# National Cybersecurity Capacity Building

Lino Santos

@ Jornadas Computação Científica

CNCS

Centro Nacional
de Cibersegurança
PORTUGAL

I do not rely on technology to run my business

I am safe… I have five layers of firewalling

Cybersecurity is a tech issue…You should talk to my IT

A Cybersecurity company offered me a solution to comply with RGPD in an fortnight, should I buy it?

# Table of contents:

1. Cyberspace and Cybersecurity
2. Portuguese National **Cybersecurity Center** (CNCS);
3. The importance of the **human factor**;
4. Developing **Cybersecurity Capabilities**;

# 1. Cyberspace and Cybersecurity

# Cyberspace

- Refers to the usage of technology
- Powerful media that magnifies communication
- Compresses space and time
- Decentralized and aterritorial
- Utopian Liberty
- Sense of anonymization

# Cybersecurity social construction

- 1988 - Morris worm
- 1990/1998 - Polymorphic viruses and worms
- 2007/2008 - Estonia and Georgia cyber attacks
- 2013 - Snowden revelations
- 2018 - Cambridge Analytica scandal

CNCS

## Defence

Sovereignty
Mission assurance
Exploitation

## Homeland security

Fight Cybercrime
Critical Infrastructure Protection

## Market

Digital market
Economy growth
Consumers confidence

## Civil Liberties

Privacy
Freedom of speech
Human rights on cyberspace

# 2. Portuguese National Cybersecurity Center (CNCS)

# Portuguese
# National Cybersecurity Centre

Established in **2014**, is the **Portuguese Cybersecurity Authority**

“Promotes the cyberspace usage in a **free, trustable and secure fashion**”

Training and awareness

Cybernorms

National and International cooperation

CERT.PT

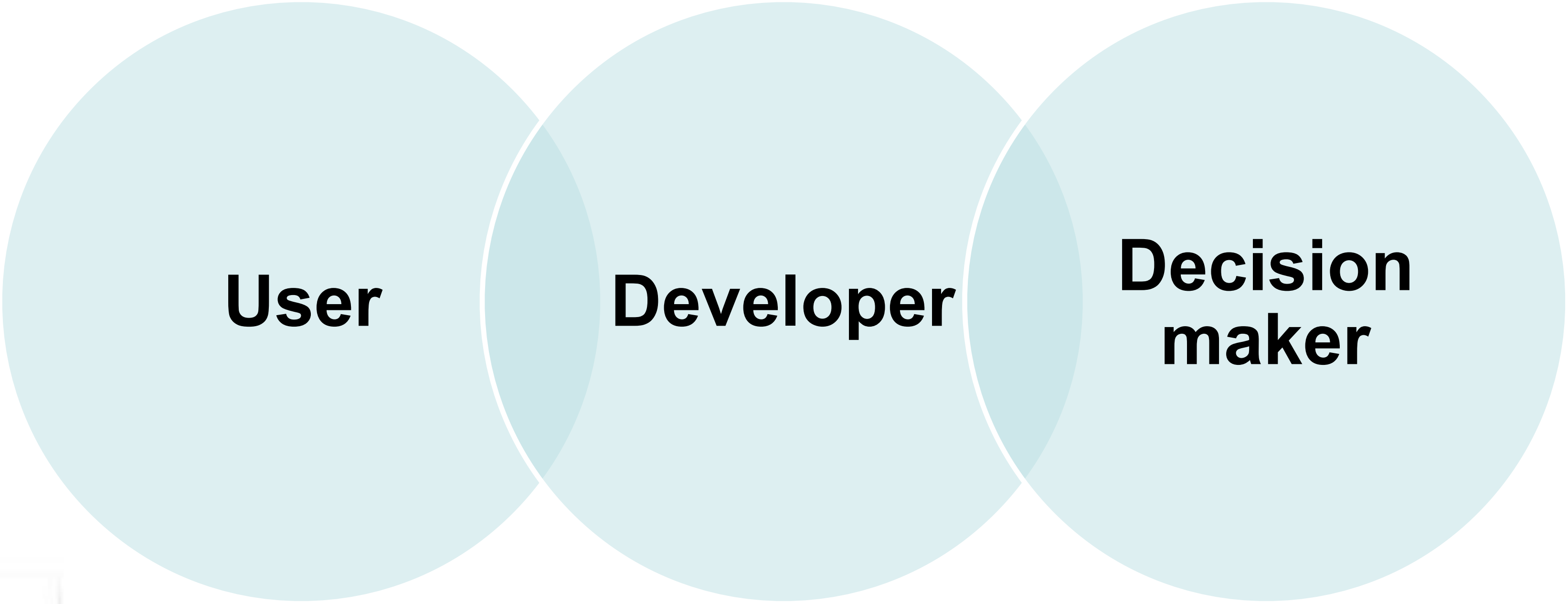
# 3. The importance of the human factor

The **technological network** we live in is also **made of humans.**

The **human factor** is not the weakest one, **it's the only one that really matters**.

Liam Burnett-Blue

It is necessary to **strengthen the human factor** at different levels:



User

Developer

Decision maker

1st keyword:

# RESPONSIBILITY of the user

# DANGER:

## NAIVETY

***Confusion** between the usefulness of technology and its benevolence.*

***Unawareness** of malicious technical possibilities*

2nd keyword:

# RESPONSIBILITY
# of developers/technicians

## Security by design and security by default

- Security features **integrated** in the **development**, avoiding **extra efforts** by the user;
- **Solve the cause,** not the symptom;
- **User-friendly** security features.

3rd keyword:

# AWARENESS of decision makers

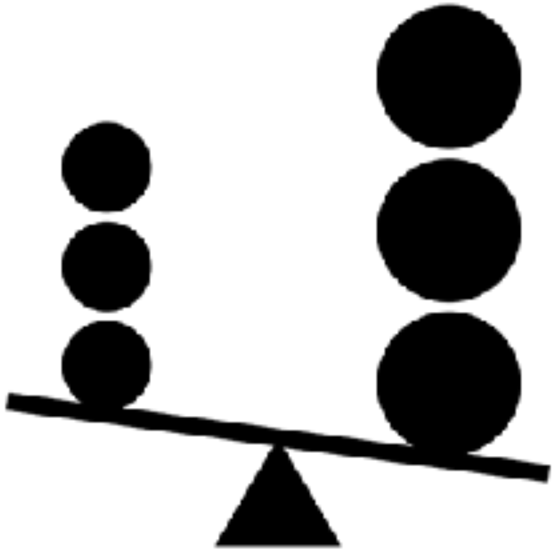
The **decision makers** must have a **cybersecurity strategic** vision in order to value cybersecurity efforts in their **organizations.**

# 4. Developing Cybersecurity Capabilities

# One of the main problems

“Growing asymmetry between the **know-how needed to commit a cybercrime** or launch a cyberattack, and the **skills needed to defend against it**. The crime-as-a-service model has lowered the barriers of entry to the cybercriminal market: **individuals without the technical knowledge** to build them can now rent botnets, exploit kits or ransomware packages.”

(ECA, 2019)



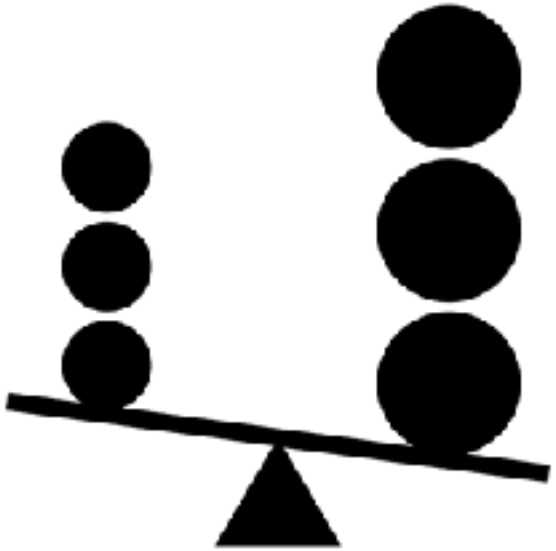
# More problems

“**Traditional** recruitment channels are **not meeting demand** (…)

Nearly **90%** of the global cybersecurity workforce is **male** (…)

At **universities**, cyber-related subjects are **under-represented** on non-technical courses.”

(ECA, 2019)



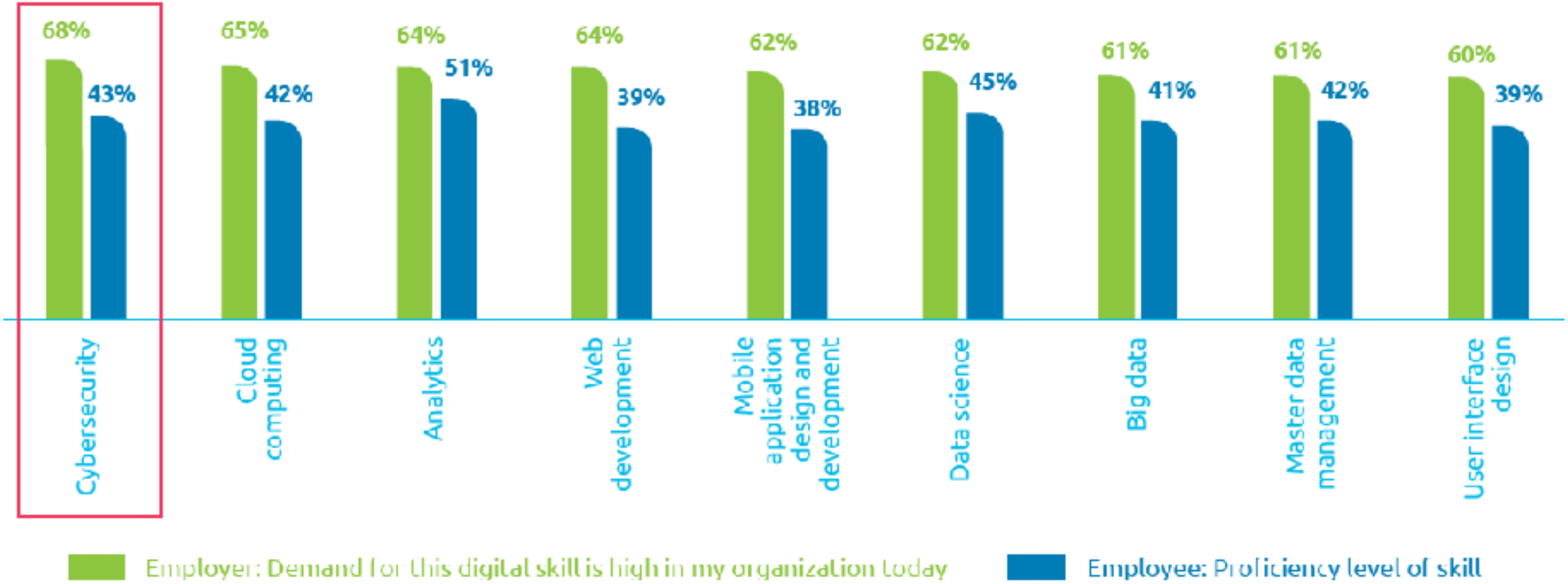
## Training and education is especially needed among

- civil servants
- law enforcement officers
- judicial authorities
- armed forces
- educators

(ECA, 2019)

# Cybersecurity has the largest demand as well as the largest gap between demand and supply

Organizations that acknowledge that demand for a hard digital skill is high today and employees who are proficient in that hard digital skill

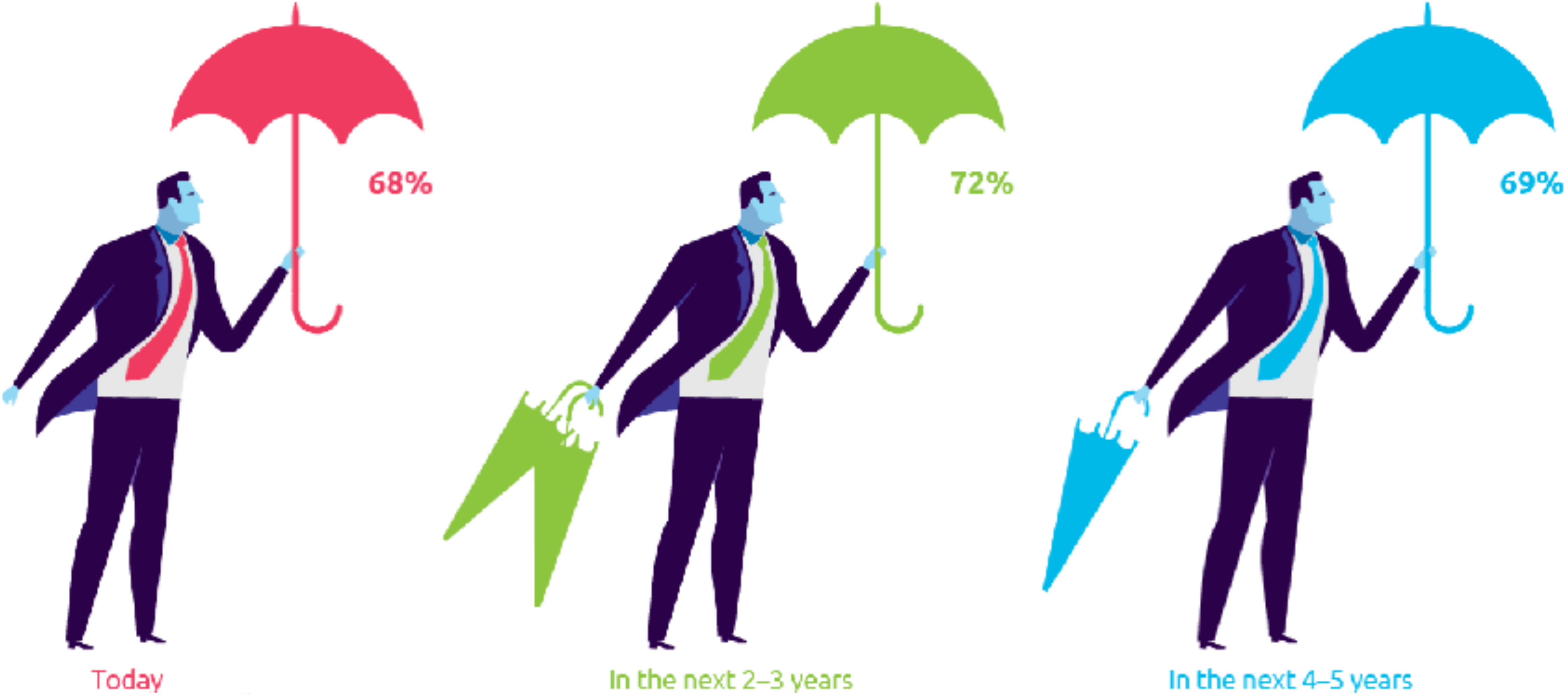


CNCS

Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap, June–July 2017

# The demand for cybersecurity is not likely to diminish in the next few years

Percentage of organizations that acknowledge demand for cybersecurity is high in their organization



Source: Capgemini Digital Transformation Institute survey, Digital Talent Gap, June–July 2017

2015

# PORTUGUESE STRATEGY 1.0

1 - Cyberspace security structure;
2 - Fighting cybercrime;
**3 - Cyberspace and infrastructures protection;**
**4 - Education, awareness and prevention**
**5 - Research and development;**
6 - Cooperation.

## 2018

## Law 46/2018

- NIS directive implementation;
- Whole-of-Government and **whole-of-Society** perspective;
- **Cyberspace Security Council;**
- **Cooperation;**
- Incident notification.

## 2018…

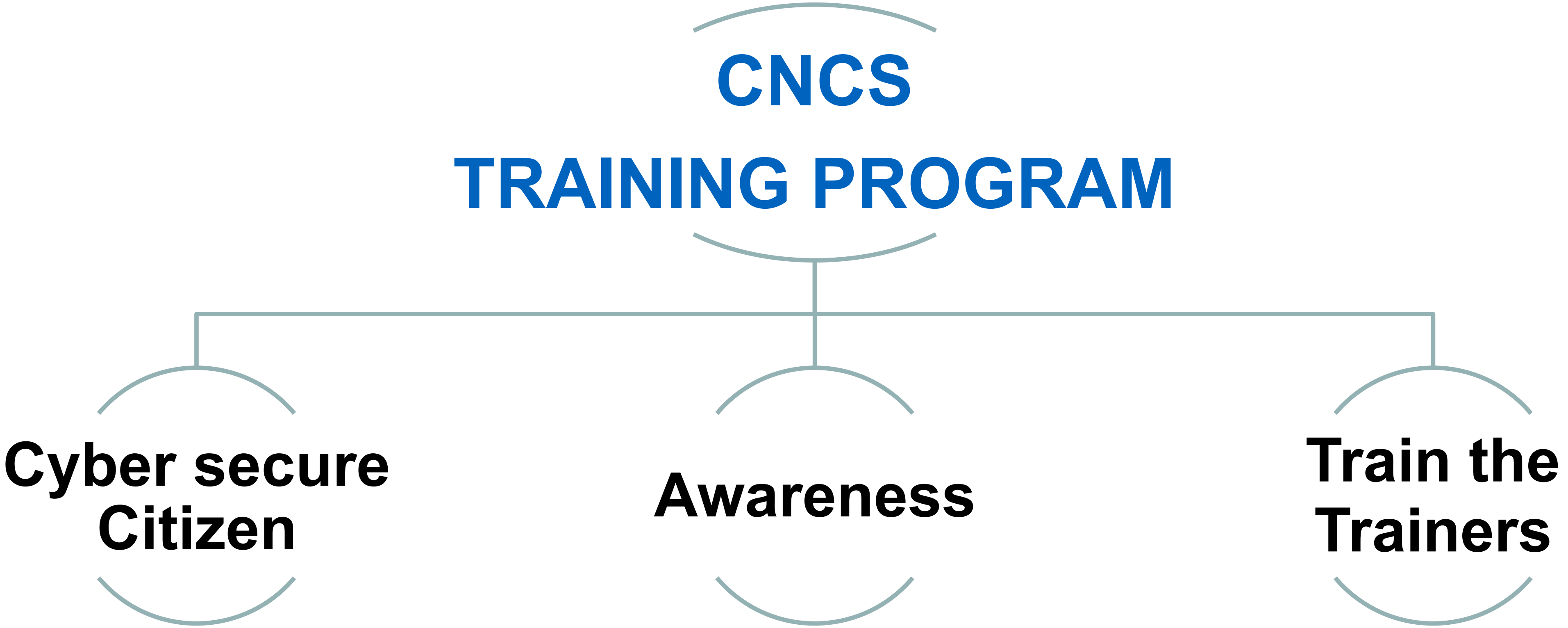
## PORTUGUESE STRATEGY 2.0 *to be*

- New technologies and new threats update;
- One of the main axes (2):
  - **prevention, education and awareness** - campaigns, literacy, training/school/ universities, young talents, CS careers, talent retention, decision-makers training, articulation with EU and NATO.

# ONE OF
# CNCS OBJECTIVES IS

to promote cybersecurity **training** and
**human resources qualification**.

CNCS



CNCS
TRAINING PROGRAM

Cyber secure Citizen

Awareness

Train the Trainers

**Cyber secure Citizen** is a short and simple **e-learning** course, accessible to all **citizens**, providing the necessary knowledge for cyber-protection and cyber-hygiene good practices adoption.

CIBERSEGURANÇA
UMA RESPONSABILIDADE DE TODOS
E PARA COM TODOS

cidadão
ciberseguro

Inscreva-se em
www.cncs.gov.pt

CNCS

**Awareness** in cybersecurity carries out actions throughout the country, addressing **citizens/employees; technical workers; and decision makers**.

PROGRAMA DE SENSIBILIZAÇÃO E TREINO EM CIBERSEGURANÇA

Ciber(in)segurança

Ação de Sensibilização em Ciber-higiene

CNCS

Módulo 1

PROGRAMA DE SENSIBILIZAÇÃO E TREINO EM CIBERSEGURANÇA

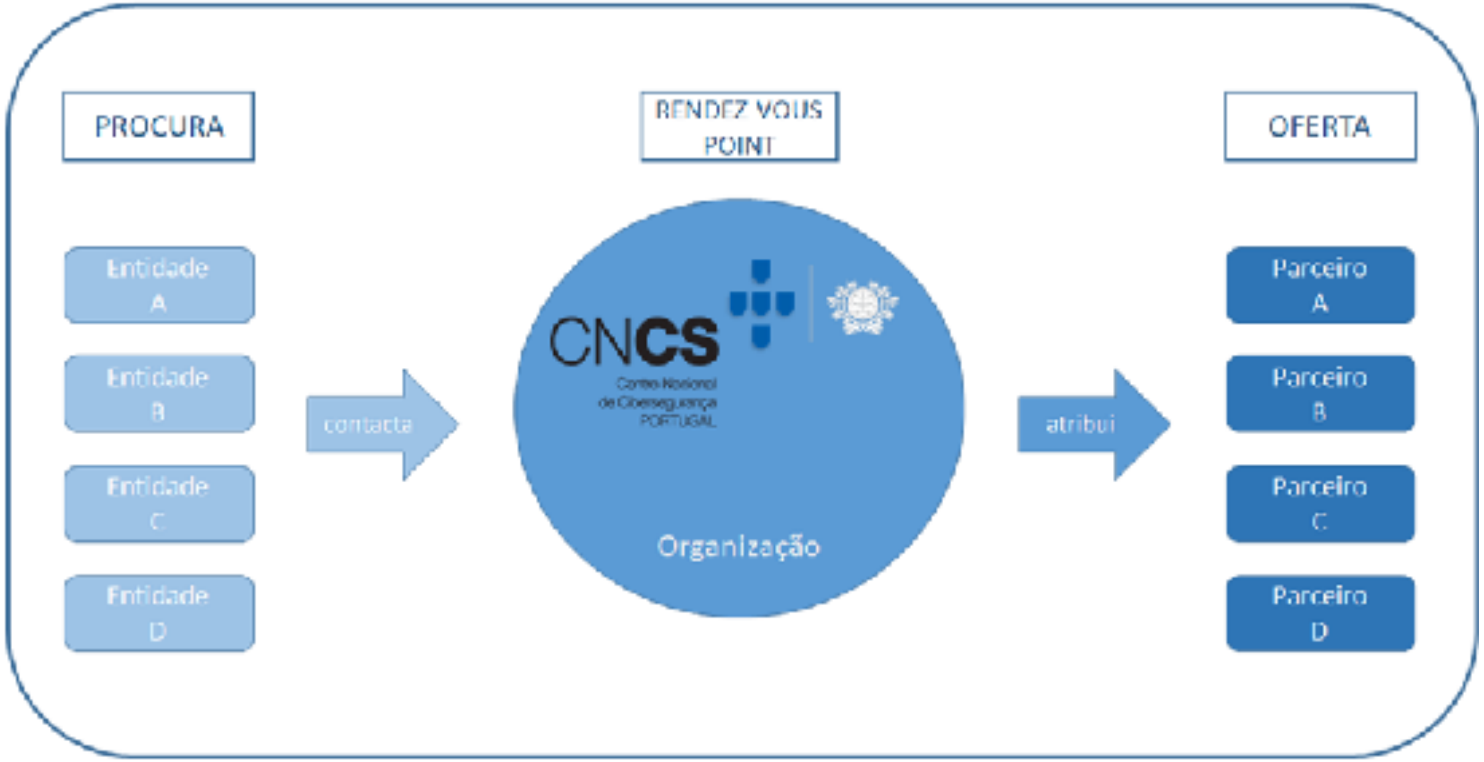
Ciber-higiene e boas práticas de cibersegurança

Ação de Sensibilização em Ciber-higiene

CNCS

Módulo 2

**Train the trainers** consists of **training trainers**, nominated by partners, who will belong to a **CNCS Trainers Stock**, and will be able to give training at their own organizations and at organizations defined by CNCS.



PROCURA

RENDEZ VOUS POINT

OFERTA

Entidade A

Entidade B

Entidade C

Entidade D

contacta

CNCS Centro Nacional de Cibersegurança PORTUGAL

Organização

atribui

Parceiro A

Parceiro B

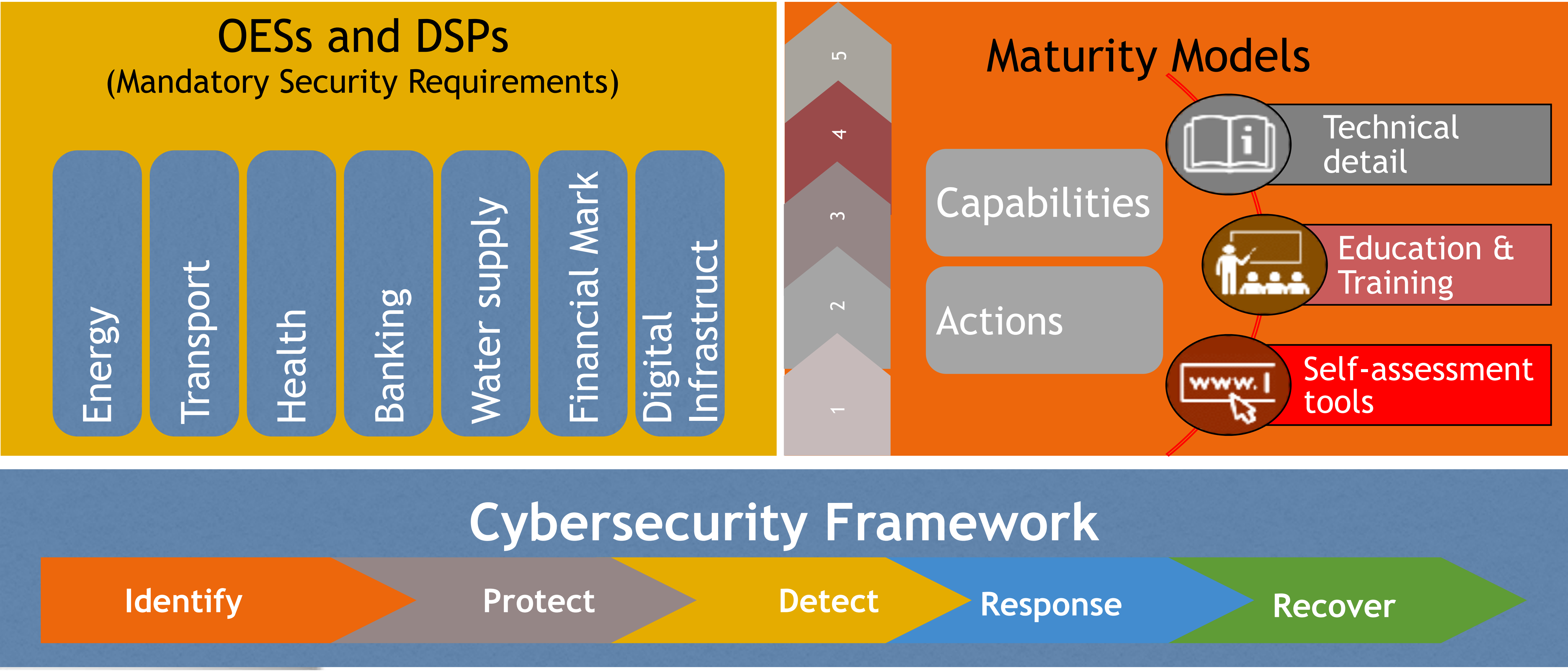
Parceiro C

Parceiro D

# ANOTHER OBJECTIVE IS

Strengthen national **Cybersecurity**.

# Cyber Assessment Framework



## OESs and DSPs

(Mandatory Security Requirements)

Energy

Transport

Health

Banking

Water supply

Financial Mark

Digital Infrastruct

## Maturity Models

Capabilities

Actions

Technical detail

Education & Training

Self-assessment tools

## Cybersecurity Framework

Identify

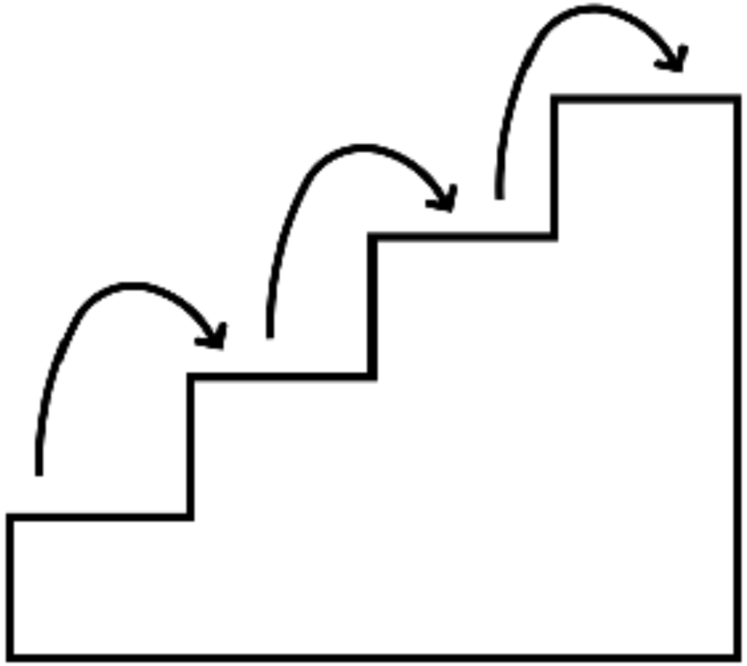
Protect

Detect

Response

Recover

# Maturity Models

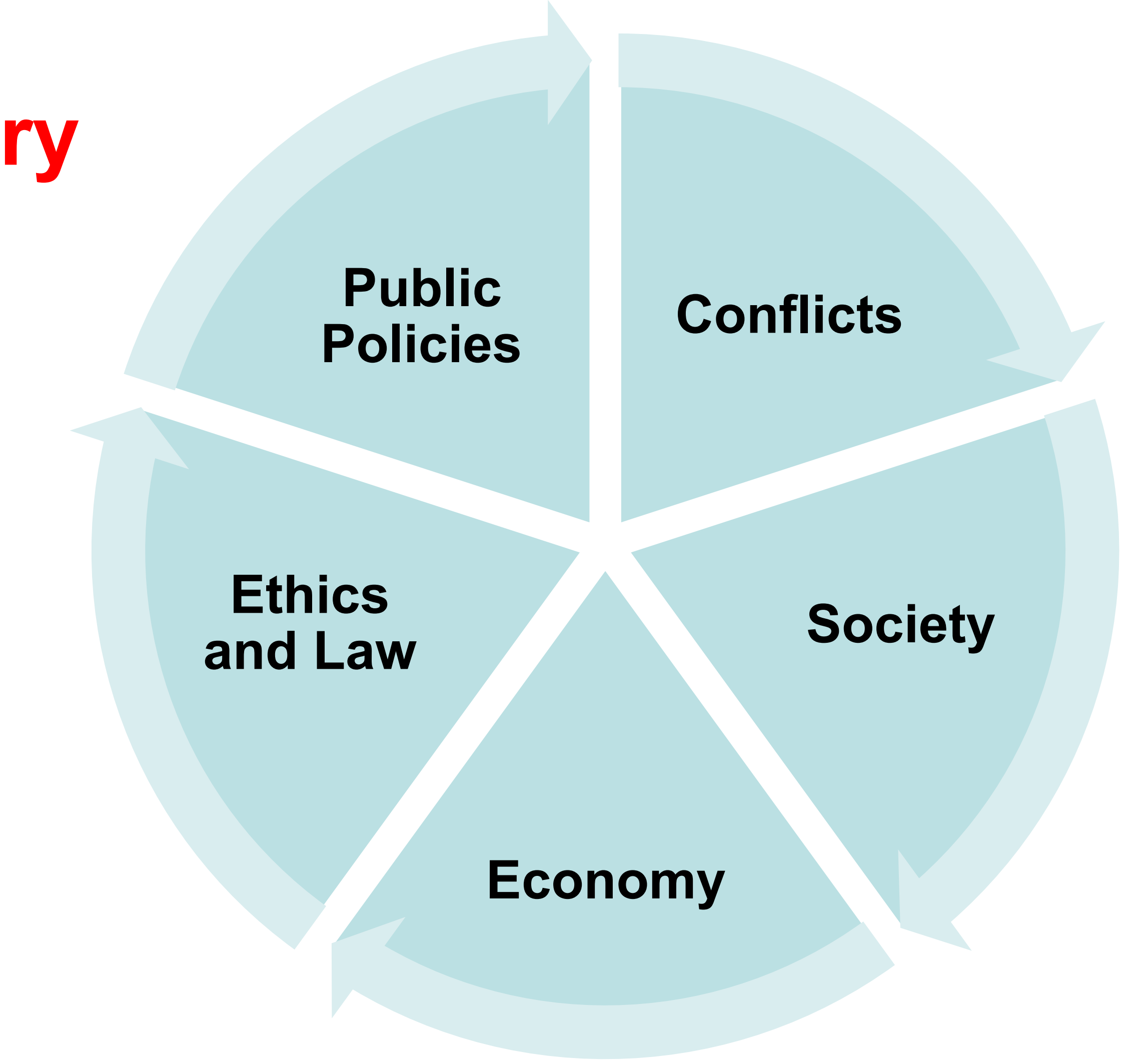


- **No just** controls and measures;
- Defines **priorities** and a way to **progress;**
- Provide technical **guidance**, training, tools and solutions;
- It is possible to **compare** with other organizations.

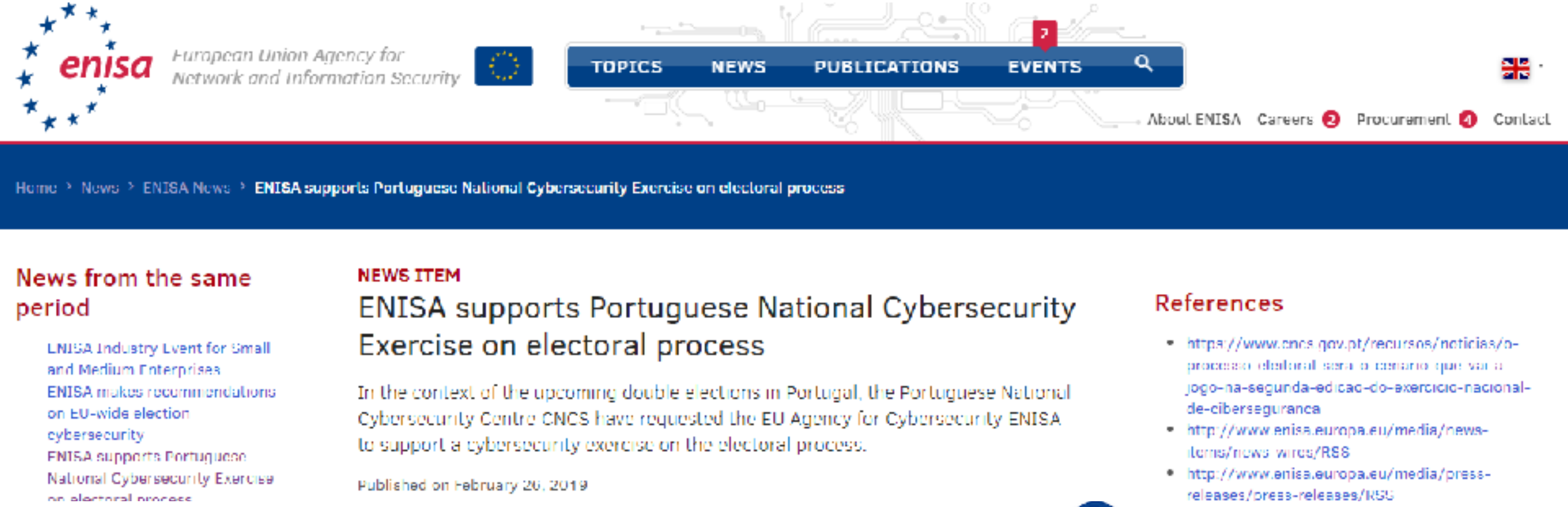
1 2 3 4 5

# Cybersecurity Observatory

A knowledge **analysis and systematization platform**, identifying trends and articulating **several stakeholders** for information collection.



2.0 Strategy Assessment


enisa
European Union Agency for Network and Information Security
TOPICS
NEWS
PUBLICATIONS
EVENTS
2
About ENISA
Careers 2
Procurement 4
Contact
Home › News › ENISA News › ENISA supports Portuguese National Cybersecurity Exercise on electoral process

News from the same period

- ENISA Industry Event for Small and Medium Enterprises
- ENISA makes recommendations on EU-wide election cybersecurity
- ENISA supports Portuguese National Cybersecurity Exercise on electoral process

NEWS ITEM

ENISA supports Portuguese National Cybersecurity Exercise on electoral process

In the context of the upcoming double elections in Portugal, the Portuguese National Cybersecurity Centre CNCS have requested the EU Agency for Cybersecurity ENISA to support a cybersecurity exercise on the electoral process.

Published on February 26, 2019

References

- https://www.cncs.gov.pt/recursos/noticias/o-processo-eleitoral-sera-o-cenario-que-vai-a-jogo-na-segunda-edicao-do-exercicio-nacional-de-ciberseguranca
- http://www.enisa.europa.eu/media/news-items/news-wires/RSS
- http://www.enisa.europa.eu/media/press-releases/press-releases/RSS

# Portuguese National Cybersecurity exercise

ExNCS
Centro Nacional de Cibersegurança PORTUGAL

CNCS

https://www.enisa.europa.eu/news/enisa-news/jenisa-supports-portuguese-national-cybersecurity-exercise-on-electoral-process

# Thank You.

CNCS

lino.santos@cncs.gov.pt