NIS2 e Legge 90/2024 – I parte

AMBITI E NUOVI SOGGETTI - AVV. LAURA GARBATI

Roadmap

- la strategia europea e italiana per la cybersicurezza: una panoramica
  - Obiettivi generali
  - Dove eravamo
- la NIS2: nuovi approcci per nuove sfide
  - I nuovi ambiti di applicazione
  - Pubbliche amministrazioni tra vecchio e nuovo
  - I nuovi soggetti
- Legge 90/2024: per una PA più sicura
  - Gli ambiti di applicazione
  - Le relazioni con la NIS2
  - I nuovi soggetti
- le sfide per la PA
  - Tempi di attuazione
  - Efficienza e resilienza: individuare soggetti competenti, organizzarsi per prevenire

La strategia europea per la cybersicurezza: un ecosistema

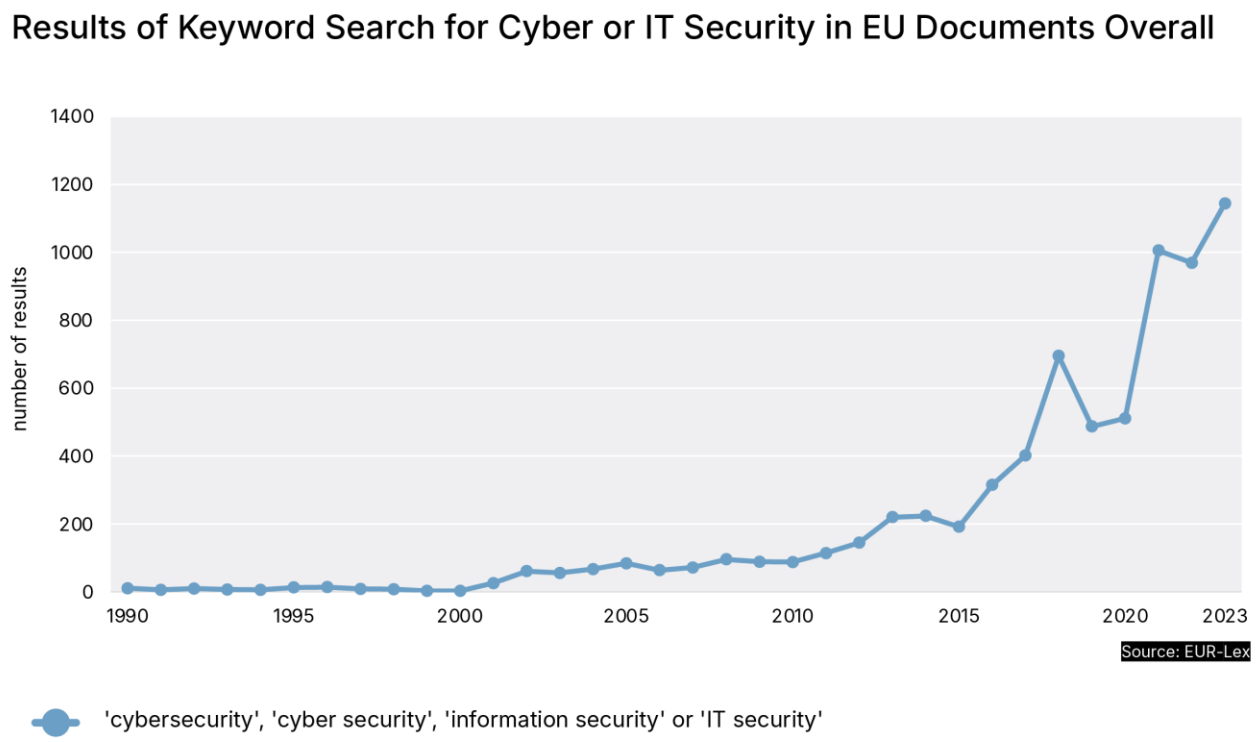
sfruttare e rafforzare tutti i suoi strumenti e risorse per essere tecnologicamente sovrani

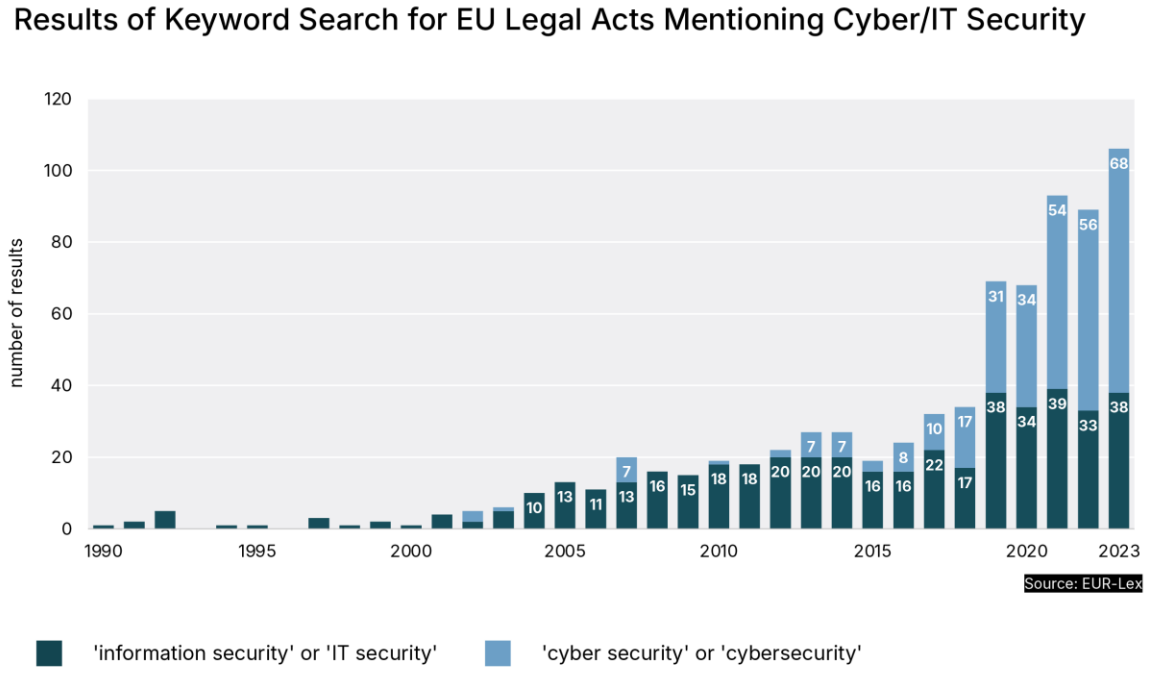
Fondata sulla **resilienza** di tutti i **servizi** e **prodotti** connessi

- prevenzione
- collaborazione
- standardizzazione
- condivisione

The EU needs an agile means for detecting and deflecting increasingly complex and frequent cyberattacks.

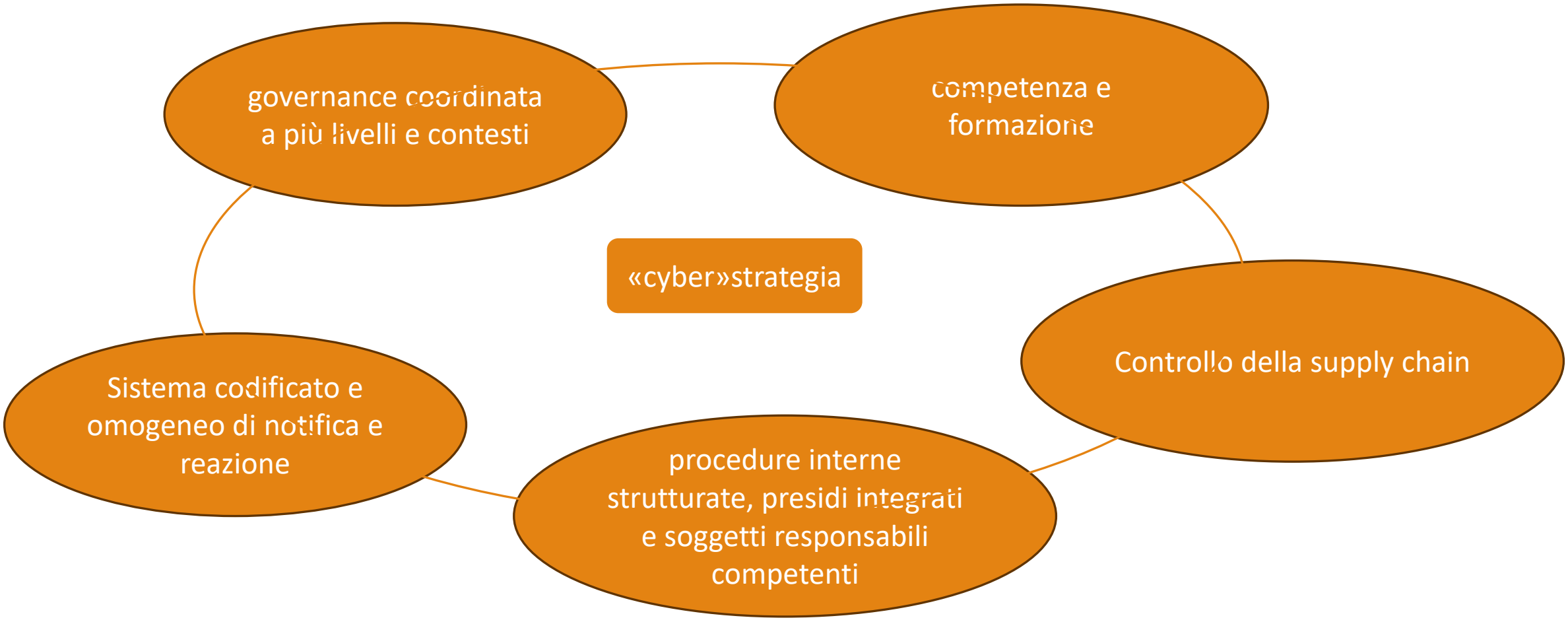
Una esigenza in continuo adeguamento





https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem

L’architettura degli obblighi «comuni»



Gli interlocutori della cybersecurity: l' *European Union Agency for Network and Information Security*

- **Sostegno all'attuazione delle politiche** nel settore della cibersicurezza, anche a supporto degli Stati membri nell'attuazione degli aspetti inerenti specificamente alla cibersicurezza delle politiche dell'Unione e della legislazione in materia di protezione dei dati e di privacy
- **Sviluppo delle capacità in materia di cibersicurezza**, per esempio mediante corsi di formazione, anche in relazione alla risposta agli incidenti e alla supervisione delle misure di regolamentazione riguardanti la cibersicurezza.
- **Compiti connessi al mercato** (normazione, certificazione della cibersicurezza), quali l'analisi delle principali tendenze del mercato della cibersicurezza per migliorare l'incontro di domanda e offerta e sostenere l'elaborazione delle politiche dell'UE nei settori della normazione TIC e della certificazione della cibersicurezza delle TIC.
- **Cooperazione operativa e gestione delle crisi -** rafforzare le capacità operative di prevenzione e sostenere la cooperazione operativa fungendo da segretariato della rete degli CSIRT - assistenza agli Stati membri che la richiederanno per gestire gli incidenti e ruolo nella risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza a livello transfrontaliero
- **Divulgazione coordinata delle vulnerabilità**: l'Agenzia dell'UE per la cibersicurezza assisterà gli Stati membri e le istituzioni, le agenzie e gli organismi dell'Unione nella definizione e nell'attuazione di politiche di divulgazione delle vulnerabilità su base volontaria; contribuirà inoltre a migliorare la cooperazione tra le organizzazioni, i fabbricanti o i fornitori di prodotti e servizi vulnerabili e i membri della comunità di ricerca sulla cibersicurezza che individuano tali vulnerabilità.

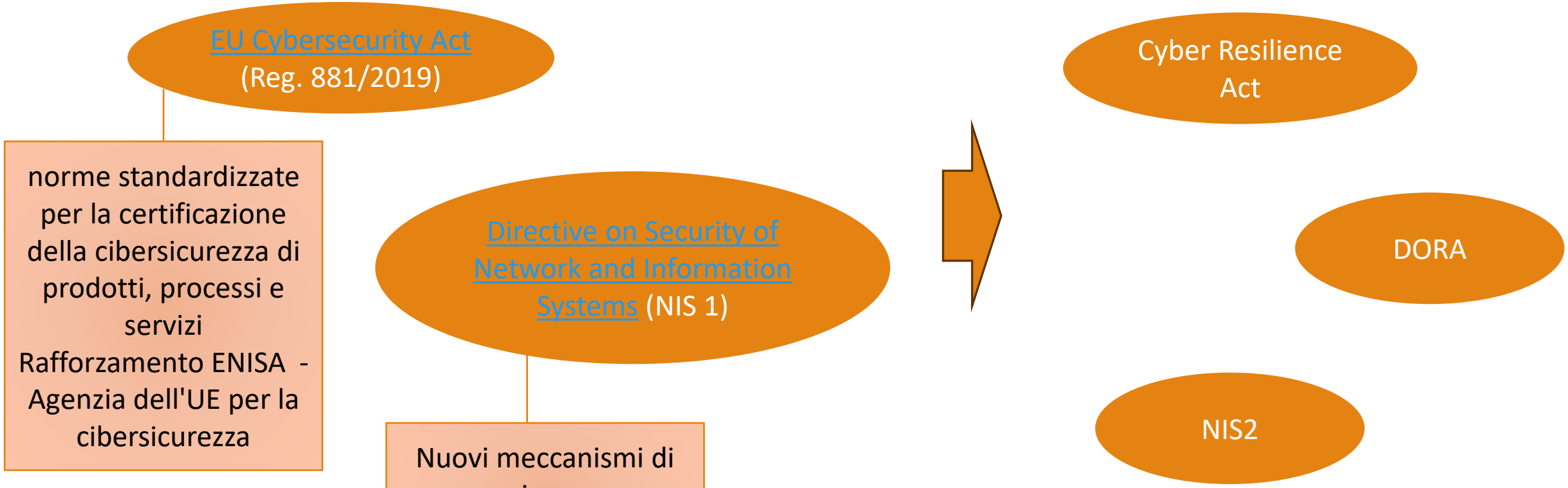
Gli interlocutori «italiani» della cybersecurity (alcuni)

Agenzia	Competenze	Legge di costituzione
Agenzia per la Cybersicurezza Nazionale (ACN)	Protezione degli asset strategici nazionali, gestione e mitigazione del rischio, coordinamento delle attività di prevenzione, monitoraggio e risposta agli incidenti di sicurezza informatica	Decreto Legge n. 82 del 14 giugno 2021
Computer Security Incident Response Team (CSIRT)	Gestione e risposta agli incidenti di sicurezza informatica a livello nazionale, supporto tecnico e operativo per la gestione degli incidenti e la mitigazione delle minacce	Parte della strategia nazionale di cybersicurezza delineata dall'ACN – già nella NIS1 – ripresa dalla NIS2
Centro di Valutazione e Certificazione Nazionale (CVCN)	compito di valutare la sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del Perimetro e che rientrano nelle categorie previste dal DPCM 15 giugno 2021	Previsto dall'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105

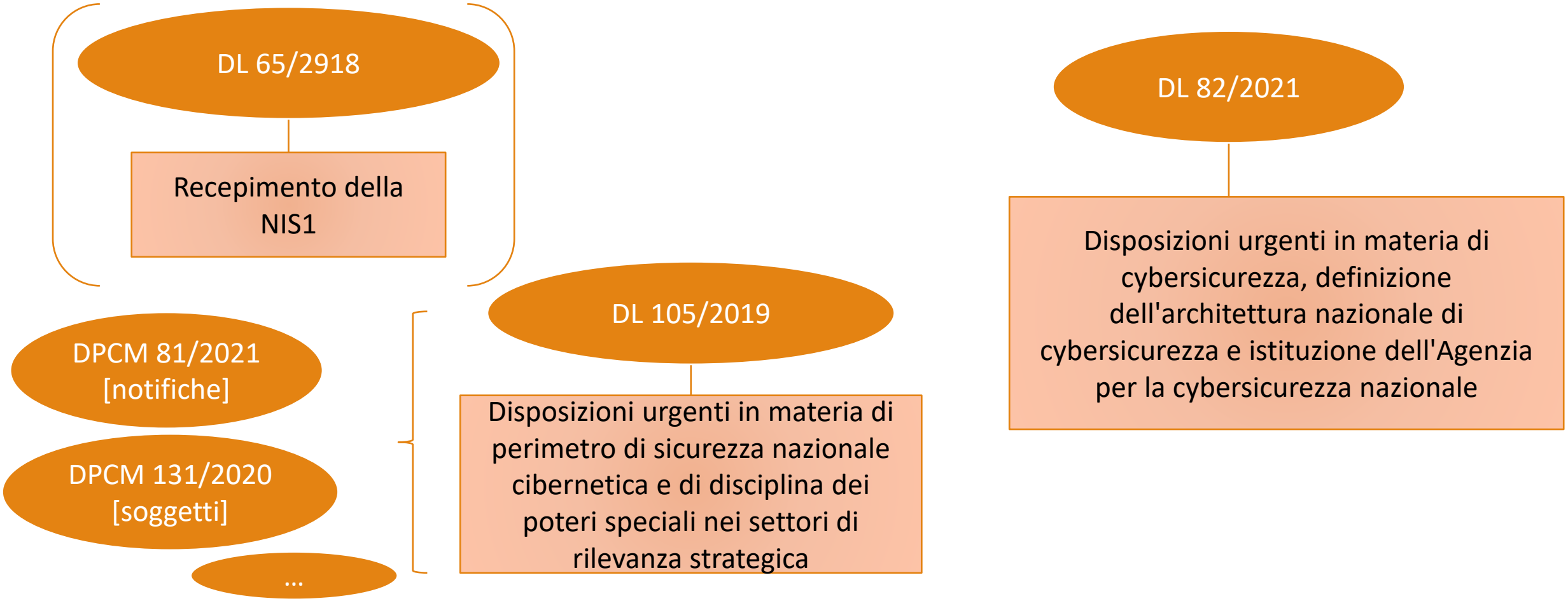
Gli interlocutori «italiani» della cybersecurity (alcuni)/1

Agenzia	Competenze	Legge di costituzione
Gruppi di coordinamento	Facilitano la cooperazione tra diverse entità nazionali e internazionali per la gestione delle crisi informatiche Coordinamento delle risposte agli incidenti, condivisione delle informazioni e delle migliori pratiche.	Già previsto dalla NIS1 - compiti ampliati dalla NIS2
EU-Cyclone	Comprende rappresentanti delle autorità nazionali di gestione delle crisi informatiche degli Stati membri, nonché la Commissione Europea in caso di incidenti di grande portata1.	Il network è stato formalizzato con l'entrata in vigore della NIS21

L’ecosistema normativo sulla cybersicurezza



La strategia italiana sulla cybersicurezza dove (già) eravamo



La strategia nazionale

[Strategia nazionale di cybersicurezza 2022 - 2026]

Il perimetro di sicurezza cibernetico (DL 105/2018) – i soggetti

esercita una **funzione essenziale** dello Stato,

se l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuita' dell'azione di Governo e degli Organi costituzionali, …;

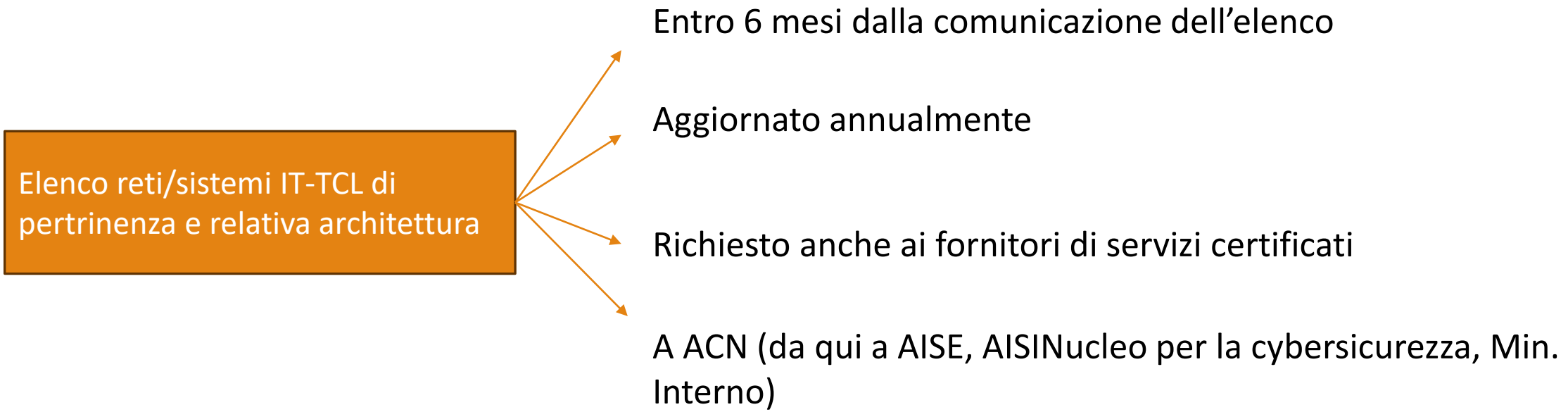
assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici (art. 1 c. 2)

attivita' strumentali all'esercizio di funzioni essenziali dello Stato; per l'esercizio e il godimento dei diritti fondamentali; per la continuita' degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attivita' di ricerca e attivita' relative alle realta' produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, --- [DPCM 131/2020]

Elenco con atto Presidente Consiglio (entro 30 gg)

No diritto accesso

Il perimetro di sicurezza cibernetico (DL 105/2018) – gli obblighi



Il perimetro di sicurezza cibernetico (DL 105/2018) – gli obblighi

Notifica incidenti aventi impatto sulle strutture individuate in elenco

- Estrema tempestività (da 1 a 6 ore: v. art. 3 DPCM 81/2021)
- Al CSIRT (da qui Nucleo per la cybersicurezza cibermetica, etc.)
- Sanzioni amministrative fino a 1.500.000 €
- Assolve nel caso anche obbligo notifica NIS1

Quali incidenti?

Tassonomia allegato A DPCM 81/2021

ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici («impatto sul bene ICT: limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali)

NB - Notifica incidente con impatto su elementi non elencati (art. 1 c. 3-bis): 24 + 72 ore [introdotto da L. 90/2024]

Il perimetro di sicurezza cibernetico (DL 105/2018) – gli obblighi

Adozione specifiche misure di sicurezza

individuazione

Allegato B DPCM 81/2021

Categoria A

6 mesi

Categoria B

30 mesi

- struttura organizzativa preposta alla gestione della sicurezza;
- politiche di sicurezza e alla gestione del rischio;
- mitigazione e gestione degli incidenti e alla loro prevenzione (anche interventi su apparati/prodotti inadeguati)
- protezione fisica e logica e dei dati;
- integrità delle reti e dei sistemi informativi;
- gestione operativa, ivi compresa la continuità del servizio, monitoraggio, test e controllo;
  formazione e consapevolezza;
- affidamento di forniture di beni, sistemi e servizi IT/ITC

xxx

NB soggetti già in NIS1 – osservano le misure ivi previste se *livello equivalente* – ACN valuta misure aggiuntive

Il perimetro di sicurezza cibernetico (DL 105/2018) – gli obblighi

Comunicazione acquisti ICT impattanti su reti e servizi in elenco

Al Centro di Valutazione e Certificazione Nazionale (CVCN)

Categorie e modalità DPCM15.6.21

Entro 45 g (+15)

NB silenzio assenso

Comprensiva della valutazione del rischioi

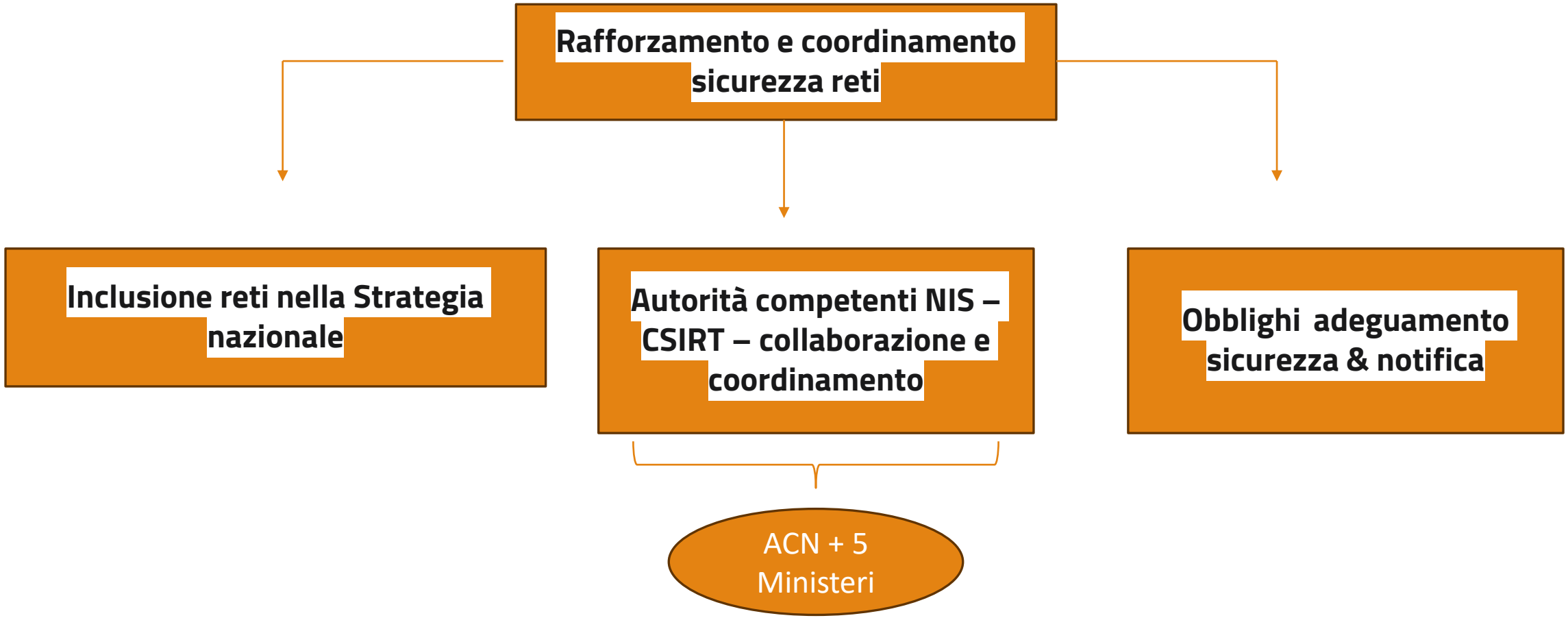
Imporre verifiche preliminari / condizioni e test hw e sw

Fornitori tenuti a collaborare

Gare e contratti devono essere integrati con clausole sospesive/risolutive (test entro 60 gg)

NB sanzioni da 300.000 a 1.800.000 €

Dove (eravamo) siamo: il DL 65/2018 (NIS1) – gli obiettivi



Dove (eravamo) siamo: il DL 65/2018 (NIS1) – i soggetti

Operatori di servizi essenziali

Energia
Trasporti
Banche
Infrastrutture del mercato finanziario
Sanità
Fornitura e distribuzione di acqua potabile
Infrastrutture digitali

Fornitori di servizi digitali

Motori di ricerca
Mercati online
Cloud computing

- essenziale per il mantenimento di attività sociali e/o economiche fondamentali
- dipende dalla rete e dai sistemi informativi
- per cui un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio

NB 500 ca enti (NO PA)

Dove (eravamo) siamo: il DL 65/2018 (NIS1) – gli obblighi

Adozione di misure tecniche e organizzative

Adeguate e proporzionate alla gestione dei rischi - per prevenire e minimizzare indicenti a carico della rete

assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente

Linee Guida Gruppo di cooperazione – Linee guida ACN

Notifica incidenti

Al CSIRT - **Senza ingiustificato ritardo**

xxx

Dove (quasi) siamo: la NIS2

Direttiva 2022/2555

Efficace dal 16.1.23 - Recepimento entro 18.10.2024
abroga NIS1

- Eccesiva frammentazione: incertezza e lentezza
- Ambiti diventati insufficienti
- Eccessiva discrezionalità requisiti sicurezza e notifica incidenti
- Mancata condivisione sistematica delle informazioni

Legge Delega 15 del 21 febbraio 2024

Decreto di attuazione Consiglio dei Ministri 7 agosto 2024
(insieme a DIR CER – in gazzetta 23.9.24)

In attesa pubblicazione

omogeneità e rapidità di informazione per maggiore resilienza

categorie

Ampliamento ambito soggettivo

sottocategorie

Tempistiche di notifica stringenti e standard

Compiti di vigilanza

Dove (quasi) siamo: la NIS2- i soggetti

Soggetti pubblici o privati

Rientrano nelle tipologie degli all. I e II

superano la soglia della media impresa

Meno 50 persone / fatturato anuo < 50ml – bilancio > 43 ml

ANCHE

- Sanità
- Gestione delle acque
- Gestione dei rifiuti
- Trasporti
- Settore alimentare e delle bevande
- Spazio
- **Pubblica Amministrazione**

- + sottocategorie infrastrutture digitali (es. social media, gestori data center)

Ma non solo!

Dove (quasi) siamo: la NIS2- i soggetti

Indipendentemente dalla dimensioni se

Rientrano nelle tipologie degli all. I e II

- **Servizi di: fornitori di reti di comunicazione elettroniche pubbliche** o di servizi di comunicazione elettronica accessibili al pubblico; prestatore di servizi di fiducia; registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio
- Il soggetto sia **unico fornitore di un servizio essenziale** per attività sociali o economiche fondamentali / una sua perturbazione potrebbe avere un impatto significativo su sicurezza e incolumità pubbliche e/o un rischio sistemico
- **Soggetto critico** in ragione sua particolare importanza
- **Ente della Pubblica Amministrazione** (v. *infra)*

Registrazione tramite piattaforma ACN dal 1 gennaio 2025 → Elenco entro il 17 aprile 2025

Dove (quasi) siamo: la NIS2- la Pubblica amministrazione

Pubblica Amministrazione «coinvolta»

Amministrazione **centrale**

Ente a livello regionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche

NB - Gli Stati membri **possono prevedere** che la presente direttiva si applichi a:
a) enti della pubblica amministrazione a livello locale;
b) istituti di istruzione, in particolare ove svolgano attività di ricerca critiche

NB2 - **Possono esentare** soggetti specifici che operano per la sicurezza nazionale

NON

enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini l'accertamento e il perseguimento dei reati

Dove (quasi) siamo: la NIS2- soggetti «essenziali» e «importanti»

La nuova Direttiva distingue tra

- Soggetti «**essenziali**» → Anche vigilanza *ex ante*
- Soggetti **«importanti»** → «solo» controllo *ex post*

Dove (quasi) siamo: la NIS2- soggetti «essenziali» e «importanti»/1

- **fornitori di reti pubbliche di comunicazione elettronica** o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese
- Prestatori di servizi fiduciari e registri DNS
- **qualsiasi altro soggetto** di cui all'allegato I o II **che uno Stato membro identifica** come soggetti essenziali;
- soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557 (soggetti critici);
- se lo Stato membro lo prevede, i soggetti che tale Stato membro ha **identificato prima del 16 gennaio 2023** come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale
- **PA centrali**

Soggetti essenziali

Sono considerati **soggetti importanti** i soggetti di una tipologia elencata negli allegati I o II non essenziali.
NB definizione da parte di ciascun Stato Membro di un elenco dei soggetti essenziali e importanti e comunicazione alla Commissione

Dove (quasi) siamo: la NIS2- vigilanza ed esecuzione – soggetti essenziali

Necessario prevedere efficace monitoraggio e adozione misure necessarie a garantire il rispetto della presente direttiva (art. 31)

Misure di vigilanza e di esecuzione - [«effettive, proporzionate e dissuasive»]

- **ispezioni in loco e vigilanza a distanza**, compresi controlli casuali, effettuati da professionisti formati;
- **audit sulla sicurezza** periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
- **audit ad hoc**, (anche per incidente significativo o rilevata violazione)
- **scansioni di sicurezza** basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;
- **richieste di informazioni** necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato;
- **richieste di accesso a dati**, documenti e altre informazioni (se necessari);
- **richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza**

Dove (quasi) siamo: la NIS2- vigilanza ed esecuzione – soggetti essenziali/1

Necessario prevedere *quantomeno* che nell'esercizio dei **poteri di esecuzione** le autorità competenti abbiano il potere di

- emanare **avvertimenti** relativi a violazioni;
- adottare **istruzioni vincolanti**, ivi inclusi misure richieste e i termini per l'attuazione o un'ingiunzione che venga posto rimedio alle carenze individuate o alle violazioni;
- imporre di porre **termine ad un comportamento o astenersi dalla ripetizione**;
- **imporre di provvedere** affinché le loro **misure** di gestione del rischio di cibersicurezza (art. 21) o di adempiere gli **obblighi di segnalazione** (art. 23) in una maniera ed entro un termine specificati;
- **imporre di informare le persone fisiche o giuridiche** cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia, nonché in merito alle eventuali misure protettive o correttive che possano essere adottate;
- imporre ai soggetti interessati di **attuare le raccomandazioni** fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

Dove (quasi) siamo: la NIS2- vigilanza ed esecuzione – soggetti essenziali/2

Se le misure non sono efficaci → Ulteriore imposizione termini → Se disatteso

- sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale;
- chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto.

NB solo finché il soggetto interessato non adotta le misure necessarie

NB2 PA escluse

Dove (quasi) siamo: la NIS2- vigilanza ed esecuzione – soggetti importanti

Se elementi di prova, indicazioni o informazioni secondo cui un soggetto **importante** non rispetta presumibilmente la presente direttiva(art. 31)

Misure di vigilanza e di esecuzione **ex post-** [sempre «efficaci, proporzionate e dissuasive»]

Azioni di vigilanza

Azioni di Esecuaione

Analoghe azioni successive

Dove (quasi) siamo: la NIS2- gli obblighi

GOVERNANCE
(art. 20)

gli organi di gestione dei soggetti essenziali e importanti e.

approvare le misure di gestione dei rischi di cibersicurezza adottate (rif. art. 21),

sovraintendano alla sua attuazione

possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo

tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti

NB «.. *qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale*» deve avere «*il potere di garantirne il rispetto della presente direttiva*» e devono «*essere ritenute responsabili dell'inadempimento dei loro doveri*» (art. 32, c.6)

Dove (quasi) siamo: la NIS2- gli obblighi/1

Adozione misure tecniche, operative e organizzative *adeguate* e *proporzionate*

Assicurare un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti

Approccio multirischio

a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi ICT;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

NB entro 17.10.24 atti esecuzione

NB possibile imporre prodotti TIC certificati ex 2019/881

Dove (quasi) siamo: la NIS2- gli obblighi/2

Obblighi di segnalazione (art. 23)

Al CSIRT

Se opportuno anche ai destinatari

Tempistiche rigorose

Incidenti con **impatti significativi** sui propri servizi

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

- Prima notifica entro 24 ore
- integrazione entro 72 ore

- Possibile richiesta relazione intermedia
- Relazione finale entro 1 mese

Dove (quasi) siamo: la NIS2- le sanzioni

Per i soggetti essenziali le sanzioni pecuniarie amministrative sono pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

Per i soggetti importanti le sanzioni pecuniarie amministrative sono pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

NIS2 e legge 90/2024: parenti?

La legge 90/2024 non è la legge di recepimento della NIS2

Si interseca già ora con il DL 150/2019 e il D.Lgs. 65/2018

Riguarda *esptressamente* le PA (più della NIS2)

Costituisce tuttavia probabilmetne anche un «viatico» per la'geduamento alla NIS2

La Legge 90/2024 : per una PA (cyber)sicura - i soggetti

- **PA centrali** come individuate da elenco ISTAT
- le **regioni** e le province autonome di Trento e di Bolzano,
- le **città metropolitane**,
- i **comuni** con popolazione superiore a 100.000 abitanti
- comunque, i **comuni capoluoghi di regione**,
- le **società di trasporto pubblico** urbano con bacino di utenza non inferiore a 100.000 abitanti /extraurbano operanti nell'ambito delle città metropolitane
- le **aziende sanitarie locali**
- **relative società in house** che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali

La Legge 90/2024 : per una PA (cyber)sicura – gli obblighi

Obblighi di notifica di incidenti (art. 1)

Qualsiasi indicente rientrante nella tassonomia

Tempistiche rigorose

Tassonomia incidenti > rimando a DL 105

Determina ACN 3 gennaio 2023

NB per comuni, società di trasporto, asl e in house

- Prima notifica entro 24 ore
- integrazione entro 72 ore

- Apposite procedure su sito ACN [NB Guida ACN alla notifica degli incidenti – 26 luglio 2024]

Da 180 giorni entrata in vigore

La Legge 90/2024 : per una PA (cyber)sicura – gli obblighi/1

Adozione interventi segnalati nel caso da ACN

Al CSIRT

Se opportuno anche ai destinatari

Entro 15 gg

NB tenuti anche

NB sanzioni fino a 125.000 €Prima notifica entro 24 ore

- Soggetti nel perimetro di sicurezza cibernetico
- Soggetti di cui all'art. 3, c. 1, lettere g) e i), D.Lgs. 65/2018
- Art. 40, c.3, Vcod. Comunicaz. elettroniche

La Legge 90/2024 : per una PA (cyber)sicura – gli obblighi – la Governance

Individuazione / costituzione di una **struttura**

- **sviluppo delle politiche e delle procedure** di sicurezza delle informazioni;
- **produzione e all'aggiornamento** di **sistemi di analisi** preventiva di rilevamento e di un piano per la gestione del rischio informatico; di un **documento che definisca i ruoli** e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; di un **piano programmatico per la sicurezza** di dati, sistemi e infrastrutture dell'amministrazione;
- pianificazione e attuazione di **interventi di potenziamento delle capacità per la gestione dei rischi informatici;**
- **adozione delle misure previste dalle linee guida per la cybersicurezza** emanate dall'Agenzia per la cybersicurezza nazionale;
- **monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità** dei sistemi per il loro pronto aggiornamento di sicurezza.

La Legge 90/2024 : per una PA (cyber)sicura – gli obblighi – la Governance/1

Nomina di un **referente per la sicurezza**

individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

Anche **punto di contatto unico ACN**

NB Se non si dispone di una simile figura

- **Delegabile a dipendente altra PA**
- **Esercitabili in forma associata (con relativa struttura)**
- **Individuabile nell'RTD (con relativa struttura)**

Soggetti ex 105 conservano loro assetto

La Legge 90/2024 : per una PA (cyber)sicura – gli obblighi – Governance e Resilienza

Verifica programmi e applicazioni utilizzate

Strutture competenti (anche ex 105 e NIS1)

Anche **punto di contatto unico ACN**

rispettino le LG sulla crittografia e sulla conservazione delle password di ACN e Garante Privacy

NON presentino vulerabilità note «atte a rendere disponibili e intellegibili a terzi i dati cifrati»

NB invarianza economica…

Conclusioni

Un obiettivo, molti interventi a perimetro parzialmente sovrapposto

Impatto significativo sulle PA per duplice intervento 90/2024 e NIS2

Essenziale costituire a stretto giro riferimenti e sistemi comuni, facendo massa critica

La sfida della collaborazione e del digitale è certamente essenziale, importante non perdersi

Certamente non ne possiamo fare a meno,
Certamente ci sarà molto da lavorare!

Grazie dell’attenzione!

Avv. Laura Garbati

Ps nessun avvocato è stato maltrattato per scrivere questa presentazione