segurança definidos (IDS/IPS, *firewalls*, *proxies*, WAFs, etc.). Registo de processos da gestão de alterações.

PR.TP-5

38 São implementados mecanismos para cumprir os requisitos de resiliência em situações adversas?

1. A incorporação de resiliência nos sistemas e redes de comunicações é aplicada de forma não sistematizada.
2. Os sistemas são protegidos contra a sobrecarga de acessos, e os sistemas críticos são resilientes.
3. A resiliência das infraestruturas às situações adversas é gerida e existe a garantia de que eventos inesperados não causam negação de serviço das operações.

Evidências

1. Redundância ocasional e isolada de sistemas ou equipamentos de rede de comunicações.
2. Adoção de soluções de balanceamento de carga. Redundância dos sistemas críticos.
3. Registo da alta disponibilidade dos sistemas críticos. Documentos de suporte ao plano de continuidade de negócios.

Detetar

DE.AE-1

1 Existe um modelo de referência de operações de rede e fluxo de dados?

1. Não
2. São detetadas as alterações na infraestrutura e estas podem ser tratadas nos modelos de referência estabelecidos.
3. Existem modelos de referência que são revistos periodicamente.

Evidências

1. N/A
2. Registos de utilização de plataforma de monitorização. Registo de formação no contexto de deteção. Registo de procedimentos para modelos de referência interna.
3. Registos de alterações/revisões.

DE.AE-2

2 Os eventos detetados são analisados de forma a serem identificados os alvos e os métodos de ataque?

1. É realizada uma análise *ad hoc* dos eventos, sem procedimento de tratamento formalizado e implementado.
2. São detetadas tentativas de ataque e incidentes de segurança e está estabelecido o tratamento apropriado de incidentes de segurança.
3. Os incidentes de segurança são identificados através da análise dos eventos coletados, e está estabelecida a resposta apropriada.

Evidências

1. Registo de análise dos eventos.
2. Registo de incidentes originados pela deteção e monitorização. Registo de análise e tratamento.
3. Documentação de sistema de correlação de eventos. Registos de incidentes e respetivo tratamento

DE.AE-3

3 Os eventos são coletados e correlacionados a partir de várias fontes e sensores?

1. Os eventos são coletados centralmente e existe correlação *ad hoc* com fontes não sistematizadas.
2. Os eventos de segurança são geridos e analisados e são considerados eventos de diversas fontes, internas e externas.
3. Existe melhoria contínua dos controlos, a partir do tratamento dos eventos anteriores, e estão estabelecidos mecanismos de controlo de um evento de segurança nas suas infraestruturas.

Evidências

1. Registo de eventos coletados num sistema central.
2. Políticas e procedimentos de gestão e correlação de eventos de segurança. Registos de fontes de conhecimento. Registos de utilização do sistema de correlação de eventos.
3. Utilização de registos e tratamentos anteriores para melhoria do sistema. Registos da existência de *honeypots* geridos nas estruturas da organização.

DE.AE-4

4 O impacto dos eventos é classificado?

1. Os eventos de segurança são classificados conforme o seu impacto percebido.
2. Está estabelecido um processo de gestão de eventos, aferindo os efeitos do impacto de um evento.
3. A gestão de incidentes é acionada a partir da gestão de eventos.

Evidências

1. Registo dos eventos categorizados.
2. Documentos de apoio ao processo de gestão de eventos. Metodologias de avaliação do impacto de um evento.
3. Registos que interliguem eventos detetados a registos na gestão de incidentes.

DE.AE-5

5 Estão definidos os limites de alerta para incidentes?

1. Os incidentes são abertos sem limite formal definido para o número de eventos relacionados.
2. Está estabelecido um processo de gestão de eventos, bem como estabelecida a definição de incidentes de segurança no contexto da organização.
3. Os incidentes são analisados e avaliados com base no risco percebido, sendo tratados conforme o seu nível de complexidade e impacto.

Evidências

1. Registos ocasionais de incidentes de segurança, sem consistência no número de eventos necessários à constituição formal de um incidente.
2. Documentos de apoio ao processo de gestão de eventos. Registo da taxonomia de incidentes e das suas prioridades no tratamento.
3. Ferramentas de correlação de eventos. Limites a serem considerados para a determinação de um incidente, ainda que sendo resultado de eventos isolados. Critérios de elevação/decréscimo de eventos numa escala.

DE.MC-1

6 As redes e sistemas de informação são monitorizados para detetar potenciais incidentes?

1. A monitorização é realizada sem um sistema automático de deteção ou com deteção manual.
2. É realizada a monitorização e proteção face a comportamentos anómalos na rede, que possam representar um incidente.
3. É realizada a associação de eventos de segurança de origens distintas. Os acessos a ativos conhecidos são restringidos. A gestão de incidentes é suportada por uma equipa dedicada.

Evidências

1. Registos ocasionais de deteções manuais.
2. Implementação de sistemas de monitorização e proteção da rede.
3. Implementação de sistema de gestão e correlação ee eventos. Regras de acesso às infraestruturas e sistemas. Existência, na organização, de uma equipa dedicada à gestão de incidentes.

DE.MC-2

7 O ambiente físico é monitorizado para detetar potenciais incidentes de segurança?

1. Os acessos físicos são monitorizados e registados, mas a deteção de incidentes de intrusão física é manual.
2. Estão estabelecidos controlos de monitorização de áreas seguras, e estão instalados alarmes para tentativas de acessos não autorizados.
3. Os acessos físicos são revistos em intervalos regulares.

Evidências

1. Registos ocasionais de deteção de incidentes de segurança física.
2. Suporte da gestão de acessos para segurança física. Instalação de sistemas de CCTV. Documentação de suporte aos alarmes instalados.
3. Registos de auditorias nos controlos de acesso e monitorização dos ambientes físicos.

DE.MC-3

8 A atividade dos colaboradores é monitorizada para detetar potenciais incidentes?

1. A atividade é monitorizada, mas a deteção de incidentes é manual.
2. Os eventos de segurança levam em conta as ações dos colaboradores, e estão estabelecidos padrões fiáveis de monotorização de colaboradores.
3. Os eventos dispersos são analisados em contexto, e existe a capacidade de antecipar incidentes de segurança a partir da análise de tendências.

Evidências

1. Registos ocasionais de incidentes originados na deteção manual, baseados no comportamento digital dos colaboradores.
2. Suporte dos registos de eventos que identificam o responsável. Formalização de padrões e métricas de referência para a monitorização das atividades dos colaboradores. Registo de sistema central de armazenamento e gestão de eventos.
3. Utilização da correlação de eventos para a monitorização e registo de incidentes. Registos de alertas preditivos.

DE.MC-4

9 A organização identifica e implementa mecanismos para deteção de código malicioso?

1. A deteção da presença de código malicioso na infraestrutura é reativa.
2. Estão estabelecidas regras formais de avaliação de códigos maliciosos, e realizam-se verificações periódicas de código malicioso.
3. Estão estabelecidos procedimentos de resposta integrada a incidentes, onde a eficácia dos sistemas de antivírus é avaliada.

Evidências

1. Implementar ferramentas de antivírus nas estações de trabalho e servidores.
2. Apoio de políticas de antivírus. Sistemas de antivírus configurados para pesquisas periódicas e recorrentes.
3. Integração do sistema de antivírus com o sistema central de gestão de eventos de segurança. Integração do sistema de análise comportamental com o sistema central de gestão de eventos de segurança. Auditorias aos sistemas de antivírus. Registo de atividades de análise de código. Registo de atividades para engenharia reversa de código malicioso.

DE.MC-5

10 A utilização de aplicações não autorizadas em dispositivos móveis é detetada?

1. As aplicações em dispositivos móveis da organização são monitorizadas, mas a deteção de aplicações não autorizadas é manual.
2. Estão definidas as aplicações permitidas nas redes e sistemas, e o comprometimento do colaborador em não utilizar sistemas não autorizados é garantido.
3. A gestão do parque de dispositivos móveis é feita de forma centralizada, de forma integrada com o sistema de gestão de eventos de segurança, existindo a capacidade de correlacionar os eventos de segurança com os dispositivos móveis.

Evidências

1. Registo ocasional de incidentes de segurança, com origem na deteção manual de aplicações não autorizadas.
2. Estabelecimento de *whitelists* e/ou *blacklists* de aplicações e sistemas. Termo de responsabilidade dos utilizadores sobre a utilização dos equipamentos.
3. Gestão dos sistemas de forma a ser capaz de monitorizar aplicações instaladas nos equipamentos. Instalação de sistema central de gestão de dispositivos móveis. Registos de incidentes de segurança, com origem na deteção automática de aplicações não autorizadas.

DE.MC-6

11 As atividades dos prestadores de serviços externos são monitorizadas para deteção de incidentes?

1. As atividades dos prestadores de serviços externos são monitorizadas, mas a deteção de incidentes é manual e não sistematizada.
2. Os pedidos de acesso remoto são identificados e avaliados, e estão estabelecidas formalmente as regras de acesso remoto para prestadores de serviços externos.
3. É realizada a avaliação dos eventos relativos aos acessos externos, sendo revistos regularmente os acessos e as permissões concedidas a prestadores de serviços externos.

Evidências

1. Registos ocasionais de incidentes de segurança, com origem em atividades suspeitas, por prestadores de serviços externos, detetadas manualmente.
2. Adoção de sistemas de deteção e prevenção de intrusões. Suporte de políticas, normas e procedimentos para a interação com prestadores de serviços externos. Gestão de acessos dos prestadores de serviços externos.
3. Integração com sistemas de correlação de eventos. Suporte de atividades de auditoria de segurança na revisão e avaliação dos acessos de prestadores de serviços externos. Registos de incidentes de segurança, com origem em atividades suspeitas detetadas automaticamente, por prestadores de serviços externos.

DE.MC-7

12 Os acessos não autorizados de colaboradores, conexões, dispositivos e software são monitorizados?

1. Os acessos são monitorizados e analisados manualmente.
2. Os pedidos de acesso às infraestruturas e servidores são monitorizados, sendo os dados dispersos recolhidos e centralizados para análise de anomalias.
3. Os eventos de acesso e incidentes relacionados são tratados.

Evidências

1. Registos ocasionais de monitorização e análise de acessos não autorizados, detetados manualmente.
2. Implementação de sistemas de deteção e prevenção de intrusões. Registos de eventos de acesso aos servidores e sistemas.
3. Sistema de correlação de eventos. Relatórios de incidentes.

DE.MC-8

13 São efetuados rastreamentos de vulnerabilidades?

1. A pesquisa por vulnerabilidades nos sistemas e redes de comunicação é feita pontualmente.
2. As vulnerabilidades identificadas nos sistemas e redes de comunicação são analisadas regularmente.
3. A análise de vulnerabilidades está integrada com outros processos da organização, e as vulnerabilidades identificadas são geridas.

Evidências

1. Relatórios ocasionais de vulnerabilidades.
2. Plano de análise de vulnerabilidades. Registos de suporte à análise e avaliação das vulnerabilidades.
3. Integrar a análise de vulnerabilidades com processos de testes e análises de segurança em sistemas e aplicações. Registo de planos de ação para o tratamento das vulnerabilidades.

DE.PD-1

14 Estão definidos os papéis e responsabilidades na deteção de eventos anómalos?

1. As responsabilidades na deteção de eventos anómalos são definidas informalmente.
2. Os responsáveis pelo tratamento de eventos anómalos são identificados, e os colaboradores são esclarecidos sobre a deteção de eventos anómalos.
3. Estão estabelecidas as responsabilidades no processo de deteção de eventos anómalos, estando envolvidos os agentes externos na deteção desses eventos.

Evidências

1. Registo das responsabilidades atribuídas.
2. Comunicados, nomeações ou qualquer outro elemento de suporte na aferição do responsável pelo tratamento dos eventos anómalos. Material de apoio às sessões de consciencialização.
3. Documentação de suporte ao estabelecimento de responsabilidades. Acordos de prestação de serviços que apresentam termos sobre a responsabilização na deteção de eventos anómalos.

DE.PD-2

15 As atividades de deteção cumprem com todos os requisitos aplicáveis?

1. As atividades de deteção seguem um processo *ad hoc*.
2. Os incidentes são detetados e identificados a partir dos eventos registados, estando os responsáveis por atividades de deteção identificados.
3. Estão estabelecidas ações de validação dos controlos, sendo a integridade dos dados garantida pela aplicação dos controlos.

Evidências

1. Registos de deteção de forma informal.
2. Relatórios ou indicadores de utilização de sistema de correlação de eventos. Matriz RASIC dos envolvidos nas atividades de deteção.
3. Registos de suporte a auditorias internas. Utilização de soluções de *hashing* na assinatura de registos.

DE.PD-3

16 Os processos de deteção são testados?

1. Os processos de deteção são medidos de forma *ad hoc*.
2. Existe um processo sistemático de analise aos processos de deteção, sendo os processos medidos regularmente.
3. A integridade e a fiabilidade dos processos de deteção são avaliadas.

Evidências

1. Registos ocasionais de testes aos serviços de deteção.
2. Planos de teste para os processos de deteção. Resultados da análise aos processos de deteção.
3. Resultados de testes de integridade aos processos de deteção. Resultados e análise da fiabilidade dos processos de deteção. Registos de aplicação de metodologias de melhoria contínua.

DE.PD-4

17 A informação sobre deteções de eventos é comunicada?

1. Os eventos de segurança são reportados internamente e de forma informal.
2. Está estabelecido internamente um canal de comunicação adequado, e os incidentes detetados são registados adequadamente.
3. Está definida a gestão centralizada e otimizada da deteção dos incidentes.

Evidências

1. Relatórios ou emails ocasionais de deteções de eventos e respetivas comunicações internas.
2. Documentos de suporte à gestão de incidentes. Registo de eventos detetados que resultam em incidentes.
3. Documentação de uma plataforma centralizada de resposta a incidentes.

DE.PD-5

18 Os processos de deteção são melhorados continuamente?

1. Os processos de deteção são melhorados de forma não sistematizada.
2. Existem mecanismos de medição e avaliação dos processos de deteção.
3. Os resultados da avaliação são usados para informar o processo de melhoria, sendo utilizados para melhorar os processos de deteção regularmente.

Evidências

1. Atualizações isoladas dos processos de deteção.
2. Resultados da avaliação dos processos de deteção quanto à eficiência.
3. Registo de tratamento dos planos de ação de melhorias.

Responder

RS.PR-1

1 Existe um plano de resposta a incidentes?

1. Existem procedimentos *ad hoc* ativados de forma reativa.
2. Os processos de resposta a incidentes são sistematizados e incluem fases de contenção e erradicação, bem como a identificação de responsáveis e o escalonamento.
3. É garantida a integridade das evidências analisadas, e a resposta é dada conforme o nível de escalonamento.

Evidências

1. Registos de execução de atividades de resposta a incidentes.
2. Documentos de suporte ao tratamento de incidentes.
3. Registos de validação de integridade. Documentos com os critérios de escalonamento.

RS.CO-1

2 Cada colaborador conhece o seu papel na resposta a um incidente?

1. Existe conhecimento informal e não estruturado das funções de cada funcionário.
2. Os colaboradores têm conhecimento sobre os procedimentos e estão estabelecidos os guiões de resposta a incidentes.
3. Existe envolvimento das partes externas relevantes na resposta a incidentes.

Evidências

1. Entrevistas/Questionários realizados aos funcionários.
2. Documentos de suporte à resposta de incidentes. Registos de sessões de formação. Guiões de resposta.
3. Mapa das partes externas relevantes. Estabelecimentos dos papéis e responsabilidades.

RS.CO-2

3 Existem critérios para reportar incidentes?

1. Existe conhecimento informal e não estruturado dos canais de reporte de incidentes.
2. Estão estabelecidos critérios de reporte de incidentes.
3. Os critérios de reporte de incidentes estabelecidos envolvem as partes externas interessadas, e são realizados de maneira integrada.

Evidências

1. Entrevistas/Questionários realizados aos funcionários.
2. Definições dos canais de reporte de incidentes. Documentos de suporte ao reporte de incidentes. Registo de divulgação dos canais adequados.
3. Registo de reportes de incidentes, envolvendo equipas externas. Documentação da plataforma de resposta a incidentes.

RS.CO-3

4 As informações são partilhadas de acordo com o plano de resposta?

1. A identificação das partes interessadas para comunicação é informal e não estruturada.
2. A comunicação de um incidente é do conhecimento de todos os envolvidos.
3. Estão estabelecidos canais seguros de comunicação, bem como as partes externas interessadas incluídas na comunicação.

Evidências

1. Registo das partes interessadas, internas e externas, para comunicação de incidentes.
2. Plano de comunicação de incidentes. Registo de formação/consciencialização sobre partilha de informação no plano de resposta a incidentes.
3. Procedimentos de comunicação de incidentes documentados através de canais seguros. Registos de comunicação às partes externas.

RS.CO-4

5 A coordenação com as partes interessadas ocorre de acordo com o plano de resposta?

1. Não.
2. Existe coordenação com partes externas interessadas.
3. Estão estabelecidos níveis de responsabilização na resposta a incidentes, existindo avaliação da comunicação de incidentes.

Evidências

1. N/A
2. Identificação das partes externas interessadas. Documentos de apoio ao plano de comunicação de incidentes.
3. Registo da definição de responsabilidades no âmbito da resposta a incidentes. Análise/avaliação dos registos de comunicação quanto aos critérios estabelecidos.

RS.CO-5

6 Existe partilha voluntária de informação com partes interessadas externas?

1. Sim, mas de forma informal e não estruturada.
2. As partes interessadas externas relevantes são identificadas.
3. Está estabelecido um plano de comunicação coerente com as necessidades da organização.

Evidências

1. Observação de comunicação informal através de entrevista aos colaboradores.
2. Registo atualizado de parceiros, fornecedores e demais partes externas relevantes.
3. Documentos de apoio ao plano de comunicação voluntária de incidentes.

RS.AN-1

7 As notificações dos sistemas de deteção são investigadas?

1. Existe registo de notificações de eventos, mesmo que não estruturado.
2. Os eventos detetados são investigados, cumprindo um plano de resposta a incidentes.
3. As notificações dos sistemas são avaliadas transversalmente, utilizando uma plataforma central de gestão de correlação de eventos.

Evidências

1. Registos de notificações elevadas a incidentes.
2. Evidências do tratamento dos eventos identificados.
3. Documentação da implementação de uma plataforma de gestão de correlação de eventos.

RS.AN-2

8 O impacto dos incidentes é avaliado?

1. Sim, de forma informal e não estruturada.
2. Os incidentes de segurança são categorizados pelo nível de impacto percebido.
3. O risco dos incidentes é avaliado, e estão estabelecidas métricas relativas às respostas e tratamento de incidentes.

Evidências

1. Observação da avaliação do impacto, por entrevista aos colaboradores.
2. Definição de padrões para categorias de incidentes. Taxonomia de impacto de incidentes.
3. Registos da avaliação de riscos. Documentação de apoio ao processo de gestão de eventos. Métricas relativas a tempos de resposta, resolução, níveis de alertas e prioridades.

RS.AN-3

9 São realizadas análises forenses?

1. Não.
2. Estão definidos procedimentos de identificação, coleta e aquisição de informação e estão definidos procedimentos para a captura dos dados no seu formato original, para análise forense.
3. É garantida a integridade e cadeia de custódia das evidências recolhidas. Existem meios específicos para a realização de análises forenses.

Evidências

1. N/A.
2. Documentos de suporte aos processos de coleta de dados e garantia. Registos de formação de colaboradores sobre procedimentos de análise forense.
3. Adoção de software de captura de dados de fins forenses. Sistema de integração da coleta de dados forenses com a gestão e correlação de eventos.

RS.AN-4

10 Os incidentes são categorizados de acordo com o plano de resposta?

1. A categorização dos incidentes é definida de formal informal e pouco estruturada.
2. Está estabelecida uma taxonomia de categorização de incidentes, e a categorização está presente no momento da resposta.
3. Estão estabelecidas metodologias de tratamento para cada tipo de incidente detetado.

Evidências

1. Observação da categorização de incidentes, através de entrevistas a colaboradores.
2. Documentação da taxonomia de categorização de incidentes. Inclusão da categorização de incidentes nos planos de resposta.
3. Documentos de suporte ao tratamento de incidentes. Registo das categorizações de incidentes.

RS.AN-5

11 Estão definidos processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas?

1. A submissão de vulnerabilidades é realizada através de processos *ad hoc*.
2. Existem múltiplos mecanismos para que a organização seja informada sobre vulnerabilidades, de forma interna e externa, estando estabelecidos processos de tratamento às vulnerabilidades.
3. As vulnerabilidades são analisadas e avaliadas sistematicamente.

Evidências

1. Observação de submissão de vulnerabilidades por entrevista a colaboradores.
2. Documento de suporte ao processo de gestão de vulnerabilidades. Formas de informar sobre vulnerabilidades estabelecidas e divulgadas. Registos de receção das comunicações. Critérios de classificação das vulnerabilidades, de forma a direcionar tratamento.
3. Documentos de suporte aos procedimentos de análise e avaliação de vulnerabilidades. Registo de controlo e acompanhamento das análises das vulnerabilidades identificadas.

RS.MI-1

12 Os incidentes são contidos?

1. A resposta aos incidentes de segurança é feita de forma não sistematizada.
2. Estão estabelecidos processos de resposta aos incidentes.
3. As causas para a origem de incidentes são analisadas e avaliadas.

Evidências

1. Registo de resposta no tratamento de incidentes.
2. Procedimentos de resposta a incidentes de segurança. Documentos de suporte ao tratamento de incidentes. Elaboração de recomendações de tratamento de incidentes.
3. Registos de investigação e análises forenses sobre as causas dos incidentes. Indicação de melhorias para a mitigação dos incidentes conhecidos.

RS.MI-2

13 Os incidentes são mitigados?

1. A resposta aos incidentes de segurança é feita de forma reativa e não estruturada.
2. Estão estabelecidas práticas para a redução de impacto dos incidentes. Os procedimentos sobre o tratamento de incidentes estão documentados.
3. Os incidentes são erradicados. É feita uma análise do tratamento dos incidentes para efeitos de melhoria contínua.

Evidências

1. Registos de ações de contenção imediata de incidentes. (bloqueio de contas, interrupção de acessos.)
2. Disponibilização de infraestrutura alternativa. Documentação da separação da rede em zonas protegidas por *firewalls*. Documentos de suporte à mitigação dos incidentes.
3. Remoção de ameaças nas infraestruturas. Uso ou melhoria dos sistemas de proteção (antivírus). Repositório de incidentes anteriores com os respetivos planos de ação.

RS.MI-3

14 As novas vulnerabilidades identificadas são mitigadas ou documentadas como riscos aceites?

1. O tratamento das vulnerabilidades é avaliado de forma não estruturada.
2. Está estabelecido um processo de gestão de vulnerabilidades, onde as vulnerabilidades são mitigadas de acordo com critérios definidos.
3. O processo de análise de risco das vulnerabilidades está definido, e a aceitação das vulnerabilidades está formalizada.

Evidências

1. Observação da avaliação das vulnerabilidades, por entrevista aos colaboradores.
2. Registo de execução do processo de gestão das vulnerabilidades.
3. Registo das análises de risco. Registos de aceitação das vulnerabilidades.

RS.ME-1

15 Os planos de resposta a incidentes incorporam as lições aprendidas?

1. N/A.
2. N/A.
3. Os procedimentos de reposta a incidentes são melhorados através da análise de lições aprendidas.

Evidências

1. N/A.
2. N/A.
3. Documentos de suporte ao plano de incidentes. Registo de reuniões (atas) no contexto da melhoria contínua. Registo do tratamento de vulnerabilidades resultantes de incidentes ocorridos.

RS.ME-2

16 As estratégias de resposta a incidente são atualizadas?

1. N/A.
2. Os procedimentos são atualizados periodicamente, não se limitando às tecnologias e sistemas utilizados.
3. Estão estabelecidos processos de melhoria contínua dos planos de resposta a incidentes, ocorrendo avaliação dos mesmos.

Evidências

1. N/A.
2. Registo de atualização de procedimentos para a reposta a incidentes, num determinado período de análise.
3. Registo de testes de validação dos procedimentos de resposta a incidentes.

Recuperar

RC.PR-1

1 A organização segue um plano de recuperação durante ou após um incidente?

1. Existem cópias de segurança, realizadas de forma *ad hoc*.
2. Existem procedimentos para a recuperação de incidentes, bem como um processo de gestão de cópias de segurança.
3. Existe uma equipa dedicada ao tratamento e monotorização de ameaças e são implementadas ações preditivas para dar respostas adequadas.

Evidências

1. Relatórios de execução de cópias
2. Documentos com procedimentos e políticas dedicados ao tema da recuperação de incidentes. Relatórios de utilização de plataforma de cópias de segurança e restauro.
3. Registo de constituição da equipa. Registo de recuperação de incidentes.

RC.ME-1

2 Os planos de recuperação incorporam as lições aprendidas?

1. Não.
2. Existem e são avaliadas métricas relativas aos planos de recuperação, identificando as fragilidades dos planos anteriores.
3. São identificadas as oportunidades de melhoria e os planos são atualizados com as melhorias encontradas.

Evidências

1. N/A
2. Registos dos indicadores e resultados analíticos de avaliação do resultado de ações relativas aos planos de recuperação.
3. Documentos com atualização dos planos. Documentos de suporte à avaliação/análise.

RC.ME-2

3 As estratégias de recuperação são continuamente revistas e atualizadas?

1. Os procedimentos *ad hoc* de análise de operação incluem pontos de discussão relativos à recuperação de incidentes.
2. Estão estabelecidos procedimentos de avaliação dos planos de recuperação. As equipas afetas à recuperação de incidentes são geridas.
3. Estão estabelecidos procedimentos de revisão periódica, por parte da gestão de topo, das estratégias de recuperação.

Evidências

1. Registos (por exemplo atas) de reuniões de discussão dos procedimentos.
2. Registos de atualização dos procedimentos. Registo de formação e/ou atualização das equipas externas ou internas envolvidas.
3. Registos de revisão de estratégias de recuperação e estratégias complementares (gestão de incidentes, plano de continuidade de negócio, gestão de vulnerabilidades…)

RC.CO-1

4 Está implementado um plano de comunicação?

1. A comunicação sobre segurança é realizada de forma reativa, pouco estruturada ou dispersa.
2. Está estabelecido um plano de comunicação sobre eventos de segurança, identificando as partes interessadas.
3. A comunicação é efetuada através de ações de consciencialização e de forma proativa.

Evidências

1. Registos de comunicações.
2. Documentos de suporte ao plano de comunicação. Registo de partes interessadas conforme o tema a ser comunicado.
3. Plano de comunicações periódicas. Registos de comunicações.

RC.CO-2

5 As atividades de recuperação são comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão?

1. A comunicação é feita de forma reativa e não estruturada.
2. Está estabelecido um plano de comunicação consoante o seu propósito, identificando as partes interessadas.
3. A comunicação é efetuada de acordo com uma estratégia adequada às equipas executivas e de gestão. Os processos de aprovação das comunicações estão bem definidos.

Evidências

1. Registos de comunicações.
2. Plano de comunicação com o detalhe do objetivo a ser comunicado e identificação da audiência.
3. Registo de comunicações para equipas executivas e de gestão. Registo dos processos de aprovação das comunicações. Avaliação da mensagem para cada audiência.