NIS Directive implementation in the Health sector

Jéssica Domingues
Chair WS on Health
Centro Nacional de Cibersegurança, Portugal

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Portuguese National Cybersecurity Centre

The **Portuguese Cybersecurity Authority** was established in **2014**

NIS Authority for all sectors since **2018**

The **Portuguese Cybersecurity Certification Authority** was established in **2021**

"Promotes a cyberspace usage in a **free, trustable and secure fashion**"

Training, Awareness and Situational Knowledge

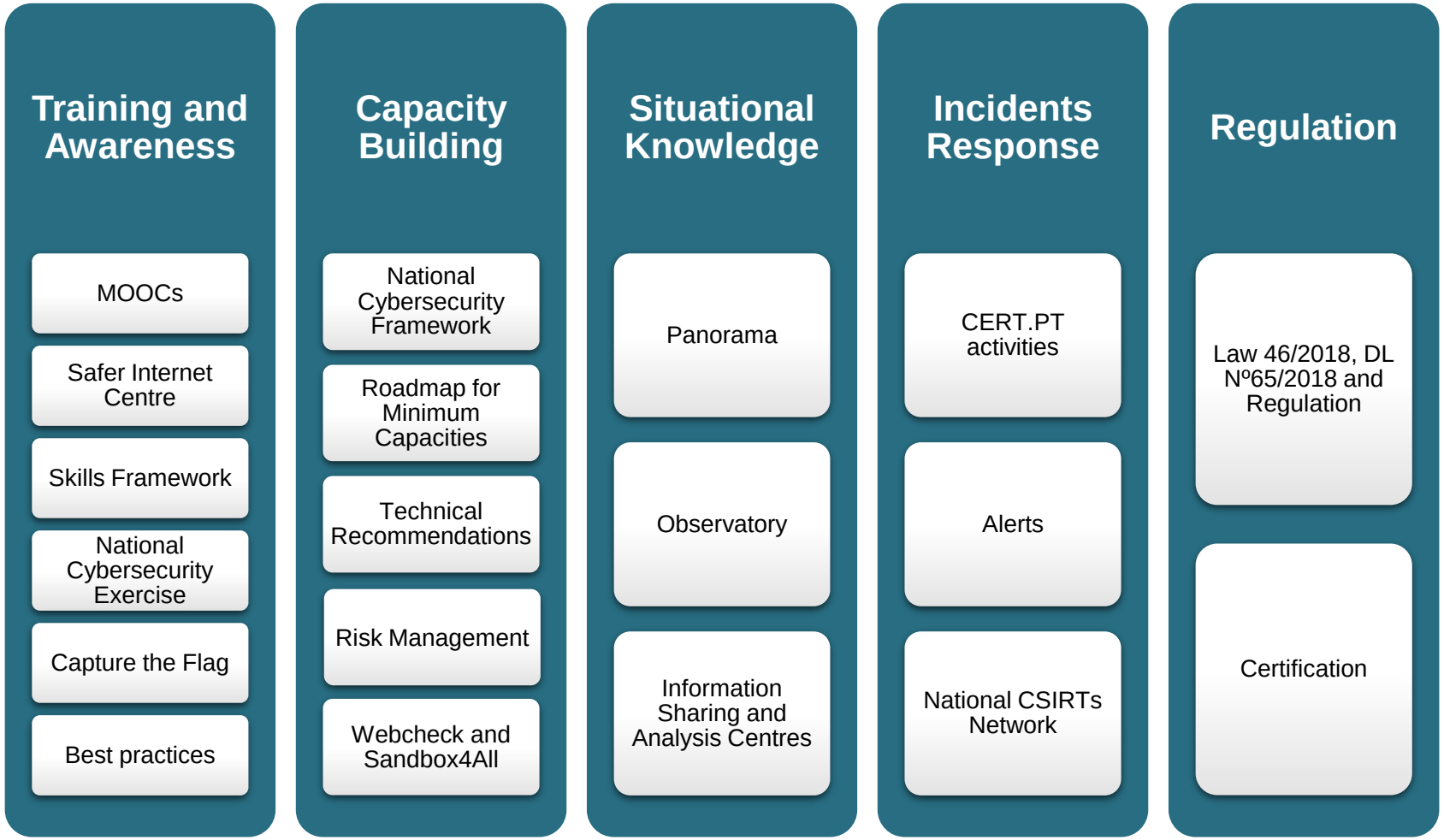
Recommendations, best practices, norms and referentials production

National and International Cooperation

CERT.PT

CNCS
Centro Nacional de Cibersegurança PORTUGAL

CNCS Activities



Projects

C-Academy
C-Hub
Competence Centres

Events

C-Days Conference
Webinars

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

NIS Directive

- First piece of EU-wide cybersecurity legislation
- Adopted in 2016
- National transposition by the EU member states on 9 May 2018

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a **high common level of security of network and information systems across the Union**

1. **National capabilities:** EU Member States must have certain national cybersecurity capabilities of the individual EU countries.
2. **Cross-border collaboration:** Cross-border collaboration between EU countries
3. **National supervision of sectors that are consider as essential for the maintenance of critical societal and economic activities:** Ex-ante supervision in sectors of energy, transport, water, health, digital infrastructure and finance.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

NIS Cooperation Group

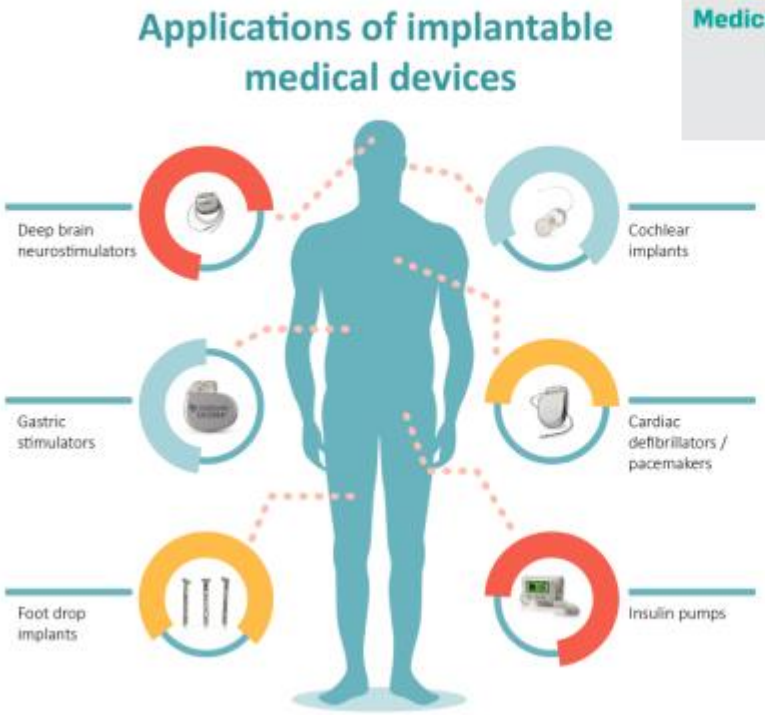
- The members of the NIS cooperation group are representatives of relevant national ministries and national cybersecurity agencies, the Commission and ENISA.
- Is the **strategic cooperation group**, where the members cooperate, exchange information and develop trust and confidence amongst them.
- Work programme every two years in respect of actions to be undertaken to implement its objectives and tasks.
- **Third Biennial Work Programme (2022-2024)**
  - **Goal 1: Facilitate Implementation of NIS2**
  - **Goal 2: Strategic Discussion on key policy files for cybersecurity in the EU**
  - **Goal 3: Operationalising the sharing of information and best practices**

CNCS
Centro Nacional de Cibersegurança PORTUGAL

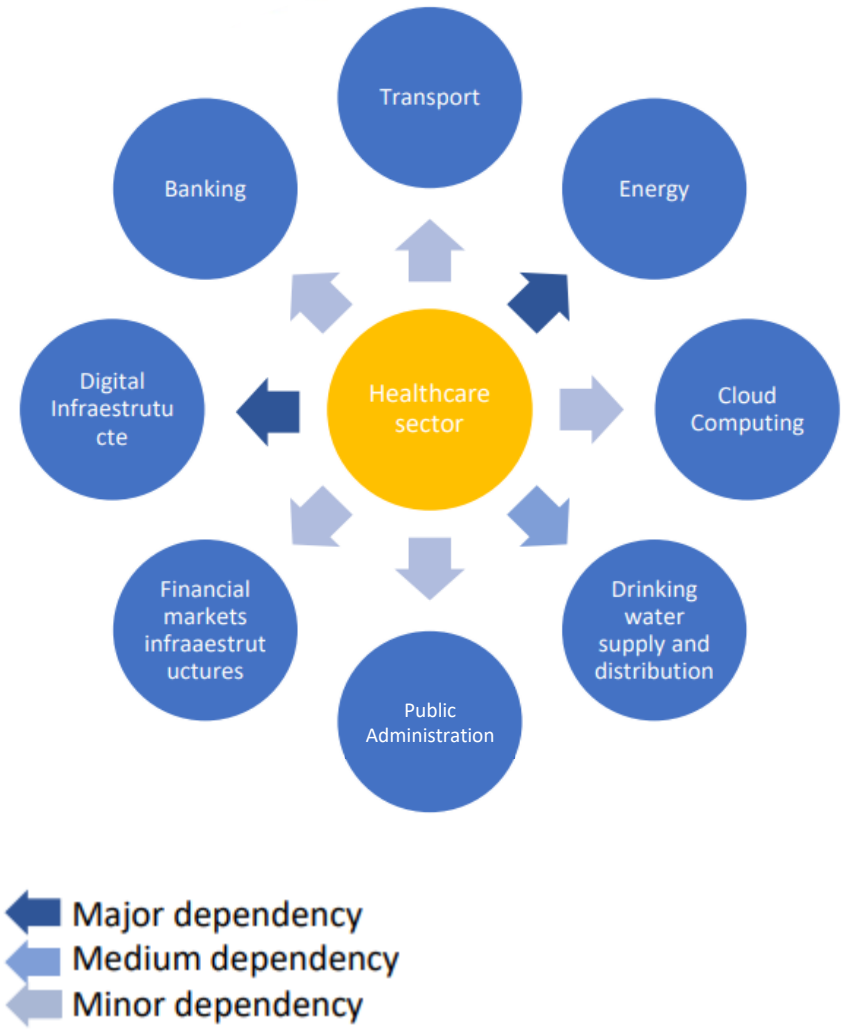
Motivation

- The **health sector** has been making growing use of technological resources and information systems. Health is one of the domains where technology **can have a substantial beneficial impact in people's lives and well-being**

- A **high common level of cybersecurity** can ensure the proper deployment of health services and the **required protection** of physical and digital infrastructure and assets, professionals and people's information, including personal and sensitive data



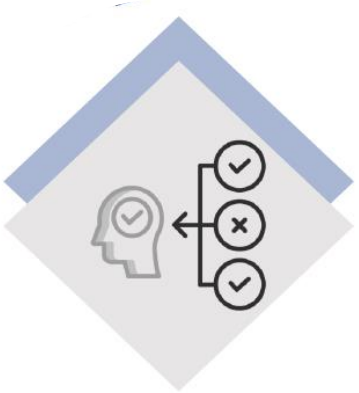
Situational Analysis



- The ability of a healthcare organization to provide essential services does not solely depend on the organization itself.
- Heterogeneous ICT systems, medical devices and institutions landscapes
- High level of sensitive information integration (interoperability)
- Legacy systems and unsupported technologies are present in almost all institutions
- Low maturity on cybersecurity and shortage of talent in cybersecurity
- Organizational culture that prioritizes patients life over information security and lack of security awareness
- Limited human and financial resources
- Hospitals are easy targets for malicious attackers

WS on Health

- The Second Biennial **Work Programme** of the Cooperation Group (2020-2022) established the **creation of a new Work Stream on Health sector.**
- Proposal made by the **eHealth Network**, supported by **DG SANTE** and **DG CONNECT**, to create a dedicated work stream to healthcare, with the initial leadership of **Portugal**
- **Kick-off** meeting on **17 june 2020**
- Online plenary meeting's per trimestre
- **92 representatives** from 28 MS + DG CONNECT + DG SANTE + ENISA



CNCS
Centro Nacional de Cibersegurança PORTUGAL

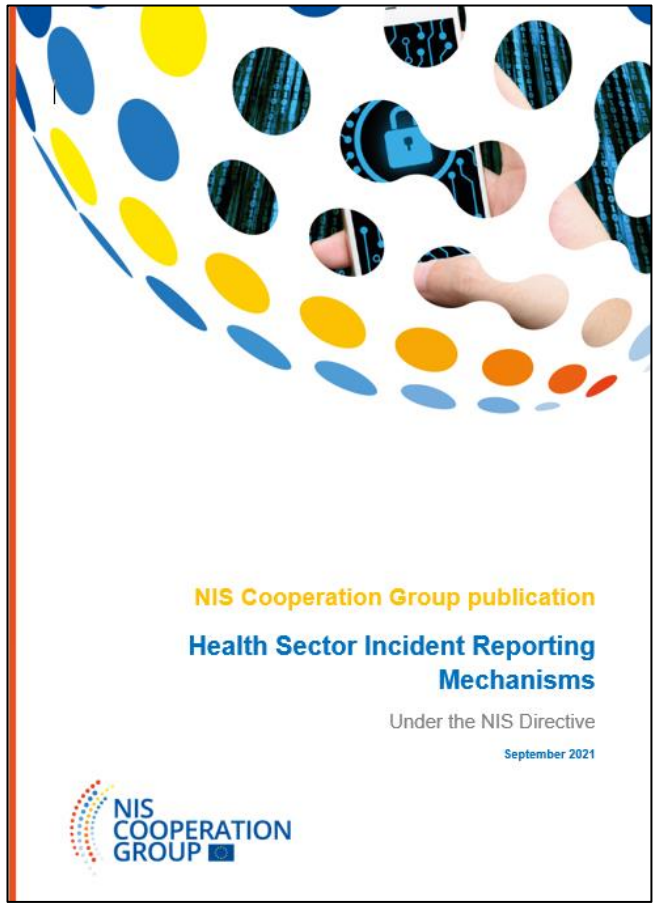
Goals - WS on Health

- Facilitate the **implementation of the NIS Directive** in the health sector, addressing its particularities.
- Identify and **share best practices** for cybersecurity in the health sector.
- Develop useful resources and documentation to **create and promote recommendations** based on a risk management approach for the health sector.
- Promote cybersecurity **capacity building activities** for NIS and relevant health authorities, as well as to operators of essential services in the health sector.
- Strengthen **communication and cooperation** between WS participants.
- Monitor discussions and providing information about the upcoming **NIS2 Directive** and other relevant regulation.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Deliverables – Health Sector Incident Reporting Mechanisms

- Task Group 2 involving **ENISA, Ireland, Luxembourg, Portugal and Sweden.**
- Interviews with **19 MS authorities** during May-July 2021
- Report on how **NISD incident reporting for health** has been implemented
  - Incident reporting thresholds
  - Incident report mechanisms
- Identification of **good practices** and **mapping to challenges**
- Approved on **December 2021** by NIS CG



CNCS
Centro Nacional de Cibersegurança PORTUGAL

Health Sector Incident Reporting Mechanisms

IDENTIFICATION

- **Formal** thresholds for OES (67%)
- **Unofficial** thresholds (32%)
- **Balance** of MS with health specific and cross-sectoral thresholds

DEFINED BY

- Central National Competent Authority
- National CSIRT
- Health Sectoral Competent Authority

CRITERIA

- **Impact** on service delivery
- Number of **users affected**
- **Duration** of the incident
- Generation of **injury** or **loss of life**
- **Geographical** coverage

CNCS Centro Nacional de Cibersegurança PORTUGAL

enisa

Health Sector Incident Reporting Thresholds

AUTHORITIES

- Central CSIRT (13 MS)
- Centralised authority (8 MS)
- Sectoral CSIRT (4 MS)
- Sectoral authority (1 MS)

PROCESSES

- Timeline of reporting
- Tools and templates used
- Format of the report
- Flow of information

COMMUNICATION, CONSULTATION AND COLLABORATION

- Legally established (47%)
- Not legally formalised (11%)
- Planned or being drafted (21%)

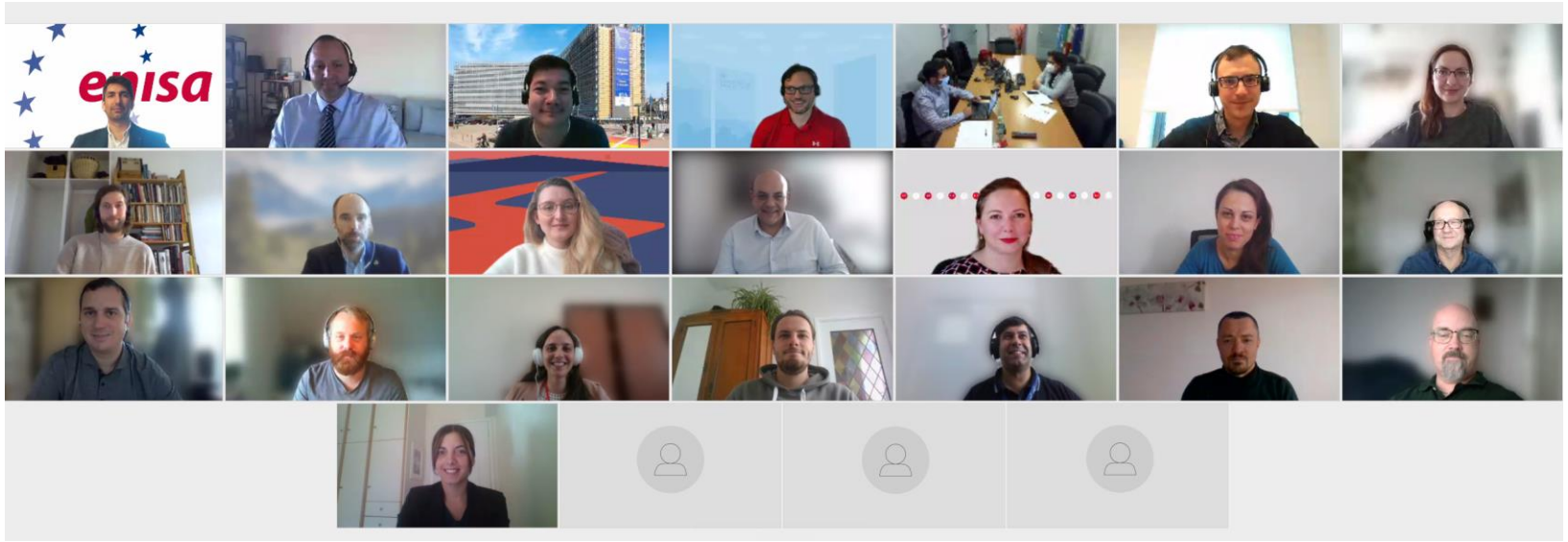
SHARING OF LESSONS LEARNED

- Forums
- Webinars and seminars
- National cooperation group
- National health working group

CNCS Centro Nacional de Cibersegurança PORTUGAL

enisa

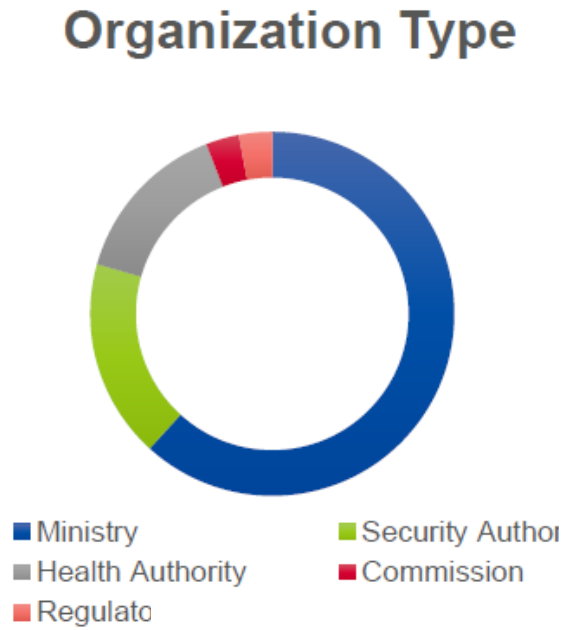
Deliverables – Capacity Building Exercise



GOAL: Increase the overall competence of NIS Authorities when addressing cybersecurity in the health sector

- Interactive Table-top Capacity Building Activity
- Occurred **online** on 20 th of October 2021
- Targeted an audience of people with responsibilities on policy making and supervising activities related with the health sector
- **19 MS Participants**

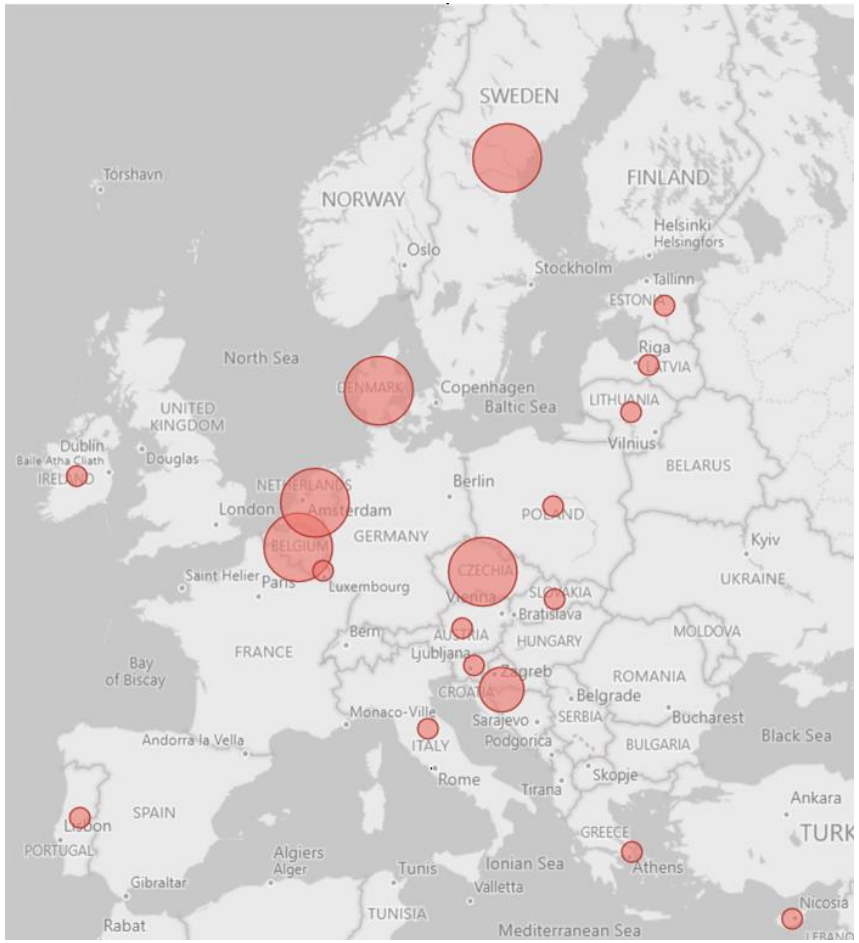
- Task Group involving **Czechia, Portugal and ENISA.**



Capacity Building Exercise

- This activity was made up of **6 sessions**, each represented by an individual chapter.
  - Introduction
  - Increase Knowledge and Provide Insights
  - Raise Awareness
  - National Regulation Policy
  - Strengthening Communication
  - Survey Results and Discussion

- The chapters were structured as 45-minute sessions, containing a 15-minute **presentation of material**, followed by a 15-minute **survey**, concluding with a 15-minute questions and **small discussion session**.



Capacity Building Exercise Key Achievements

- Brought MS parties together; involved with cybersecurity at a policy level
- Provided an opportunity to examine national procedures, identify improvements, and consider how they inform sector, national, and international policy, and guidance
- Expanded participation to include stakeholders across ministries, regulators, e-health organizations, and health operators of essential services across the Health Sector
- Examined the processes necessary to convene a policy discussion based on potential future attacks against the EU health sector
- Enabled NIS inter-authority discussion of relevant policy issues
- Identified opportunities to improve the flow of information between private sector and governmental organizations to ensure situational awareness
- Tested the capacity to communicate and coordinate on health policy topics as the need arises.
- Planned for and exercised different types of communication models based on who the audience receiving the information is and what is their capacity as per services offered within the health sector.

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Deliverables – Comming soon...

Cybersecurity requirements in the health sector

I. **Governance and Health Security in the Member States**
II. **Mapping of security measures with health subsector specific standards and EC recommendation**
III. **Policy measures in the Health Sector**
    - *Risk analysis*
    - *Guidance and training*
    - *Technical support*
    - *Capacity building*
    - Public-private collaboration
IV. **Methodologies to Identify the OES in the Health Sector**
V. **National Approaches on Identification Services and Criteria**
VI. **Outlook and Conclusions**

- Task Group 1 involving **Portugal and ENISA**

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Deliverables – Comming soon...

Use some cybereurope incidents for this event and provide training about how to prevent and react to an incident

Capacity Building to OES (by Train the Trainers)

Create a scenario to train individuals so that they can organize a similar event and readapt to their own National reality.

- Task Group 4 involving **Portugal, ENISA and Sweden**

CNCS
Centro Nacional de Cibersegurança PORTUGAL

Deliverables – Comming soon...

Consolidated Threat Landscape matrix specific for the health sector

12.25 - 12.40	Sectorial threat landscape by the Work Stream on Health / ENISA	**Pascal Bertrand**, Chargé d'études, The Luxembourg Regulatory Institute (ILR)

- Task Group 3 involving **Luxembourg, ENISA, Portugal and Denmark**

CNCS
Centro Nacional de Cibersegurança PORTUGAL

NIS2 Directive (Health Sector)

NIS1	NIS2
Healthcare providers	Healthcare providers
	EU reference laboratories
	• Entities carrying out research and development activities of medicinal products • Entities manufacturing basic pharmaceutical products and pharmaceutical preparations • Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’)

- Broader scope in the application of the Directive in the Health sector
- The Health sector will become a Critical Importance Sector

Thank you

Obrigada

Tak

CNCS
Centro Nacional de Cibersegurança
PORTUGAL