



FEDERCHIMICA
ASSOGASTECNICI
Associazione nazionale imprese gas tecnici,
speciali e medicinali

Riunione Nazionale di Sicurezza

AI Act e implementazione
delle misure di
cybersicurezza introdotte
dalla direttiva NIS2

Il fattore umano
nell'evoluzione tecnologica

Stresa, Grand Hotel des Iles Borromées
12 e 13 novembre 2025

Lucia Giommoni e Francesca Belinghieri
Federchimica

1

Definizione di sistema di IA secondo l'AI Act (art. 3)

Dal Reg. (UE) 2024/1689 entrato in vigore ad agosto 2024:

«sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;



29/07/25: Orientamenti della Commissione sulla definizione di sistema di intelligenza artificiale

2

Sistemi esclusi dal campo di applicazione

Finalità

Ottimizzazione matematica di funzioni o parametri

Elaborazione di base dei dati

Analisi descrittiva e visualizzazione dei dati

Previsioni semplici



Esempi

Modelli di machine learning per approssimazione di funzioni o parametri

Filtri di selezione in sistemi di gestione delle banche dati; fogli di calcolo elettronici senza funzionalità basate sull'IA

Metodi statistici di sintesi e visualizzazione dei dati sotto forma di grafici e diagrammi

Sistemi di previsione dei tempi di risposta di supporto al cliente e del numero di articoli venduti

3

I soggetti a cui si applica (art. 3)

«fornitore»: **sviluppa** un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato **o mette in servizio il sistema di IA con il proprio nome o marchio**, a titolo oneroso o gratuito;

«deployer»: **utilizza** un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;



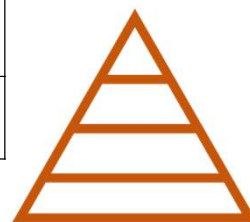
Il **deployer** diventa **fornitore** di un sistema ad alto rischio **se** apporta una **modifica sostanziale** o modifica la **finalità** prevista di un sistema di IA ad alto rischio (art. 25)



4

Approccio basato sul rischio

Livello di rischio	Esempi di applicazioni	Disposizioni	Entrata in applicazione
Inaccettabile	Sistemi di: attribuzione punteggio sociale, riconoscimento delle emozioni, sfruttamento vulnerabilità	Divieto	2 febbraio 2025
Alto	Componenti di sicurezza di un prodotto, sistemi impiegati in alcuni settori (e.g. istruzione e formazione professionale, occupazione e gestione dei lavoratori)	Adozione di misure tecniche e organizzative	2 agosto 2026 – 2 agosto 2027
Limitato	Chatbot, deepfake	Trasparenza	2 agosto 2026
Minimo	Filtri spam, videogiochi	Codice di condotta volontario	2 agosto 2026



5

Rischio inaccettabile (art. 5)

Pratiche vietate

- ⊗ Manipolazione dannosa e inganno
- ⊗ Sfruttamento dannoso delle vulnerabilità
- ⊗ Attribuzione di un punteggio sociale
- ⊗ Valutazione del rischio che una persona commetta un reato
- ⊗ Scraping non mirato per sviluppare banche dati di riconoscimento facciale
- ⊗ Riconoscimento delle emozioni
- ⊗ Categorizzazione biometrica
- ⊗ Identificazione biometrica remota in tempo reale

Sono esclusi (e dunque consentiti)

- ✓ Sistemi di riconoscimento degli stati fisici, quali dolore o affaticamento
- ✓ Sistemi biometrici per confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali



29/07/25: [Orientamenti della Commissione](#) relativi alle pratiche di intelligenza artificiale vietate

6

Rischio alto (capo III)

Rientrano nella definizione (art. 6) i sistemi di IA

1. Che sono componenti di sicurezza di prodotti/prodotti disciplinati e soggetti alla valutazione di conformità ai sensi della normativa di armonizzazione in **allegato I** (e.g. regolamento macchine, direttiva DPI, direttiva ATEX)
2. Di cui all'**allegato III** e che presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche. Sono sempre considerati ad alto rischio se effettuano profilazione di persone fisiche

Obblighi del deployer (art. 26)

- ✓ Applicazione delle istruzioni per l'uso date dal fornitore
- ✓ Sorveglianza umana
- ✓ Monitoraggio del funzionamento e segnalazione degli incidenti
- ✓ Conservazione dei log
- ✓ Informazione ai lavoratori su uso di sistemi ad alto rischio



Pubblicazione degli **Orientamenti della Commissione** prevista nel **Q2 2026**

7

Modelli di IA per finalità generali (GPAI) (capo V)



Sono caratterizzati da una **generalità significativa** e sono in grado di svolgere con competenza un'**ampia gamma di compiti distinti**; possono essere integrati in una varietà di sistemi o applicazioni a valle (sono esclusi i modelli per la sola attività di R&S)



Sono classificati a rischio sistemico se presentano capacità di impatto elevato (art. 51)



Gli **obblighi a carico dei fornitori** sono entrati in applicazione il 2 agosto 2025. Per i modelli GPAI messi sul mercato prima del 2 agosto 2025 la conformità è richiesta entro il 2 agosto 2027



Documenti di orientamento per i fornitori: [Linee guida sugli obblighi](#) e [Codice di buone pratiche](#)

8

Alfabetizzazione in materia di IA (art. 4)

«I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.»



L'obbligo è entrato in applicazione il **2 febbraio 2025**



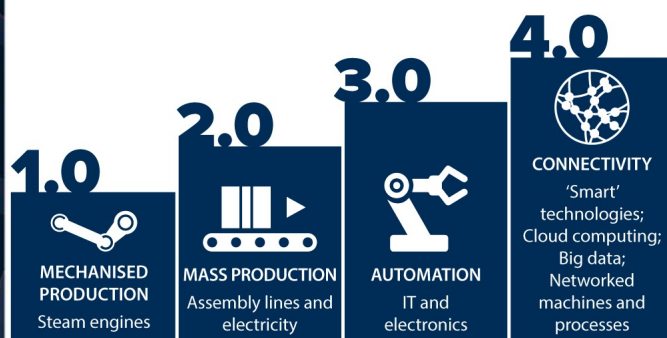
Archivio “vivente” di buone pratiche e Database su programmi di alfabetizzazione



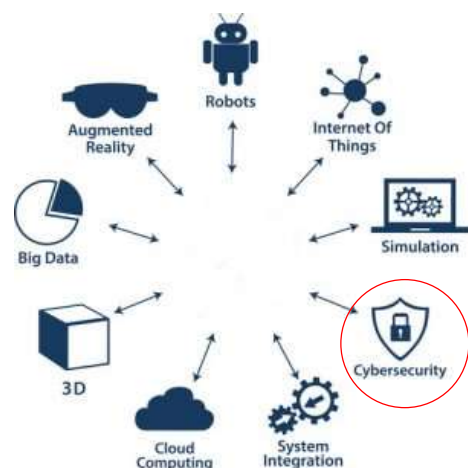
08/10/25: lancio dell' AI Act Single Information Platform che offre i seguenti strumenti: Compliance Checker, AI Act Explorer e AI Act Service Desk

9

Industria 4.0 e i rischi Cyber



The stages of industrial development
Source: Oxford Analytica



Cybersecurity: Capacità di proteggere tutti gli asset materiali ed immateriali (proprietà intellettuale, danno reputazionale) che possono essere aggrediti tramite il «cyberspazio» o che dipendono da esso, garantendo allo stesso tempo la Governance e la Business Continuity di tutta l'infrastruttura digitale a supporto.

10

I rischi Cyber

THE REVIEW OF THE ENISA FORESIGHT CYBER- SECURITY THREATS FOR 2030



Fonte: enisa – European Union Agency for Cybersecurity

11

Attacchi Cyber in Italia, primo semestre 2025

Analisi

Nel **primo semestre 2025** ACN ha censito **1.549 eventi cyber**, in aumento del **53%** rispetto allo stesso periodo dell'anno precedente (1° semestre 2024). Il numero di incidenti con **impatto confermato** è stato a **346**, in aumento del **98%**.

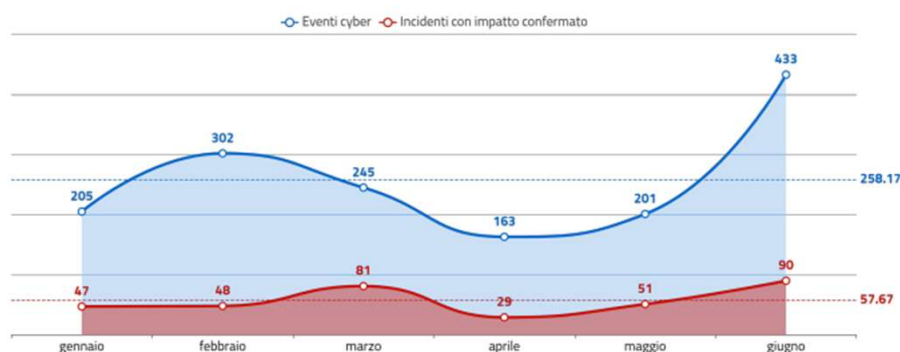


Figura 2 - andamento del numero di eventi e incidenti del 1° semestre 2025

Mappa attacchi in tempo reale: <https://fortiguard.fortinet.com/threat-map>

Fonte: «Operational summary 1° semestre 2025» – Agenzia per la Cybersecurity nazionale (ACN)

12

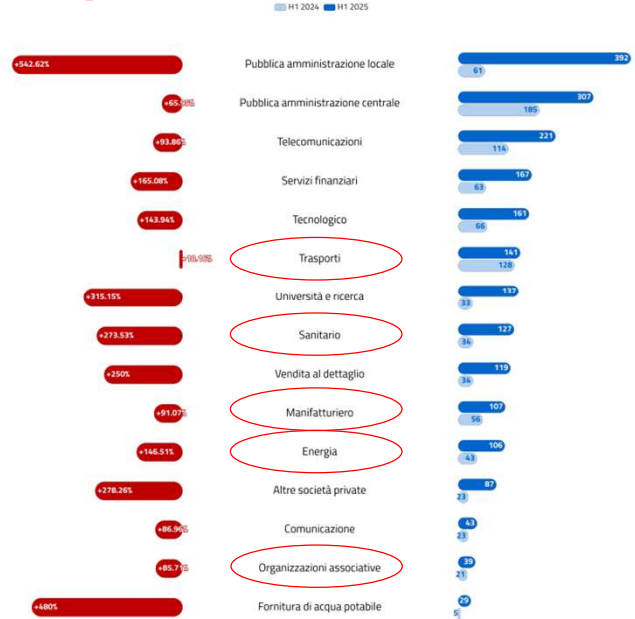
Attacchi Cyber in Italia, primo semestre 2025

Tipologie

- campagne DDoS - 598 attacchi + 77%
- esposizione dati – 186 eventi (vendita di credenziali compromesse)
- Phishing - 1.530 URL di phishing bloccati

Vittime

- Pubblica amministrazione locale (392)
- Pubblica amministrazione centrale (307)
- Telecomunicazioni (221)
- Manifatturiero (107)



Fonte: «Operational summary 1° semestre 2025» – Agenzia per la Cybersicurezza nazionale (ACN)

13

Campo di applicazione (D. 138 del 4 settembre 2024)

In rosso Settori, sottosectori e tipologie di soggetti introdotti dalla NIS2

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia (+)	19 tipologie di soggetto	Essenziali	Importanti ¹	Fuori ambito ²
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario (+)				
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali (+)	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto			
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto			
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali (+)	4 tipologie di soggetto			
Ricerca	1 tipologia di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA			
Pubblica Amministrazione regionale, locale e di altro tipo	11 categorie di PA			
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione governativa		

Fonte: ACN

Schema degli ambiti di applicazione
1 Possibile identificazione dell'Autorità come essenziali
2 Possibile identificazione dell'Autorità come importanti o essenziali

14

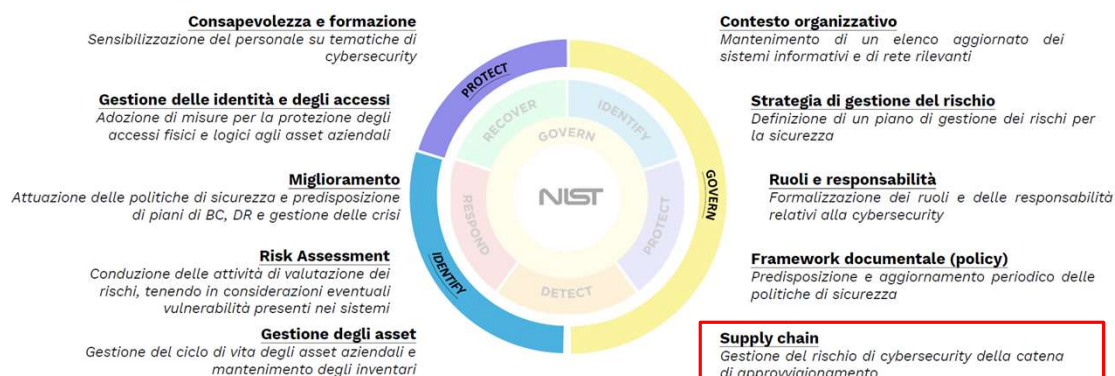
Obblighi per le imprese e tempistiche

Obbligo (D. 138 del 4 settembre 2024)	Tempistica di prima applicazione	Tempistica generale
➤ registrarsi all'interno di una piattaforma digitale messa a disposizione dall'Autorità (determina ACN pubblicata 28 novembre)	1° dicembre 2024 - 28 febbraio 2025	dal 1° gennaio al 28 febbraio di ogni anno
➤ verificare di essere soggetto inserito nell'elenco NIS	Aprile 2025	Mese di aprile di ogni anno
➤ adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi (Determina ACN aprile 2025)	In fase di prima applicazione entro 18 mesi dalla notifica di inclusione (ottobre 2026)	Senza indebito ritardo
➤ Nominare un referente CSIRT e sostituti referenti CSIRT responsabili della notifica in caso di incidente significativo (Determina ACN settembre 2025)	Dal 20 novembre al 31 dicembre 2025	
➤ comunicare ed aggiornare un elenco delle proprie attività e dei propri servizi , con modalità successivamente definite dall'Agenzia;	-	Dal 1° gennaio 2026
➤ in caso di incidente significativo, notificare l'evento al CSIRT Italia	in caso di prima applicazione, 9 mesi dalla notifica di inclusione (1° gennaio 2026)	senza ingiustificato ritardo , massimo 24 ore la pre-notifica e 72 ore la notifica; relazione finale entro un mese dalla notifica
➤ effettuare una notifica volontaria su quasi-incidenti e minacce informatiche	-	-

15

Cybersecurity e Supply Chain

Le **misure di sicurezza** di base contenute negli **Allegati I e II** della Determinazione ACN n. 164179 si articolano nei **seguenti ambiti**:



Fonte: BIP Group

16

Cybersecurity e Supply Chain (Misure di base)

Gestione del rischio di cybersecurity della catena di approvvigionamento (GV.SC): I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.

Misura	Breve descrizione	Soggetti Importanti (I) o Soggetti essenziali (E)
GV.SC-01	Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia , obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.	I + E (con alcuni obblighi aggiuntivi)
GV.SC-02	I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.	I + E
GV.SC-04	I fornitori sono noti e prioritizzati in base alla criticità.	I + E
GV.SC-05	I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.	I + E
GV.SC-07	I rischi posti da un fornitore , dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.	I + E

17

Sanzioni massime (D. 138 del 4 settembre 2024)

Violazione	Sanzione "Soggetti essenziali"	Sanzione "Soggetti importanti"
Mancato rispetto degli obblighi per gli organi direttivi	€10.000.000 o 2% del fatturato su scala mondiale	€7.000.000 o 1,4% del fatturato su scala mondiale
Mancata implementazione delle misure tecniche di Cybersecurity		
Mancata notifica a seguito di un incidente significativo		
Mancato rispetto della diffida		
Mancata registrazione al portale ACN	0,1% del fatturato su scala mondiale	0,07% del fatturato su scala mondiale
Mancata comunicazione o aggiornamento delle attività e dei servizi		
Mancata implementazione degli obblighi di uso degli schemi di certificazione		
Mancata collaborazione con ACN o CSIRT		
Reiterazione specifica	Sanzione raddoppiata	Sanzione raddoppiata

18