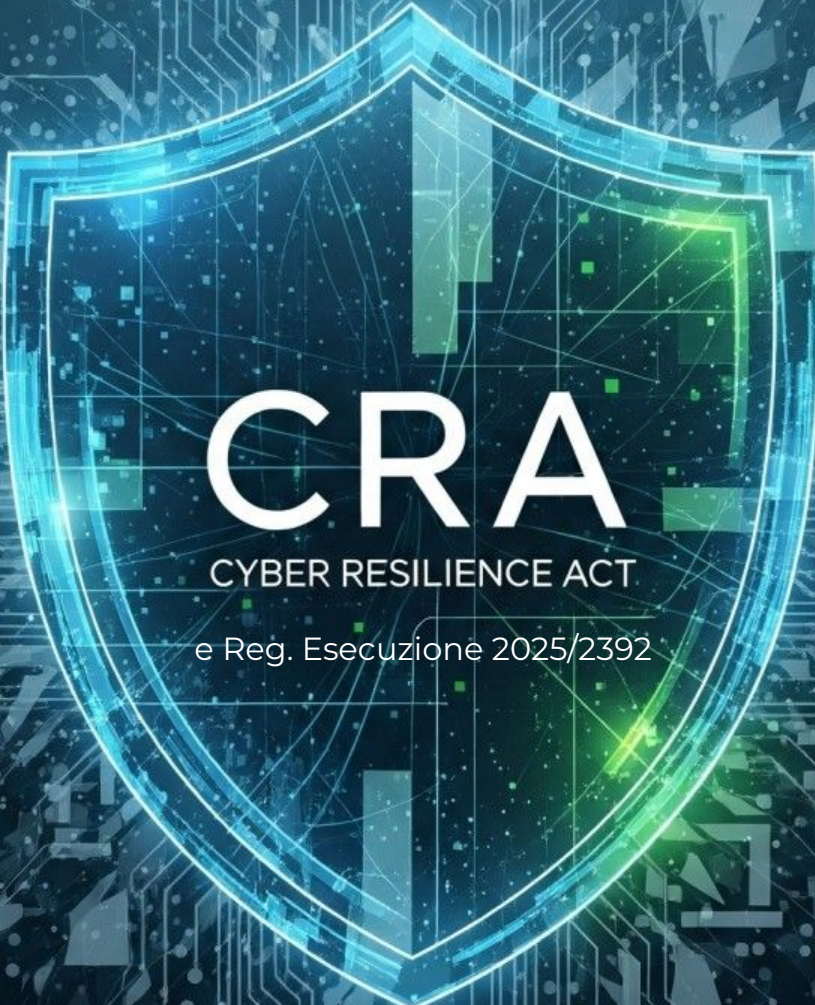




CRA

CYBER RESILIENCE ACT

e Reg. Esecuzione 2025/2392

Il CRA in sintesi



Cosa è

Regolamento che prevede requisiti di cyber security dei prodotti con elementi digitali.

Si applica a qualsiasi prodotto, hw o sw, che abbia una **connessione dati**, diretta o indiretta, a un dispositivo o a una rete, immesso sul mercato UE nel corso di un'attività commerciale.

Obiettivo

- garantire un livello adeguato di sicurezza informatica
- mantenuto per tutta il ciclo di vita del prodotto, con obblighi di gestione delle vulnerabilità, notifica degli incidenti e aggiornamenti di sicurezza.



Obiettivi

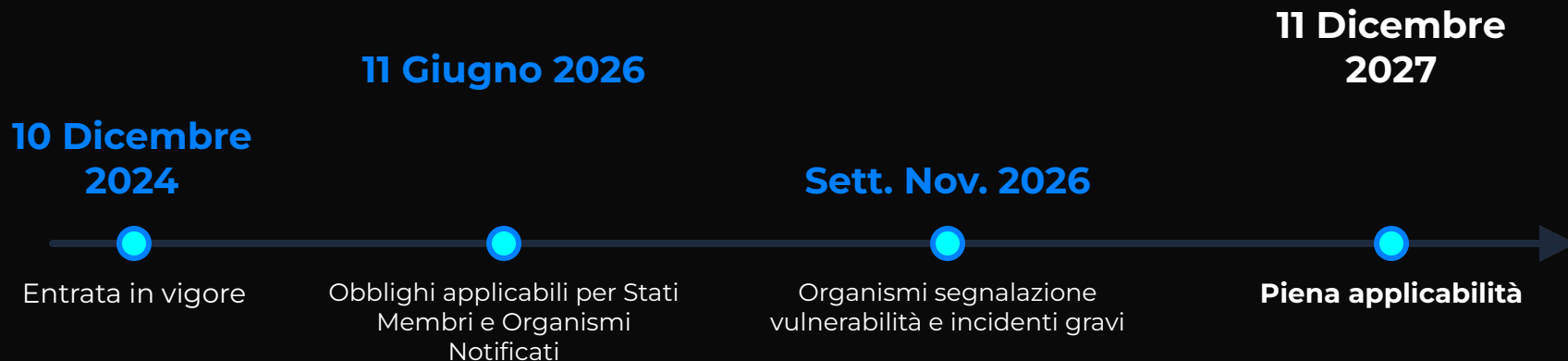
- ✓ **Migliorare la sicurezza dei prodotti con elementi digitali (PED)**
 - Progettazione e sviluppo
 - Intero ciclo di vita
- ✓ **Fornire quadro coerente in UE per facilitare conformità**
- ✓ **Migliorare trasparenza delle proprietà di sicurezza**



Capacità di scambiare informazioni



Timeline di Attuazione



3 “direzioni”

- ✓ **Framework comune di requisiti** essenziali per tutti i PED
- ✓ **Approccio basato sui rischi**
- ✓ **Approccio di sicurezza** dei prodotti



Non si applica

SaaS, PaaS, IaaS, **con precisazioni**

Software Open Source, **se non in ambito commerciale**

Dispositivi medici, medico diagnostici in vitro

Sicurezza autoveicoli

Sicurezza aviazione e nautica

Sicurezza nazionale e settore militare

Se le soluzioni sw sono necessarie per svolgere una delle sue funzioni: rientra

Se fornito per distribuzione o utilizzo nel corso di un'attività commerciale: rientra





Framework comune



- ✓ Framework comune di requisiti essenziali per tutti i PED
- ✓ Approccio basato sui rischi
- ✓ Approccio di sicurezza dei prodotti

Prodotti con elementi digitali



Un prodotto software o hardware e le sue soluzioni di elaborazione dati a distanza, compresi i componenti software o hardware immessi sul mercato separatamente

Prodotti con elementi digitali messi a disposizione sul mercato, la cui destinazione o il cui uso ragionevolmente prevedibile comprende una **connessione di dati logica o fisica diretta o indiretta a un dispositivo o a una rete**

Prodotti CT: portatili, smartphone, microprocessori, routers e dispositivi smart, software stand alone, firewall, App mobile, videogames, sistemi AI, applicazioni desktop



Software “stand alone”

Si considera immesso sul mercato nel momento in cui il produttore lo rende **per la prima volta disponibile per distribuzione o uso** sul mercato UE, nel corso di un'attività commerciale.



Aggiornamenti Nuovo prodotto

Solo le iterazioni con **modifica sostanziale** sono considerate nuovo prodotto.

Nuovi obblighi di valutazione della conformità



Solo per sw via canali digitali



Aggiornamenti

Nuovo prodotto

Supporto fisico

Hw - Sw forniti separati

Immissione sul
mercato

Consegna





- ✓ Framework comune di requisiti essenziali per tutti i PED
- ✓ Approccio basato sui rischi
- ✓ Approccio di sicurezza dei prodotti

Approccio basato sui rischi

Default

Prodotti con
elementi digitali

Importanti Classe 1 (All. III)

Funzioni di
sicurezza cyber di
altri prodotti

Importanti Classe 2 (All. III)

Funzioni che, se
compromesse,
rischio
significativo ad
altri PED

Critici (All. IV)

Sistemi con
requisiti di
sicurezza estremi



Importanti - Classe I

Sistt. gestione identità e accessi

Browser autonomi e incorporati

Password manager

Spyware e anti malware

VPN

Sistemi di gestione della rete

SIEM

Boot manager

Infrastrutt. rilascio chiavi pubbl.

Interfacce di rete

Sistemi operativi

Router, modem, switch

Microprocessori per sicurezza

Microcontrollori

Circuiti ASIC - FPGA

Home assistant AI

Prodotti home sicurezza smart

Giocattoli connessi

Wearable salute



Importanti - 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

Microprocessori a prova di manomissione

Microcontrollori a prova di manomissione



Critici

**Dispositivi hardware
con cassette di
sicurezza**

**Gateway per contatori
intelligenti nell'ambito
di sistemi di
misurazione intelligenti;

altri dispositivi a fini di
sicurezza avanzati,
compreso il trattamento
crittografico sicuro**

**Carte intelligenti o
dispositivi analoghi,
compresi gli elementi
sicuri**





3 “direzioni”

- ✓ Framework comune di requisiti essenziali per tutti i PED
- ✓ Approccio basato sui rischi
- ✓ Approccio di sicurezza dei prodotti

Approccio di sicurezza

Pre - messa a disposizione

Soddisfare i requisiti essenziali (All. I)

Presunzione di conformità

Standard comuni, sistemi di certificazione

Una serie di obblighi specifici

Pre, durante, post messa a disposizione



Effettuare valutazione rischi prima, durante e dopo; valutare conformità, ottenere marcatura



✓ Obblighi

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Assistenza

5 Anni o durata prevista

Notifiche: CSIRT o Enisa (vulnerabilità sfruttata o incidente significativo)



Obblighi

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Valutazione dei rischi

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità

Val. Rischi cyber associati a un prodotto

Documentazione aggiornata

Scopo, uso prevedibile, condizioni d'uso,
applicazione requisiti essenziali

Tenerne conto in progettazione,
consegna, produzione, manutenzione



Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità

Requisiti proprietà prodotto e di gestione vulnerabilità

Progettati, sviluppati e prodotti per
garantire un livello adeguato di
cybersicurezza in base ai rischi

Sulla base della valutazione dei rischi:
resi disponibili **senza vulnerabilità
note** sfruttabili; resi disponibili con
una **configurazione sicura by default**

Identificazione vulnerabilità (SBOM),
mitigazione, test e revisioni,
divulgazione sulle vulnerabilità risolte



Requisiti proprietà prodotto e di gestione vulnerabilità

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Messa a disposizione

- Prodotti senza vulnerabilità note
- Security by default
- Aggiornamenti automatici e facili da eseguire



Protezione e Sicurezza

- Protezione accessi non autorizzati
- Riservatezza dei dati
- Integrità dati e configurazioni



Ottimizzazione risorse

- Minimizzazione dei dati trattati
- Disponibilità funzioni essenziali
- Riduzione superficie attacco



Gestione ciclo di vita

- Riduzione impatto incidenti
- Monitoraggio attività
- Rimozione sicura dei dati



Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità

Altri obblighi



Documentali



Due diligence



Politiche divulgazione vulnerabilità



Informativi



Conformità

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità

Dichiarazione di conformità

GU L 46/20.11.2024 IT

ALLEGATO V
DICHIARAZIONE DI CONFORMITÀ UE

La dichiarazione di conformità UE di cui all'articolo 22 contiene tutte le informazioni seguenti:

1. nome e tipo e qualsiasi altra informazione che consenta l'identificazione univoca del prodotto con elementi digitali
2. nome e indirizzo del dichiarante e del suo rappresentante autorizzato
3. un'attestazione secondo cui la dichiarazione di conformità UE è rilasciata sotto la responsabilità esclusiva del firmatario
4. oggetto della dichiarazione (identificazione del prodotto con elementi digitali che sia coerente in univocità, che può, se del caso, includere una fotografia)
5. un'attestazione secondo la quale l'oggetto della dichiarazione di cui sopra è conforme alle pertinenti norme armonizzate di armonizzazione dell'Unione
6. riferimenti alle pertinenti norme armonizzate utilizzate e a qualsiasi altra specifica comune o certificazione di omologazione in materia alla quale è dichiarata la conformità
7. ove applicabile, il nome e il numero dell'organismo notificato, una decisione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato
8. informazioni supplementari:

Rimane a nome e per conto di:
(sempre a data della dichiarazione)
nome, funzione (firma): _____

IT <http://data.europa.eu/eli/reg/2024/2247/oj> 7/10

Dichiarazione semplificata

IT GU L 46/20.11.2024

ALLEGATO VI
DICHIARAZIONE DI CONFORMITÀ UE SEMPLIFICATA

La dichiarazione di conformità UE semplificata di cui all'articolo 17, paragrafo 20, deve essere presentata come segue:
Cui la presente, ... (nome del dichiarante digitale del prodotto con elementi digitali) ... (presentazione del tipo di prodotto con elementi digitali) è conforme al regolamento (UE) 2024/2247(1).
Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: ...

IT <http://data.europa.eu/eli/reg/2024/2247/oj> 7/10





Conformità

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Presunzione: si presume che i prodotti con elementi digitali e processi messi in atto dal fabbricante che sono

- conformi agli standard armonizzati (in GU UE)
- alle specifiche comuni
- per i quali è stata rilasciata una dichiarazione di conformità UE o un certificato nell'ambito di un ECCS siano conformi ai requisiti essenziali di cui all'Allegato I



Conformità

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Procedura di valutazione di terze parti

Se, nel valutare la conformità del prodotto e dei processi ai requisiti essenziali, il fabbricante non ha applicato (anche perché inesistenti) o ha applicato solo in parte norme armonizzate (standard), specifiche comuni, sistemi europei di certificazione della ciphersicurezza a livello di affidabilità almeno sostanziale, il prodotto e i processi sono sottoposti a una procedura di valutazione di terze parti (Modulo B+C; Modulo H)



Conformità

Design e sviluppo

Valutazione dei rischi

Requisiti proprietà prodotti
Requisiti gestione vulnerabilità
Obblighi

Valutazione conformità



Altre modalità

Vi sono poi altre specifiche modalità e procedure per la dimostrazione della conformità in relazione alla tipologia di prodotti



✓ Obblighi



*Stabilire il periodo di supporto,
garantirlo e comunicarlo.*

Gestire incidenti e vulnerabilità

Assistenza

5 Anni o durata prevista

Notifiche: CSIRT o Enisa (vulnerabilità
sfruttata o incidente significativo)



Sintesi degli Obblighi



Informazione Utenti

Circa incidenti e vulnerabilità; misure correttive.



Notifica Autorità (CSIRT/ENISA)

Timeline: Early Warning 24h; Notifica Incidente 72h.



Assistenza

5 Anni (o durata prevista); supporto continuo.



Sicurezza e Divulgazione

Gestione vulnerabilità e condivisione patch.



CRA: Obblighi di Segnalazione



Vulnerabilità Attivamente Sfruttate

24 ore



Pre-allarme

72 ore



Notifica Generale

14 giorni



Relazione Finale
(post misura correttiva)



Incidenti Gravi

24 ore



Pre-allarme

72 ore



Notifica Generale

1 mese



Relazione Finale
(post notifica incidente)



Requisiti di Gestione Vulnerabilità (Dettagli)



Compliance Continua

Mantenere conformità RE in materia di gestione vulnerabilità (All. I, Sez. 2)



Finestra di Supporto

Aggiornamenti di sicurezza disponibili per **minimo 10 Anni**



Versioni Successive

Fornire aggiornamenti all'ultima versione *solo* se gli utilizzatori hanno accesso **gratuito**



Misure e Cooperazione

Prendere misure necessarie per conformità; cooperazione con autorità



SORVEGLIANZA E SANZIONI CRA

RUOLO E POTERI MSA



COOPERAZIONE

- Collaborazione (ENISA, altre MSA, CSA)
- Attività congiunte (sweep)
- Protezione Consumatori



INTERVENTO SUL MERCATO

- Misure correttive su prodotti non conformi/rischiosi
- Ritiro o richiamo dal mercato
- Annual reporting alla Commissione



SANZIONI AMMINISTRATIVE PECUNIARIE



NON CONFORMITÀ AI RE o ART. 13/14: fino a €15M o 2.5% fatturato mondiale



INIOSSERVANZA ALTRI OBBLIGHI: fino a €10M o 2% fatturato mondiale



INFO INESATTE/FUORVIANTI: fino a €5M o 1% fatturato mondiale





BRUGLIA
STUDIO LEGALE SL3



CIPP/E Certified Information Privacy Professional | A/LA ISO IEC 27001:2022 | A/LA ISO IEC 42001:2023