



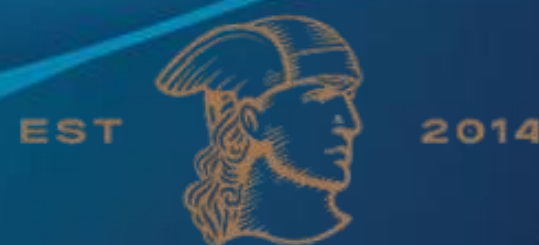
CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Cybersecurity di prodotto e governance

Dal CRA agli obblighi, ai processi e alle responsabilità aziendali



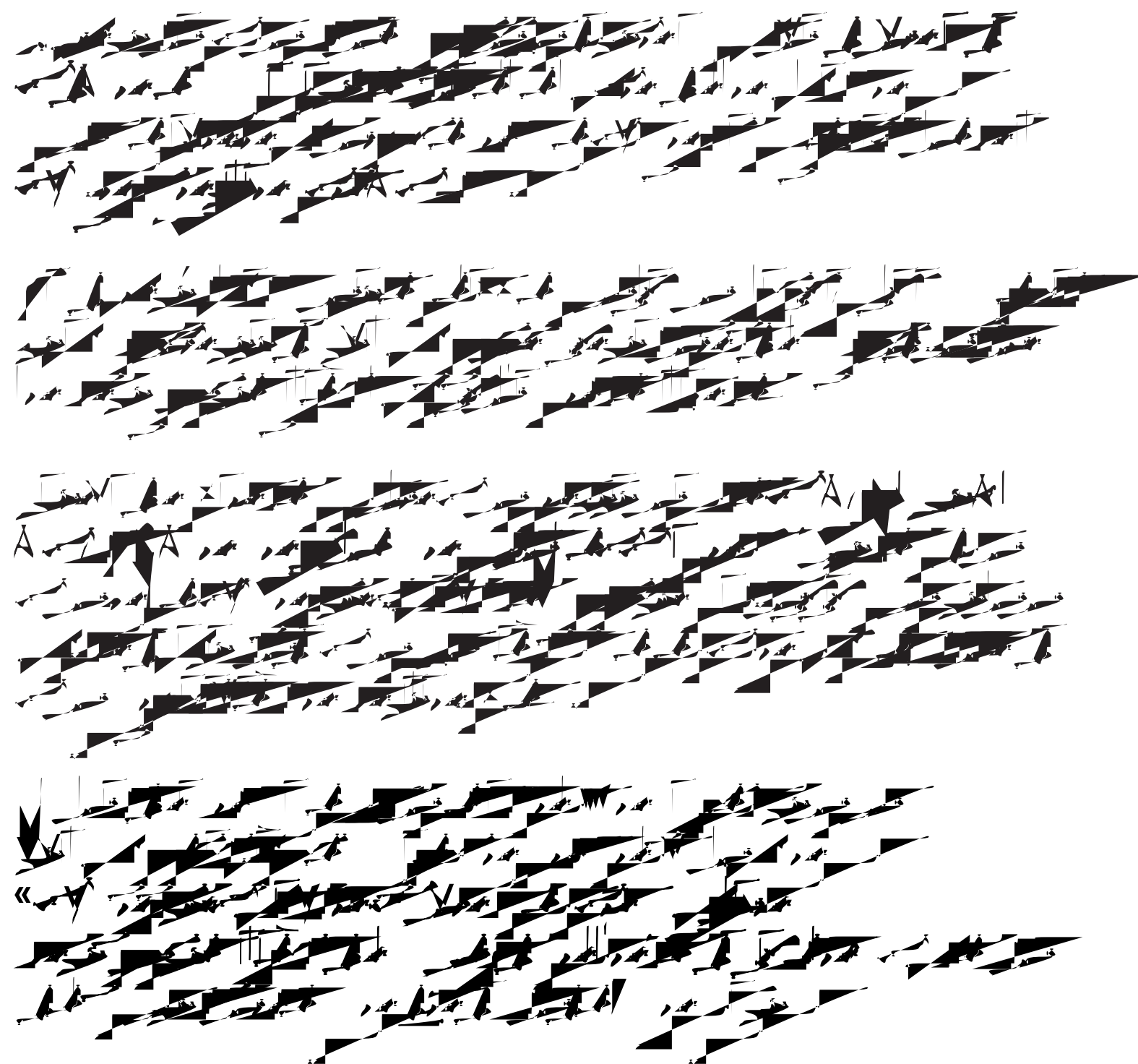
HERMES BAY

ENHANCED AWARENESS



Cybersecurity di prodotto e governance:

Dal CRA agli obblighi,
ai processi e alle
responsabilità
aziendali



CONFINDUSTRIA
VENETO EST

START4.0



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Indice

Introduzione	4
Obblighi per il CdA	13
Principi e applicazioni del CRA	22
Il panorama normativo europeo	32
Link utili	42





Rischio cyber e responsabilità aziendale



- La cybersecurity è diventata un **rischio d'impresa**
- le normative europee stanno convergendo verso un **modello comune**
- la sicurezza non può più essere affrontata solo dall'IT: **la responsabilità coinvolge direttamente l'amministrazione**

Che cosa deve fare concretamente un'organizzazione?



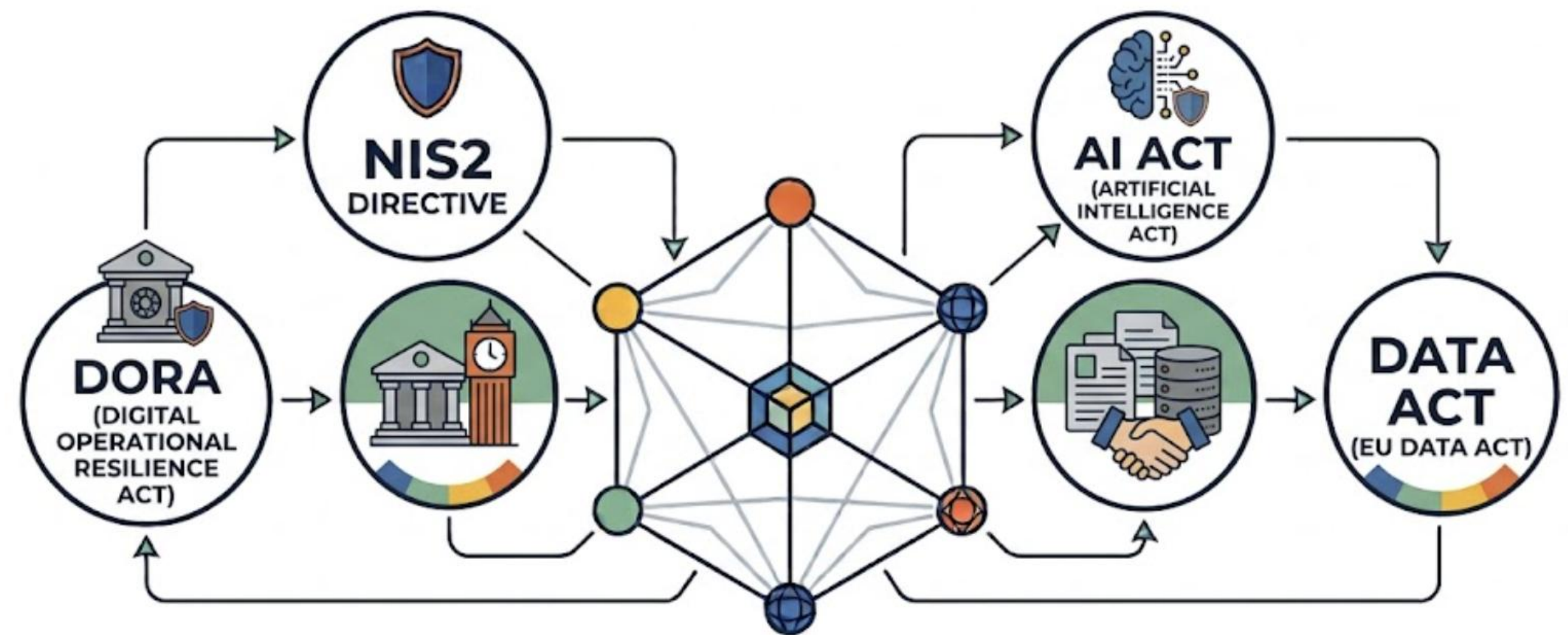


Un unico ecosistema normativo europeo

Il Cyber Resilience Act è un tassello di un ecosistema normativo europeo in costruzione, insieme a **NIS2, AI Act, Cybersecurity Act, Digital Networks Act e Regolamento Macchine**.

Ciascun atto disciplina un aspetto specifico — prodotti, reti, IA, certificazione — ma tutti condividono l'obiettivo di **innalzare la cybersicurezza nel mercato unico**.

La sfida per le imprese è l'integrazione coerente di **obblighi che si sovrappongono**.





Il Cyber Resilience Act

Negli ultimi anni l'Unione Europea ha osservato una crescita costante di:

- prodotti digitali immessi sul mercato **senza adeguati requisiti di sicurezza**
- **vulnerabilità note non corrette** per lunghi periodi
- attacchi alla **supply chain software**
- difficoltà per clienti e imprese nel valutare il livello di sicurezza dei prodotti acquistati



➔ **La sicurezza veniva spesso considerata un costo aggiuntivo anziché un requisito essenziale del prodotto.**

Il CRA nasce per cambiare questo paradigma.



Il cambio di paradigma: PRIMA

La sicurezza del prodotto non seguiva un unico standard europeo orizzontale.

- Requisiti differenti tra produttori, categorie di prodotto e settori
- Vulnerability management definito in larga parte dalle policy e dai processi del singolo produttore
- La sicurezza poteva essere affrontata soprattutto come caratteristica del prodotto al momento del rilascio, senza un obbligo orizzontale uniforme lungo l'intero ciclo di vita
- Una parte della sicurezza poteva ricadere sull'utilizzatore, attraverso configurazione, aggiornamenti e misure compensative



Il cambio di paradigma: OGGI

- Requisiti essenziali comuni di cybersecurity per i prodotti con elementi digitali immessi sul mercato UE
- Il produttore deve adottare un processo strutturato di gestione delle vulnerabilità durante il periodo di supporto
- Il prodotto deve essere progettato, sviluppato e prodotto con un livello di sicurezza adeguato al rischio
- Secure by default, protezione dagli accessi non autorizzati, protezione dei dati e possibilità di intervenire sulle vulnerabilità tramite aggiornamenti di sicurezza

Il CRA richiede, tra l'altro, che i prodotti siano immessi sul mercato senza vulnerabilità sfruttabili note, abbiano configurazioni sicure per impostazione predefinita e consentano di affrontare le vulnerabilità attraverso aggiornamenti di sicurezza.



Il cambio di paradigma: esempi concreti (1/2)

Dispositivo IoT con autenticazione debole

Un dispositivo smart permette l'accesso con una password predefinita uguale per tutti gli esemplari, oppure con credenziali facilmente prevedibili.

Prima: la sicurezza poteva dipendere dalle scelte del produttore e dall'attenzione dell'utilizzatore.

Oggi: il prodotto deve essere progettato con adeguati meccanismi di controllo degli accessi e una configurazione sicura per impostazione predefinita.



CONFINDUSTRIA
VENETO EST



Il cambio di paradigma: esempi concreti (2/2)

Dispositivo con componente vulnerabile non patchata

Un hub domestico, una telecamera o un altro dispositivo connesso utilizza una libreria software in cui viene scoperta una vulnerabilità, ma il produttore non ha predisposto un meccanismo efficace per distribuire patch.

Prima: la possibilità di intervenire poteva dipendere dalle pratiche del produttore.

Oggi: la gestione delle vulnerabilità e la disponibilità di aggiornamenti di sicurezza entrano negli obblighi del fabbricante per il periodo di supporto.



CONFINDUSTRIA
VENETO EST



Obblighi per il CdA

il Board deve:

- **approvare** le modalità di implementazione delle misure di gestione del rischio cyber;
- **sovrintendere** alla loro attuazione e al rispetto degli obblighi previsti dalla normativa;
- **seguire una formazione** in materia di cybersecurity e promuovere la formazione del personale;
- assicurare che siano disponibili **risorse, responsabilità e presidi adeguati** rispetto al livello di rischio dell'organizzazione.
- presidiare **security by design, valutazione del rischio, gestione delle vulnerabilità e aggiornamenti** lungo il ciclo di vita del prodotto.
- garantire risorse, responsabilità e processi per **conformità, documentazione, marcatura CE e reporting degli incidenti e delle vulnerabilità**.



CRA e NIS2: cosa rischia il Board

NIS2 colpisce **direttamente la persona** dell'amministratore (interdizione, sospensione); CRA colpisce **l'ente** ma la responsabilità gestoria ricade comunque sugli amministratori.

Alcune delle sanzioni previste:

- **Interdizione dalle funzioni dirigenziali** — l'amministratore può essere dichiarato temporaneamente incapace di svolgere funzioni dirigenziali all'interno dell'ente, fino all'adozione delle misure correttive (NIS2 — art. 38, D.Lgs. 138/2024).
- **Sospensione dell'operatività** — in caso di mancato adempimento alla diffida dell'ACN, l'azienda può subire la sospensione temporanea, parziale o totale, di attività o servizi, con impatto diretto su ricavi e continuità (NIS2 — art. 37, comma 4, D.Lgs. 138/2024).
- **Sanzione pecuniaria fino a 10 milioni € o 2% del fatturato mondiale** per i soggetti essenziali inadempienti (NIS2 — art. 38, D.Lgs. 138/2024).
- **Azione di responsabilità da soci, creditori o terzi** per i danni derivanti da assetti organizzativi inadeguati (CRA — principio generale ex artt. 2392-2394 c.c.).
- **Sanzione pecuniaria fino a 15 milioni € o 2,5% del fatturato mondiale** per violazione degli obblighi sugli artt. 13-14 (CRA — art. 64, par. 2).





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Obblighi per il CdA



Fabbricanti, importatori, distributori

I fabbricanti

Devono **valutare la conformità** su base **valutazione del rischio** secondo procedure indicate nell'art. 24 a seguito delle quali possono (e devono) apporre il **marchio CE**.
Prevedere security by design, produrre documentazione adeguata, seguire i prodotti e i loro aggiornamenti al variare delle minacce per la durata del prodotto o per almeno 5 anni, relazionarsi con autorità di vigilanza e organismi di valutazione della conformità.
Se assemblano prodotti di altri verificano la loro conformità prioritariamente.



I rappresentanti autorizzati

Hanno obblighi solo formali legati alla documentazione.

Gli importatori

Hanno obblighi formali e documentali di controllo e di relazione con le autorità locali.

Autorità di vigilanza e organismi notificati

Autorità di vigilanza

Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un prodotto con elementi digitali, compresa la relativa gestione delle vulnerabilità, presenti un rischio di sicurezza cibernetica significativo, essa effettua una valutazione del prodotto con elementi digitali interessato per quanto riguarda la sua conformità a tutti i requisiti di cui al presente regolamento.



Classe I - Valutazione di conformità

Viene fatta dal fabbricante su sua esclusiva responsabilità secondo requisiti minimi e procedure definite con produzione di documentazione completa e adeguata e aggiornamento continuo.

Se non completa o se standard assenti



CONFINDUSTRIA
VENETO EST

Procedura

Classe I - Valutazione di conformità per prodotti critici

Nel caso di non conformità o impossibilità di definire la conformità entra in azione l'organismo di valutazione e il fabbricante collabora con l'organismo secondo la procedura definita «modulo B e modulo C» o la valutazione della conformità basata sulla garanzia della qualità totale.

Classe II - Valutazione di conformità



Viene fatta direttamente dal fabbricante con l'organismo di valutazione secondo la procedura definita «modulo B e modulo C» o la valutazione della conformità basata sulla garanzia della qualità totale.

16



Gli obblighi di governance per il CdA

Per garantire la conformità, il management deve assicurare:

- **Assetti organizzativi adeguati** per gestire gli obblighi previsti dal CRA
- **Ruoli e responsabilità definiti** per la sicurezza del prodotto e la gestione delle vulnerabilità
- **Valutazione dei rischi cyber** con impatto sul prodotto e sul business





Dai requisiti all'implementazione tecnica

Il fabbricante deve dimostrare **come ogni requisito di sicurezza è stato applicato nel prodotto**.

Deve quindi predisporre:

•**Matrice di tracciabilità**: collegamento tra requisiti dell'Allegato I e componenti, funzioni o misure implementate

•**Evidenze tecniche**: configurazioni, risultati di test, codice, procedure e verifiche che dimostrano l'applicazione dei requisiti

•**Analisi dei requisiti non applicabili**: ogni esclusione deve essere motivata e documentata

ALLEGATO I

REQUISITI ESSENZIALI DI CIBERSICUREZZA

Parte I Requisiti di cibersecurity relativi alle proprietà dei prodotti con elementi digitali

- 1) I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersecurity in base ai rischi.
- 2) Sulla base della valutazione dei rischi di cibersecurity di cui all'articolo 13, paragrafo 2, e ove applicabile, i prodotti con elementi digitali:
 - a) sono messi a disposizione sul mercato senza vulnerabilità sfruttabili note;
 - b) sono messi a disposizione sul mercato con una configurazione sicura per impostazione predefinita, salvo diverso accordo tra il fabbricante e l'utilizzatore commerciale in relazione a un prodotto su misura con elementi digitali, con la possibilità di ripristinare il prodotto allo stato originale;
 - c) garantiscono che le vulnerabilità possano essere affrontate mediante aggiornamenti di sicurezza, anche, se del caso, mediante aggiornamenti di sicurezza automatici installati entro un periodo di tempo adeguato, abilitato come impostazione predefinita, con un meccanismo di disattivazione chiaro e di facile utilizzo, attraverso la notifica agli utilizzatori degli aggiornamenti disponibili e la possibilità di rinviarli temporaneamente;
 - d) garantiscono la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo, tra cui, a titolo esemplificativo ma non esaustivo, sistemi di autenticazione e di gestione dell'identità o dell'accesso, e segnalano eventuali accessi non autorizzati;
 - e) proteggono la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, ad esempio criptando i pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia, e utilizzando altri mezzi tecnici;
 - f) proteggono l'integrità dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni;
 - g) trattano solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione alla finalità prevista del prodotto con elementi digitali («minimizzazione dei dati»);
 - h) proteggono la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di attenuazione contro gli attacchi di negazione del servizio (*denial of service*);



CONFINDUSTRIA
VENETO EST



Supporto e aggiornamenti

il fabbricante deve garantire la sicurezza del prodotto durante tutto il periodo di supporto.

Deve quindi definire processi per:

- **Gestione delle vulnerabilità:** identificazione, analisi e correzione delle vulnerabilità rilevate
- **Distribuzione degli aggiornamenti di sicurezza:** rilascio tempestivo delle correzioni necessarie alla protezione del prodotto
- **Informazione agli utilizzatori:** comunicazione della disponibilità degli aggiornamenti e delle indicazioni necessarie per applicarli





La Direttiva NIS2: gli obblighi di gestione

La NIS2 attribuisce una responsabilità diretta agli organi di gestione dei soggetti essenziali e importanti.



Gli organi di gestione devono:

- **approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica;**
- **sovrintendere all'implementazione degli obblighi** previsti dalla normativa;
- **rispondere delle violazioni** degli obblighi previsti dal D.Lgs. 138/2024;
- **seguire una formazione in materia di sicurezza informatica;**
- promuovere una **formazione periodica in materia di sicurezza informatica per i dipendenti.**



Notifica incidenti: cosa deve presidiare il CdA

CRA — Reg. UE 2024/2847, artt. 13-14

Il Board è garante della conformità. L'obbligo formale ricade sul fabbricante, ma il CdA deve assicurare processi, responsabilità e risorse.

- Designare 1 rappresentante primario e fino a 20 secondari per la Single Reporting Platform (ENISA)
- Garantire risorse e processi per il rispetto dei termini
- Presidiare la supply chain nel processo di segnalazione
- Approvare la Dichiarazione UE di Conformità
- Oggetto della notifica: vulnerabilità attivamente sfruttate e incidenti gravi.

NIS2 — D.Lgs. 138/2024, artt. 23 e 25;

Il CdA è soggetto attivo della notifica. La responsabilità della segnalazione è stata trasferita direttamente su dirigenti e amministratori.

- Definire chi, tra i delegati, ha il potere di valutare se un incidente è segnalabile
- Approvare il runbook di escalation e notifica al CSIRT Italia
- Ricevere informazioni tempestive sugli incidenti
- Tenere un decision log aggiornato e consultabile
- Il termine decorre dalla verifica dell'autorità delegata



CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

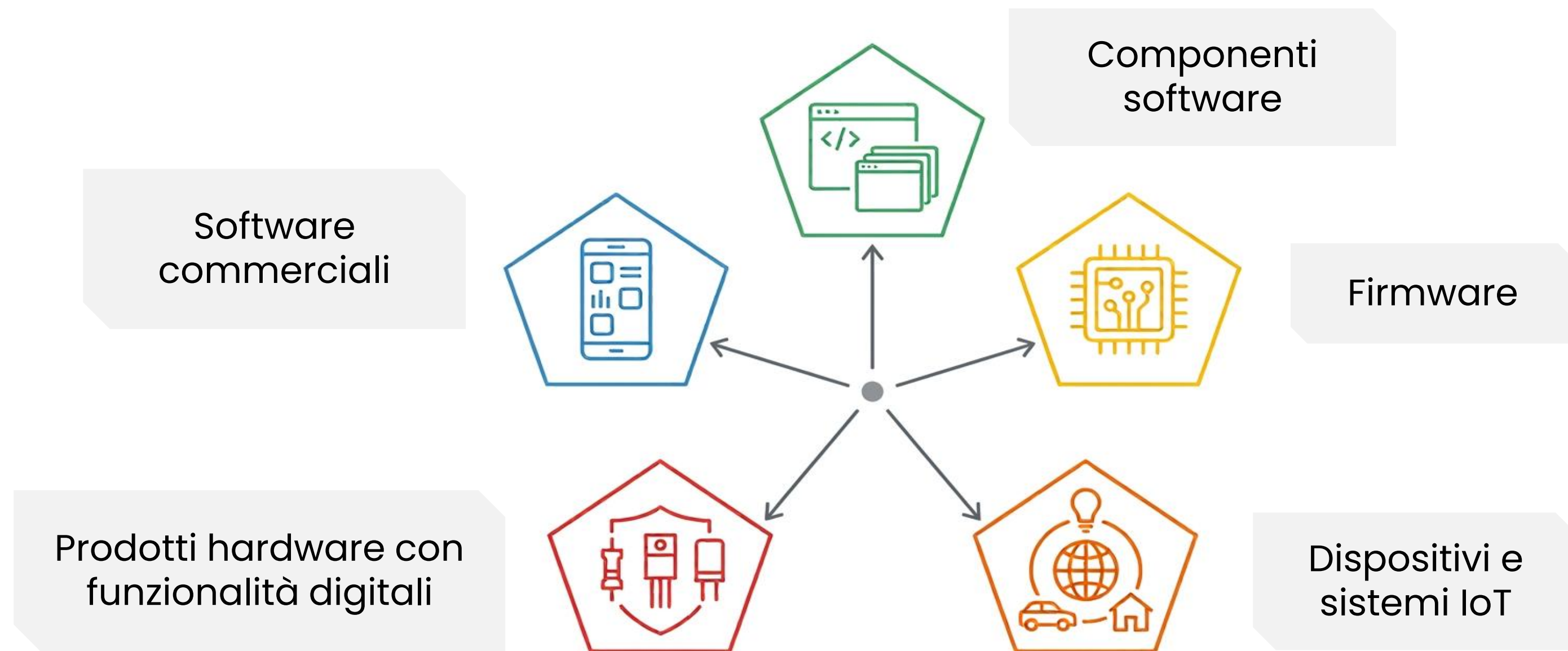
START4.0

Principi e applicazioni del CRA





A chi si applica il CRA?



Il CRA riguarda chiunque immetta sul mercato europeo prodotti che incorporano elementi digitali.



CONFINDUSTRIA
VENETO EST



Software e SaaS

Il CRA si applica ai **software immessi sul mercato come prodotti**, ad esempio applicazioni desktop, app mobili o altri software destinati a essere installati ed eseguiti sui sistemi dell'utilizzatore, purché soddisfino i requisiti previsti dal Regolamento.

Diverso è il caso del **SaaS standalone**: quando il software viene fornito esclusivamente come servizio ed è eseguito sull'infrastruttura del fornitore, il servizio non rientra di per sé nel CRA.

Il discorso cambia quando il software remoto costituisce una **“remote data processing solution” necessaria al funzionamento di un prodotto con elementi digitali**. In questo caso, il servizio remoto può rientrare nel perimetro del CRA insieme al prodotto.

Esempio: un dispositivo IoT che necessita del backend cloud sviluppato dal proprio fabbricante per svolgere una delle sue funzioni rientra nel CRA anche rispetto a quella componente remota.



Firmware e software embedded

Il **firmware integrato in un dispositivo** rientra nel CRA quando fa parte di un prodotto con elementi digitali che soddisfa i requisiti del Regolamento. È il caso, ad esempio, di router, sensori IoT, dispositivi industriali e altri prodotti con funzionalità digitali e connessione a dispositivi o reti.

Anche il **firmware immesso separatamente sul mercato** può costituire un prodotto con elementi digitali, quando è destinato a essere integrato in un sistema elettronico.

Non tutto il firmware, però, ricade automaticamente nel CRA: un dispositivo che utilizza firmware esclusivamente per funzioni locali e **non presenta una connessione, diretta o indiretta, a dispositivi o reti** può essere escluso dal campo di applicazione.

Esempio: il firmware di un sensore IoT connesso alla rete rientra nel perimetro; il firmware di un semplice dispositivo elettronico autonomo che svolge esclusivamente funzioni locali può invece esserne escluso.





Gli obblighi del produttore





La sicurezza lungo l'intero ciclo di vita del prodotto

Il CRA introduce un principio fondamentale:

La cybersecurity deve essere **integrata** nel prodotto **fin dalle prime fasi del suo sviluppo** e **mantenuta per tutto il ciclo di vita**.

Il fabbricante deve garantire che il prodotto rimanga sicuro durante tutto il periodo previsto di utilizzo.





Fasi del ciclo di vita

1. Progettazione

Analisi dei rischi cyber
Definizione dei requisiti di sicurezza
Scelte architettureali coerenti con il rischio

3. Immissione sul mercato

Valutazione di conformità
Documentazione tecnica
Informazioni di sicurezza per gli utilizzatori

5. Fine supporto

Comunicazione trasparente della fine del supporto
Gestione del rischio residuo

2. Sviluppo

Secure coding
Verifica delle dipendenze software
Test e valutazioni di sicurezza

4. Post-market

Monitoraggio delle vulnerabilità
Gestione delle segnalazioni
Rilascio degli aggiornamenti di sicurezza

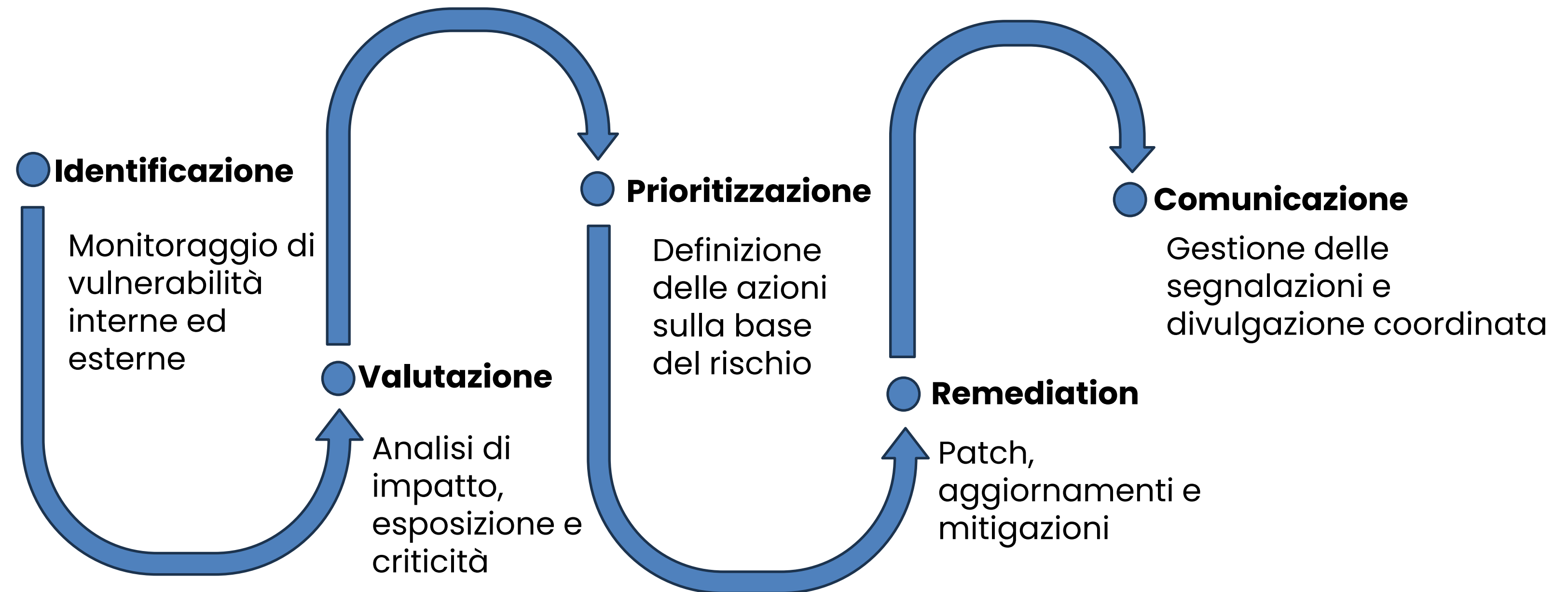


CONFINDUSTRIA
VENETO EST



Vulnerability Management

Un processo efficace comprende:





Aggiornamenti: comunicazione e tracciabilità

Il CRA rende l'aggiornamento un elemento verificabile e documentato.

Comunicazione agli utenti

Le informazioni devono essere **chiare e accessibili**:

- vulnerabilità risolte
- problemi corretti
- modalità di installazione dell'aggiornamento



Tracciabilità degli aggiornamenti

Il fabbricante deve mantenere evidenza di:

- versioni software/firmware rilasciate
- modifiche introdotte
- vulnerabilità corrette
- periodo di disponibilità del supporto



CONFINDUSTRIA
VENETO EST



Security by Design e by Default

Security by Design:

La sicurezza viene considerata **fin dalla progettazione** del prodotto.

- analizzare i rischi cyber prima dello sviluppo;
- identificare minacce e vulnerabilità potenziali;
- progettare architetture e funzionalità resilienti;
- ridurre la superficie di attacco.

Security by Default

Il prodotto deve essere fornito con **configurazioni di base che garantiscano un livello adeguato di sicurezza.**

- impostazioni sicure predefinite;
- minimizzazione dei privilegi;
- servizi non necessari disabilitati;
- protezione delle credenziali;





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Il panorama normativo Europeo





La Direttiva NIS2



La **Direttiva (UE) 2022/2555 (NIS2)** stabilisce un quadro comune europeo per innalzare il livello di cibersecurity degli Stati membri e delle organizzazioni che operano in settori critici.

La direttiva amplia significativamente il perimetro rispetto alla precedente NIS, includendo nuovi settori e un numero maggiore di soggetti. Impone alle organizzazioni interessate **misure di gestione del rischio cyber**, obblighi di **notifica degli incidenti**, responsabilità degli organi di gestione e requisiti di supervisione e cooperazione tra le autorità nazionali.

L'obiettivo è quindi proteggere **reti, sistemi informativi e servizi essenziali**, intervenendo principalmente sulla sicurezza delle organizzazioni che li gestiscono.

Entrata in vigore: 16 gennaio 2023

Applicazione negli Stati membri: dal 18 ottobre 2024.



CONFINDUSTRIA
VENETO EST



Il CRA e la Direttiva NIS2



Il **CRA** e la **NIS2** sono normative complementari, ma intervengono su ambiti differenti:

- il **CRA** disciplina la **sicurezza dei prodotti con elementi digitali**, imponendo ai fabbricanti requisiti di cybersecurity lungo tutto il ciclo di vita del prodotto;
- la **NIS2** disciplina la **sicurezza di reti e sistemi informativi degli enti essenziali e importanti**, imponendo obblighi di gestione del rischio cyber a livello organizzativo.

Il CRA agisce **a monte della catena del valore**, richiedendo che hardware e software siano progettati, sviluppati e mantenuti sicuri.

La NIS2 agisce **sull'organizzazione che utilizza tali tecnologie**.

Un'organizzazione può essere soggetta a entrambi i regolamenti: in questo caso deve garantire sia la **sicurezza intrinseca dei prodotti sviluppati (CRA)** sia una **adeguata governance del rischio cyber interno (NIS2)**.



Il CRA e la NIS2 a confronto



CONFINDUSTRIA
VENETO EST



AI Act

Il **Regolamento (UE) 2024/1689 (AI Act)** introduce il primo quadro normativo europeo generale sull'intelligenza artificiale.

La disciplina adotta un **approccio basato sul rischio**: gli obblighi variano in funzione del livello di rischio associato al sistema di IA. Prevede il divieto di determinate pratiche, requisiti specifici per i sistemi ad alto rischio, obblighi di trasparenza per determinati sistemi e regole specifiche per i modelli di IA per finalità generali.

Per i sistemi ad alto rischio sono previsti, tra gli altri, requisiti relativi a **gestione del rischio, dati, documentazione, registrazione, supervisione umana, accuratezza, robustezza e cybersecurity**.

Entrata in vigore: 1° agosto 2024

Applicazione: progressiva dal 2 febbraio 2025; la maggior parte delle disposizioni si applica dal 2 dicembre 2027, con ulteriori scadenze fino al 2028.





Il CRA e l'AI Act

Il rapporto con il CRA nasce quando l'AI è integrata in un **prodotto con elementi digitali**:

- **AI Act** → disciplina il sistema di intelligenza artificiale (rischi, dati, trasparenza, supervisione umana, governance);
- **CRA** → disciplina la sicurezza informatica del prodotto che incorpora l'AI (vulnerabilità, aggiornamenti, protezione da compromissioni).

I due regolamenti sono quindi **complementari**: uno governa il rischio dell'AI, l'altro la sicurezza cyber del prodotto.

Inoltre, Il CRA contiene una disposizione specifica per i **prodotti con elementi digitali che sono anche sistemi di IA ad alto rischio**.





Il Cybersecurity Act (CSA)

Il **Regolamento (UE) 2019/881 (Cybersecurity Act)** rafforza il ruolo dell'**ENISA**, e istituisce un quadro europeo per la **certificazione della cibersicurezza**.

Il regolamento attribuisce a ENISA un **mandato permanente** e un ruolo centrale nella cooperazione europea e nella gestione delle crisi cyber. Introduce inoltre l'**European Cybersecurity Certification Framework**, attraverso il quale possono essere sviluppati schemi europei di certificazione per prodotti, servizi e processi ICT.



L'obiettivo è creare criteri comuni a livello europeo e ridurre la frammentazione dei sistemi nazionali di certificazione.

Entrata in vigore: 27 giugno 2019

Applicazione di alcune disposizioni sulla certificazione: dal 28 giugno 2021.



Il CRA e il Cybersecurity Act (CSA)

La certificazione CSA rimane uno **strumento volontario**: dimostra un determinato livello di sicurezza secondo uno schema europeo.

Il CRA integra il CSA: una certificazione ottenuta tramite uno schema CSA riconosciuto può fornire **presunzione di conformità** ai requisiti essenziali del CRA.

Il CRA prevede infatti che:

- I prodotti con elementi digitali certificati secondo determinati **schemi europei di certificazione** possano beneficiare di una **presunzione di conformità** ai requisiti del CRA
- Per determinati prodotti, un certificato europeo almeno al livello di garanzia **“substantial”** può eliminare l’obbligo di una distinta valutazione di conformità da parte di terzi per i requisiti coperti dal certificato





CYBERSECURITY ACT 2

Il nuovo Cybersecurity Act (CSA2)

Cosa cambia con il CSA 2?

- **Dalla teoria alla pratica:** Il CSA 2 supera i vecchi schemi generici, introducendo **schemi di certificazione specifici per categorie di prodotti**, ricalcati esattamente sui requisiti del CRA.
- **Presunzione di conformità automatica:** Il CSA 2 definisce le regole per cui una certificazione (es. EUCC o i nuovi schemi IoT) soddisfa *direttamente* i requisiti obbligatori del CRA, azzerando i tempi di audit.
- **Principio di reciprocità "One-Stop-Shop":** Una sola certificazione sotto CSA 2 copre contemporaneamente i requisiti di prodotto (CRA), di catena di fornitura (NIS2) e finanziari (DORA).



CONFINDUSTRIA
VENETO EST



Il Digital Networks Act

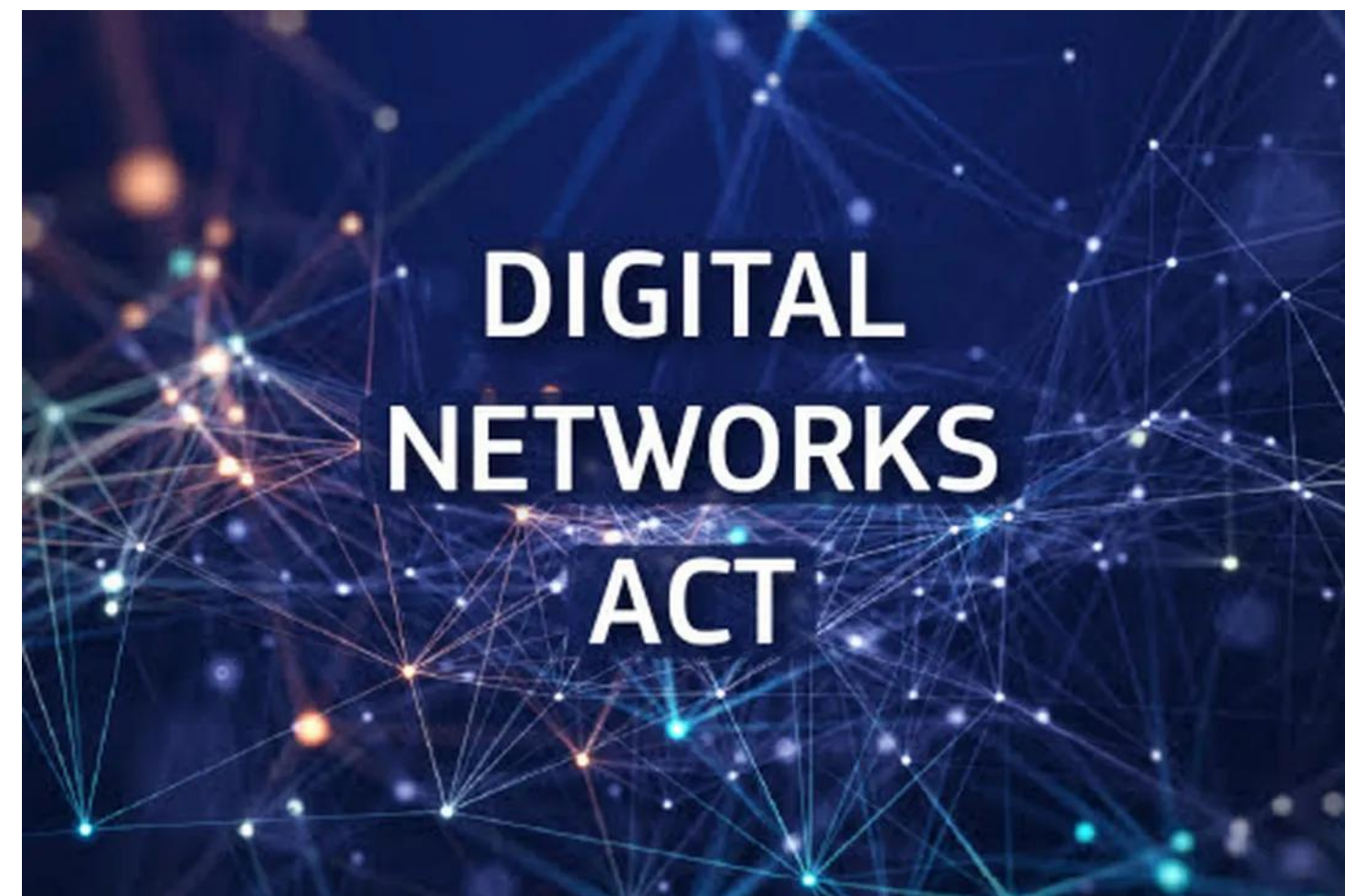
Il **Digital Networks Act (DNA)** è la proposta di regolamento presentata dalla Commissione europea nel gennaio 2026 per modernizzare e armonizzare il quadro europeo delle comunicazioni elettroniche.

La proposta mira a **sostituire il Codice europeo delle comunicazioni elettroniche**, riducendo la frammentazione normativa e creando condizioni più omogenee per gli operatori delle reti.

Il DNA interviene, tra l'altro, su **reti ad alta capacità, fibra, 5G, accesso alle infrastrutture e servizi TLC**, con l'obiettivo di favorire gli investimenti e lo sviluppo di un mercato unico della connettività. La proposta contiene inoltre misure relative alla **sicurezza e resilienza delle reti** e alla riduzione delle dipendenze nella catena di fornitura.

Stato: proposta legislativa, **non ancora in vigore**.

Presentazione della proposta: 21 gennaio



CONFINDUSTRIA
VENETO EST



Il CRA e il Digital Networks Act

Il DNA e il CRA intervengono su due componenti dello stesso ecosistema digitale:

- il **DNA** aumenta la resilienza delle **reti e delle infrastrutture di comunicazione** che permettono ai servizi digitali di funzionare;
- il **CRA** garantisce che i **prodotti connessi a tali reti** non introducano vulnerabilità nella catena digitale.

Un apparato di rete può quindi essere sottoposto ai requisiti del CRA in quanto **prodotto con elementi digitali**, mentre l'utilizzo dell'apparato all'interno di una rete e gli obblighi del relativo operatore possono ricadere nel quadro del DNA.

La conformità al CRA non sostituisce gli obblighi applicabili alla rete o al suo operatore: le due discipline agiscono su **livelli differenti e complementari**.

DIGITAL NETWORKS ACT



CONFINDUSTRIA
VENETO EST



Regolamento Macchine

Il **Regolamento (UE) 2023/1230** stabilisce i requisiti di **salute e sicurezza** che devono essere rispettati nella progettazione e costruzione di macchine e prodotti correlati immessi sul mercato o messi in servizio nell'Unione europea.

Il regolamento sostituisce la precedente **Direttiva Macchine 2006/42/CE** e mantiene il principio secondo cui i prodotti devono soddisfare requisiti essenziali di sicurezza prima di poter circolare nel mercato europeo.

La nuova disciplina tiene conto anche dell'evoluzione tecnologica delle macchine, comprese le **macchine con componenti digitali e sistemi di controllo**, e introduce requisiti aggiornati per affrontare i rischi derivanti dalle nuove tecnologie.

Entrata in vigore: 19 luglio 2023

Applicazione generale: dal 14 gennaio 2027.



CONFINDUSTRIA
VENETO EST



Il CRA e il Regolamento Macchine

Il rapporto tra le due discipline riguarda soprattutto i rischi cyber che possono avere effetti sulla **sicurezza della macchina**:

Il CRA impone requisiti di cybersecurity sul prodotto e sul relativo **ciclo di vita**, mentre Il Regolamento Macchine considera anche la **protezione dei sistemi di controllo** dagli effetti che una compromissione digitale può avere sulla sicurezza della macchina.

Il Regolamento Macchine prevede una **presunzione di conformità** per alcuni requisiti di sicurezza quando la macchina è certificata secondo determinati schemi europei di cybersecurity previsti dal Cybersecurity Act. La stessa attività di valutazione del rischio e la documentazione tecnica possono quindi essere utilizzate come base per affrontare gli adempimenti delle due normative.





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Link utili

- **Cyber Resilience Act**, documento PDF integrale in italiano:

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202402847

- Libro «**Cybersecurity e Governance**: Ruoli e responsabilità del Board nell'era digitale»:

<https://amoz.onl/79J>





CONFINDUSTRIA
VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

START4.0

Grazie.

Dott. Ing. Luisa Franchina
CEO

Via Nazionale, 214 - 00184 Roma
l.franchina@hermesbay.com
3387815902

HERMESBAY.COM

