CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Cybersecurity Competencies Framework

INDEX

1. EXECUTIVE SUMMARY

The Cybersecurity Competencies Framework (the **Framework**) identifies and maps competencies –both transversal and specialised– in cybersecurity, thus proposing a set of reference knowledge required to fulfil the roles and tasks in Cybersecurity.

The Framework intends to serve as a document for supporting the development of the cybersecurity sector in its different areas, also contributing to the definition and formulation of public policies.

In the present context of the digital economy, the Framework aims to become a reference document for the preparation and certification of training programmes, the definition of work roles and selection of profiles for recruitment, as well as a career planning tool for professionals.

Aligned with the Portuguese National Strategy for Cyberspace Security 2019-2023 [7], the Framework aims at identifying competencies and knowledge for cybersecurity, thus facilitating the inclusion of these subject matters in the curricular structure of primary, secondary, higher education, and in the continuing training of teachers, as well as the promotion of advanced technical training in cybersecurity in university and polytechnic institutions, in order to meet the national needs of professionals in the field.

Aiming at these objectives, the Framework is proposed as a reference document –not as a normative or prescriptive recipe– and should be taken as a starting point for the development of strategies, policies, and specific proposals, that should be adapted to the context of each organisation and of each training and education initiative.

2. INTRODUCTION

The Cybersecurity Competencies Framework (the Framework), identifies and maps the competencies that constitute the capabilities in the field of cybersecurity.

Having as conceptual basis several national and international reference frameworks [1][2][3][4][5][6] and responding to the Portuguese National Strategy for Cyberspace Security 2019-2023 [7], the Framework constitutes the reference document for the development and certification of training programmes, the definition of work roles and the selection of profiles for recruitment, and as a career planning tool for professionals.

2.1 Legal and strategic context

Considering the Law 46/2018, of 13th of August, establishing the legal framework for cybersecurity, transposing Directive (EU) 2016/1148, of the European Parliament and of the Council of 6th of July 2016, on measures to ensure a high common level of network and information security across the Union, the Portuguese National Cybersecurity Centre ensures cyberspace use in a free, reliable and secure manner, through the promotion of continuous improvement of national cyber security and international cooperation, in liaison with the competent authorities.

Considering also the terms of the Portuguese National Strategy for Cyberspace Security 2019-2023 [7], approved by the Council of Ministers, on 23rd of May 2019, and published through Resolution No. 92/2019, of 5th of June 2019, which defines six axis of intervention, a need arises to identify and map the competencies that constitute the capabilities in the field of cybersecurity.

To this end, the Framework provides a body of knowledge capable of mapping the competencies needed to fulfil the roles in cybersecurity, serving as a document to support the development of the cybersecurity sector in its different areas, also contributing to the definition and formulation of public policies.

2.2 Objectives

Considering the legal and strategic context of the Framework and considering its practical utility, the conceptualisation and construction of the Framework had in mind the following objectives:

- Identify and explore the strengths of different national and international frameworks, both in terms of conceptual aspects and in terms of the instantiations of content related to competencies.
- Explore synergies between the same frameworks, minimising conceptual discrepancies and maximising interoperability.
- Facilitate updating and continuous improvement of the Framework.
- Facilitate its use, making the relevant lists and mappings available as annexes in digital format (tables).
- Adapt to the national context, considering the high relevance of small and medium enterprises (SMEs) in the national business fabric.

Accordingly, the conceptualisation and construction of the Framework was guided by the principles of simplicity, clarity, modularity, agility and interoperability.

2.3 Framework background

The following reference frameworks were considered for the development of the Framework:

National Initiative for Cybersecurity Education Framework (NICE)

The National Initiative for Cybersecurity Education (NICE) of the National Institute of Standards and Technology (NIST) is a framework that provides a set of basic elements for the description of tasks, knowledge and skills needed in cybersecurity[1]. This reference framework allows organisations to plan and foster the development of their human resources with the skills necessary to ensure cybersecurity. It also allows candidates and trainees in cybersecurity to better understand where they are at the level of competences, knowledge, tasks and skills, and thus establish clear learning paths in the field of cybersecurity.

Singapore Skills Framework

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

The *Singapore Skills Framework* is a framework developed by the Government of Singapore, Industry Associations, Education Institutions, among other entities, which encompasses general and technical skills and competencies that are required in various areas of information technology, including cybersecurity, and has created a common language for individuals, employers, and education, training and coaching organisations[2]. The objectives of this framework are to facilitate the acknowledgement of skills and competencies and to support the design of training programmes for career development.

The following structuring documents for cybersecurity in Portugal were also taken into consideration as a resource for requirements:

- National Cybersecurity Framework [1].
- Roadmap for Minimum Capabilities in Cybersecurity [2].

2.4 Document structure

The section "Conceptual model" presents the definitions for the fundamental concepts of task, role, competency, and knowledge, as well as the conceptual map that relates these concepts.

Next, in the section "Framework and applications", the architecture of the Framework is detailed and possible applications are presented.

Finally, the chapter "Conclusions and recommendations" discusses the practical application of the Framework, as well as its limitations.

[2] https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html

3. CONCEPTUAL MODEL

The conceptualisation of the Framework is based on a simple and clear model, aiming at interoperability with other frameworks for cybersecurity competencies and management, as well as the need to facilitate its updating given the rapid evolution of the cybersecurity field.

3.1 Definitions

The following table presents the definitions used in the Framework.

Term	Definition
Role	Function to perform in the organisation.
Competency	Set of professional capacities useful to perform tasks and/or representative of proven knowledge and skills.
Task	Activity aimed at achieving functional objectives within the organisation.
Knowledge	Set of associated concepts, memorable, intelligible and communicable, as well as recallable, testable and task-oriented.
Skill	Practical knowledge, ability to perform an observable and task-oriented action.
Cyberspace	Consists of the complex environment, of values and interests, materialised in an area of collective responsibility, which results from the interaction between people, networks and information systems [7].
Cybersecurity	Consists of a set of prevention, monitoring, detection, reaction, analysis and correction measures and actions that are aimed to maintain the desired security state and to ensure the confidentiality, integrity, availability and non-repudiation of networks and information systems in cyberspace, and of the people who interact in it [7].
Cyberdefence	Consists of the activity that aims to ensure national defence in, or through, cyberspace [7].
Cybercrime	Facts corresponding to crimes defined in the Cybercrime Law and also other criminal offences committed with the use of technological means, in which these means are essential to the practice of the considered crime [7].

3.2 Conceptual map

The relation between the concepts of task, role, competency, and knowledge is developed and clarified in the following conceptual map, which illustrates the semantic relation between these key concepts.

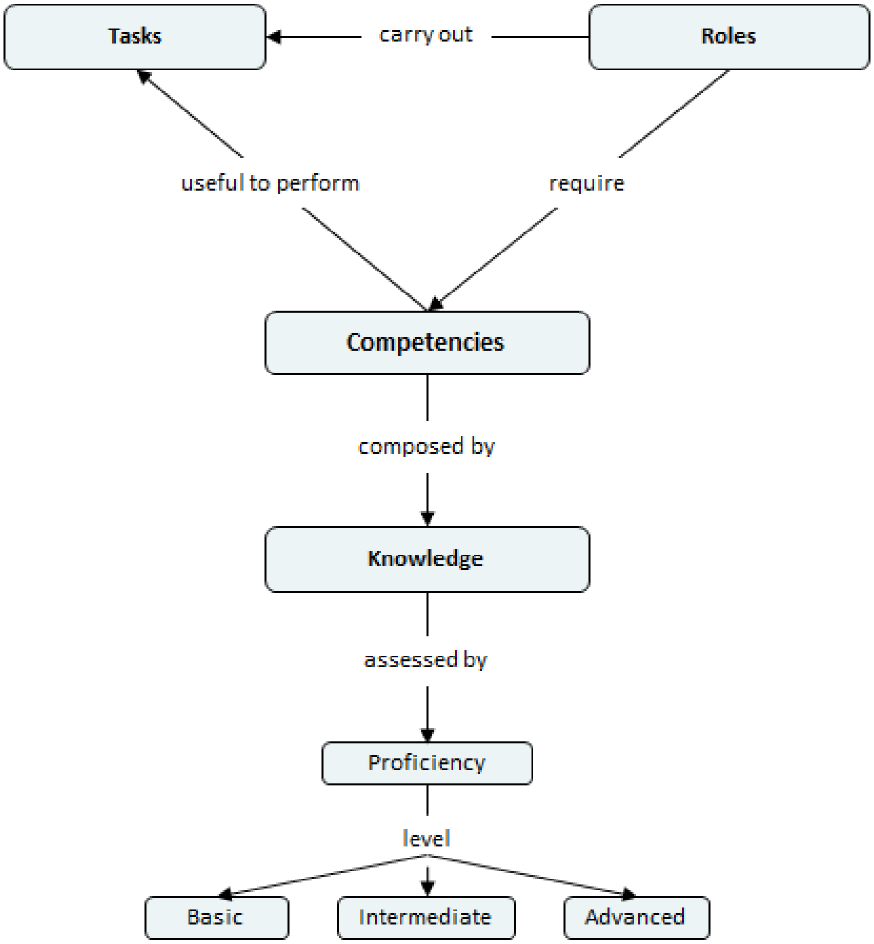


Figure 1 – Conceptual map of competencies for cybersecurity, relating the concepts of competencies, role, task, knowledge, as well as listing the proficiency levels.

It should be noted that the present Framework opts for the specification of the concept of skill as knowledge, defining skill as practical knowledge, i.e. as the ability to perform an observable action.

4. FRAMEWORK AND APPLICATIONS

In the following section, the architecture of the Framework is presented and detailed, based on a structured set of transversal and specialised competencies.

4.1 Competencies and knowledge

The Cybersecurity Competencies Framework was designed to facilitate the identification of knowledge and proficiency levels in cybersecurity necessary to perform activities for any type of role, in any organisation.

The architecture of the Framework is organised into domains and subdomains of competencies, as presented in **Error! Reference source not found.**.

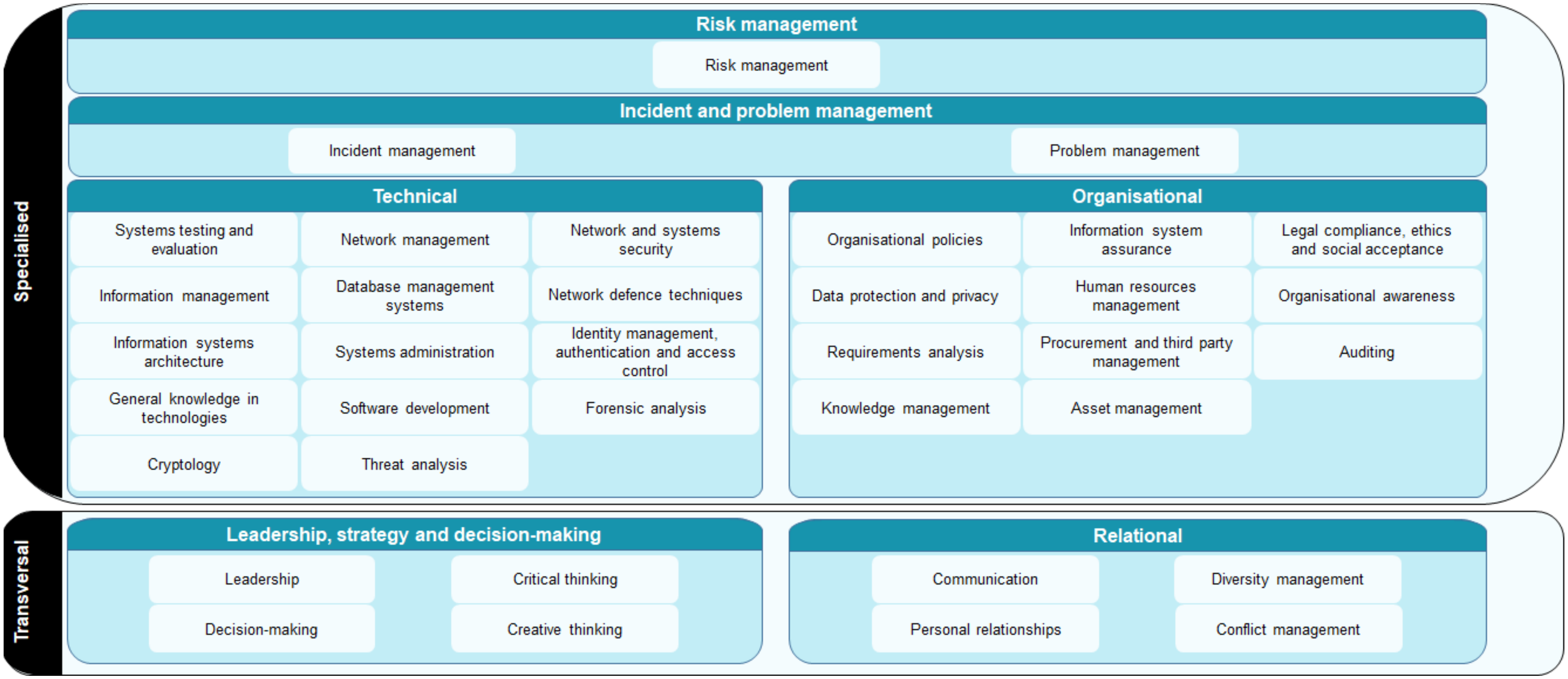
The Framework considers the following distinction between competency domains:

- **Specialised** competencies;
- **Transversal** competencies.

The specialised competencies domain includes specific competencies to the implementation, operation, and management of cybersecurity. This domain comprises the subdomains of **risk management**, **incident and problem management**, as well as the subdomains of **technical** and **organisational** competencies.

The transversal competencies domain includes competencies that are transversal to the areas of specialisation, that are crucial to perform all cybersecurity-related activities. These activities typically take place in stressful environments, requiring appropriate leadership, planning, and decision-making competencies, as well as high cooperation, collaboration, and communication competencies. These are organised in the subdomains of **leadership, strategic, and decision-making** competencies and **relational** competencies.

<



Specialised

Risk management
- Risk management

Incident and problem management
- Incident management
- Problem management

Technical
- Systems testing and evaluation
- Network management
- Network and systems security
- Information management
- Database management systems
- Network defence techniques
- Information systems architecture
- Systems administration
- Identity management, authentication and access control
- General knowledge in technologies
- Software development
- Forensic analysis
- Cryptology
- Threat analysis

Organisational
- Organisational policies
- Information system assurance
- Legal compliance, ethics and social acceptance
- Data protection and privacy
- Human resources management
- Organisational awareness
- Requirements analysis
- Procurement and third party management
- Auditing
- Knowledge management
- Asset management

Transversal

Leadership, strategy and decision-making
- Leadership
- Critical thinking
- Decision-making
- Creative thinking

Relational
- Communication
- Diversity management
- Personal relationships
- Conflict management

Figure 2 – Architecture of the Cybersecurity Competencies Framework, structured in domains and subdomains.

4.2 Risk management

The National Cybersecurity Framework [1] proposes «a risk-oriented procedural implementation, that enables informed and prioritised decision-making by organisations, in the cybersecurity context. These decisions should always be equally oriented towards ensuring confidentiality, availability and integrity in the provision of the goods or services for a particular organisation».

Competent risk management empowers cybersecurity actors for proper awareness and insight into the context, assets at risk, threats and vulnerabilities, as well as the effective identification, analysis, assessment, and treatment of risks. Thus, it serves as the basis for implementing and maintaining cybersecurity controls, as well as to inform decision-making for incident and problem management purposes.

4.3 Incident and problem management

The subdomain of **incident and problem management** comprises competencies that cover all aspects related to incident and problem management, namely:

- Principles, processes and technologies for analysing, prioritising, and handling cybersecurity incidents;
- Tools for determining the accuracy and relevance of information and judgement to create and evaluate alternatives to problem management in order to assess the impacts and implications of decisions.

4.4 Technical competencies

The **technical** subdomain includes all competencies and knowledge related to the mechanisms, processes, and technical procedures for the design, implementation, operationalisation, management, and protection of digital assets. Technical competencies also support risk management, and incident and problem management.

4.5 Organisational competencies

The subdomain of **organisational** competencies complements the technical competencies by including competencies related to aspects of organisational excellence, namely:

- Information security policies and procedures to be followed in the organisation;
- Management of the organisational resources, such as assets, partnerships, human resources, and knowledge;
- Decision-making support activities such as audits and analysis of functional and infrastructure requirements of an organisation;

Organisational competencies also support risk management and incident and problem management.

4.6 Transversal competencies

For an effective execution of cybersecurity tasks, there is a need for communication and coordination among several people and teams from distinct areas, both technical and non-technical, as well as inside and outside of the organisation. There are also activities, such as incident and problem response, where the decision-making process takes place in stressful environments.

These competencies are thus indispensable and are included in the domain of transversal competencies:

- **Relational** competencies, which include communication, personal relationships, diversity management, and conflict management;
- Competencies related to **leadership, strategy, and decision-making**.

4.7 Other competencies to consider

The Framework presents only the relevant competencies for activities that are specific to cybersecurity. It does not intend to propose a comprehensive list of all the socio-technical competencies that an organisation should have to support its mission and operations.

However, it may be interesting to consider competencies that contribute to the governance and management of the organisational information system, namely those that support the objectives of the COBIT reference framework[3], referred to in the National Cybersecurity Framework [1]. In the most recent version of the COBIT reference framework, 40 areas are proposed:

- *Ensured Governance Framework Setting and Maintenance*
- *Ensured Benefits Delivery*
- *Ensured Risk Optimization*
- *Ensured Resource Optimization*
- *Ensured Stakeholder Engagement*
- *Managed I&T Management Framework*
- *Managed Strategy*
- *Managed Enterprise Architecture*
- *Managed Innovation*
- *Managed Portfolio*
- *Managed Budget and Costs*
- *Managed Human Resources*
- *Managed Relationships*
- *Managed Service Agreements*
- *Managed Vendors*
- *Managed Quality*
- *Managed Risk*
- *Managed Security*
- *Managed Data*
- *Managed Programs*
- *Managed Requirements Definition*

[3] https://www.isaca.org/resources/cobit

- *Managed Solutions Identification and Build*
- *Managed Availability and Capacity*
- *Managed Organizational Change*
- *Managed IT Changes*
- *Managed IT Change Acceptance and Transitioning*
- *Managed Knowledge*
- *Managed Assets*
- *Managed Configuration*
- *Managed Projects*
- *Managed Operations*
- *Managed Service Requests and Incidents*
- *Managed Problems*
- *Managed Continuity*
- *Managed Security Services*
- *Managed Business Process Controls*
- *Managed Performance and Conformance Monitoring*
- *Managed System of Internal Control*
- *Managed Compliance With External Requirements*
- *Managed Assurance*

Note that these areas are broader in scope than cybersecurity, covering the fundamental aspects of governance and management of information and related technologies.

4.8 Proficiency levels

Considering the definitions of the proficiency levels of the Dynamic Reference Framework of Digital Competences for Portugal [6], three proficiency levels are defined for knowledge in cybersecurity:

- **Basic**: the tested knowledge demonstrates understanding of the presented problem, as well as effectiveness in carrying out the necessary tasks related to the professional role, as long as support is given.
- **Intermediate**: the tested knowledge demonstrates understanding of the presented problem, as well as effectiveness in carrying out the necessary tasks related to the professional role, with autonomy.
- **Advanced**: the tested knowledge demonstrates understanding of the presented complex problems, as well as effectiveness in carrying out the necessary tasks related to the professional role, with high autonomy and creativity.

Note that these definitions of proficiency take into account the role to be performed as well as the task (or process) to be accomplished. They can therefore be adapted to each organisational context, as well as to the level of ambition and to the objectives to be achieved.

The distinction between different levels is based on the level of autonomy and the level of complexity and creativity.

4.9 Framework applications

The Framework may be used:

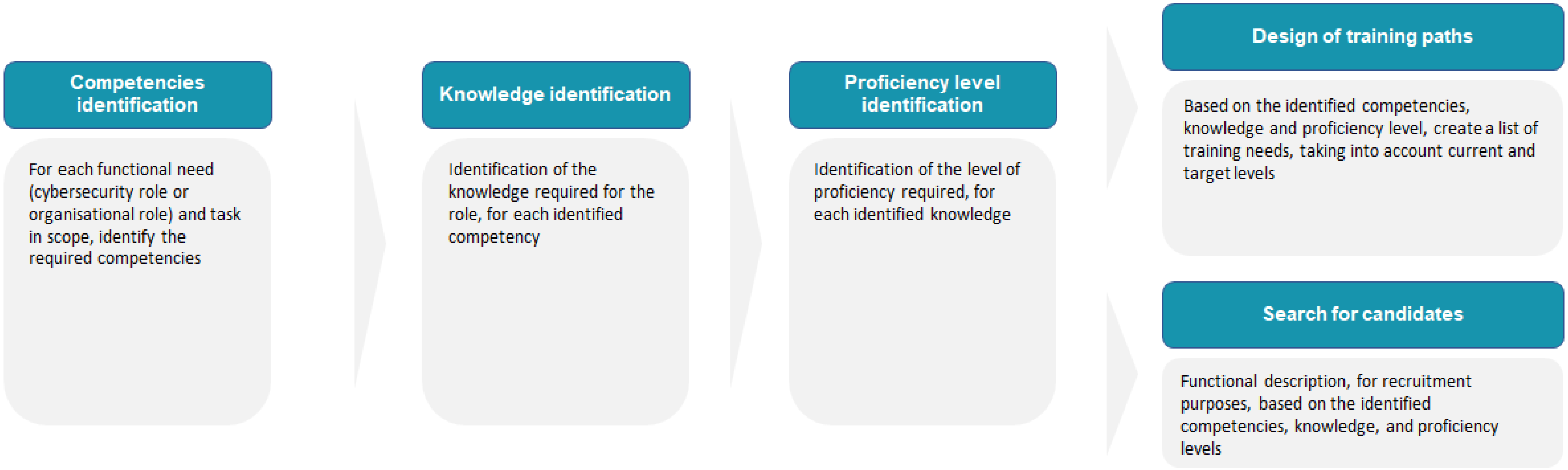
- For the design of training paths, both within organisations and in institutions providing training courses, facilitating the alignment of competency terminology and the clarification of proficiency levels to be considered;
- By the human resources departments of organisations, for the definition of profiles and roles based on the competencies and knowledge proposed by the Framework, including the respective proficiency levels;
- By cybersecurity professionals who wish to expand their knowledge, using the Framework to make a self-assessment of knowledge, as well as to design their own training path;
- By the governance and management teams of organisations to assess organisational competencies in cybersecurity, thus allowing training and hiring strategies to be defined to address identified needs.

For the use cases indicated above, four phases are proposed for the use of the Framework, as shown in **Error! Reference source not found.**, with the first three phases being common to the different use cases:

- The **competencies identification phase**, in which the competencies required for each functional need (cybersecurity role or organisational role) and task in scope are identified;
- The **knowledge identification phase**, in which the knowledge required for the role is identified for each identified competency;
- The **proficiency levels identification phase**, in which the required proficiency level is determined, for each knowledge identified;

The last phase will depend on the use case. We present here two examples of application:

- The **design of training paths**, to create a list of training needs, considering current levels and levels to be reached, on the basis of identified competencies, knowledge, and proficiency levels;
- The **search for candidates**, for recruitment purposes, on the basis of the identified competencies, knowledge, and proficiency levels.



Competencies identification

For each functional need (cybersecurity role or organisational role) and task in scope, identify the required competencies

Knowledge identification

Identification of the knowledge required for the role, for each identified competency

Proficiency level identification

Identification of the level of proficiency required, for each identified knowledge

Design of training paths

Based on the identified competencies, knowledge and proficiency level, create a list of training needs, taking into account current and target levels

Search for candidates

Functional description, for recruitment purposes, based on the identified competencies, knowledge, and proficiency levels

Figure 3 – Examples of applications for the Framework, from functional needs and tasks to the design of training paths and search for candidates.

5. CONCLUSIONS AND RECOMMENDATIONS

This Framework aims to respond to the need to identify and map the competencies that constitute the capabilities –both transversal and specialised– in the field of cybersecurity. It proposes a body of knowledge capable of mapping the necessary competencies for the fulfilment of specific roles in cybersecurity, in the national context.

To this end, the Framework proposes conceptual definitions, an architecture, as well as a list of competencies and associated knowledge. As a reference framework, it should not be taken as prescriptive, nor as a comprehensive list of all that is necessary and sufficient to cover the cognitive complexity of the rapidly changing cybersecurity field. In particular, no generic governance and management areas are covered, but only those that appear as critical for the management and operationalisation of cybersecurity. Thus, it should be used as a reference, to be adapted to each practical context of use, that facilitates semantic and pragmatic alignment in the cybersecurity universe of discourse.

6. REFERENCES

[1] Quadro Nacional de Referência para a Cibersegurança, Centro Nacional de Cibersegurança, April 2020. Available in: https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf

[2] Roteiro para Capacidades Mínimas de Cibersegurança, Centro Nacional de Cibersegurança, October 2019. Available in: https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf

[3] NIST Special Publication 800-181 Revision 1, Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology, U.S. Department of Commerce, November 2020.

[4] Draft (2nd) NISTIR 8355, NICE Framework Competencies: 4 Assessing Learners for Cybersecurity Work, National Institute of Standards and Technology, U.S. Department of Commerce, December 2021.

[5] Singapura SkillsFuture, Skills Framework for ICT / Cyber Security, Available in: https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html .

[6] Quadro Dinâmico de Referência de Competência Digital para Portugal, Iniciativa Nacional Competências Digitais e.2030 - INCoDe.2030, September 2019. Available in: https://www.incode2030.gov.pt/sites/default/files/qdrcd_set2019.pdf

[7] Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Presidência do Conselho de Ministros, Diário da República n.º 108/2019, Série I de 2019-06-05. Available in: https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf