QUADRI SINOTTICI

della

CYBERSICUREZZA

1. Le fonti
2. L'assetto istituzionale e l'Agenzia per la cybersicurezza nazionale
3. I soggetti obbligati ai sensi della normativa NIS2, PSNC, DORA
4. Adempimenti, prescrizioni e scadenze: *focus* NIS2
5. Adempimenti negli altri settori cyber
6. Controlli e sanzioni
7. Aggiornamenti a livello europeo: implementazione della normativa e rischi attuali

1. Le fonti

ATTI NORMATIVI

Disciplina sovranazionale

- Regolamento (CE) n. 460/2004 del Parlamento e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)
- Direttiva UE/2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante *Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione* (**Direttiva NIS 1**)
- Direttiva (Ue) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, relativa a *Misure per un livello comune elevato di cibersicurezza nell'Unione*, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (**Direttiva NIS 2**)
- Direttiva (Ue) 2022/2557 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa alla *Resilienza dei soggetti critici* e che abroga la direttiva 2008/114/CE del Consiglio (DIRETTIVA CER - *Critical Entity Resilience*)
- Regolamento (Ue) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla *Resilienza operativa digitale per il settore finanziario* (*Digital Operational Resilience Act*, o "**DORA**")
- Regolamento UE 2023/2841 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

Disciplina nazionale

- Leggi n. 124/2007 e n. 133/2012 di adozione e di riforma del "*Sistema di informazione per la sicurezza della Repubblica e del segreto di Stato*"
- Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 in GU del 13.4.2017 n. 87 – "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*" (Decreto Gentiloni)
- **Decreto Legislativo 18 maggio 2018, n. 65** in GU del 9.6. 2018, n. 132 - "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" (**Recepimento Direttiva NIS1**)
- **Decreto legge 21 settembre 2019, n. 105** - "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*" (**Decreto Perimetro** o **PSNC**)
    - DPCM 30 luglio 2020 n. 131 - Regolamento in materia di perimetro di sicurezza nazionale cibernetica;
    - DPCM 14 aprile 2021, n. 81 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici
- **Decreto legge 14 giugno 2021 n. 82** in GU 14.6.2021 n. 140 - "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 (**Decreto ACN**)
- **Legge 28 giugno 2024, n. 90**, in GU n.153 del 2.7.2024 - "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*"
    - DPCM 30 aprile 2025 recante "*Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale*"
- **Decreto legislativo 4 settembre 2024, n. 138** in GU 1.10.2024 n. 230 - "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*" (**Decreto NIS**)
- **Decreto legislativo 10 marzo 2025, n. 23** in GU dell'11 marzo 2025, n. 58 - "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario*" (**Decreto DORA**)

Principali atti normativi dell'Autorità (ACN)

- ❖ Strategia Nazionale per la cybersicurezza 2022-2026
- ❖ Piano di Implementazione Strategica

- Piano Strategico
- Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala
- Determinazione 26 novembre 2024 n. 38565 (Piattaforma ACN e specifiche su Punto di Contatto)
- Determinazione 14 aprile 2025 n. 164179 (Definizione obblighi di base e tassonomia incidenti)
- Determinazione 30 settembre 2025 n. 333017 (Referente CSIRT interno)

2. L'assetto istituzionale e l'agenzia per la cybersicurezza nazionale

AUTORITA' E FUNZIONI

Network internazionali

- Gruppo di lavoro delle agenzie del G7
- Financial Times Cyber Resilience Summit Europe (Londra, novembre 2024)

Organismi unionali

- Consiglio dell'Unione europea – Comitato Horizontal Working Party on Cyber Issues (HWPCI): coordina i lavori del Consiglio in merito alle questioni relative alla normativa di cybersicurezza, definisce le priorità e gli obiettivi strategici, facilita lo scambio di informazioni
- Commissione europea – DG CONNECT - Reti di comunicazione, dei contenuti e delle tecnologie: elabora e attua le politiche in ambito digitale, elabora la strategia europea per la cybersicurezza
- Agenzia dell'Unione Europea per la Cybersecurity (ENISA): supporta le Istituzioni dell'Unione e gli Stati membri nell'elaborazione e attuazione delle politiche di cybersicurezza e della normativa in materia, promuove la cooperazione e lo sviluppo delle capacità di resilienza, svolge attività di addestramento
  - ✓ Gruppo di cooperazione NIS tra autorità competenti NIS e Punti di Contatto nazionali (*presso ENISA*)
  - ✓ Rete di CSIRT nazionali
  - ✓ Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe, per la raccolta di informazioni sugli incidenti e sulle crisi cibernetiche su vasta scala)
  - ✓ Cyber Europe (*nota 1*): gruppo che svolge attività di verifica della capacità di reazione a eventi cyber tramite esercitazioni (simulazioni di incidenti informatici su larga scala), destinate sia al settore pubblico che a quello privato negli Stati membri dell'Unione Europea e dell'Associazione Europea di Libero Scambio (EFTA)
- Centro Europeo di Competenza per la Cybersicurezza nell'ambito industriale (ECCC): ha il compito di potenziare l'autonomia strategica dell'Unione in materia di cybersicurezza e accrescere la competitività dell'industria cyber europea

Autorità Nazionali

PRINCIPI

- Il Decreto NIS2 ha definitivamente stabilizzato l'attuale assetto della governance istituzionale delineando un quadro dialogico tra due poli: da un lato, con funzione di direzione strategica, la Presidenza del Consiglio e, dall'altro lato, l'ACN con funzioni di vigilanza, regolazione e attuazione delle politiche di cybersicurezza.
- La competenza di ACN è "generale", nel senso che si estende dai settori critici presi in considerazione dalla disciplina NIS ai settori di interesse nazionale strategico.

ASSETTO ISTITUZIONALE

- **Presidente del Consiglio dei Ministri**: funzioni di alta amministrazione per la direzione e la responsabilità generale delle politiche di cybersicurezza; nomina e revoca del Direttore e Vice-Direttore generale dell'Agenzia per la cybersicurezza; approva la *Strategia nazionale per la cybersicurezza* predisposta dall'ACN sentito il parere del CIC
  - **Comitato Interministeriale per la Cybersicurezza** (CIC – *presso la Presidenza del Consiglio*): alta sorveglianza sull'attuazione della strategia; funzioni consultive nell'ambito della definizione degli indirizzi generali e nel quadro delle politiche di cybersicurezza; organo di riferimento rispetto a eventi di crisi cibernetica sotto il profilo sia dell'intervento sia della pianificazione di misure di prevenzione.
    Il Comitato è presieduto dal Presidente del Consiglio dei ministri, che ne dispone la convocazione, ed è composto da:
    - ✓ Autorità Delegata per la sicurezza della Repubblica (attualmente è il Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri), Ministro degli affari esteri, Ministro dell'interno, Ministro della difesa, Ministro della giustizia, Ministro dell'economia e delle finanze, Ministro delle imprese e del made in Italy, Ministro dell'ambiente e della sicurezza energetica, Ministro delle infrastrutture

e dei trasporti, Ministro dell'università e della ricerca, Ministro delegato per l'innovazione tecnologica. Il Direttore generale di ACN svolge le funzioni di segretario.

- **Agenzia per la cybersicurezza nazionale (ACN)**: autorità nazionale di riferimento per l'attuazione e l'applicazione della disciplina cyber; autorità di vigilanza di settore (vd. sotto):
  - Nucleo per la cybersicurezza (*presso ACN*): organo espressione sia dell'ACN (è presieduto dal suo Direttore Generale) sia dell'esecutivo, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e risoluzione di situazioni di crisi[1]
  - CSIRT Italia (*Computer Security Response Team*) interno all'Agenzia con il compito di analizzare gli eventi rilevanti, anche in collaborazione con altri Stati membri e organi UE, raccogliere ed elaborare le informazioni tramite report settimanali e aggiornamenti periodici di vulnerabilità (nel 2023, ha analizzato n. 1.411 casi e confermato n. 303 incidenti)
  - Tavolo Interministeriale per il Perimetro di sicurezza nazionale cibernetica: punto di raccordo con il CIC e organo che concorre a individuare i singoli soggetti nazionali da includere nel Perimetro
- **Autorità di settore NIS (Ministeri)**: attività di supporto dell'ACN in ambito NIS, tra cui la convalida dell'elenco dei soggetti obbligati e l'eventuale proposta di inserimento di ulteriori soggetti e la partecipazione a tavoli di lavoro di settore; sono le seguenti:
  - Ministero dell'Economia e delle Finanze
  - Ministero delle Imprese e del Made in Italy
  - Ministero dell'Agricoltura, della Sovranità Alimentare e delle Foreste
  - Ministero dell'Ambiente e della Sicurezza Energetica
  - Ministero delle Infrastrutture e dei Trasporti
  - Ministero dell'Università e della Ricerca
  - Ministero della Cultura
  - Ministero della Salute
- **Ministero della Difesa:** insieme ad ACN è Autorità nazionale di gestione delle crisi informatiche ai sensi del Decreto NIS: insieme, individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi e definiscono il *Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala*, aggiornandolo periodicamente e, comunque, ogni tre anni
- **Intelligence**: facendo parte del Nucleo per la Cybersicurezza presso ACN, sono fonte di informazione strategica e portatori del punto di vista della sicurezza nazionale nei tavoli tecnici ACN; rispetto al Governo, sono fonte di flussi informativi di cyber intelligence:
  - ✓ Dipartimento delle informazioni per la sicurezza (DIS)
  - ✓ Agenzia per le informazioni e la sicurezza esterna (AISE)
  - ✓ Agenzia per le informazioni e la sicurezza interna (AISI)

[1] Il Nucleo per la cybersicurezza è presieduto dal Direttore Generale dell'Agenzia o, per sua delega, dal Vice Direttore Generale, ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri (PCM), del Ministero degli esteri e della cooperazione internazionale (MAECI), del Ministero dell'interno, del Ministero della giustizia, del Ministero della difesa, del Ministero dell'economia e delle finanze (MEF), del Ministero delle imprese e del made in Italy (MIMIT), del Ministero dell'ambiente e della sicurezza energetica (MASE), del Ministero dell'università e della ricerca (MUR), del Ministero delle infrastrutture e dei trasporti (MIT) e del Dipartimento della protezione civile della PCM.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE – ACN

Attribuzioni

- Personalità giuridica di diritto pubblico: autorità incardinata presso l'esecutivo sotto la responsabilità politica della Presidenza del Consiglio; con il compito di dare attuazione delle politiche stabilite dall'esecutivo, accentra le competenze e le funzioni in materia di cybersicurezza e dispone di poteri di regolazione (dalla redazione della strategia nazione di cybersicurezza, all'emanazione di atti normativi di dettaglio in punto di misure di sicurezza obbligatorie, presidi di governance aziendali, tassonomia degli incidenti), di supervisione, ispettivi e sanzionatori; pur non potendosi qualificare come autorità indipendente, dispone di un'ampia autonomia organizzativa e attuativa condividendo con le *authorities* non il profilo strutturale ma quello funzionale
- Potestà regolatorie: predisposizione (e attuazione) della *Strategia Nazionale per la cybersicurezza 2022-2026*; aggiornamento costante del quadro regolamentare; elaborazione delle misure di sicurezza a carico dei soggetti obbligati (*baseline* tecniche e linee guida); linee guida per l'identificazione degli incidenti rilevanti
- Promozione di azioni comuni per assicurare la sicurezza e la resilienza cibernetiche e lo sviluppo della digitalizzazione
- Autonomia amministrativa: può stipulare convenzioni per la collaborazione con altri organi dello Stato, amministrazioni ed enti pubblici, Forze armate o di polizia
- Autonomia finanziaria: è esercitata nei limiti delle dotazioni finanziarie previste, le quali constano, per gli anni dal 2025 al 2027, rispettivamente, di 100 mln, 110 mln, 122 mln
- Autonomia organizzativa: è esercitata nei limiti della disciplina stabilita con DPCM → Nel 2024, si è dotata di una nuova struttura organizzativa, che prevede otto articolazioni tutte a riporto del Vice Direttore Generale: Gabinetto, Regolazione, Certificazione e vigilanza, Operazioni e gestione delle crisi, Programmi industriali, tecnologici e di ricerca, Strategie e cooperazione, Risorse umane, Amministrazione e bilancio, alle quali sono affidati tre o quattro uffici ciascuna → L'autonomia organizzativa incontra un limite nella previsione ex lege di due organi necessari: il Direttore Generale e il Collegio dei revisori dei conti, le cui funzioni e attribuzioni sono stabilite con DPCM
- Poteri ispettivi e sanzionatori
- Attività di coordinamento con le autorità competenti DORA tramite la stipulazione di protocolli di intesa
- Relazione annuale al Parlamento

Ruoli

- ✓ Autorità nazionale competente ai fini NIS
- ✓ Punto di contatto unico NIS a livello UE (art. 2 co. 1 lett. g), decreto NIS)
- ✓ Autorità nazionale di gestione delle crisi informatiche insieme al Ministero della Difesa: individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi e definiscono il *Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala*, aggiornandolo periodicamente e, comunque, ogni tre anni
- ✓ CSIRT nazionale o CSIRT Italia
- ✓ Autorità nazionale di certificazione della cybersicurezza (CVCN): organismo di valutazione della conformità dei sistemi ed emissione del *certificato di sicurezza cibernetica* (funzione in precedenza affidata al MISE)
- ✓ Centro Nazionale di Coordinamento Italiano (NCC-IT) individuato dal Centro Europeo di Competenza per la Cybersicurezza (ECCC) all'interno della rete dei Centri nazionali di coordinamento (NCC o Cyber Innovation Network) presenti in ciascuno Stato membro (Reg. UE/2021/887) e designato con D.L. n. 82/2021
- ✓ Punto di riferimento per la cooperazione internazionale
- ✓ Soggetto attuatore dei progetti previsti dal PNRR in tema di cyber sicurezza (620 mln da investire in misure di resilienza, certificazione tecnologica, digitalizzazione della PA)

FUNZIONI ACN IN AMBITO NIS e PERIMETRO

(il decreto-legge 82/2021 ha attribuito ad ACN le funzioni in ambito Perimetro in precedenza conferite a organi dell'Esecutivo)

- Allestimento e gestione della piattaforma per la registrazione dei soggetti obbligati e per l'aggiornamento annuale delle informazioni fornite
- Redazione dell'elenco dei soggetti *essenziali* e *importanti* in ambito NIS comunicazione del relativo inserimento ai destinatari (**solo NIS**)
- Ricezione delle notifiche e gestione degli incidenti informatici tramite il CSIRT Italia
- Definizione del dettaglio delle misure di sicurezza e dei presidi che i soggetti obbligati sono tenuti ad attuare, divise in:
  - ✓ obblighi di base → definiti ad aprile 2025
  - ✓ obblighi di lungo termine → da definire per aprile 2026
  - ✓ modello di categorizzazione delle attività e dei servizi
- Svolgimento delle attività di monitoraggio sui soggetti obbligati
- Svolgimento dell'attività ispettiva
- Potere sanzionatorio

FUNZIONI ACN CON SPECIFICO RIGUARDO AL PERIMETRO

- Identificazione e notifica dell'inserimento nel Perimetro ai soggetti che vi rientrano sulla base dei criteri indicati dal Decreto Perimetro e meglio specificati dalle fonti secondarie (DPCM)
- Ricezione delle comunicazioni relative all'"Elenco dei Beni ICT" che i soggetti inclusi nel Perimetro sono tenuti a inviare ad ACN e analisi del rischio effettuata su tali beni
- Definizione della tassonomia degli incidenti (valida anche in ambito NIS[2])
- Ruolo di Centro di valutazione e certificazione nazionale (CVCN), con il compito di valutare e certificare i beni, sistemi e servizi ICT che formano oggetto di fornitura per l'approvvigionamento (soprattutto da parte di soggetti pubblici) di servizi e funzioni essenziali; accreditamento dei Laboratori Accreditati di Prova (LAP) nell'ambito della valutazione della sicurezza di beni, sistemi e servizi ICT destinati a essere impiegati nel contesto del Perimetro
- Definizione della metodologia di analisi del rischio per consentire alle **PA** di svolgere il *self assesment* (analisi di contesto, catalogazione dei servizi digitali).

RAPPORTI ACN e MAGISTRATURA

dovere di collaborazione dell'ACN

- trasmettere alla Procura nazionale antimafia *"i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di cui all'art. 371-bis co. 4-bis cp.p."* e informarla "*senza ritardo*" in presenza di reati *ex* art. 371-bis co. 4-bis c.p.p. commessi a danni di reti e sistemi inclusi nel Perimetro

regole speciali applicabili ai procedimenti penali

- nell'ambito di indagini relative ai delitti *ex* art. 371-bis co. 4 bis c.p.p.: regole procedurali speciali, quali il dovere del pubblico ministero procedente di informare ACN di tutte le notizie riguardanti tali reati; in caso di incidenti *cyber*, di tenere conto delle attività di analisi e delle misure di contenimento eventualmente già intraprese da ACN ed eventualmente differire o sospendere gli accertamenti urgenti; di sottoporre al controllo dell'ACN il conferimento degli incarichi da attribuire per l'espletamento degli accertamenti tecnici irripetibili

[2] Al riguardo, si segnala che, per un verso, il Decreto NIS2 contiene una definizione di cosa si intende per incidenti rilevanti e, per altro verso, il Decreto Perimetro incarica ACN di definire una tassonomia degli incidenti da segnalare. Nondimeno, si ritiene che la tassonomia elaborata da ACN sia valida anche ai fini delle notifiche NIS in quanto contiene indicazioni più specifiche e tecniche rispetto alla definizione contenuta nel Decreto NIS2.

3. I soggetti obbligati ai sensi della normativa NIS2, PSNC, DORA

SOGGETTI OBBLIGATI

A fronte del quadro normativo vigente in materia, si possono individuare le seguenti quattro categorie di soggetti obbligati, le quali sono destinatarie di obblighi che si caratterizzano per un nucleo comune ma anche per elementi specializzanti.

- **Soggetti obbligati NIS** (soggetti *essenziali* e *importanti*)
- **Soggetti che ricadono nel Perimetro** (gestori di infrastrutture critiche per funzioni fondamentali dello Stato)
- **Pubbliche amministrazioni**
- **Soggetti obbligati DORA** (banche, intermediari finanziari inclusi IP e IMEL e loro fornitori di beni e servizi ICT)

SOGGETTI OBBLIGATI NIS

- La disciplina NIS (Direttiva e Decreto di recepimento) introduce **uno statuto europeo della cybersicurezza** e della resilienza di soggetti pubblici e privati rispetto ad attacchi *cyber*, il quale si basa sulla adozione obbligatoria di presidi a tutela delle infrastrutture ICT dei soggetti obbligati, sul presupposto per cui la sicurezza informatica è fondamentale per garantire il funzionamento degli Stati e del mercato UE
- L'ambito di applicazione NIS è quindi molto vasto ed è delimitato secondo un criterio "per settori" (sono contemplati oltre 80 tipologie di soggetti obbligati, raggruppate in 18 settori)
- destinatari della normativa sono i soggetti che rientrano nei settori considerati ai sensi del Decreto NIS; essi sono chiamati a una auto-valutazione in merito alla propria soggezione alla normativa NIS, in esito alla quale si registrano sulla piattaforma appositamente predisposta da ACN (fornendo le informazioni e nei termini di cui *infra*) → entro metà aprile 2025, ACN stilerà un elenco dei soggetti NIS registrati e notificherà ai destinatari la conferma della loro inclusione

Settori NIS (di cui agli allegati alla Direttiva e al Decreto NIS):

- I primi due allegati descrivono tipologie di settori in cui si svolgono attività di interesse pubblico e sono suddivisi in settori:
  - "*altamente critici*" i quali includono energia, trasporti, settore bancario e finanziario, sanità, acque pubbliche, spazio, servizi ICT e infrastrutture digitali
  - "*critici*" i quali includono rifiuti, servizi postali, produzione e distribuzione di sostanze chimiche e di alimenti, fabbricazione, fornitura di servizi digitali, ricerca
- Gli altri due allegati prendono in considerazione le pubbliche amministrazioni e i settori che coinvolgono l'erogazione di servizi di pubblici, quali il trasporto pubblico locale, l'istruzione, le attività di interesse culturale e le società partecipate da soggetti pubblici.

- È prevista un'ulteriore distinzione rilevante ai fini di differenziare: (i) la portata degli obblighi da attuare; (ii) il regime di supervisione di ACN; (iii) il regime sanzionatorio, tra:
  - ***Soggetti essenziali***: le imprese "non piccole" che operano nei settori altamente critici o critici; i fornitori di reti pubbliche di comunicazione elettrica o di servizi di comunicazione elettronica accessibili al pubblico; i prestatori di servizi fiduciari; i gestori di registri di nomi a dominio e relativi fornitori di servizi (e altri)
  - ***Soggetti importanti***: categoria residuale che comprende tutti i soggetti rientranti nei settori NIS (di cui sopra) e che non sono *essenziali*

- Sono altresì soggetti NIS le imprese **associate o collegate** a un soggetto essenziale o importante che: (i) adottano decisioni o esercitano una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale; (ii) detengono o gestiscono sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale; (iii) effettuano operazioni di sicurezza informatica del soggetto importante o essenziale; (iv) forniscono servizi ICT o di sicurezza, anche gestiti, al soggetto importante o essenziale.

SOGGETTI CHE RICADONO NEL PERIMETRO (PSNC) - art.1 DL 105/2019

- Il Perimetro regola la sicurezza delle reti, dei sistemi informativi e dei servizi informatici ("beni ICT") da cui dipende l'esercizio di funzioni e servizi fondamentali dello Stato e il cui malfunzionamento, utilizzo improprio, o interruzione può causare un pregiudizio alla sicurezza nazionale → dunque i **destinatari** della normativa sono tutti quei soggetti, pubblici e privati, che esercitano dette funzioni o servizi
- In fase di prima applicazione, ACN ha stabilito che funzioni e servizi fondamentali si riscontrano nei seguenti settori: governativo; interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche; enti previdenziali/ lavoro
- I singoli Ministeri competenti per settore, coadiuvati dal CIC e dal Tavolo Perimetro, provvedono a individuare gli specifici soggetti (e.g. aziende, enti, pa) da includere nel Perimetro
- L'inclusione è formalizzata con atto del Presidente del Consiglio (non soggetto a pubblicazione) ed è comunicato all'interessato e all'ACN

COORDINAMENTO NIS e PSNC (Art. 33 del D.Lgs. 138/2024)

- La disciplina del Perimetro è antecedente al Decreto NIS e successivamente alla sua adozione è rimasta in vigore in quanto essa ha come obiettivo ultimo la tutela della *sicurezza nazionale* mentre la disciplina NIS regola la sicurezza informatica come strumento di tutela del *mercato UE*
- Nondimeno, le due discipline producono impatti su settori di attività affini e in alcuni casi identici
  - *Caso*: un'azienda con operatività transfrontaliera che produce ed eroga energia elettrica (*i.e.* settore NIS) a soggetti nazionali, tra i quali figura la Camera dei Deputati (i servizi digitali alimentati rientrano nelle infrastrutture incluse nel Perimetro)
- è quindi possibile che un gestore di infrastrutture strategiche rientranti nel Perimetro sia anche operatore "essenziale" o "importante" in ambito NIS: in tal caso, ai sensi dell'art. 33 del Decreto NIS tale soggetto è tenuto all'osservanza ***anche*** delle prescrizioni NIS per ciò che concerne tutti i sistemi (*i.e.* reti, sistemi informativi e servizi informatici) ***diversi*** da quelli inclusi nel Perimetro, ove presenti

SOGGETTI OBBLIGATI DORA e coordinamento NIS

Soggetti obbligati

- "entità finanziarie", nozione ampia nella quale rientrano, essenzialmente, tutti i soggetti sottoposti a vigilanza → secondo i chiarimenti forniti da Banca d'Italia: banche, imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di crowdfunding
- *e anche* i loro fornitori di servizi informatici (sinora esclusi dalla supervisione delle autorità di settore)

Coordinamento con disciplina NIS

I settori bancario e finanziario sono inclusi nell'Allegato I alla Direttiva NIS, quindi le "entità finanziarie" oggetto della regolamentazione DORA rientrano astrattamente tra i soggetti obbligati NIS

Nondimeno, il Regolamento DORA è espressamente definito *lex specialis* rispetto alla maggior parte delle previsioni della Direttiva NIS → ai soggetti DORA riconducibili a medie o grandi imprese si applicano **soltanto le disposizioni del decreto NIS relative all'obbligo di registrazione sulla piattaforma ACN** (*infra*)

PUBBLICHE AMMINISTRAZIONI

Le pubbliche amministrazioni sono prese in considerazione sia ai sensi degli Allegati III e IV del Decreto NIS 2, sia ai sensi della **Legge n. 90/2024**, ove sono previste diverse regole costitutive di uno statuto speciale di cyber sicurezza per le pubbliche amministrazioni (*cfr infra* - sezione Adempimenti e prescrizioni Pubbliche Amministrazioni)

Nozione di PA considerata dalla L. 90/2024

- pubbliche amministrazioni centrali ed enti locali; società di trasporto pubblico urbano ed extraurbano nell'ambito delle città metropolitane; aziende sanitarie locali
- loro società in house se forniscono servizi informatici o gestiscono i medesimi servizi pubblici locali

4. Adempimenti, prescrizioni e scadenze: *focus* NIS2

ADEMPIMENTI E PRESCRIZIONI IN AMBITO NIS2

La **responsabilità** per l'adempimento degli obblighi NIS è posta in capo agli **organi di vertice** (*Art. 23, comma 1: "Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti: [...] c) sono **responsabili** delle **violazioni** di cui al presente decreto"*) → di regola, Consiglio di amministrazione e amministratori delegati.

Prescrizioni

1. **Auto-identificazione dei soggetti obbligati e comunicazione ad ACN**
   - autovalutazione in ordine alla propria soggezione alla normativa e conseguente registrazione sulla piattaforma predisposta da ACN, a seguito della quale l'Autorità notifica un provvedimento individuale di conferma ed eventualmente comunica la natura degli interventi da realizzare
     → **completata** tra il 1° gennaio 2025 e il 28 febbraio 2025
     → in occasione della registrazione designare e comunicare ad ACN il Punto di Contatto e il Referente CSIRT (*cfr infra*)
   - **tra il 1° maggio e il 30 giugno di ogni anno:** predisposizione e comunicazione all'Autorità di un elenco dettagliato delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro individuazione e distinzione in base al livello di rischio e aggiornamento annuale → Entro novanta giorni dalla comunicazione tramite la piattaforma, ACN fornisce riscontro circa la conformità di quanto comunicato o richiede integrazioni (in mancanza, la conformità può presumersi soddisfatta)
     → **entro aprile 2026** ACN adotterà un **"**modello di caratterizzazione delle attività" per orientare i soggetti obbligati nell'identificare e distinguere i diversi livelli di esposizione al rischio dei propri sistemi informativi e di rete.

2. **Prescrizioni e presidi sicurezza**
   - obblighi a carico di organi di amministrazione e direttivi (comunque investiti della responsabilità generale sul rispetto delle prescrizioni previste dal Decreto NIS) *cfr art. 23*
     - ✓ approvare policy di implementazione delle misure di gestione dei rischi (*infra* - punto seguente); sovrintendere all'attuazione delle misure di sicurezza; formalizzare procedure di informazione periodica (e tempestiva per ciò che concerne gli incidenti e le relative notifiche); seguire percorsi di formazione in materia di sicurezza informatica e promuovere un'adeguata offerta formativa nei confronti dei propri dipendenti
   - misure di gestione dei rischi per i sistemi informativi e di rete (*cfr art. 24*): complesso di presidi tecnici, organizzativi e operativi da definire in base al grado di rischio inerente dei propri reti e sistemi, attuando le **misure minime** (c.d. *baseline* o "obblighi di base"):
     → definite con Delibera ACN del 14 aprile 2025 n. 164179/2025 *cfr infra*
     → dovranno essere implementate **entro ottobre 2026**
   - definizione e attuazione del processo di notifica degli incidenti rilevanti **entro gennaio 2026**
   - obbligo di imporre ai propri fornitori le condizioni contrattuali indicate dal Decreto e dall'ACN per garantire la qualità e la sicurezza dei beni e servizi oggetto di fornitura

3. **Incidenti rilevanti**: attacchi suscettibili di produrre un pregiudizio rilevante sulle reti, sui sistemi informativi e sulla continuità dei servizi essenziali" e "violazioni di dati" (tassonomia ACN Delibera n. 164179/2025 cfr *infra*)
   A partire da gennaio 2026, in caso di incidente, inoltrare al CSIRT:
   - una prima notifica di carattere generale (pre-notifica): *senza ingiustificato ritardo, e comunque* entro 24 ore dal momento in cui si ha contezza dell'incidente indicando se, allo stato degli atti, l'incidente è frutto di attività illecita e se può avere un impatto transfrontaliero

→ senza ingiustificato ritardo e, ove possibile, entro 24 ore dal ricevimento della pre-notifica, il CSIRT fornisce un riscontro

   - una successiva segnalazione più dettagliata: *senza ingiustificato ritardo, e comunque* entro 72 ore che rechi una valutazione dell'incidente sotto i profili di gravità e impatto
   - un report finale: entro un mese dall'ultima notifica, in cui si riporti l'analisi dell'incidente, la causa, le misure di mitigazione adottate

SCADENZE E ADEMPIMENTI NIS2 IN ITALIA
LA TIME LINE AGGIORNATA

Obiettivi raggiunti [3]

FASE 1

Recepimento direttiva NIS 2 e Prima Fase Attuativa (metà ottobre 2024 – metà aprile 2025)

- ✓ *16 ottobre 2024*: entrata in vigore Decreto NIS 2 (D.Lgs. 138/2024)
- ✓ *febbraio 2025*: censimento e registrazione dei soggetti NIS sulla Piattaforma ACN
  - resta aperta una finestra di registrazione tra il 1° maggio e il 30 giugno di ogni anno
  - i soggetti già registrati dovranno comunicare il soggetto che hanno designato come Referente CSIRT **entro il 31 dicembre 2025** (procedura *ad hoc* operativa dal 20 novembre al 31 dicembre 2025)
- ✓ *marzo 2025*: ACN ha adottato un elenco completo dei soggetti NIS e ha provveduto alle notifiche individuali
- ✓ *aprile 2025*: con Determinazione n. 164179 del 14 aprile 2025, ACN ha adottato gli "obblighi di base" (o "misure di sicurezza di base" o *baseline measures*) e ha definito la tassonomia degli "incidenti significativi di base" che sono oggetto dell'obbligo di notifica
- ✓ *maggio 2025*: i soggetti confermati hanno registrato sulla Piattaforma il dettagli dei propri servizi e attività
  - l'aggiornamento dei dati deve essere rinnovato ogni anno tra il 15 aprile e il 31 maggio

Obiettivi da raggiungere

FASE 2

Seconda Fase Attuativa (metà aprile 2025 – metà aprile 2026)

Soggetti obbligati:

- ✓ *entro il 31 dicembre 2025*: **nomina del Referente CSIRT** interno e comunicazione ad ACN tramite Piattaforma
- ✓ *da gennaio 2026*: diventa efficace **l'obbligo di notifica** degli incidenti
- ✓ *entro settembre 2026*: completa **implementazione delle misure di sicurezza di base**

ACN

- ✓ *entro aprile 2026*: ACN adotterà:
  - gli obblighi a lungo termine (o *advanced obligations*) che i soggetti NIS dovranno implementare a partire da aprile 2026
  - il modello di categorizzazione delle attività e dei servizi

FASE 3

Terza Fase Attuativa (da metà aprile 2026)

- ✓ Categorizzazione delle attività e dei servizi
- ✓ Implementazione degli obblighi a lungo termine

Focus Determinazione ACN 164179/2025

La definizione degli incidenti rilevanti

- accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale
- perdita di riservatezza e/o di integrità, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale
- violazione dei livelli di servizio attesi

[3] Salvo nuovi adempimenti evidenziati in rosso

Focus Determinazione ACN 164179/2025

Alcuni tra i principali obblighi di base o Misure di sicurezza di base

Sono suddivisi nelle seguenti sei categorie, con qualche distinzione a seconda che i destinatari siano soggetti "essenziali" o "importanti"

- ***Governo***: Ruoli, responsabilità e correlati poteri in materia di cybersecurity sono stabiliti e comunicati, con un elenco aggiornato del personale coinvolto; è adottata una valutazione del rischio; sono adottate policy per la gestione del rischio di cybersecurity, in una serie di ambiti aziendali predefiniti (n. 16, tra cui il piano di gestione e di ripristino incidenti)
- ***Identificazione***: Gestione degli asset: sono tenuti inventari aggiornati di hardware e software, dei flussi di dati di rete interni ed esterni, dei servizi erogati dai fornitori e le relative vulnerabilità sono identificate, confermate e registrate
- ***Protezione***: Gestione delle identità, autenticazione e controllo degli accessi (alcuni con protezione fisica): sono verificate periodicamente le utenze e le relative autorizzazioni; il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity (formazione dedicata al personale con ruoli specializzati)
- ***Rilevamento***: Monitoraggio continuo: per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi, sono monitorati gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti
- ***Risposta***: Gestione degli incidenti: deve essere sempre aggiornato e documentato un piano - approvato dagli organi di amministrazione e direttivi - per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia
- ***Ripristino***: Esecuzione del piano di ripristino dagli incidenti: le misure seguono il piano programmato, sono documentate e comunicate agli stakeholder interni ed esterni interessati.

Focus Determinazione ACN 333017/2025 (30 settembre 2025)

LA "NUOVA" FIGURA DEL REFERENTE CSIRT INTERNO
Rapporti e suddivisione di ruoli rispetto al Punto di Contatto

- Con Determinazione n. 38565/2024, ACN aveva precisato il ruolo del **Punto di Contatto** interno, già previsto dal Decreto NIS come unico referente aziendale per i rapporti con ACN
- La Determinazione n. 333017/2025 ha aggiornato il quadro della *governance* aziendale affiancando al PoC la figura del **Referente CSIRT interno** il cui ruolo è di interfacciarsi con l'organo tecnico di ACN, ossia il CSIRT Italia

Il Referente CSIRT interno (*custode della resilienza digitale*)

- Figura individuale o collegiale, dotata di elevate e specifiche competenze tecniche (e.g. *incident response, digital forensics, threat intelligence* e gestione SOC)
- È esternalizzabile a fornitori esterni o Managed Security Service Provider (MSSP)
- Designato dal Punto di Contatto e da questo registrato sulla Piattaforma ACN insieme a un sostituto
  - è prevista una procedura *ad hoc* operativa dal 20 novembre al 31 dicembre 2025

Ruolo preventivo

- ✓ compito di valutare il rischio inerente (*vulnerability assessment*), di effettuare il monitoraggio costante, identificare le vulnerabilità e comunicarle al Punto di Contatto
- ✓ conoscenza approfondita dell'infrastruttura di rete e dei sistemi aziendali, ai quali deve avere accesso anche se è esternalizzato

Rapporti con CSIRT Italia - Ruolo tecnico operativo in caso di incidente

- ✓ interlocutore unico di CSIRT Italia: effettua le segnalazioni (24/72 ore) e riceve istruzioni operative
- ✓ incident response: gestione gli incidenti e degli adempimenti conseguenti (report post-incidente, entro 30 giorni); può agire direttamente e/o coordinare *team* tecnici interni

Rapporti con gli Organi direttivi e con i sistemi aziendali

- ✓ in caso di incidente: interlocutore operativo organi direttivi: garantisce la comunicazione immediata al CdA e al Punto di Contatto, secondo le procedure di notifica definite da ACN

- ✓ verifica e adempimenti di sicurezza: controlla che le misure di sicurezza deliberate dal CdA e pianificate dal CISO siano effettivamente implementate e funzionanti; collabora con audit interni e revisori
- ✓ flussi informativi: fornisce al CdA informazioni strutturate su incidenti, vulnerabilità rilevanti e stato delle contromisure e supporta la Direzione nella valutazione del rischio cibernetico e nella definizione delle priorità di *remediation*
- ✓ gestione delle vulnerabilità: applicazione delle patch, validazione dei piani di aggiornamento, segnalazione vulnerabilità critiche e supporto alle esercitazioni interne di sicurezza e alla formazione del personale tecnico
  - ✓ responsabilità: anche se è esternalizzato riporta al CISO (*Chief Information Security Officer*, funzione aziendale responsabile della sicurezza informatica)

Il Punto di Contatto (dopo l'istituzione del referente CSIRT)

- ❖ è designato dal componente del CdA responsabile della compliance che può investire della funzione il rappresentante legale, un procuratore generale o un dipendente
- ❖ a sua volta designa il Referente CSIRT e lo registra sulla Piattaforma ACN
- ❖ svolge un ruolo manageriale e amministrativo, incentrato sulla conformità e sulla comunicazione istituzionale con ACN

Nei rapporti con ACN

- ❖ Il Punto di Contatto è responsabile di qualsiasi **scambio di informazioni di carattere amministrativo-istituzionale** tra l'azienda, o le compagnie del gruppo, e ACN/le autorità di Governo
- ❖ **In particolare, svolge i seguenti ruoli**
  - registrazione e aggiornamento: è responsabile del processo di censimento, e del relativo aggiornamento annuale obbligatorio, dei dati aziendali rilevanti per la sicurezza informatica e oggetto di pubblicazione obbligatoria, previa convalida de DG
  - mantiene aggiornati i dati dell'organizzazione nel Portale ACN (denominazione, sedi, rappresentanti legali, asset critici)
  - convalida entro le scadenze fissate da ACN la correttezza delle informazioni inserite
  - coordinamento istituzionale e comunicazioni ufficiali: in qualità di interfaccia ufficiale tra l'organizzazione e ACN, è il canale autorizzato per scambi di dati e comunicazioni con ACN, CSIRT Italia e autorità competenti
  - cura la tracciabilità delle comunicazioni e conserva evidenze formali delle interazioni con ACN/CSIRT, da esibire in caso di ispezione o audit (Art. 26, comma 3 D.Lgs. 138/2024).

Nei rapporti con gli Organi Amministrativi e Direttivi

- ❖ **Supervisiona e coadiuva il CdA nell'attuazione degli obblighi che sono di responsabilità del CdA. A tal fine, svolge i seguenti ruoli:**
  - *flussi informativi*: garantisce il flusso informativo verso il CdA in materia di adempimenti NIS 2, fornendo aggiornamenti periodici sullo stato di conformità, incidenti segnalati e azioni correttive (cfr Art. 21, commi 2 e 4 D.Lgs. 138/2024)
  - strategy e rapporti con CSIRT: traduce le direttive strategiche in azioni operative di coordinamento con CSIRT e le altre strutture interne coinvolte (Art. 26, comma 2 D.Lgs. 138/2024)
  - *reporting*: presenta alla DG e al CdA un report annuale sullo stato di conformità, vulnerabilità e segnalazioni effettuate, utile per la relazione di governance e il bilancio di sostenibilità (Art. 21, comma 5 D.Lgs. 138/2024).

5. Adempimenti negli altri settori cyber

ADEMPIMENTI E PRESCRIZIONI
In ambito PERIMETRO

- **Identificazione di beni e infrastrutture a servizio di funzioni fondamentali dello Stato**
  - predisposizione e trasmissione, entro 6 mesi dalla ricezione della comunicazione di avvenuto inserimento nel Perimetro, di un elenco delle reti, dei sistemi informativi e dei servizi informatici dal cui funzionamento dipende l'esercizio di funzioni e servizi essenziali dello Stato, comprensivi della relativa architettura e componentistica. L'elenco deve essere aggiornato con cadenza almeno annuale, anche in assenza di variazioni, e comunicato attraverso la piattaforma digitale predisposta da ACN
- **Misure di sicurezza di cui all' allegato B del regolamento adottato con DPCM n. 81/2021**
  - dotarsi di una struttura organizzativa preposta alla gestione della sicurezza informatica
  - adottare politiche di sicurezza e gestione del rischio, di mitigazione e gestione degli incidenti e di prevenzione; dispositivi di protezione fisica e logica e dei dati; assicurare l'integrità delle reti e dei sistemi informativi
  - istituzionalizzare attività di monitoraggio, test e controllo
  - svolgere attività di formazione
- **Incidenti**
  - incidenti aventi impatto sui beni ICT: notifica entro 1 o 6 ore, in relazione alla gravità dell'incidente
  - incidenti aventi impatto sui sistemi informativi e di rete diversi dai citati beni ICT: notifica entro 72 ore
- **Certificazione di qualità**
  - comunicazione preventiva ad ACN in qualità di CVCN in ordine alla stipulazione di contratti di affidamento di beni e servizi ICT destinati a essere impiegati su reti, sistemi e servizi inclusi nel Perimetro
  - rispetto delle prescrizioni eventualmente impartite da ACN e sottoposizione ad attività di test
  - obbligo di collaborazione nell'ambito dei test e di rendere informazioni veritiere
  - *i fornitori* di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici inclusi nel Perimetro sono tenuti a collaborare con ACN nell'esecuzione delle attività di test (*sanzione art. 1 co. 9 lett.f)*)

ADEMPIMENTI E PRESCRIZIONI DORA

Adempimenti

La disciplina degli adempimenti di sicurezza informatica è simile a quella dettata in ambito NIS, con alcune peculiarità.

Principali misure di sicurezza

- misure preventive: (i) predisposizione, da parte degli organi di gestione e controllo, di un *quadro di gestione dei rischi* che comprenda strategie, politiche, procedure, protocolli e strumenti per proteggere i patrimoni informativi e le risorse ICT nonché le infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili; (ii) identificazione dei rischi informatici tramite la mappatura di tutte le funzioni aziendali interessate dall'utilizzo di beni ICT; (iii) monitoraggio del regolare funzionamento dei sistemi; (iv) predisposizione di procedure per la tempestiva identificazione delle anomalie
- misure di resilienza: (i) predisposizione di misure per "*rispondere in maniera rapida, appropriata ed efficace ..agli incidenti connessi alle TIC*"; (ii) sistemi di *back up*;(iii) definizione e aggiornamento di un programma di test di resilienza operativa
- rapporti con i fornitori: inserire nei contratti condizioni, requisiti, obblighi di audit e risolvere i contratti non conformi

Incidenti

- il regolamento distingue tra tre tipologie di incidenti per i quali è prevista la notifica obbligatoria ("*gravi incidenti TIC*"; "*grave incidente operativo o di sicurezza dei pagamenti*"; "*incidente operativo o di sicurezza dei pagamenti*") e "minacce" per le quali è prevista la notifica volontaria
- la competenza a ricevere le notifiche degli incidenti è attribuita all'autorità di vigilanza - nel nostro ordinamento, quindi, alla **Banca d'Italia, Consob, ISVAP, COVIP** - che poi trasmette le informazioni ricevute al Punto di Contatto Unico NIS (ACN) e, con riferimento agli intermediari "*significant*", alla BCE; le notifiche dei "gravi incidenti" devono essere trasmesse anche a CSIRT Italia

PUBBLICHE AMMINISTRAZIONI

- **Dotarsi di una struttura per la cybersicurezza**
  - La struttura, che può essere individuata anche in quella dell'ufficio del *responsabile per la transizione al digitale*, è responsabile degli adempimenti di cybersicurezza e punto di riferimento esterno dell'ente (tra le responsabilità della struttura: sviluppo di politiche e procedure di sicurezza delle informazioni; predisposizione e aggiornamento di un piano per il rischio informatico; produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni; monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento)
- **Nominare un referente per la cybersicurezza**
  - designare un "referente per la cybersicurezza" in ragione delle sue specifiche professionalità e competenze possedute in materia, il cui nominativo deve essere comunicato all'ACN con funzioni di Punto di Contatto (può essere individuato anche nella figura del responsabile per la transizione al digitale)
- **Notifica degli incidenti** (analogamente a quanto previsto dalla disciplina NIS)
  - pre-notifica entro 24 ore
  - notifica entro 72 ore comunicando tutte le informazioni disponibili
  - diversamente da quanto previsto dalla disciplina NIS, nel caso di omessa notifica, ACN avvisa che il reiterato inadempimento nell'arco di 5 anni comporta l'applicazione della sanzione e può costituire causa di responsabilità disciplinare e amministrativo contabile a carico dei funzionari dirigenti responsabili

6. Controlli e sanzioni

ATTIVITA' DI SUPERVISIONE ACN

ACN è l'autorità di supervisione designata ed esercita la vigilanza per monitorare e valutare il rispetto delle prescrizioni da parte dei soggetti obbligati (NIS, Perimetro, PA); nell'esercizio delle potestà attribuite, può disporre ispezioni, verifiche, *audit* periodici

Con riferimento ai soggetti NIS è previsto un regime di supervisione differenziato a seconda che il soggetto vigilato sia *essenziale* o *importante*

- Soggetti *essenziali*: ***ex ante*** e su impulso dell'Autorità
- Soggetti *importanti*: solo ***ex post*** se sussistono elementi, indicazioni o informazioni dalle quali emerge il sospetto che il soggetto non rispetti le prescrizioni applicabili

Oggetto dell'attività ispettiva (comune a tutti i soggetti obbligati)

- ispezioni *in loco* e vigilanza *offsite*, controlli casuali e periodici
- *audit* periodici/casuali per testare la sicurezza di reti, sistemi informativi e servizi informatici, svolti eventualmente avvalendosi di professionisti dedicati e *scansioni di sicurezza*
- *audit ad hoc*, anche in funzione di "misure di rimedio" successivamente a un incidente, al riscontro di irregolarità o a un esito di *audit* negativo
- *richieste di informazioni* con diverse finalità, dalla valutazione dell'efficienza e proporzionalità delle eventuali misure prescritte a un soggetto specifico, alla verifica in ordine alla effettiva attuazione delle *policy* aziendali di gestione dei rischi, alla valutazione in merito all'adempimento degli obblighi di legge

SANZIONI NIS

Tipologia di violazione

- ✓ violazione di doveri e obblighi degli organi di amministrazione e direzione
- ✓ violazione delle prescrizioni a breve o a lungo termine
- ✓ omessa registrazione e/o comunicazione e/o aggiornamento delle informazioni riguardanti i soggetti obbligati
- ✓ omessa notifica di incidente rilevante (per le ***PA*** la responsabilità sorge solo se si ha reiterazione della violazione nell'arco di cinque anni)
- ✓ violazione delle disposizioni esecutive impartite da ACN (ordini di esecuzione/inibitori)
- ✓ omessa collaborazione a fronte di richieste (di informazioni o altre attività) da parte di ACN o del CSIRT

➔ **l'omessa** o la **tardiva registrazione dei soggetti NIS** autorizza ACN a contestare tutte le violazioni sopra elencate e comporta l'applicazione della **sanzione** per la **violazione più grave**, **aumentata fino al triplo**

Natura delle sanzioni

Sanzione amministrativa pecuniaria per le persone giuridiche

- **soggetti essenziali:** fino a € 10mln oppure al 2% del fatturato annuo globale per l'esercizio precedente (se di importo superiore)
- **soggetti importanti:** fino a € 7mln oppure all'1,4% del fatturato annuo globale per l'esercizio precedente (se di importo superiore)
  - ✓ se il soggetto è una **PA**: la cornice edittale della sanzione è ridotta di un terzo

Sanzioni accessorie (solo per **soggetti essenziali)**

- nei confronti delle persone giuridiche: sospensione temporanea dall'esercizio dell'attività
- nei confronti delle persone fisiche che svolgono funzioni dirigenziali o di rappresentanza legale: sospensione temporanea dalla capacità di svolgere i compiti del proprio ufficio

SANZIONI PERIMETRO (art. 1 co. 9 Decreto Perimetro)

Salvo che il fatto costituisca reato:

a) il mancato **adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco** delle reti, dei sistemi informativi e dei servizi informatici è punito con la sanzione amministrativa pecuniaria *da euro 200.000 a euro 1.200.000*

b) il mancato adempimento **dell'obbligo di notifica** è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000

c) **l'inosservanza delle misure di sicurezza** è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000

d) la **mancata comunicazione** preventiva al CVCN in ordine alla stipulazione di contratti di affidamento di beni e servizi ICT è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici in violazione delle condizioni imposte dall'ACN in qualità di CVCN o **in assenza del superamento dei test** è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000 **+** sanzione amministrativa accessoria a carico delle persone fisiche (organi di amministrazione) della incapacità ad assumere incarichi di direzione, amministrazione e controllo per un periodo di tre anni a decorrere dalla data di accertamento della violazione

f) **la mancata collaborazione per l'effettuazione delle attività di test** è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000

g) il **mancato adempimento delle prescrizioni impartite da ACN è** punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000

h) il mancato rispetto delle prescrizioni imposte da ACN a seguito dei test è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti o delle attività ispettive e di vigilanza **fornisce informazioni, dati o elementi di fatto non rispondenti al vero**, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni **od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto**, è punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote.

SANZIONI DORA

Responsabilità

- L'organo di gestione "*assume la responsabilità finale per la gestione dei rischi informatici*" e definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle infrastrutture ICT e stabilisce adeguati meccanismi di *governance*.

Sanzioni amministrative pecuniarie nei confronti delle persone giuridiche

- differenziate in base alla natura del soggetto (banche, sgr, IP, IMEL) e alla tipologia di violazione e caratterizzate da una cornice edittale particolarmente ampia (*e.g.* da euro 30.000 fino a euro 5 milioni, ovvero fino al 10 per cento del fatturato)

Sanzioni amministrative pecuniarie nei confronti delle persone fisiche

- *salvo che il fatto costituisca reato*; sanzioni differenziate in base alla tipologia di violazione e caratterizzate da una cornice edittale particolarmente ampia (da euro 5.000 fino a euro 5 milioni; e da euro 5.000 fino a euro 3 milioni)

Sanzioni accessorie

- per alcune tipologie di violazioni è prevista la sanzione accessoria dell'interdizione, per un periodo non inferiore a sei mesi e non superiore a tre anni, dallo svolgimento di funzioni di amministrazione, direzione e controllo presso intermediari e imprese autorizzati

7. Aggiornamenti a livello europeo: implementazione della normativa e rischi attuali

LO STATO DI RECEPIMENTO DELLA DIRETTIVA NIS2 NEI PAESI UE

- **N. 15 Stati membri hanno recepito la Direttiva NIS2** (Belgio, Croazia, Cipro, Repubblica Ceca, Danimarca, Finlandia, Italia, Grecia, Lettonia, Lituania, Malta, Romania, Slovacchia, Slovenia)
- **N. 12 Stati membri hanno elaborato proposte di recepimento non ancora in vigore** (Francia, Germania, Austria, Bulgaria, Estonia, Lussemburgo, Irlanda, Paesi Bassi, Polonia, Portogallo, Spagna, Svezia)

La reazione della Commissione Europea

- ❖ Nel novembre del 2024 la Commissione aveva annunciato l'avvio di n. 23 procedure di infrazione per mancato recepimento della direttiva NIS2 entro il 17 ottobre 2024
- ❖ Al 7 maggio 2025, la Commissione ne ha archiviate quattro e ha inviato **il parere motivato (*reasoned opinion*) a 19 Stati** membri a causa nella mancata notifica o della trasposizione non soddisfacente
- ❖ Gli Stati sono: Bulgaria, Repubblica Ceca, Danimarca, Germania, Estonia, Irlanda, Spagna, Francia, Cipro, Lettonia, Lussemburgo, Ungheria, Paesi Bassi, Austria, Polonia, Portogallo, Slovenia, Finlandia e Svezia

La Difesa UE dalle minacce esterne

- Nel 2019 l'UE ha istituito un quadro di misure restrittive contro gli attacchi informatici che minacciano l'UE e i suoi Stati membri
- Il quadro **consente all'UE di imporre misure restrittive mirate** nei confronti di **persone o entità** coinvolte in attacchi informatici che hanno un impatto significativo e che costituiscono una **minaccia esterna per l'UE o i suoi Stati membri**. Misure restrittive possono essere decise anche in risposta ad attacchi informatici nei confronti di Stati terzi o organizzazioni internazionali qualora tali misure siano ritenute necessarie per conseguire gli obiettivi della politica estera e di sicurezza comune
- **Il quadro giuridico relativo a tali misure è prorogato fino al 18 maggio 2028**

Le misure restrittive individuali attualmente in vigore

- Misure restrittive individuali sono applicate attualmente a **17 persone e quattro entità** e comprendono: il divieto di viaggio verso l'UE (persone fisiche), il congelamento dei beni e il divieto di fornire fondi o risorse economiche, direttamente o indirettamente.
- Sono in vigore fino al maggio del 2026 e sono riesaminate ogni 12 mesi.

L'ultimo caso sanzionato (Russia contro Estonia)

- ✓ Ufficiali di Stato maggiore russi (la cui Unità era già stata coinvolta in attacchi verso l'Ucraina)
- ✓ Accesso abusivo a sistemi informatici ministeriali con furto di migliaia di dati riservati (e.g. segreti commerciali, cartelle cliniche)[4]

Cybersicurezza UE entra nell'ONU

- Il **13 ottobre 2025**, il **Consiglio** dell'UE **ha autorizzato la Commissione e gli Stati membri a firmare la Convenzione delle Nazioni Unite contro la criminalità informatica.**
- La Convenzione è un trattato internazionale che stabilisce norme comuni a livello mondiale per rafforzare la cooperazione in materia di criminalità informatica (armonizzazione di alcuni reati) e lo scambio di prove in formato elettronico a fini di indagini o procedimenti penali.
- La Convenzione sarà aperta alla firma dal 25 ottobre 2025 al 31 dicembre 2026 ed entrerà in vigore novanta giorni dopo il deposito del quarantesimo strumento di ratifica, accettazione, approvazione o adesione.

[4] https://www.consilium.europa.eu/it/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/

THREAT INTELLIGENCE in UE

ENISA THREAT LANDSCAPE 2025

- l'Agenzia europea per la cybersicurezza (ENISA) ha analizzato lo stato della sicurezza informatica in Europa tra luglio 2024 e giugno 2025 su un campione di più di 4.000 incidenti

SETTORI MAGGIORMENTE INTERESSATI

- il 53,7% dei soggetti coinvolti sono "soggetti essenziali NIS"
- **PA** e in generale organizzazioni degli Stati UE (38%), trasporti (7,5%), infrastrutture e servizi digitali (4,8%, soprattutto servizi cloud, provider terzi e supply chain digitale), finanza (4,7%) e produzione (2,9%)

TIPOLOGIA DI ATTACCHI

Sovente non sono attacchi isolati ma "campagne" di hacking

- il **phishing** è la principale modalità di intrusione iniziale, avviene attraverso vere e proprie campagne, la cui diffusione capillare è agevolata dall'utilizzo dell'**intelligenza artificiale** anche al fine di attribuire al phishing maggiore capacità decettiva (maggiore verosimiglianza, credibilità)
  - ✓ frequente nel settore finanziario tramite phishing, banking trojan, furto di credenziali
- il **DDoS** (*Distributed Denial of Service*) è la principale tipologia di attacco → immissione nel sistema di una molte molto ingente di traffico dati in modo tale che il server *target* non riesca a gestire l'enorme mole di input ricevuti e si blocchi
  - ✓ frequente nei confronti di Stati e PA anche a mezzo campagne di c.d. Hacktivismo, anche nel settore dei trasporti
- il **ramsonware** è la minaccia più impattante: le varianti Akira e SafePay sono le più diffuse e hanno generato incidenti con interruzioni di servizio e data breach

THREAT INTELLIGENCE in ITALIA

ACN settembre 2025

- **270 casi (+103% rispetto al mese precedente) e 55 incidenti confermati**

SETTORI MAGGIORMENTE INTERESSATI

- **PA, Telecomunicazioni e settori critici**

TIPOLOGIA DI ATTACCHI

Rivendicati da gruppi auto identificati come filo-russi o pro-Hamas

- **DDoS** ma a basso impatto: sembra che di 124 attacchi solo il 6% abbia prodotto impatti effettivi, come temporanea indisponibilità di servizi
- **Ramsonware** tramite email, accessi abusivi sfruttando vulnerabilità di sistema, creazione di account appositi