Referencial
de Competências
em Cibersegurança
2022

Centro Nacional
de Cibersegurança

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

ÍNDICE

01 SUMÁRIO EXECUTIVO

O Referencial de Competências em Cibersegurança (Referencial), através da identificação e mapeamento das competências que constituem as capacidades transversais e especializadas da área da cibersegurança, apresenta-se como um conjunto de conhecimentos de referência necessários para o cumprimento de funções e tarefas em cibersegurança.

O Referencial pretende servir como documento de suporte ao desenvolvimento do setor da cibersegurança nas suas diferentes áreas, contribuindo, também, para a definição e formulação de políticas públicas nesta área.

No contexto atual da economia digital, o Referencial visa constituir-se como documento de referência para a elaboração e certificação de programas de docência, para a definição de cargos e seleção de perfis profissionais, bem como ferramenta de planeamento de carreiras para profissionais.

Alinhado com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 [7], o Referencial pretende identificar competências e conhecimentos em cibersegurança, para assim facilitar a inclusão destas temáticas na estrutura curricular dos ensinos básico, secundário e superior e na formação contínua de professores, bem como promover a formação técnica avançada em cibersegurança no ensino superior universitário e politécnico, de modo a suprir as necessidades nacionais de profissionais do setor.

Tendo em vista estes objetivos, o Referencial não deve ser entendido como normativo ou receita prescritiva, mas sim como referência de partida para a elaboração de estratégias, de políticas e de propostas concretas de oferta formativa, que devem ser adaptadas ao contexto de cada organização e de cada iniciativa de formação e treino.

02 INTRODUÇÃO

O Referencial de Competências em Cibersegurança, adiante designado de forma abreviada como Referencial, identifica e mapeia as competências que constituem as capacidades da área da cibersegurança.

Tendo como base conceptual vários referenciais nacionais e internacionais [1][2][3][4][5][6] e dando resposta à Estratégia Nacional de Segurança do Ciberespaço 2019-2023 [7], o Referencial, no contexto atual da economia digital em Portugal, constitui um documento de referência para a elaboração e certificação de programas de docência, para a definição de cargos e seleção de perfis profissionais em contexto de oferta de trabalho e como ferramenta de planeamento de carreiras profissionais.

2.1 Enquadramento

Considerando a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, o Centro Nacional de Cibersegurança contribui para o uso do ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes.

Considerando ainda os termos da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada em Conselho de Ministros, no dia 23 de maio de 2019, e publicada através da resolução nº 92/2019, de 5 de junho de 2019, que define seis eixos de intervenção, decorre a necessidade de identificar e mapear as competências que constituem as capacidades da área da cibersegurança.

Neste sentido, com o Referencial disponibiliza-se um corpo de conhecimento capaz de mapear as valências necessárias para o cumprimento de funções em cibersegurança, servindo como documento de suporte ao desenvolvimento do setor da cibersegurança nas suas diferentes áreas, contribuindo também para a definição e formulação de políticas públicas nesta área.

02

2.2 Objetivos

Atendendo ao enquadramento estratégico e jurídico do Referencial e tendo em vista a sua utilidade prática, a conceptualização e construção do Referencial teve como objetivos:

- Identificar e explorar os pontos fortes dos vários referenciais nacionais e internacionais relativamente aos aspetos conceptuais, bem como no que concerne à definição dos conteúdos relacionados com competências;
- Explorar as sinergias entre os referenciais, minimizando as discrepâncias conceptuais e maximizando a interoperabilidade;
- Facilitar a atualização e a melhoria contínua do Referencial;
- Facilitar a sua utilização, disponibilizando como anexos as listas e mapeamentos relevantes em formato digital (tabelas);
- Adaptar o conteúdo ao contexto nacional tendo em atenção a elevada relevância das pequenas e médias empresas (PME) no tecido empresarial nacional.

Tendo em vista estes objetivos, a conceptualização e construção do Referencial orientou-se pelos princípios da simplicidade, clareza, modularidade, agilidade e interoperabilidade.

2.3 Contexto do Referencial

De seguida, contextualizam-se os quadros de referência que serviram de suporte à elaboração do Referencial.

National Initiative for Cybersecurity Education Framework (NICE)

A National Initiative for Cybersecurity Education (NICE) da National Institute of Standards and Technology (NIST) é um quadro de referência que disponibiliza um conjunto de elementos base para a descrição de tarefas, conhecimento e habilidades necessárias em cibersegurança1. Este referencial permite às organizações planearem e fomentarem o desenvolvimento dos seus recursos humanos nas competências necessárias para garantir a cibersegurança. Permite também a candidatos e formandos em cibersegurança perceberem melhor o seu nível de competências, conhecimentos, tarefas e habilidades, e assim estabelecer caminhos de aprendizagem claros na área de cibersegurança.

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

02

Singapore Skills Framework

A Singapore Skills Framework é um referencial desenvolvido pelo Governo de Singapura, Associações Industriais, Instituições de Ensino, e outras entidades, que engloba as competências e habilidades técnicas e genéricas necessárias em várias áreas das tecnologias de informação, incluindo a cibersegurança, tendo criado uma língua comum para os indivíduos, empregadores e organizações de educação, formação e treino[2] . Os objetivos deste referencial são facilitar o reconhecimento de habilidades e competências e suportar o desenho de programas de treino para o desenvolvimento de carreiras.

Foram ainda tidos em consideração, como fontes de requisitos, os seguintes documentos estruturantes para a cibersegurança em Portugal:

- Quadro Nacional de Referência para a Cibersegurança [1].
- Roteiro para Capacidades Mínimas de Cibersegurança [2].

2.4 Estrutura do documento

No capítulo “Modelo conceptual”, apresentam-se as definições fundamentais de tarefa, função, competência e conhecimento, bem como o mapa conceptual que relaciona os mesmos conceitos.

No capítulo “O Referencial e sua aplicação”, detalha-se a arquitetura do Referencial e apresentam-se possíveis aplicações do mesmo.

Finalmente, no capítulo “Conclusões e recomendações”, discute-se o âmbito de aplicação prática do Referencial e as suas limitações.

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

03 MODELO CONCEPTUAL

A conceptualização do Referencial é baseada num modelo simples e claro, tendo em vista a interoperabilidade com outros referenciais de competências e de gestão da cibersegurança, bem como a necessidade de facilitar a sua atualização face às rápidas evoluções do setor da cibersegurança.

3.1 Definições

Na tabela seguinte apresentam-se as definições utilizadas no Referencial.

TERMO	DEFINIÇÃO
Função	Papel funcional a desempenhar na organização.
Competência	Conjunto de capacidades profissionais úteis para a realização de tarefas e/ou representativas de conhecimentos e habilidades comprovadas.
Tarefa	Atividade que tem em vista o atingimento de objetivos funcionais na organização.
Conhecimento	Conjunto de conceitos associados, memorizável, inteligível e comunicável, bem como recordável e testável, orientado para a realização de tarefas.
Habilidade	Conhecimento prático, capacidade para realizar uma ação observável, orientado para a realização de tarefas.
Ciberespaço	Consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação [7].
Cibersegurança	Consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem [7].
Ciberdefesa	Consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço [7].
Cibercrime	Factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa [7].

03

3.2 Mapa conceptual

A relação entre os conceitos de tarefa, função, competência e conhecimento é desenvolvida e clarificada no seguinte mapa conceptual, que ilustra as relações semânticas entre estes conceitos fundamentais.

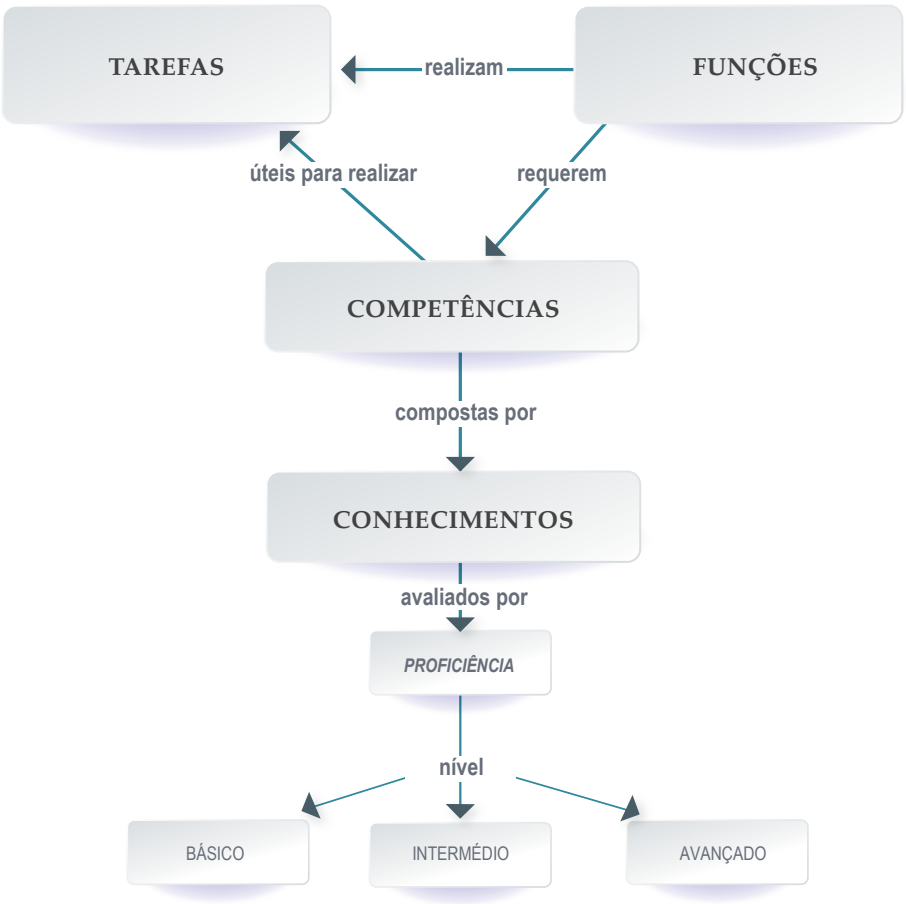


Figura 1 – Mapa conceptual das Competências para a Cibersegurança, relacionando os conceitos de Competências, Funções, Tarefas, Conhecimentos, bem como enumerando os níveis de proficiência.

Note-se que no presente Referencial opta-se pela especialização do conceito de habilidade como conhecimento, definindo-se habilidade como conhecimento prático, isto é, como capacidade para realizar uma ação observável.

04
O REFERENCIAL E A SUA APLICAÇÃO

De seguida, apresenta-se e detalha-se a arquitetura do Referencial, com base num conjunto estruturado de competências transversais e de competências especializadas.

4.1 Competências e conhecimentos

O Referencial foi desenhado de forma a facilitar a identificação de conhecimentos e níveis de proficiência em cibersegurança necessários para o desempenho de atividades para qualquer tipo de função, em qualquer organização.

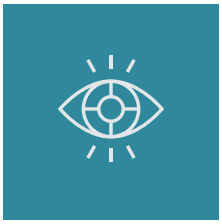
A arquitetura do Referencial está organizada em domínios e subdomínios de competências, conforme apresentado na Figura 2.

Ao nível dos domínios, o Referencial considera a seguinte distinção:

- O domínio das competências **especializadas;**
- O domínio das competências **transversais.**

O domínio das competências especializadas inclui competências específicas para a implementação, operação e gestão da cibersegurança. Este domínio engloba os subdomínios de competências de **gestão de risco, gestão de incidentes e problemas**, bem como os subdomínios de competências **técnicas** e **organizacionais.**

O domínio das competências transversais inclui competências transversais às áreas de especialização que são cruciais para a realização de todas as atividades de cibersegurança. Estas atividades desenvolvem-se tipicamente em ambientes de elevada pressão, exigindo capacidades adequadas de liderança, planeamento e decisão, bem como elevadas capacidades de cooperação, colaboração e comunicação. Estas capacidades estão inseridas nos subdomínios de competências de **liderança, estratégia e decisão**, e de competências **relacionais**.



Arquitetura do referencial de competências

Figura 2 – Arquitetura do Referencial de Competências em Cibersegurança, estruturada em domínios e subdomínios.

04

4.2 Gestão do risco

O Quadro Nacional de Referência para a Cibersegurança [1] propõe «uma implementação processual orientada à gestão do risco, que permite às organizações a tomada de decisão de forma priorizada e informada, no contexto da cibersegurança. Estas decisões devem, sempre, estar igualmente orientadas à garantia da confidencialidade, disponibilidade e integridade na prestação do bem ou serviço para uma determinada organização».

Uma gestão de risco competente capacita os agentes da cibersegurança para a correta consciencialização e discernimento do contexto, ativos em risco, ameaças e vulnerabilidades, bem como a eficaz identificação, análise, avaliação e tratamento dos riscos.

A gestão de risco é da maior importância, servindo de base à implementação e manutenção de controlos de cibersegurança, bem como à tomada de decisão para a gestão de incidentes e de problemas.

4.3 Gestão de incidentes e problemas

O subdomínio de competências de gestão de incidentes e problemas é constituído pelas competências que englobam todos os aspetos relacionados com a gestão de incidentes e a gestão de problemas, nomeadamente:

Os princípios, processos e tecnologias de análise, priorização e tratamento de incidentes de cibersegurança.

As ferramentas para a determinação da precisão e da relevância da informação e utilização de discernimento para criar e considerar alternativas à gestão de problemas, de forma a avaliar os impactos e implicações das decisões.

4.4 Competências técnicas

Dentro do subdomínio das competências técnicas, incluem-se todas as competências e conhecimentos relacionados com os mecanismos, processos e procedimentos técnicos para o desenho, implementação, operacionalização, gestão e proteção dos ativos digitais. As competências técnicas suportam também a gestão de risco e a gestão de incidentes e problemas.

04

4.5 Competências organizacionais

O subdomínio das competências organizacionais complementa o das competências técnicas, incluindo as competências relacionadas com aspetos de excelência organizacional, nomeadamente:

As políticas e procedimentos de segurança de informação a serem seguidas na organização.

A gestão dos vários recursos da organização, como os ativos, as parcerias, os recursos humanos e o conhecimento.

As atividades de suporte às tomadas de decisão como as auditorias e a análise de requisitos funcionais e de infraestrutura de uma organização.

As competências organizacionais suportam também a gestão de risco e a gestão de incidentes e problemas.

4.6 Competências transversais

Para a eficaz execução de tarefas de cibersegurança, existe a necessidade de comunicação e de coordenação entre várias pessoas e equipas de áreas díspares, técnicas e não técnicas, dentro e fora da organização. Existem também atividades, como as de resposta a incidentes e problemas, onde o processo de tomada de decisão decorre num ambiente de elevada tensão e urgência.

Por serem indispensáveis, o subdomínio das competências transversais inclui:

As competências **relacionais**, que incluem a comunicação, relacionamento interpessoal, gestão da diversidade e gestão de conflitos;

As competências relacionadas com a **liderança, estratégia e decisão**.

04

4.7 Outras competências a considerar

O Referencial apresenta apenas as competências relevantes para as atividades específicas de cibersegurança, não pretendendo elencar de forma exaustiva todas as competências sociotécnicas que uma organização deverá assegurar para suportar a sua missão e as suas operações.

No entanto, pode interessar a consideração de competências que contribuem para a governança e gestão do sistema de informação da organização, nomeadamente as que suportam os objetivos do referencial COBIT [3], referido no Quadro Nacional de Referência para a Cibersegurança [1].

Na mais recente versão do quadro de referência COBIT, são elen-cadas 40 áreas de objetivos[4]:

- *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*

[3] https://www.isaca.org/resources/cobit
[4] Manteve-se a terminologia em língua inglesa, para facilidade de referenciação.

04

- *Managed Programs*
- *Managed Requirements Definition*
- *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-se que estas áreas de objetivos têm um âmbito mais vasto do que o da cibersegurança, abarcando os aspetos fundamentais de governança e gestão da informação e das tecnologias relacionadas.

04

4.8 Níveis de proficiência

Tendo em conta as definições dos níveis de proficiência do Quadro Dinâmico de Referência de Competências Digital para Portugal [6], definem-se três níveis de proficiência para os conhecimentos de cibersegurança:

Básico: o conhecimento testado demonstra compreensão do problema apresentado, bem como eficácia para realizar as tarefas necessárias relacionadas com as funções da responsabilidade do profissional, desde que seja recebido apoio.

Intermédio: o conhecimento testado demonstra compreensão do problema apresentado, bem como eficácia para realizar as tarefas necessárias relacionadas com as funções da responsabilidade do profissional, com autonomia.

Avançado: o conhecimento testado demonstra compreensão do problema complexo apresentado, bem como eficácia para realizar as tarefas necessárias relacionadas com as funções da responsabilidade do profissional, com autonomia e criatividade elevadas.

Note-se que estas definições de proficiência têm em conta a função a desempenhar, bem como a tarefa (ou processo) a realizar. Podem assim ser adaptadas a cada contexto organizacional, bem como ao nível de ambição e aos objetivos a atingir.

A distinção dos vários níveis tem como base o nível de autonomia e o nível de complexidade e de criatividade.

04

4.9 Aplicação do Referencial

O Referencial será usado tipicamente:

- Para o desenho de percursos de formação, tanto dentro das organizações como em instituições que fornecem cursos de formação, facilitando o alinhamento da terminologia de competências e a clarificação dos níveis de proficiência a considerar;
- Pelos departamentos de recursos humanos das organizações, para a definição de perfis e de funções com base nas competências e nos conhecimentos propostos pelo Referencial, incluindo os respetivos níveis de proficiência;
- Pelos profissionais de cibersegurança que desejem expandir os seus conhecimentos, utilizando o referencial para fazer uma autoavaliação de conhecimentos, bem como para desenhar o seu próprio percurso de formação;
- Pelas equipas de governança e de gestão das organizações, para avaliarem as competências organizacionais em cibersegurança, permitindo assim definir estratégias de formação e de contratação para colmatar as necessidades identificadas.

Para os usos indicados acima, propõe-se quatro fases para a utilização do Referencial, conforme a Figura 3, sendo as três primeiras fases comuns aos vários tipos de uso:

- A fase de **identificação das competências**, na qual se identificam as competências requeridas para cada necessidade funcional (função de cibersegurança ou função na organização) e tarefa em âmbito;
- A fase de **identificação dos conhecimentos**, na qual se identificam os conhecimentos requeridos para a função, para cada competência identificada;
- A fase de **identificação dos níveis de proficiência**, na qual se determina o nível de proficiência requerido, para cada conhecimento identificado.

A quarta e última fase irá depender do tipo de uso. Apresentamos aqui dois exemplos de aplicação:

- O **desenho de percursos de formação**, tendo em vista a elaboração de uma lista de necessidades formativas, tomando em consideração os níveis atuais e os níveis a atingir, com base nas competências, conhecimentos e níveis de proficiência identificados;
- A **procura de candidatos**, tendo em vista uma contratação, com base nas competências, conhecimentos e níveis de proficiência identificados.

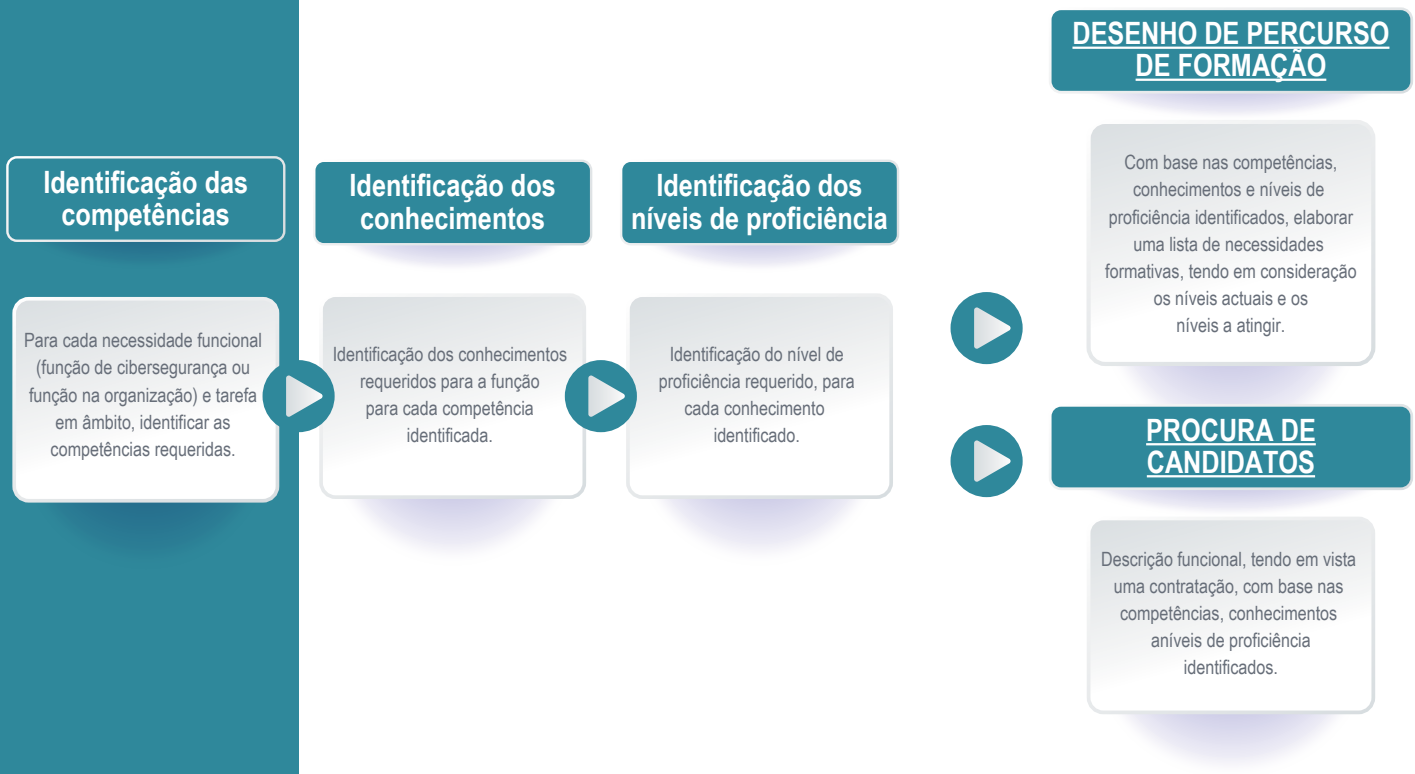


Figura 3 – Exemplos de utilização do referencial de competências, desde as necessidades funcionais e tarefas ao desenho de percursos de formação e à procura de candidatos.

05 CONCLUSÕES E RECOMENDAÇÕES

O presente Referencial pretende dar resposta à necessidade de identificar e mapear as competências que constituem as capacidades – transversais e especializadas – da área da cibersegurança. Desta forma, pretendeu-se criar um corpo de conhecimento capaz de mapear as valências necessárias para o cumprimento das funções específicas da cibersegurança, no contexto nacional.

Para tal, o Referencial propõe definições concetuais, uma arquitetura, bem como uma lista concreta de competências e de conhecimentos associados. Como quadro de referência, não deve ser entendido como prescritivo, nem como lista exaustiva e suficiente para abarcar a complexidade cognitiva da área da Cibersegurança que se encontra em rápida evolução. Em particular, não são cobertas áreas de governação e gestão genéricas, mas apenas aquelas que se afiguram como críticas para a gestão e operacionalização da Cibersegurança. Assim, deve ser usado como uma referência, a adaptar a cada contexto prático de utilização, que facilita o alinhamento semântico e pragmático no universo de discurso endereçado.

06 REFERÊNCIAS

[1] Quadro Nacional de Referência para a Cibersegurança, Centro Nacional de Cibersegurança, 2019.

[2] Roteiro para Capacidades Mínimas de Cibersegurança, Centro Nacional de Cibersegurança, outubro de 2019.

[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] Referencial de Singapura SkillsFuture, Skills Framework for ICT / Cyber Security, disponível online em https://ww w.imda.gov.sg/cwp/assets/imtalent/skills-frame work-for-ict/index.html .

[6] Quadro Dinâmico de Referência de Competência Digital para Portugal, Iniciativa Nacional Competências Digitais e.2030 - INCoDe.2030, setembro 2019.

[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.

CNCS

Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt • (+351) 210 497 400