

Iniziativa organizzata
all'interno del progetto



UNIVERSITÀ
DEGLI STUDI
FIRENZE

Torino, 6 febbraio 2024

LA CYBERSICUREZZA: DALLA DIRETTIVA NIS ALLA NIS2

Erik Longo – Matteo Giannelli

PRINCIPALI FONTI A TUTELA DEL CYBERSPAZIO



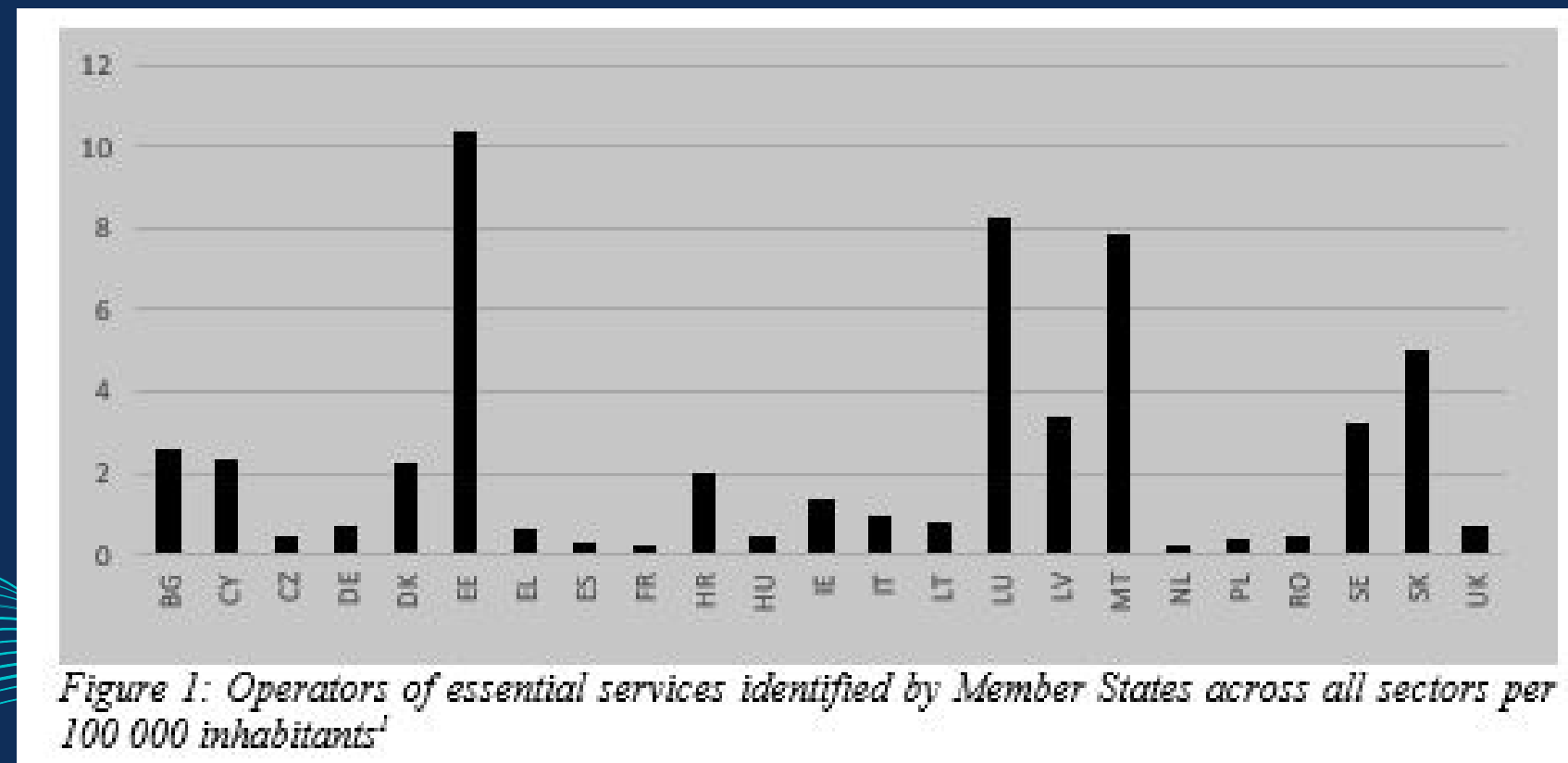
LA DIRETTIVA NIS 2016

1 Finalità

- Strategia nazionale Cyber
- Istituire gruppi di cooperazione per favorire lo scambio di informazioni
- Creare rete CSIRT
- Designate autorità di contatto nazionale (ACN – di 82/2021)
- Obblighi di sicurezza e notifica tra operatori di servizi essenziali e fornitori di servizi digitali

2 Esclusioni

- Funzioni essenziali (Sicurezza nazionale)
- Coordinamento e Armonizzazione minima



LA NIS 2: OBIETTIVI GENERALI

1 **Supplire alle carenze della NIS**

- basso livello di ciberresilienza delle imprese operanti nell'UE
- diversi livelli di resilienza tra Stati membri e tra settori
- mancanza di una risposta comune alle crisi
- Riduzione dei costi degli incidenti
- Superamento della distinzione tra **operatori di servizi essenziali** e **fornitori di servizi digitali**

2 **Un quadro comune per la gestione dei rischi**

- Gestione dei rischi a livello statale
- Meccanismi per una cooperazione efficace tra le autorità competenti
- Obblighi di segnalazione
- Elenco dei settori e delle attività interessate (all. 1)
 - Soggetti «essenziali»
 - Soggetti «importanti»
- Soglie dimensionali: medie e grandi

3 **Rafforzare l'autonomia strategica dell'UE**

- Ruolo dell' Agenzia dell'Unione per la cibersecurity (ENISA)
- Istituzione della rete europea delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe
- Modello per cooperazione con paesi terzi

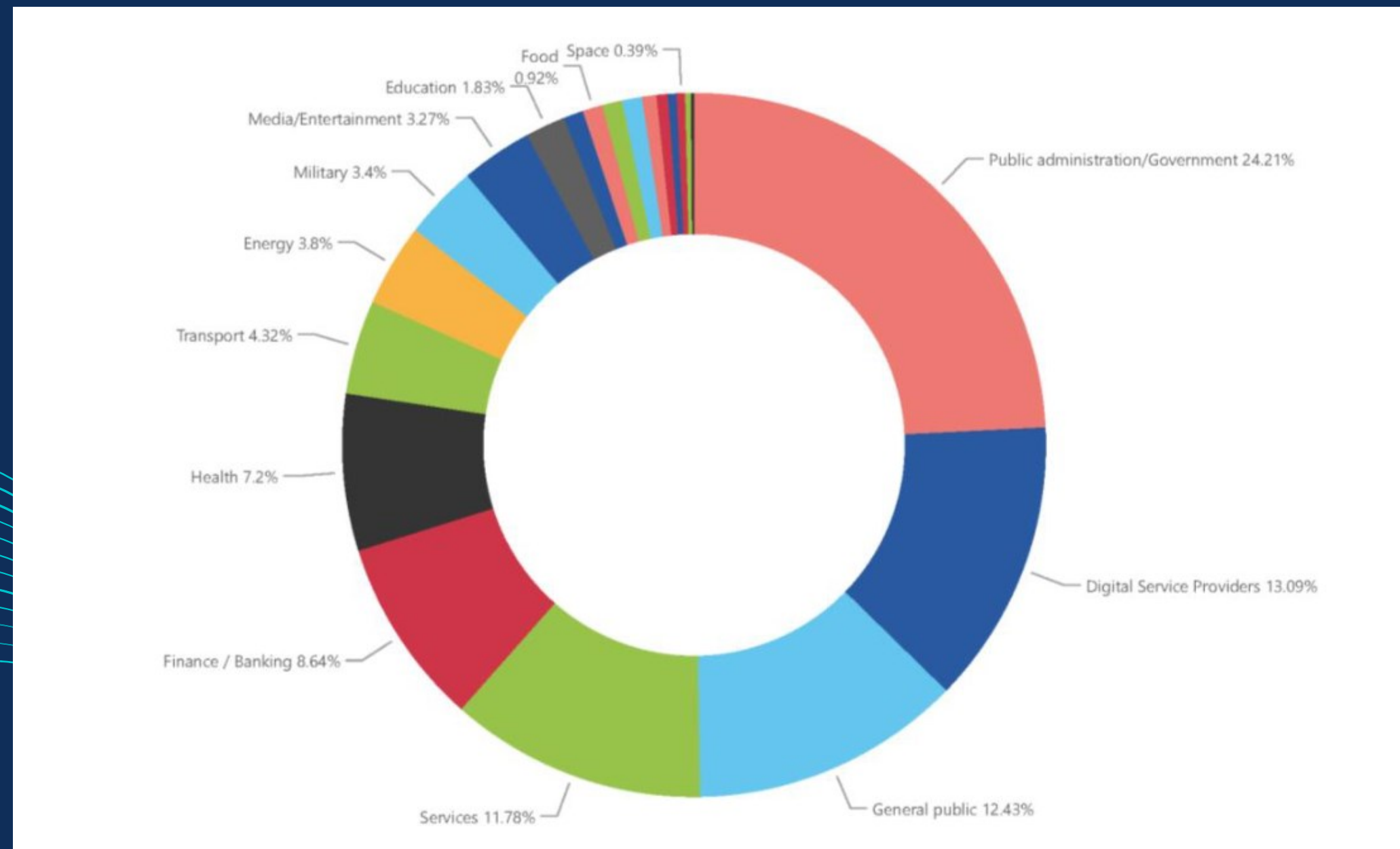
OBIETTIVI GENERALI

[ENISA Threat Landscape 2022](#) – Minacce principali



OBIETTIVI GENERALI

[ENISA Threat Landscape 2022](#) – Settori coinvolti (giugno 21-22)



L'INTERVENTO UE

4 Proporzionalità e sussidiarietà dell'intervento UE

- Rischi e costi;
- la natura sempre più transfrontaliera delle minacce;
- le potenzialità degli interventi dell'Unione volti ad agevolare strategie nazionali efficaci e coordinate
- il contributo degli interventi strategici concertati e collaborativi volti a un'efficace protezione dei dati e della vita privata.

5 Impatto sui diritti fondamentali

- «L'UE si impegna a garantire standard elevati in materia di tutela dei diritti fondamentali. Tutti gli accordi volontari di condivisione delle informazioni tra soggetti promossi dalla presente direttiva sarebbero attuati in ambienti sicuri nel pieno rispetto delle norme dell'Unione in materia di protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio»

6 Normativa complementare

- La direttiva non preclude l'adozione di ulteriori atti settoriali dell'Unione riguardanti le misure di gestione dei rischi di cibersecurity e le notifiche degli incidenti.
- Parte essenziale della strategia dell'UE per l'Unione della sicurezza.

DESTINATARI

7 (II) Soggetti essenziali

- Soggetti essenziali pubblici o privati che operano nei settori elencati nell'allegato I:
- energia; trasporti; settore bancario; infrastrutture dei mercati finanziari; settore sanitario, acqua potabile; acque reflue; infrastrutture digitali; **pubblica amministrazione** e spazio.
- **Vigilanza ex ante**

8 (II) Soggetti importanti

- Soggetti importanti che operano nei settori elencati nell'allegato II:
- servizi postali e di corriere; gestione dei rifiuti; fabbr., prod. e distr. di prodotti chimici; prod., trasf. e distr. di alimenti; settore della fabbricazione e fornitori di servizi digitali.
- **Vigilanza ex post.**

9 Esclusioni

- Amministrazioni locali e istituti di ricerca, salvo decisione degli Stati membri
- La NIS 2 non è applicabile alle articolazioni statali che hanno compiti di sicurezza nazionale e pubblica, della difesa e del perseguimento dei reati.
- Microimprese e piccole imprese salvo che si ricada in 7 o 8 (Racc. 2003/361)

MISURE IN MATERIA DI GESTIONE DEI RISCHI

A (I) Misure in senso stretto (art. 21)

- Basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da guasti del sistema, incidenti, azioni malevole e errori umani.
- Gli operatori potranno servirsi di prodotti sviluppati da soggetti che abbiamo acquisito la certificazione di cybersicurezza ai sensi del Cybersecurity Act (2019).

B (II) Ruolo dei membri degli organi gestori (art. 20)

- Dovranno approvare le misure di gestione dei rischi di cybersicurezza adottate.
- Attuazione e responsabilità per omessa vigilanza (?)

C (III) Obblighi di formazione

- Conoscenze e competenze non solo degli organi gestori ma anche dei dipendenti.

OBBLIGHI DI SEGNALAZIONE

A (I) Ruolo dei CSIRT (art. 23)

- Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi

B (II) Definizioni di incidenti significativi

Eventi in grado di causare

- (i) una grave perturbazione dei servizi o perdite finanziarie;
- (ii) di avere ripercussioni su altre persone fisiche o giuridiche.

C (III) Obblighi di comunicazione

- Entro 24 ore un preallarme;
- Entro 72 ore una notifica dell'incidente;
- Un relazione intermedia (se richiesta);
- Una relazione finale.

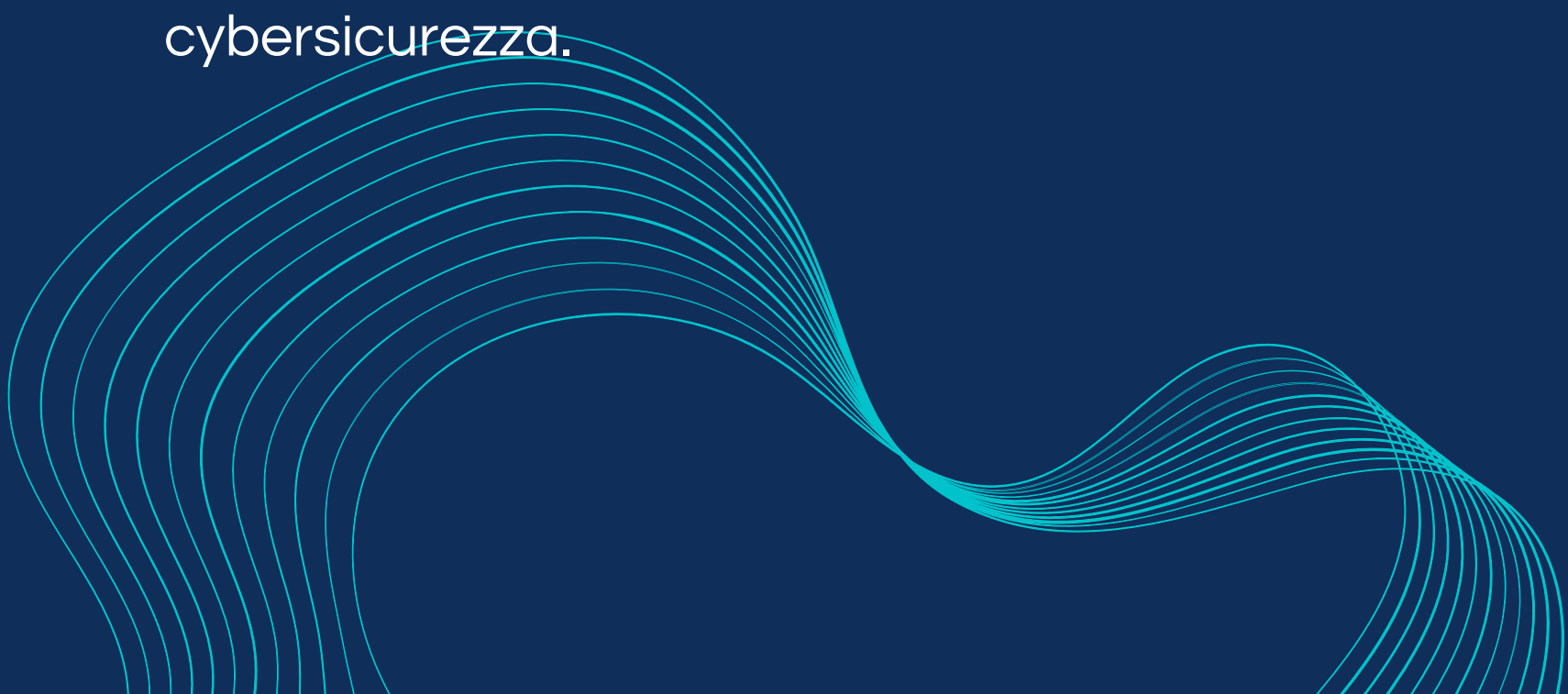
CONDIVISIONE DELLE INFORMAZIONI

A (I) Accordi di condivisione delle informazioni (art. 29)

- Possibilità per i soggetti essenziali e importanti di scambiare, su base volontaria, pertinenti informazioni sulla cybersicurezza.

B (II) Notifica volontaria di informazioni pertinenti

- Trasmissione al CSIRT delle minacce informatiche e dei quasi incidenti.



MISURE DI VIGILANZA E DI ESECUZIONE

A (I) Tipologie (art. 32)

- Ispezioni in loco e vigilanza a distanza;
- Audit, anche ad hoc;
- Scansioni di sicurezza;
- Richieste di informazioni;
- Richieste di accesso ai dati, documenti e altre informazioni;
- Richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza.

B (II) Conseguenze

- Le autorità competenti, in caso di accertamento delle violazioni, avranno il potere di emanare avvertimenti, adottare istruzioni vincolanti o ingiunzioni che impongano agli operatori di adottare le misure necessarie per porre fine alle violazioni riscontrate e, financo, di irrogare sanzioni..

MISURE SANZIONATORIE

A (I) Soggetti essenziali (art. 34)

- In caso di violazione delle misure in materia di gestione dei rischi o di obblighi di segnalazione: sanzioni pecuniarie amministrative pari a un massimo di almeno 10.000.000 EUR o a un massimo di almeno il 2% del totale del fatturato annuo.

B (II) Soggetti importanti (art. 34)

- In caso di violazione delle misure in materia di gestione dei rischi o di obblighi di segnalazione: sanzioni pecuniarie amministrative pari a un massimo di almeno 7.000.000 EUR o a un massimo di almeno l' 1,4% del totale del fatturato annuo.

C (III) Data breach (art. 35)

- Se le ipotesi I e II comportano anche una violazione dei dati personali, informazione senza indebito ritardo al GPDP. In caso di sanzione amministrativa ai sensi del GDPR, le autorità competenti non imporranno una sanzione amministrativa pecuniaria a norma dell'art. 34 della direttiva per una violazione imputabile al medesimo comportamento.

POLICY INSTRUMENTS

1 Hard Rules

- Obbligo per gli Stati di adottare una strategia nazionale per la cibersecurity (art. 5)
 - Designare autorità competenti (art. 7)
 - Obblighi di gestione e segnalazione dei rischi (art. 17)
 - Obblighi in materia di condivisione delle informazioni (art. 26)
 - Gruppo di cooperazione (art. 12)
 - Rete di CSIRT (art. 13)
 - Sistema di revisioni tra pari per valutare l'efficacia delle politiche di cibersecurity degli Stati membri (art. 16)
 - Poteri di vigilanza delle autorità competenti (art. 29): meri supervisor
- FOCUS:
Strumenti
di co-regulation**
- Possibile uso degli Stati dei sistemi europei di certificazione della cibersecurity (art. 21)
 - Gli Stati incoraggiano l'uso di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza dei sistemi informatici e di rete (art. 22)

SPUNTI CRITICI

1 Tempi

- 21 mesi per il recepimento (16 gennaio 2023 entrata in vigore – 17 ottobre 2024 termine)
- Monitoraggio e valutazione di impatto dopo 54 mesi

2 Capacità di risposta

- Scelta opportuna o obbligata dello strumento regolatorio?
- Armonizzazione mirata e flessibilità per le autorità competenti.

3 Questioni critiche

- Lacune nelle catene di approvvigionamento di servizi, sistemi o prodotti ICT critiche.
- Sovraccaricare gli attori privati e pubblici di costosi adempimenti normativi. Costi di compliance.

RECEPIMENTO DELLA NIS 2 IN ITALIA

1 Punti nodali

- Individuazioni enti pubblici considerati PA ed esclusioni;
- Soggetti operanti (distinzione tra ACN e alter autorità);
- Soggetti destinatari: definire entro il 17 Aprile 2025 elenco (da aggiornare periodicamente);
- Modifica alla legislazione vigente (anche penale), per assicurare divulgazione coordinate delle vulnerabilità;
- Sistema sanzionatorio e di vigilanza

2 Prossimi passaggi

- Art. 3 ddl di delegazione europea (in corso di esame al Senato – A.S. 969)
- Approvazione decreti delegati entro il termine del 17 ottobre 2024