



SIMPOSIO AFI

65° SIMPOSIO AFI **L'Industria della Salute** **nel tempo dell'Intelligenza** **Artificiale**

Rimini, 10/12 Giugno 2026

LifeScience e nuove normative EU

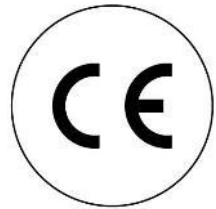
A che punto siamo?

Mario Testino - ServiTecno



Orizzonte Normativo Europeo 2026-2027

Prodotti con elementi digitali (PDE) software o hardware che abbiano una connessione dati diretta o indiretta alla rete internet.



Product
Security

Machine
Safety

Cyber
Resilience
Act (CRA)

NIS 2

Machinery
Regulation

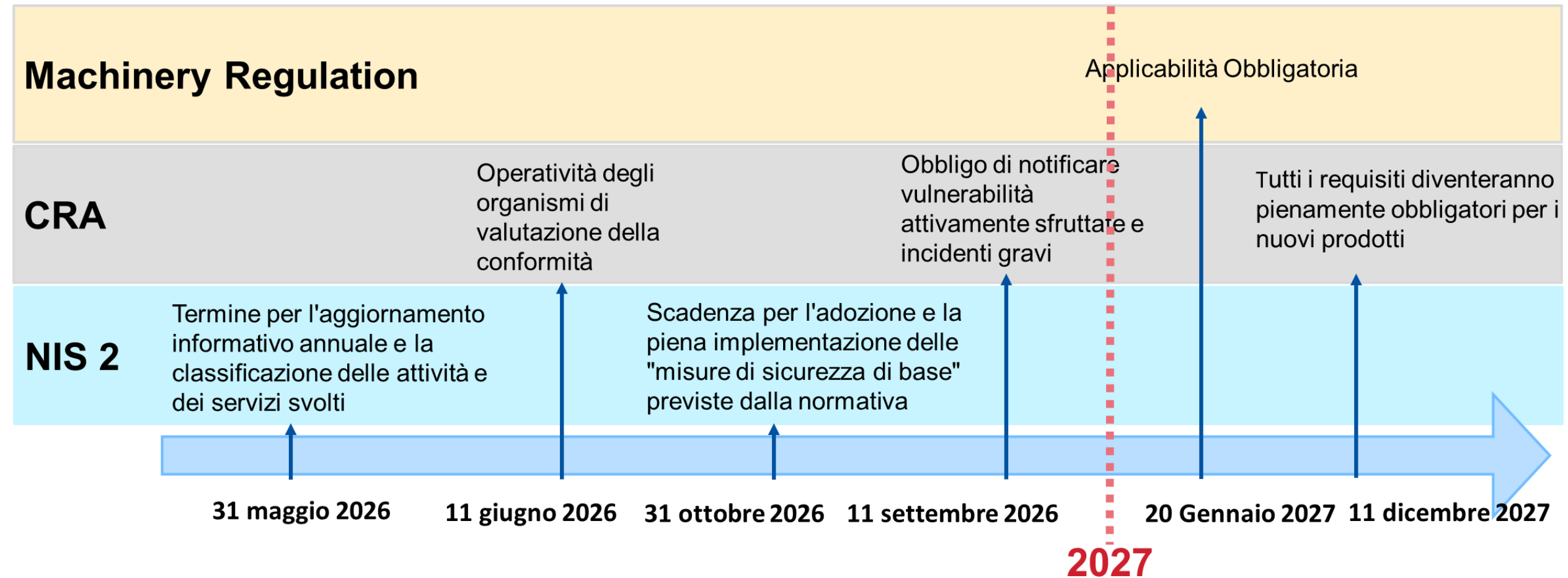
Cybersecurity
Management
System

L'organizzazione della
Cybersicurezza e la notifica
degli incidenti in azienda



Macchine, quasi macchine,
attrezzature intercambiabili,
componenti di sicurezza,
accessori di sollevamento

Orizzonte Normativo Europeo Timeline



Data and information protection
Business continuity
Incident notification

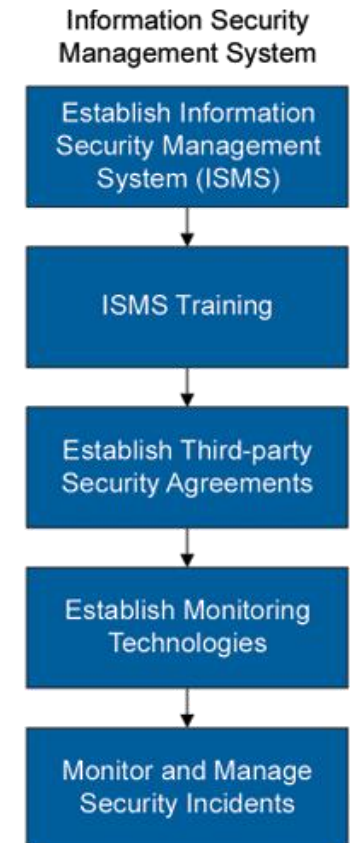
Appendix O10 – Business Continuity Management
Appendix O11 – Security Management

Framework Nazionale
per la Cybersecurity
e la Data Protection
Febbraio 2019



Appendix O10-O11

Figure 43.1



Requisiti di Base NIS 2 e impatto sull'OT

Specificità OT

Ambiti Politiche	IT	OT
Gestione del rischio.		?
Ruoli e responsabilità.		?
Affidabilità delle risorse umane.		
Conformità e audit di sicurezza.		?
Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.		?
Gestione degli asset.		?
Gestione delle vulnerabilità.		?
Continuità operativa, ripristino in caso di disastro e gestione delle crisi.		?
Gestione dell'autenticazione, delle identità digitali e del controllo accessi.		?
Sicurezza fisica		?
Formazione del personale e consapevolezza.		
Sicurezza dei dati.		?
Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.		?
Protezione delle reti e delle comunicazioni.		?
Monitoraggio degli eventi di sicurezza.		?
Risposta agli incidenti e ripristino.		?



Requisiti CRA (Cyber Resilience Act)

Progettazione e Sviluppo Sicuro (Security by Design/Default) : I prodotti devono presentare una superficie di attacco ridotta, configurazioni iniziali sicure e protezione dei dati predefinita.

Gestione del Ciclo di Vita e delle Vulnerabilità : Obbligo di disporre di processi per gestire le vulnerabilità per l'intera vita del prodotto o per un periodo di 5 anni. Questo include l'analisi continua (SAST/DAST), patch gratuite tempestive e la segnalazione delle vulnerabilità sfruttate.

Documentazione Tecnica e Trasparenza: I produttori devono redigere una documentazione tecnica dettagliata, compresa la Software Bill of Materials (SBOM), per elencare i componenti software e identificare eventuali rischi.



Cyber Resilience Act (CRA) quali prodotti

Prodotti con elementi digitali (PDE) software o hardware che abbiano una connessione dati diretta o indiretta alla rete internet.

2025/2392

REGOLAMENTO DI ESECUZIONE (UE) 2025/2392 DELLA COMMISSIONE

del 28 novembre 2025

relativo alla descrizione tecnica delle categorie di prodotti con elementi digitali importanti e critici a norma del regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

Classe I

- Sistemi di gestione dell'identità e software e hardware per la gestione degli accessi privilegiati.
- Browser autonomi e incorporati
- Sistemi di gestione delle password

Autovalutazione

Classe II

- Ipervisor e sistemi di runtime container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili
- Firewall, sistemi di rilevamento e prevenzione delle intrusioni

Coinvolgimento Organismo Accreditato

Prodotti Critici

- Dispositivi hardware con cassette di sicurezza
- Gateway per contatori intelligenti nell'ambito di sistemi di misurazione
- Carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri

Certificazione Europea (EUCC)

Automazione Industriale



SIMPOSIO EFI



Società Benefit

Regolamento Macchine e Sistemi Informatici

Macchine, quasi macchine, attrezzature intercambiabili, componenti di sicurezza, accessori di sollevamento

Integrità del software: I sistemi di comando e i software legati alla sicurezza devono essere protetti contro alterazioni accidentali o intenzionali (es. attacchi malware o accessi non autorizzati).

Identificazione del guasto: I circuiti di comando devono essere progettati in modo che guasti o difetti nella logica software non portino a situazioni pericolose.

Limiti di apprendimento: I sistemi di IA non devono apportare modifiche in fase di apprendimento che possano comportare rischi o comportamenti imprevisti non inclusi nella valutazione iniziale.

Circuiti di sicurezza: È necessario implementare limitazioni adeguate, tramite circuiti di sicurezza, per evitare che la macchina superi i limiti di rischio stabiliti.

Software
di
Controllo

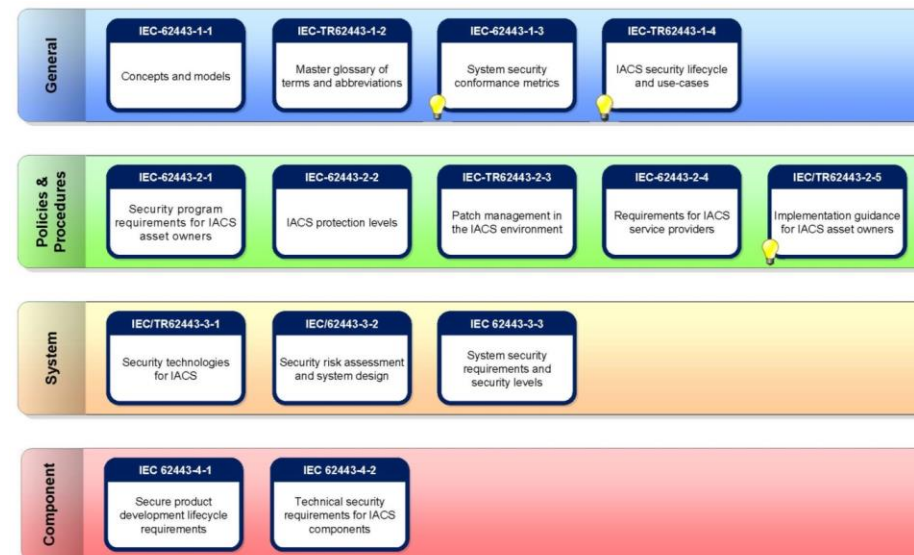
AI



ISA/IEC 62443-4-1 definizione dei requisiti del ciclo di vita per lo **sviluppo sicuro** (SDL) dei prodotti destinati ai sistemi di automazione e controllo industriale (IACS)

ISA/IEC 62443-4-2 stabilisce i requisiti tecnici di cybersecurity per i singoli **componenti** dei sistemi di automazione industriale (IACS), come PLC, sensori, gateway e HMI.

ISA/IEC 62443-3-3 è lo standard internazionale che definisce i requisiti tecnici di sicurezza informatica per i **sistemi** di automazione e controllo industriale (IACS).



TM



Annex 11 and 22 (in aggiornamento)

Gestione del rischio e ciclo di vita: L'infrastruttura IT deve essere qualificata non solo all'avvio, ma per tutto il ciclo di vita, implementando aggiornamenti continui e patch management per prevenire le vulnerabilità.

Controllo dei fornitori Grande attenzione è posta sui fornitori di servizi cloud e terze parti. Le aziende devono garantire che i partner esterni mantengano standard di sicurezza stringenti e conformi.

Protezione dell'Audit Trail: Gli audit trail sono ora protetti da requisiti più rigidi per impedire modifiche non autorizzate, garantendo che le attività degli utenti vengano monitorate, salvate e riviste regolarmente.

Annex 11

Modelli Statici e Deterministici: Divieto dell'uso di AI dinamiche (che si auto-addestrano continuamente) o di AI generative (tipo ChatGPT). Sono ammessi solo modelli statici e deterministici, cioè sistemi in cui a input identici corrispondono output identici.

No ai Sistemi "Black Box": Trasparenza totale sull'origine dei dati di addestramento e un monitoraggio continuo contro le manomissioni (data poisoning).

Integrità dei Dati e Cloud: La responsabilità sulla sicurezza e sul controllo dei modelli di AI ricade sull'azienda farmaceutica, anche quando sono gestiti da provider esterni in cloud.

Annex 22

EMA Topic 6: Cybersecurity and Outsourced activities

ISPE proposed nomination to lead and members of EFPIA working groups

Topic Group	ISPE representative	Email contact
1 Member	Margarte Leahey	Leahey, Margaret /IE margaret.leahey@sanofi.com
2 Member	BenStevens	Ben Stevens bstevens@alnylam.com
3 Member	Brandi Stockton	Brandi Stockton brandi.stockton@thetrialitygroup.com
4 LEAD	Martin Heitmann	Martin Heitmann martin.b.heitmann@mh-ca.com
5 Member	Alice Redmond	Alice Redmond alice.redmond@caiready.com
6 Member	Mario Testino	mtestino@servitecno.it



Come possiamo aiutarvi?

Mario Testino

mtestino@servitecno.it

Servitecno.it