Enti organizzatori

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA | DIPARTIMENTO
DI INGEGNERIA INDUSTRIALE

aias
Associazione Italiana Ambiente e Sicurezza

Con il patrocinio di

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO
DIREZIONE REGIONALE
EMILIA ROMAGNA

Innovazione tecnologica, digitale, AI

Quale impatto sulla Safety?

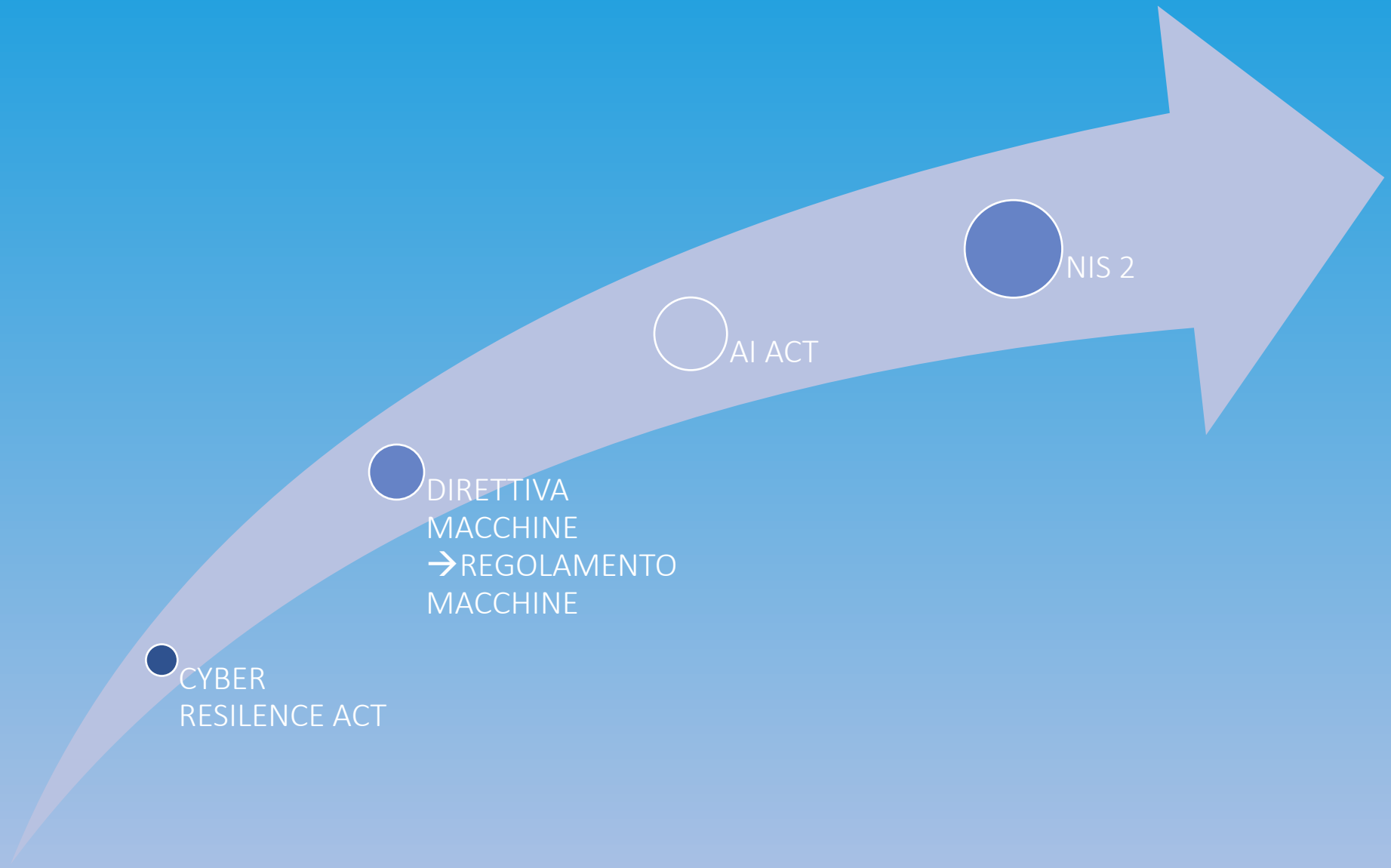
Cybersecurity: nuovi rischi per la governance Health & Safety

Avv. Francesco Piccaglia De Eccher
Avv.ta Chiara Piccaglia De Eccher

Coordinatore e Segretario AIAS ER
Partners Studio Legale Piccaglia

Bologna, 10 aprile 2026

UN CONTESTO NORMATIVO IN EVOLUZIONE



CYBER RESILIENCE ACT

OBIETTIVO DELLA NORMA	COSA PREVEDE	TEMPISTICHE	DESTINATARI	TO DO
Il regolamento (UE) 2024/2847 cerca di aumentare il livello di sicurezza informatica dei prodotti con **elementi digitali** e le conoscenze delle imprese e dei consumatori sulla sicurezza dei prodotti. Sono state definite le sanzioni in caso di non compliance.	Un quadro normativo **orizzontale** dell'UE basato su una serie completa di requisiti di cibersicurezza per i prodotti con elementi digitali, tra cui il *software* tangibile e non incorporato. Introducendo norme per proteggere i prodotti digitali non coperti da alcuna regolamentazione precedente	Dall'11 dicembre 2024, gli operatori economici degli Stati membri avranno 36 mesi di tempo (11 dicembre 2027) per adeguarsi ai nuovi requisiti. 21 mesi (11 settembre 2026) nei casi di obblighi di segnalazione di vulnerabilità sfruttate e incidenti, e 18 mesi per definire i processi di notifica alle autorità responsabili (applicazione solo a autorità nazionali)	Fabbricanti, importatori, distributori di prodotti con elementi digitali	Definizione e imposizione dei requisiti essenziali di cibersicurezza (comprese le norme armonizzate) da soddisfare prima dell'immissione dei prodotti sul mercato e durante l'intero ciclo di vita del prodotto.

Ambito di applicazione Art. 2, paragrafo 1 CRA

«prodotti con elementi digitali messi a disposizione sul mercato, la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete»

Definizione di «prodotti con elementi digitali» dell'art. 3 del CRA:

1. Prodotto con elementi digitali: qualsiasi prodotto *software* o *hardware* e le relative soluzioni di elaborazione dati da *remoto,* compresi i componenti *software* o *hardware* immessi sul mercato separatamente.

2. «elaborazione dati da *remoto»:* qualsiasi elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità e la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni;

8. «connessione logica»: rappresentazione virtuale di una connessione dati realizzata attraverso un'interfaccia *software*;

9. «connessione fisica»: qualsiasi connessione tra sistemi di informazione elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche, ottiche o meccaniche, fili od onde radio;

10. «connessione indiretta»: una connessione a un dispositivo o a una rete che non avviene direttamente, ma piuttosto nell'ambito di un sistema più ampio che è direttamente collegabile a tale dispositivo o rete.

Gli operatori economici:

FABBRICANTE

ovvero una persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o che fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio

IMPORTATORE

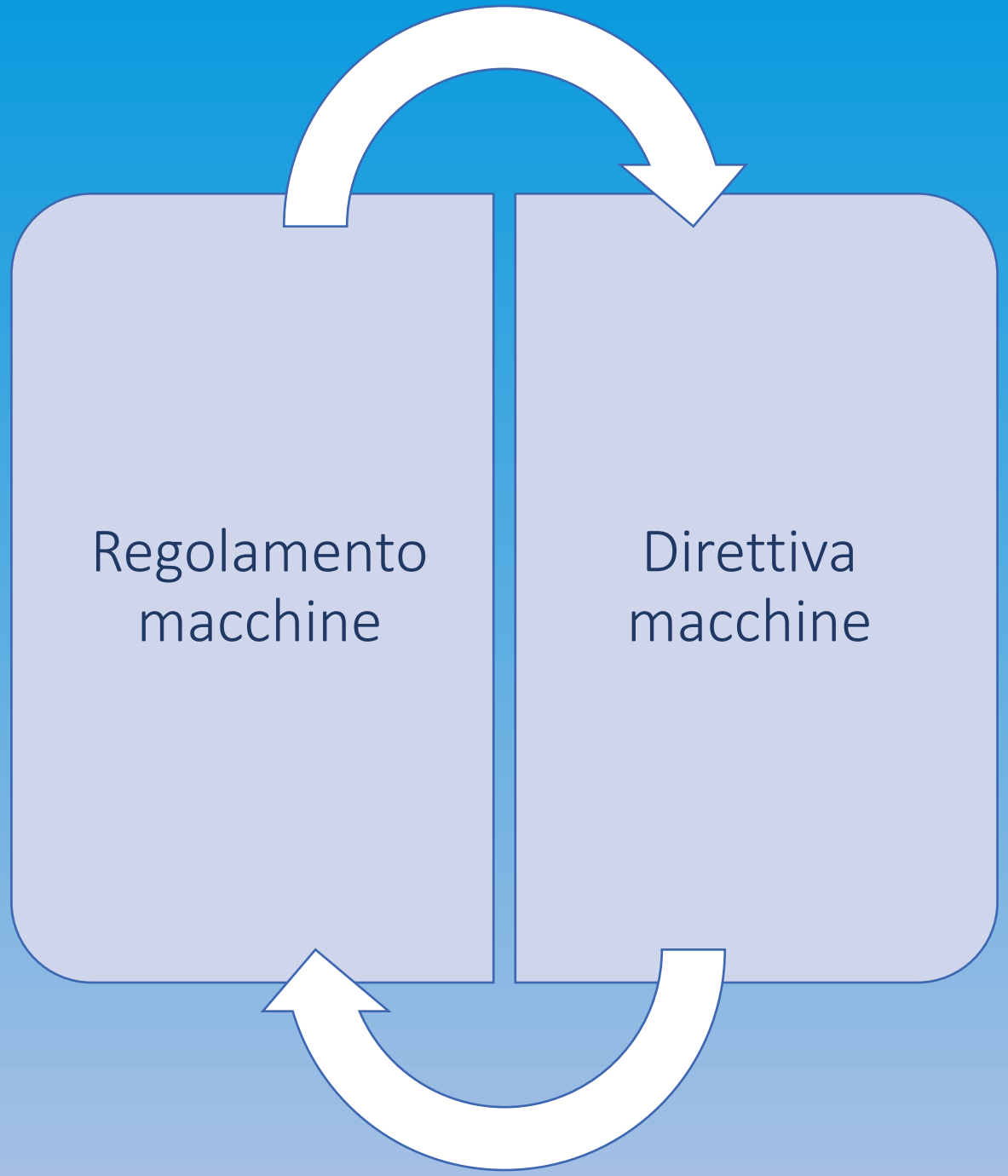
ovvero persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione

DISTRIBUTORI

ovvero persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà

Cyber Resilience Act (CRA)

Sicurezza by design	• Il CRA richiede che la sicurezza sia integrata fin dalla progettazione dei prodotti digitali per prevenire vulnerabilità.
Gestione delle vulnerabilità	• La legge impone una gestione strutturata delle vulnerabilità per garantire aggiornamenti e mitigazioni tempestive.
Responsabilità estesa supply chain	• Il CRA estende la responsabilità lungo tutta la catena di fornitura digitale per migliorare la sicurezza complessiva.
Impatto su sistemi industriali	• La normativa influenza gli impianti industriali integrati digitalmente, aumentando la responsabilità e la sicurezza operativa.


Regolamento macchine
Direttiva macchine

Nuovo Regolamento Macchine: cambio di paradigma

Cybersecurity come requisito di sicurezza

- La cybersecurity è ora un requisito obbligatorio per la sicurezza delle macchine industriali, proteggendo gli operatori da rischi fisici.

Implicazioni per produttori e utilizzatori

- Produttori e utilizzatori devono integrare misure di cybersecurity durante progettazione, validazione e manutenzione delle macchine.

Sicurezza OT nel quadro regolatorio europeo

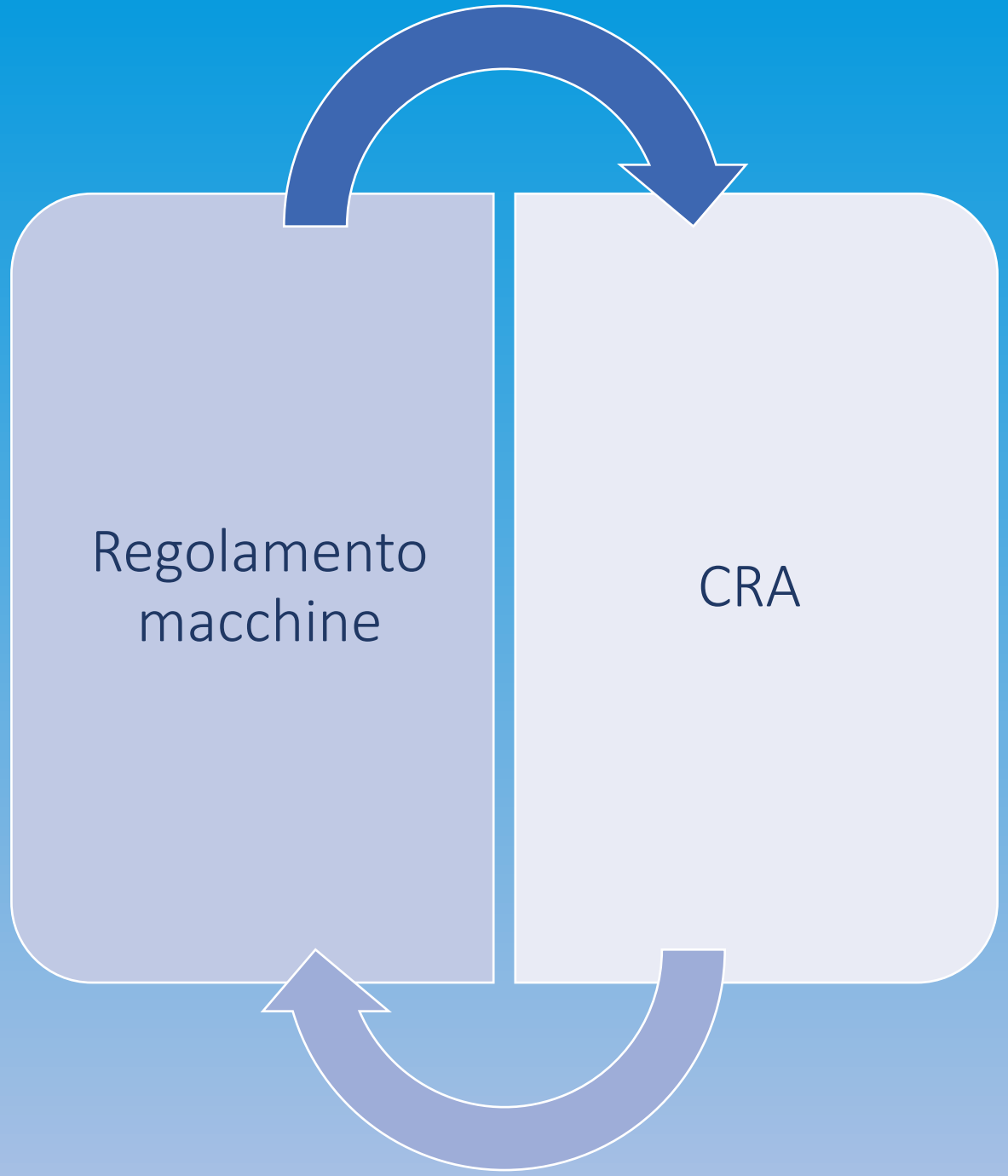
- La sicurezza operativa tecnologica è ufficialmente parte delle normative europee, richiedendo rigore pari alle misure tradizionali.

Relazione della Commissione europea del 19 febbraio 2020, dedicata alle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica

Il concetto di sicurezza nell'attuale normativa dell'Unione in materia di sicurezza dei prodotti è in linea con il concetto esteso di sicurezza al fine di proteggere i consumatori e gli utilizzatori. Pertanto, il concetto di sicurezza dei prodotti include la protezione contro tutti i tipi di rischi derivanti dal prodotto, non solo i rischi meccanici, chimici o elettrici ma anche i rischi informatici e i rischi connessi alla perdita di connettività dei dispositivi.

I Principali Rischi Cyber nel Regolamento Macchine

- **Accesso non autorizzato**: potenziale manipolazione delle macchine da parte degli attori malevoli
- **Interruzione operative:** attacchi che compromettono la funzionalità e la sicurezza delle macchine
- **Manomissione del software:** alterazione del codice per compromettere le prestazioni o la sicurezza
- **Malfunzionamento degli algoritmi:** bias degli algoritmi


Regolamento macchine
CRA

DOPPIA DICHIARAZIONE DI CONFORMITÀ

Entrambi i regolamenti richiedono una dichiarazione UE di conformità che certifichi che il prodotto rispetta i requisiti essenziali applicabili. Questa dichiarazione può essere unica e coprire tutte le normative UE pertinenti applicabili al prodotto, riducendo l'onere amministrativo per i produttori.

In entrambi i casi, la dichiarazione di conformità e la documentazione tecnica devono essere conservate e rese disponibili per almeno 10 anni dopo l'immissione del prodotto sul mercato oppure per l'intero periodo di supporto o assistenza del prodotto.

	NIS 2 DIRECTIVE	CYBER RESILIENCE ACT (CRA)	
Una normativa esclude l'altra?	Si applica a organizzazioni che operano in settori critici o importanti e che garantiscono reti e sistemi informativi.	Si applica ai prodotti con elementi digitali immessi sul mercato dell'UE.	Le due normative sono complementari ma indipendenti. Possono applicarsi allo stesso soggetto ma per aspetti diversi, così come applicarsi una sola delle due.
Se adempio alla NIS 2 sono automaticamente conforme anche al CRA?	Impone obblighi di gestione del rischio, sicurezza operativa e incident reporting.	Impone requisiti di security by design, gestione delle vulnerabilità e aggiornamenti di sicurezza dei prodotti.	No. La conformità alla NIS2 non implica automaticamente la conformità CRA.
Quali adempimenti hanno in comune?	Gestione del rischio cyber, sicurezza della supply chain, gestione degli incidenti.	Gestione delle vulnerabilità, aggiornamenti di sicurezza, sicurezza lungo il ciclo vita del prodotto.	Entrambe richiedono misure di cybersecurity strutturate, ma applicate a livelli diversi dell'ecosistema digitale.

AI ACT:

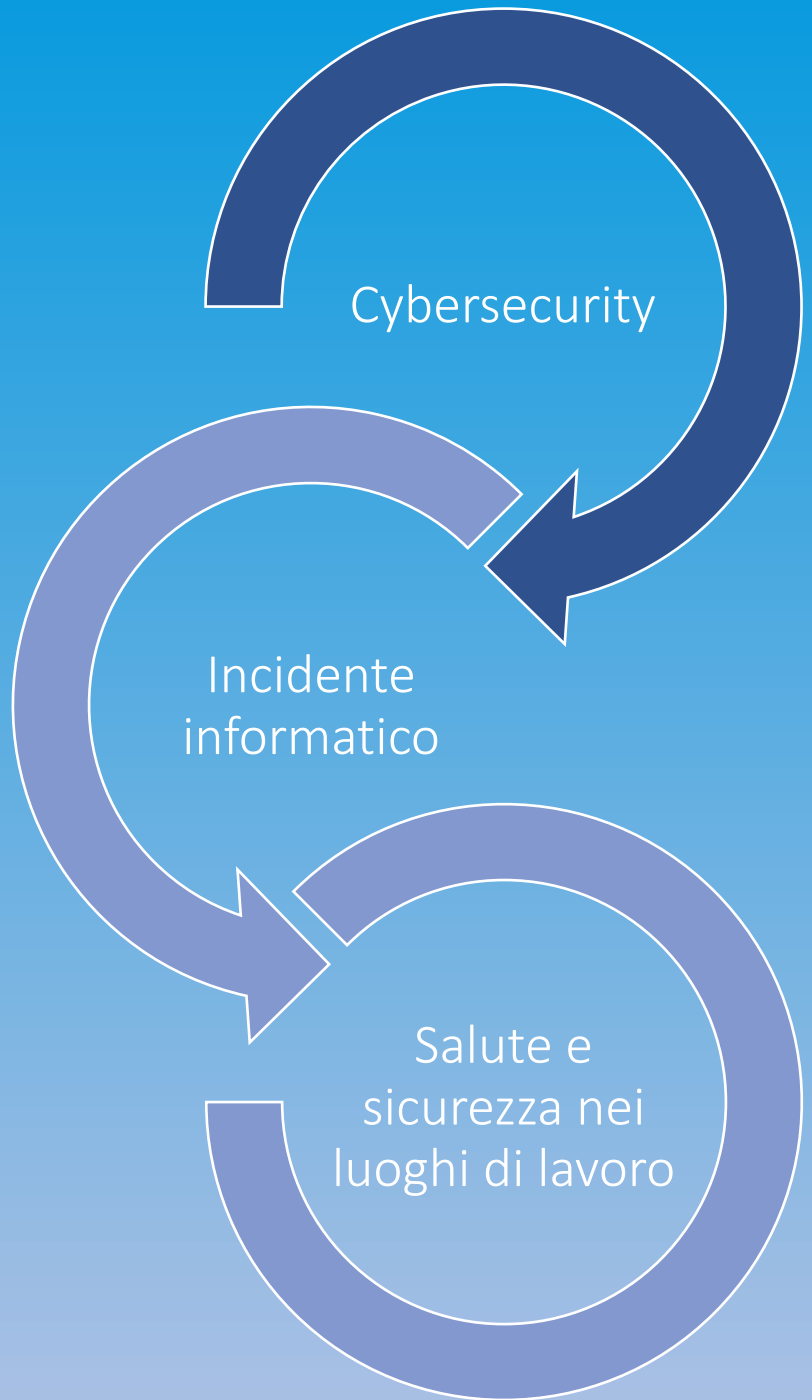
SICUREZZA DEL PRODOTTO E DEI LAVORATORI

SICUREZZA PRODOTTO IA

(47) I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati.

SICUREZZA PRODOTTO IA

(50) Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici, dispositivi medico-diagnostici *in vitro*, veicoli automobilistici e aeronautici.


Cybersecurity
Incidente informatico
Salute e sicurezza nei luoghi di lavoro

Il *cyber incident* non è SOLO un evento “IT”

Impatti diretti su:

- produzione
- sicurezza
- responsabilità legali

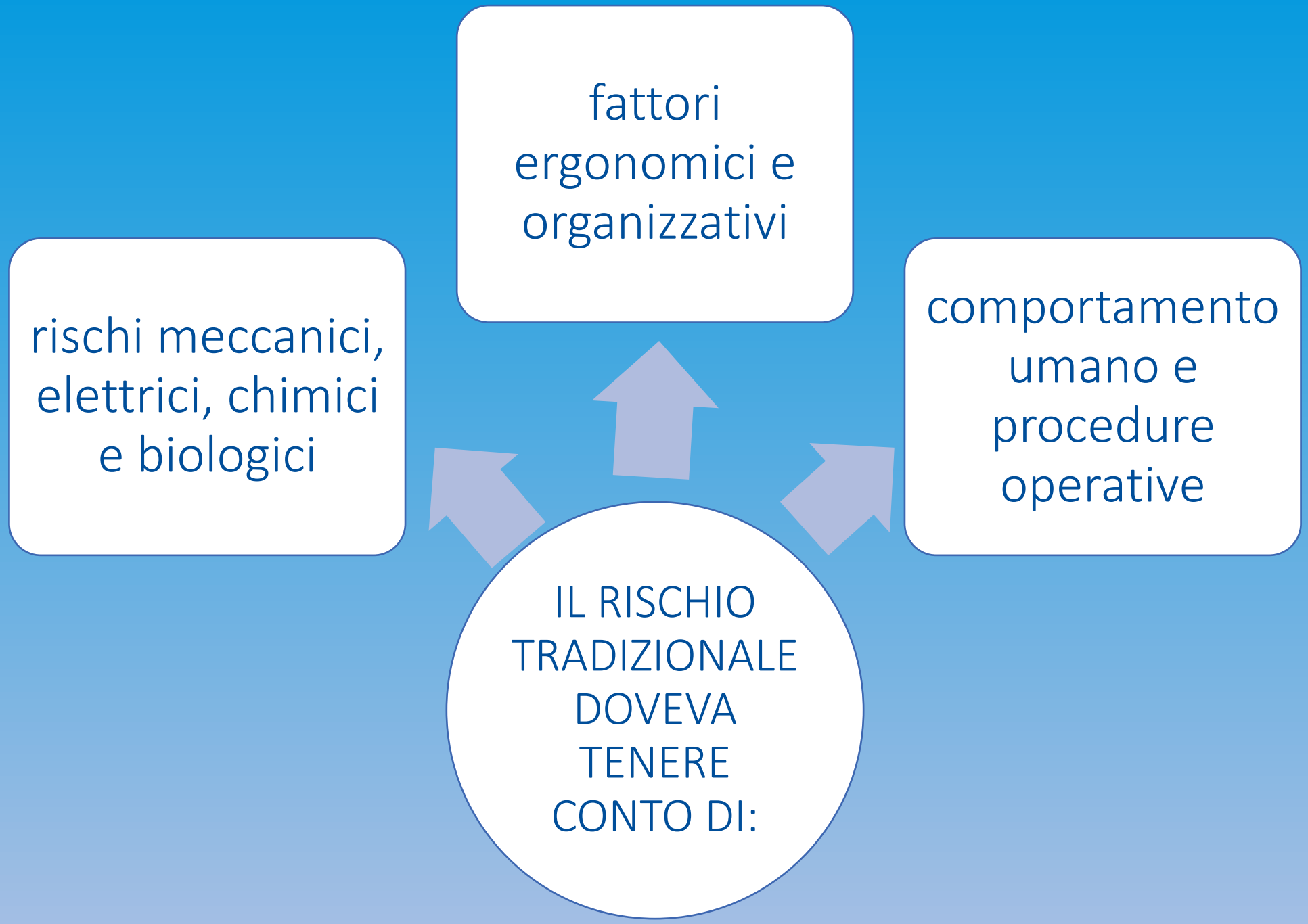
Impatto degli attacchi informatici	• Gli attacchi informatici colpiscono impianti, processi produttivi, sicurezza e responsabilità legale del management.
Nuove normative di sicurezza	• *Cyber Resilience Act,* Regolamento Macchine E AI ACT elevano gli *standard* di sicurezza e richiedono valutazioni più rigorose.
Gestione integrata del rischio *cyber*	• Le imprese devono integrare OT e *supply chain* in un controllo continuo del rischio *cyber.*
Cybersecurity come governance industriale	• La *cybersecurity* diventa un tema centrale di governance con impatti su decisioni e organizzazione aziendale.

IT ≠ OT: una differenza cruciale

OT Cyber Risk Assessment: cosa manca spesso

Mappatura accurata degli asset OT	• Spesso manca una mappatura dettagliata degli asset OT, fondamentale per una valutazione del rischio completa.
Analisi scenari di fermo impianto	• L’analisi degli impatti dovuti a fermo impianto è spesso insufficiente nelle valutazioni di rischio OT.
Coinvolgimento multidisciplinare	• Manca il coinvolgimento efficace di funzioni HSE, produzione, manutenzione e legale per valutazioni complete.
Specificità ambiente industriale	• Molte valutazioni usano modelli IT che non considerano le specificità operative dell’ambiente industriale OT.

Evoluzione nell’analisi del rischio?


fattori ergonomici e organizzativi
rischi meccanici, elettrici, chimici e biologici
comportamento umano e procedure operative
IL RISCHIO TRADIZIONALE DOVEVA TENERE CONTO DI:

RISCHIO TRADIZIONALE

RISCHIO INTEGRATO
CYBER - FISICO

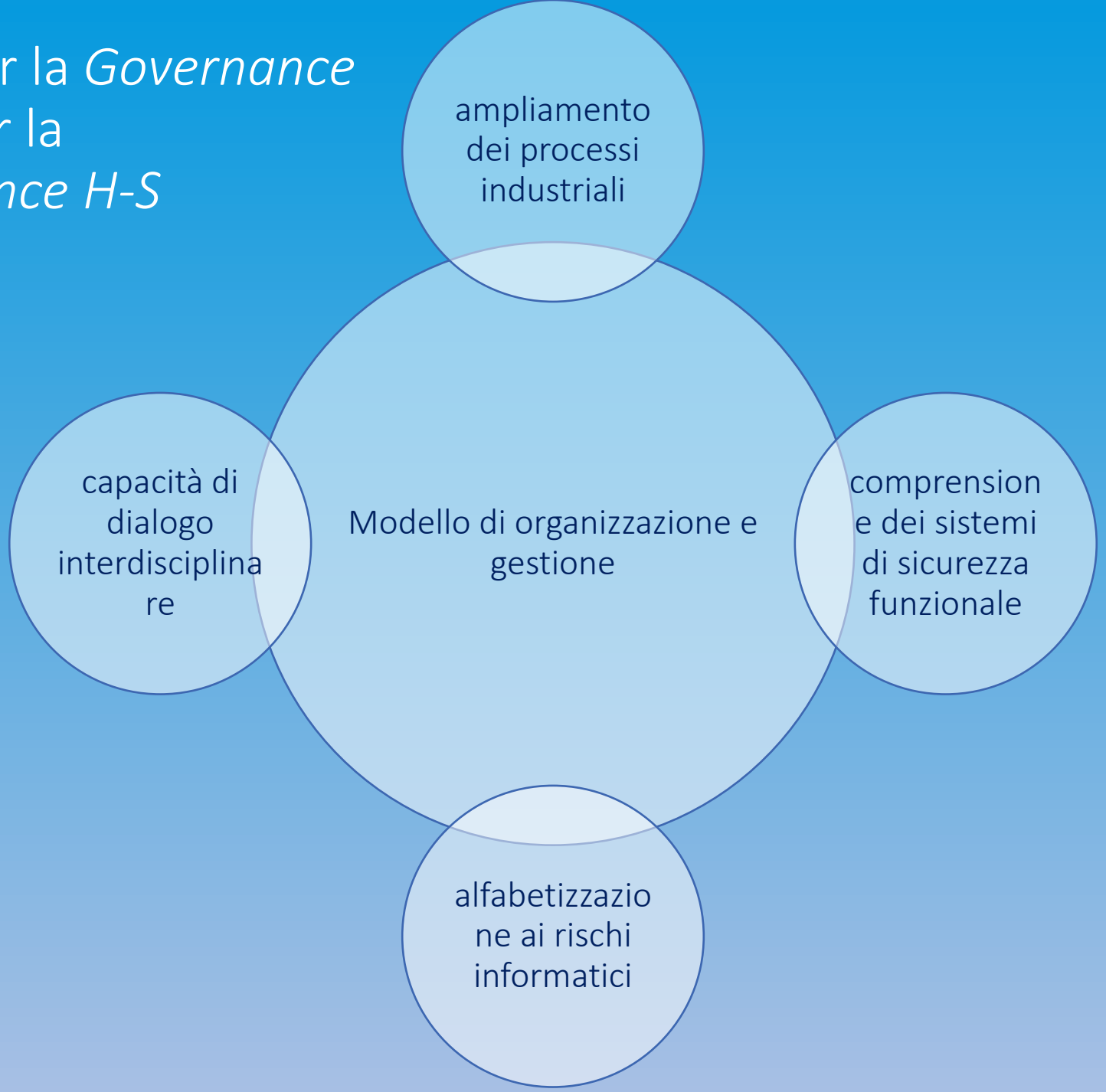
RISCHIO CYBER

Regolamento Macchine – Allegato III parte B

La valutazione del rischio e la riduzione del rischio includono i pericoli che possono manifestarsi durante il ciclo di vita della macchina o del prodotto correlato prevedibili al momento dell'immissione della macchina o del prodotto correlato sul mercato come un'evoluzione prevista del suo comportamento o della sua logica integralmente o parzialmente autoevolutivi in ragione del fatto che tale macchina o prodotto correlato è progettato per funzionare con livelli variabili di autonomia. La valutazione del rischio e la riduzione del rischio comprendono i rischi derivanti dalle interazioni tra macchine che per raggiungere uno stesso risultato sono disposte e comandate in modo da avere un funzionamento solidale, formando così una macchina come definita all'articolo 3, punto 1), lettera d).


fattori ergonomici e organizzativi
comportamento umano e procedure operative
rischi meccanici, elettrici, chimici e biologici
IL RISCHIO ODIERNO DEVE TENERE CONTO DI:
comportamento del software o dell'algoritmo

I cambiamenti per la *Governance* e per la *Governance H-S*



GRAZIE
per l'attenzione

Avv.ta Chiara Piccaglia De Eccher
Avv. Francesco Piccaglia De Eccher

Coordinatore e Segretario AIAS ER
Partners Studio Legale Piccaglia