CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

Guida pratica per le PMI: Conformità al Cyber Resilience Act (CRA)

Data di pubblicazione: 30/10/2025
Stato: Definitivo
Versione: 1.0

Il progetto finanziato nell'ambito della convenzione di sovvenzione **n. 101190193** è sostenuto dal Centro europeo di competenza per la sicurezza informatica. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o del Centro europeo di competenza per la sicurezza informatica. Né l'Unione europea né l'autorità che eroga la sovvenzione possono essere ritenute responsabili per essi.

Elenco delle modifiche

Versione	Data	Descrizione	Autore
0.1	07.04.2025	Bozza iniziale	CYEN
0.2	27.06.2025	Testo aggiuntivo	CYEN
0,3	06.08.2025	Prima versione completata, testo aggiuntivo / guida aggiunta	CYEN
0.4	03.09.2025	Versione revisionata dai partner del progetto, da distribuire per la revisione esterna tra pari	CYEN
0.5	24.10.2025	Versione rivista tenendo conto della revisione tra pari	CYEN
1.0	30.10.2025	Versione finale pubblicata	CYEN

Collaboratori

Ruolo	Nome del collaboratore	Nome dell'ente - Beneficiario
Responsabile del risultato	Iva Tasheva, Steve Purser, Krasimir Simonski, Azeez Kamal	CYEN
Collaboratore	Christine Demeter, Gabriel Niculescu	DNSC
Collaboratore	Andreas Binder	AISEC Fraunhofer
Revisione tra pari	Harald Fischer	Balena
Revisione tra pari	Argyro Chatzopoulou et al.	Progetto CURIUM
Revisione tra pari	Romain Muguet et al.	Red Alert Labs

Dichiarazione di non responsabilità: Gli output del progetto CONFIRMATE, compresa la guida alla conformità CRA, sono destinati esclusivamente a scopi informativi e didattici di carattere generale. Essi forniscono un'introduzione di alto livello al processo di conformità CRA e non sono adattati alle circostanze di alcuna organizzazione, prodotto o situazione specifici. Il contenuto riflette l'esperienza e le opinioni individuali degli esperti, degli autori e dei revisori che hanno contribuito alla sua realizzazione e potrebbe non essere completo, aggiornato continuamente o applicabile a tutti i casi.

Nulla in questi strumenti costituisce una consulenza legale, normativa o professionale. Confirmate non si assume alcuna responsabilità per le azioni intraprese sulla base delle informazioni fornite. Spetta esclusivamente agli utenti garantire la conformità alle leggi, ai regolamenti e agli standard vigenti.

Poiché i requisiti normativi sono in continua evoluzione, raccomandiamo vivamente di consultare un professionista legale qualificato o un esperto in materia di regolamentazione per ottenere una consulenza specifica per la propria situazione.

Contenuti

1. Glossario: acronimi, termini e abbreviazioni

Nel testo delle presenti linee guida compaiono i seguenti termini:

Rappresentante autorizzato:	Persona fisica o giuridica stabilita nell'Unione che ha ricevuto un mandato scritto da un fabbricante per agire per suo conto in relazione a compiti specifici.
Marcatura CE:	Marcatura con cui un fabbricante indica che un prodotto con elementi digitali e i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di sicurezza informatica di cui all'allegato I del CRA e ad altre normative di armonizzazione dell'Unione applicabili che ne prevedono l'apposizione.
Dichiarazione di conformità (DICO):	Documento legale, redatto dal fabbricante, che attesta che un prodotto soddisfa i requisiti essenziali applicabili del CRA. Deve essere messo a disposizione delle autorità competenti e degli utenti come parte della documentazione tecnica.
Valutazione di conformità:	Il processo di verifica del rispetto dei requisiti essenziali di sicurezza informatica di cui all'allegato I del CRA.
Norma armonizzata:	Una specifica tecnica elaborata da un organismo europeo di normazione (ESO) su richiesta della Commissione europea per contribuire all'attuazione della legislazione europea. Si tratta di norme europee ufficialmente riconosciute che conferiscono la presunzione di conformità a specifici requisiti giuridici della legislazione dell'UE.
Incidente:	Un evento che influisce negativamente o è in grado di influire negativamente sulla capacità di un prodotto con elementi digitali di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o delle funzioni.
Distributore	Una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che rende disponibile sul mercato dell'Unione un prodotto con elementi digitali senza alterarne le proprietà.

Importatore	Una persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali che reca il nome o il marchio di un fabbricante stabilito al di fuori dell'Unione.
Produttore	Persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali o fa progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializza con il proprio nome o marchio, a titolo oneroso, a fini di monetizzazione o gratuitamente.
Nuovo quadro legislativo (NLF):	Regolamenti che stabiliscono requisiti strutturati e armonizzati per la valutazione della conformità dei prodotti prima della loro immissione sul mercato dell'UE.
Prodotto con elementi digitali (PDE):	Un prodotto software o hardware e le relative soluzioni di elaborazione dati a distanza, compresi i componenti software o hardware immessi sul mercato separatamente.
PMI:	La categoria delle piccole e medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone e che hanno un fatturato annuo non superiore a 50 milioni di EUR e/o un totale di bilancio annuo non superiore a 43 milioni di EUR. All'interno della categoria delle PMI, le piccole imprese sono definite come imprese che occupano meno di 50 persone e il cui fatturato annuo e/o totale di bilancio annuo non supera i 10 milioni di EUR, mentre per le microimprese tali soglie sono inferiori a 10 dipendenti e a 2 milioni di EUR.
Distinta base software:	Un registro formale contenente i dettagli e le relazioni della catena di fornitura dei componenti inclusi negli elementi software di un prodotto con elementi digitali.
Periodo di assistenza:	Il periodo durante il quale un produttore è tenuto a garantire che le vulnerabilità di un prodotto con elementi digitali siano gestite in modo efficace e in conformità con i requisiti essenziali di sicurezza informatica di cui alla parte II dell'allegato I del CRA.
Vulnerabilità:	Debolezza, vulnerabilità o difetto di un prodotto con elementi digitali che può essere sfruttato da una minaccia informatica. - Una vulnerabilità sfruttabile è una vulnerabilità che può essere efficacemente utilizzata da un avversario in condizioni operative pratiche; - Una vulnerabilità sfruttata attivamente è una vulnerabilità per la quale esistono prove affidabili che un malintenzionato l'ha sfruttata in un sistema senza l'autorizzazione del proprietario del sistema.

2. Introduzione

Informazioni sul progetto CONFIRMATE

CONFIRMATE è un progetto innovativo cofinanziato dall'Unione Europea (UE) e dal Centro e Rete europea di competenza per la cybersicurezza (ECCC), progettato per aiutare le PMI manifatturiere a stare al passo con l'evoluzione delle normative in materia di sicurezza informatica. Semplificando la conformità al Cyber Resilience Act (CRA) dell'UE (in italiano: legge sulla ciberresilienza), CONFIRMATE fornisce strumenti open source, formazione pratica e metodi standardizzati che rendono la conformità al CRA più accessibile, efficiente ed economica.

Il nome del progetto sta per Conformity Assessment, Metrics, and Automation for the Cyber Resilience Act (Valutazione della conformità, metriche e automazione per il Cyber Resilience Act). Basato sul framework open source Clouditor, CONFIRMATE fornisce una scomposizione automatizzata dei servizi e panoramiche sulla conformità, risultati di valutazione chiari, una solida metodologia di penetration testing, moduli di formazione multilingue sulla sicurezza informatica[1] e una guida completa alla conformità CRA (il presente documento). Vedere i materiali pubblicati nell'Appendice E.

Coinvolgendo partner di rilievo come CYEN, Fraunhofer AISEC, ITKAM e la Direzione nazionale per la sicurezza informatica della Romania (DNSC), CONFIRMATE fornisce alle PMI le conoscenze e le risorse necessarie per soddisfare con sicurezza i requisiti essenziali di cybersecurity e garantire la resilienza dei loro prodotti digitali. Altri progetti UE attualmente in corso e la conformità delle PMI al CRA sono elencati nell'Appendice F.

2.1 Scopo e destinatari della presente guida

La guida alla conformità è una risorsa gratuita dedicata a supportare le PMI manifatturiere europee nella comprensione dei requisiti essenziali di sicurezza informatica del Cyber Resilience Act (CRA) dell'UE, in italiano legge sulla ciberresilienza[2] . La guida è specificamente progettata per fornire una panoramica dei requisiti di conformità e aiutare le PMI a suddividere le aspettative in passaggi attuabili e di facile comprensione. È adattata alle esigenze e alle sfide specifiche delle PMI del settore manifatturiero. Redatta originariamente in inglese, sarà tradotta in quattro lingue

[1] Guarda il video introduttivo su YouTube: https://youtu.be/QeIjDeVvbL0
[2] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

europee: tedesco, francese, italiano e rumeno, raggiungendo oltre il 60% della popolazione dell'UE.

La guida fornisce una panoramica completa del Cyber Resilience Act (CRA) dell'UE, coprendo aspetti chiave quali ruoli e responsabilità, requisiti essenziali di sicurezza informatica, procedure di valutazione della conformità e segnalazione di incidenti con obblighi post-commercializzazione. Offre inoltre misure pratiche per l'attuazione della CRA da parte delle PMI, insieme a suggerimenti su strumenti di supporto, modelli e risorse per migliorare la loro posizione in materia di sicurezza e favorire un miglioramento continuo.

Scopo: lo scopo principale della guida è quello di responsabilizzare le PMI fornendo loro le conoscenze e gli strumenti necessari per raggiungere e mantenere la conformità al CRA. Essa mira a ridurre la complessità della navigazione tra i requisiti normativi, consentendo alle imprese di adempiere con sicurezza ai propri obblighi concentrandosi al contempo sulle loro attività principali. Inoltre, la guida serve a sottolineare l'importanza per le PMI di gestire i rischi di sicurezza informatica, proteggere la propria reputazione e garantire la sicurezza e l'affidabilità dei propri prodotti digitali. In definitiva, fornirà alle PMI le conoscenze e le misure pratiche necessarie per migliorare la resilienza informatica dei loro prodotti.

Destinatari: la guida è pensata specificamente per le PMI europee che sviluppano, producono o commercializzano prodotti con elementi digitali. Queste imprese spesso non dispongono delle risorse e delle competenze delle organizzazioni più grandi, il che rende la conformità a normative complesse come il CRA una sfida significativa. Concentrandosi sulle PMI, la guida cerca di affrontare le loro sfide specifiche, come i budget limitati, i team più piccoli e la necessità di soluzioni pratiche e scalabili.

Nonostante la comprensione delle sfide sopra descritte che le PMI devono affrontare, gli obblighi CRA sono gli stessi sia per le PMI che per le grandi imprese, con poche eccezioni, ovvero modelli di documentazione semplificati (documentazione tecnica e dichiarazione di conformità) e orientamenti prioritari, che sono anche oggetto della presente guida.

In questo senso, salvo diversamente specificato, tutte le indicazioni contenute nel presente documento si applicano alle PMI.

In sintesi, questa guida alla conformità è una risorsa preziosa per le PMI manifatturiere dell'UE, offrendo loro chiarezza, fiducia e strumenti pratici per orientarsi tra i requisiti della legge dell'UE sulla resilienza informatica. Non solo supporta la conformità, ma promuove anche una cultura della maturità in materia di sicurezza informatica, aiutando le PMI a proteggere i loro prodotti, i loro clienti e la loro reputazione in un mercato sempre più digitalizzato.

2.2 Domande e risposte chiave sul Cyber Resilience Act (CRA)

D1. Che cos'è il Cyber Resilience Act (CRA) / Legge sulla ciberresilienza?
Il CRA è un regolamento dell'UE che mira a garantire la sicurezza informatica dei prodotti con elementi digitali (PDE), come i dispositivi connessi e i software. Introduce requisiti di sicurezza obbligatori durante tutto il ciclo di vita del prodotto, dalla progettazione all'assistenza post-vendita.

Sebbene ampiamente riconosciuta, la definizione di "prodotti con elementi digitali, PDE" del CRA merita di essere approfondita, in quanto è correlata alla necessità che i prodotti delle PMI soddisfino i suoi requisiti.

Per definizione, i PDE includono prodotti software o hardware e le relative soluzioni di elaborazione dati in remoto. Per quanto riguarda il software, non vi è spazio per interpretazioni, poiché è facilmente riconoscibile come codice di programmazione. Per quanto riguarda l'hardware, invece, è necessario chiarire che deve essere in grado di elaborare, memorizzare o trasmettere dati digitali, oltre a essere immesso sul mercato separatamente, anche se fa parte di una catena di fornitura come componente di un altro prodotto.

Q2. Il CRA si applica ai nostri prodotti?
Se la vostra azienda produce o immette sul mercato dell'UE prodotti con elementi digitali (ad esempio dispositivi IoT, software integrato, macchinari industriali con interfacce di rete), allora sì, il CRA è probabilmente applicabile. Esistono esenzioni per i prodotti già regolamentati, come i dispositivi medici, i veicoli leggeri, l'aviazione, i prodotti progettati esclusivamente per uso militare, di sicurezza nazionale e per informazioni classificate.

Q3. Il CRA mi riguarda?
Se siete produttori, importatori, distributori e amministratori open source di un PDE immesso sul mercato dell'UE, avete obblighi specifici ai sensi del CRA.

Q4. Quali sono i principali obblighi per i produttori?

- Condurre e documentare **valutazioni dei rischi per la sicurezza informatica,** compresi i rischi della catena di approvvigionamento
- Garantire pratiche **di sicurezza intrinseca** e **sicurezza predefinita**
- Implementare processi **di gestione delle vulnerabilità**, compresa la segnalazione e la tolleranza zero per le vulnerabilità attivamente sfruttate e note al pubblico.
- Fornire **aggiornamenti di sicurezza** per il ciclo di vita del prodotto
- **Intraprendere procedure di valutazione della conformità** adeguate alla classe di prodotti.

- Creazione e mantenimento **della documentazione tecnica, dei file informativi per gli utenti, della Dichiarazione di conformità UE** (nelle lingue del paese di commercializzazione)

D5. Quando entrerà in vigore il CRA?
Il CRA sarà applicato in modo graduale. Le date chiave per i produttori sono:

➔ **11 settembre 2026,** data in cui entreranno in vigore gli obblighi di segnalazione delle vulnerabilità e degli incidenti di sicurezza
➔ **11 dicembre 2027**, data di piena applicazione del CRA.

D6. Quali sono le sanzioni in caso di inadempienza?
La non conformità può comportare multe fino a **15 milioni di euro o al 2,5% del fatturato annuo globale**, a seconda di quale sia l'importo più elevato. Anche il ritiro dal mercato e il danno alla reputazione sono dei rischi.

D7. Cosa devono fare ora i produttori?

- **Mappare il proprio portafoglio prodotti** per verificarne l'applicabilità al CRA
- Avviare **valutazioni dei rischi di sicurezza informatica e analisi delle lacune**
- Aggiornare **la progettazione, la documentazione tecnica e le politiche di supporto**
- **Valutare l'allineamento con gli standard di sicurezza informatica** (ad esempio EUCC, ISO/IEC 2700x, ETSI EN 303 645)

2.3 Contesto e obiettivo del Cyber Resilience Act (CRA) / Legge sulla ciberresilienza

Il Cyber Resilience Act è il proseguimento della prima normativa orizzontale sulla sicurezza dei prodotti, la direttiva sulle apparecchiature radio (RED)[3] , che ha introdotto i primi requisiti di sicurezza informatica per un'ampia gamma di prodotti venduti nell'UE, in particolare per i dispositivi connessi a Internet e quelli che trattano dati personali, che diventeranno obbligatori a partire dal 1° agosto 2025. Tali requisiti, delineati nell'articolo 3, paragrafo 3, della RED, mirano a migliorare la sicurezza degli utenti e delle reti affrontando le questioni della protezione delle reti, della riservatezza dei dati e della prevenzione delle frodi. Il CRA è anche correlato alla direttiva sulla responsabilità per danno da prodotti difettosi (PLD)[4] , che disciplina la responsabilità per i prodotti difettosi, compresi quelli con elementi digitali.

[3] Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053
[4] Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

Gli obiettivi della legge sulla ciberresilienza (CRA) sono quelli di *"migliorare gli standard di sicurezza informatica dei prodotti che contengono una componente digitale, richiedendo ai produttori e ai rivenditori di garantire la sicurezza informatica durante tutto il ciclo di vita dei loro prodotti (...) La legge sulla ciberresilienza affronta il livello inadeguato di sicurezza informatica di molti prodotti e la mancanza di aggiornamenti di sicurezza tempestivi per prodotti e software"*[5] . Essa mira a stabilire un livello elevato e coerente di sicurezza informatica fissando requisiti chiari per i produttori, gli sviluppatori, gli importatori e i distributori, promuovendo al contempo la trasparenza in materia di rischi per la sicurezza informatica.

"Il Cyber Resilience Act garantirà che:

- *I prodotti cablati e wireless connessi a Internet e i software immessi sul mercato dell'UE siano più sicuri;*
- *i produttori rimangano responsabili della sicurezza informatica di un prodotto durante tutto il suo ciclo di vita;*
- *i consumatori siano adeguatamente informati sulla sicurezza informatica dei prodotti che acquistano e utilizzano".*[6]

Esso *"introduce requisiti obbligatori in materia di sicurezza informatica per i produttori e i rivenditori, che disciplinano la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti"*[7] . Tali obblighi devono essere rispettati in ogni fase della catena del valore. Il CRA pone l'accento sui principi di sicurezza fin dalla progettazione, sulle valutazioni di conformità e sulla segnalazione di incidenti informatici e vulnerabilità attivamente sfruttate, al fine di creare un ecosistema digitale più sicuro.

Il CRA non è limitato a un settore specifico, ciò che consente un impatto più ampio e stabilisce un livello minimo di sicurezza accettabile per i prodotti venduti nell'UE, contribuendo così a una migliore resilienza informatica. Per le PMI, in particolare, il CRA fornisce un quadro di riferimento per integrare la sicurezza informatica nei loro processi, migliorando la loro competitività in un mercato sicuro e affidabile.

Il collegamento e la relazione tra il CRA e altre normative UE pertinenti in materia di sicurezza sono descritti nell'appendice G Relazione con altre normative UE.

2.4 Ambito di applicazione del Cyber Resilience Act (CRA)

Ambito di applicazione: il CRA si applica a tutti i prodotti con elementi digitali immessi sul mercato dell'UE (cioè venduti separatamente, non come parte di un servizio),

[5] Commissione europea (2025) Cyber Resilience Act, consultato il 14 aprile 2025 qui: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[6] Commissione europea (2025) Cyber Resilience Act - Domande e risposte, consultato il 14 aprile 2025 qui: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375
[7] Commissione europea (2025) Cyber Resilience Act, consultato il 14 aprile 2025 qui: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

"collegati direttamente o indirettamente a un altro dispositivo o rete, ad eccezione di specifiche esclusioni quali alcuni prodotti software o servizi open source già coperti dalle norme esistenti, come nel caso dei dispositivi medici, dell'aviazione e delle automobili. I prodotti recheranno il marchio CE per indicare che sono conformi ai requisiti del CRA".[8] Gli obblighi si estendono all'intero ciclo di vita del prodotto, dalla concezione, alla progettazione, alla produzione e alla manutenzione, fino allo smaltimento.

Vale la pena chiarire che se un PDE non è collegato direttamente a una rete o a un altro sistema informatico, può comunque propagare indirettamente una minaccia a un determinato obiettivo tramite file infetti, unità flash, ecc. (considerando 9). Potrebbe trattarsi di un dispositivo autonomo come una serratura intelligente, un giocattolo e altri (considerando 10).

"In base al nuovo quadro legislativo per la legislazione sui prodotti nell'UE, i fabbricanti sarebbero sottoposti a un processo di valutazione della conformità per dimostrare se i requisiti specificati relativi a un prodotto sono stati soddisfatti. Ciò potrebbe essere fatto tramite un'autovalutazione o una valutazione della conformità da parte di terzi, a seconda del livello di rischio associato al prodotto in questione".[9]

Il CRA classifica i prodotti con elementi digitali in quattro categorie (Predefinito, Classe I importante, Classe II importante, Critico). Tutte le categorie di prodotti devono implementare gli stessi requisiti essenziali di sicurezza informatica (stabiliti dalla legge, discussi nella sezione 3 del presente documento), ma presuppongono un livello adeguato di protezione in base al rischio e alla necessità di seguire diverse procedure di applicazione (valutazione della conformità):

- **I prodotti con elementi digitali di default** rappresentano circa il 90% di tutti i prodotti con elementi digitali. Essi devono soddisfare i requisiti essenziali di sicurezza informatica, attestandone la conformità tramite autovalutazione e dichiarazione di conformità.
- **I prodotti con elementi digitali importanti sono** elencati nell'allegato III e suddivisi in due categorie: Classe I e Classe II**.** Si ritiene che questi prodotti svolgano funzioni critiche per la sicurezza informatica di altri prodotti, reti o servizi e, in questo senso, comportino un rischio significativo. Oltre a soddisfare i requisiti essenziali di sicurezza informatica, sono soggetti a requisiti di verifica della sicurezza informatica più rigorosi prima di essere immessi sul mercato.
- **I prodotti con elementi digitali critici** sono elencati nell'allegato IV. Si tratta di un elenco molto limitato di prodotti, considerati i più rischiosi, che dovranno ottenere un certificato europeo di sicurezza informatica con un livello di garanzia

[8] ibid
[9] Commissione europea (2025) Cyber Resilience Act, consultato il 14 aprile 2025 qui: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

almeno "sostanziale" nell'ambito di un sistema europeo di certificazione della sicurezza informatica adottato a norma del regolamento (UE) 2019/881.

3. Ruoli e responsabilità

Gli obblighi delineati dal CRA riguardano una serie di attori nella catena di fornitura di un prodotto, senza distinzione di dimensioni o origine, ma concentrandosi sul ruolo della persona giuridica o fisica in relazione al PDE in questione. Tuttavia, saranno pubblicate linee guida (come indicato nel presente documento) e modelli semplificati per consentire in particolare alle PMI di adempiere in modo efficace ed efficiente ai propri ruoli e responsabilità.

Il CRA definisce i ruoli specifici e le rispettive responsabilità come segue:

3.1 Fabbricanti

Il fabbricante svolge un ruolo fondamentale per la sicurezza informatica dei prodotti con elementi digitali nelle fasi di progettazione, sviluppo, produzione e assistenza. In quanto tale, il fabbricante è il profilo aziendale principale nel CRA, e si assume l'intera responsabilità (ovvero l'attuazione dei requisiti essenziali di sicurezza informatica e delle procedure di valutazione della conformità).

Il CRA definisce un fabbricante come *"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, a titolo oneroso, a fini di monetizzazione o gratuitamente".

Questa definizione implica che tutte le fasi della vita di un prodotto siano gestite da un unico fabbricante, il quale si assume pienamente la responsabilità della sicurezza informatica del prodotto. In pratica, come è noto, la catena produttiva è spesso molto più complessa e coinvolge fornitori, terzi e altri attori; ciò non comporta tuttavia una responsabilità condivisa. Per ciascuna fase del ciclo di vita del prodotto sono previsti requisiti specifici di sicurezza informatica, applicabili a ogni attività, fase e operazione. Le responsabilità del fabbricante non si esauriscono con l'immissione sul mercato del prodotto con elementi digitali

Gli obblighi dei fabbricanti (vedi Tabella 1) sono riassunti negli articoli 13 e 14 del testo ufficiale del CRA e sono interpretati nel presente documento.

Obbligo	Attività
Attuazione dei requisiti essenziali di sicurezza informatica del CRA	Quando immettono sul mercato un prodotto con elementi digitali, i fabbricanti devono garantire che esso sia stato progettato, sviluppato e prodotto in conformità ai requisiti essenziali di sicurezza informatica di cui alla parte I dell'allegato I.
Valutazione periodica dei rischi	Effettuare e aggiornare periodicamente le valutazioni dei rischi di sicurezza informatica per i prodotti e la catena di fornitura. Tenere conto dei risultati della valutazione per la pianificazione, la progettazione, lo sviluppo, la produzione, la consegna e la manutenzione dei PDE al fine di ridurre al minimo i rischi di sicurezza informatica, prevenire gli incidenti e minimizzare l'impatto, anche in relazione alla salute e alla sicurezza degli utenti. La valutazione dei rischi di sicurezza informatica deve indicare in che modo sono attuati i requisiti essenziali di sicurezza informatica (compresa la gestione delle vulnerabilità).
Sicurezza intrinseca e predefinita	Garantire che i prodotti siano progettati in modo sicuro e dotati di configurazioni predefinite sicure.
Gestione delle vulnerabilità	Implementare processi definiti per la gestione delle vulnerabilità note e attivamente sfruttate
Aggiornamenti di sicurezza	Fornire aggiornamenti di sicurezza tempestivi e gratuiti durante tutto il ciclo di vita del prodotto, separatamente dagli aggiornamenti delle funzionalità.
Conformità e marcatura CE	Eseguire una valutazione di conformità (autovalutazione o di terze parti) e applicare il marchio CE.

Documentazione e DICO	Creare e conservare la documentazione tecnica e la Dichiarazione di conformità UE (nelle lingue del mercato di destinazione).
Segnalazione	Segnalare attivamente le vulnerabilità sfruttate e gli incidenti significativi con impatto sulla sicurezza, contemporaneamente al CSIRT e all'ENISA, tramite l'unica piattaforma di segnalazione (UE), come indicato di seguito:
	- Allerta precoce: entro 24 ore
	- Segnalazione iniziale: entro 72 ore
	- Segnalazione finale: entro 14 giorni (vulnerabilità) / 1 mese (incidente)
	Informare gli utenti dei prodotti con elementi digitali interessati da vulnerabilità o incidenti di sicurezza.

Tabella 1: Obblighi dei fabbricanti

La sezione 3 del presente documento descrive in dettaglio i requisiti essenziali di sicurezza informatica stabiliti dall'allegato I della legge sulla ciberresilienza, riassunti qui di seguito:

- Condurre e documentare **la valutazione dei rischi di sicurezza informatica,** compresi i rischi della catena di approvvigionamento**;**
- Garantire pratiche **di sicurezza intrinseca** e **sicurezza predefinita**
- Implementare processi **di gestione delle vulnerabilità**, compresa la segnalazione e la tolleranza zero per le vulnerabilità attivamente sfruttate e note al pubblico.
- Fornire **aggiornamenti di sicurezza** per il ciclo di vita del prodotto
- Intraprendere procedure **di valutazione della conformità** adeguate alla classe di prodotti.
- Creare e mantenere **la documentazione tecnica, i file informativi per gli utenti, la Dichiarazione di conformità UE** (nelle lingue del paese in cui il prodotto è commercializzato, comprese le informazioni richieste. Un modello semplificato della Dichiarazione di conformità è disponibile per le PMI nell'Allegato VI del CRA e nell'Allegato I del presente documento).

Le PMI riconosciute come produttori devono essere informate che il CRA introduce l'obbligo di segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi quando il produttore ne viene a conoscenza. Un incidente è considerato grave quando è causato da o può introdurre codice dannoso o influisce sulla disponibilità, l'autenticità, l'integrità o la riservatezza di dati o funzioni sensibili o importanti del PDE.

Sebbene le microimprese e le piccole imprese non siano soggette a sanzioni amministrative se non rispettano il termine di 24 ore per la segnalazione tempestiva, si

raccomanda loro di farlo il prima possibile. Gli obblighi di segnalazione sono discussi in dettaglio nel capitolo 6.

3.2 Fornitori di software open source

Il ruolo dei fornitori di software open source è molto diffuso tra le PMI, poiché il concetto di codice libero e open source ha origine dalle PMI e dai liberi professionisti ed è di natura comunitaria piuttosto che commerciale. Di conseguenza, l'introduzione di obblighi per i fornitori di software open source risulta complessa quando essi fanno parte della catena di fornitura di prodotti con elementi digitali.

La definizione di fornitore di software open source qualifica il loro PDE come software libero e open source, prevedendo che sia supportato in modo sistematico e continuativo e sottolineando che è destinato ad attività commerciali.
I fornitori di software open source non sono considerati come produttori ai sensi del CRA, salvo quando svolgono attività commerciali con il software open source, ad esempio addebitando il costo del software, fornendo assistenza tecnica a pagamento o monetizzando attraverso servizi correlati. Ciò è chiaramente indicato nel considerando 18 del CRA: "solo il software libero e open source reso disponibile sul mercato, e quindi fornito per la distribuzione o l'uso nel corso di un'attività commerciale, dovrebbe rientrare nell'ambito di applicazione del presente regolamento".

Sebbene il CRA non preveda sanzioni amministrative per i fornitori di software open source, questi ultimi sono soggetti a un regime normativo leggero, con obblighi elencati nell'articolo 24 del CRA e riassunti nella tabella 2 qui di seguito.

Obbligo	Attività
Politica in materia di sicurezza informatica e gestione delle vulnerabilità	Mettere in atto e documentare una politica di sicurezza informatica per promuovere lo sviluppo di un PDE sicuro e una gestione efficace delle vulnerabilità da parte degli sviluppatori di tale prodotto, incoraggiando la segnalazione volontaria delle vulnerabilità e la condivisione delle informazioni relative alle vulnerabilità scoperte all'interno della comunità open source.
Cooperazione	Cooperare con le autorità di vigilanza del mercato, su loro richiesta, al fine di mitigare i rischi per la sicurezza informatica posti dai prodotti software liberi e open source.
Notifica	Notificare alle autorità competenti e agli utenti interessati (o a tutti gli utenti) le vulnerabilità attivamente sfruttate (se coinvolti nello sviluppo del prodotto) e gli incidenti gravi che hanno un impatto sulla sicurezza dei prodotti con elementi digitali nella misura in cui influenzano i sistemi di rete e informativi forniti dai gestori di software open source per lo sviluppo di tali prodotti.
	Comunicare, se necessario, eventuali misure di mitigazione dei rischi e correttive che gli utenti possono adottare per mitigare l'impatto di tale vulnerabilità o incidente.

Tabella 2: Obblighi dei fornitori di software open source

Gli articoli 21 e 22 del CRA trattano i casi in cui gli obblighi dei produttori si applicano ad altre parti. Le presenti linee guida sono quindi rilevanti anche in questi casi.

3.3 Importatori e distributori

Anche le PMI possono svolgere il ruolo di importatori o distributori di prodotti con elementi digitali. Per tali funzioni, il CRA prevede obblighi specifici negli articoli 19 e 20, tra cui il rispetto dei requisiti essenziali di sicurezza informatica illustrati nel capitolo 3 e l'assunzione di una parte degli obblighi previsti per i fabbricanti.

Un importatore è definito come *"una persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali che porta il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione".*

Un distributore, invece, è *"una persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o dall'importatore, che mette a disposizione sul mercato dell'Unione un prodotto con elementi digitali senza alterarne le proprietà".*

Sebbene queste linee guida siano state elaborate pensando ai fabbricanti, possono essere utilizzate in modo ragionevole sia dagli importatori che dai distributori, purché siano comprese le differenze negli obblighi che si applicano a questi gruppi.

Gli obblighi principali sia per gli importatori (articolo 19) che per i distributori (articolo 20) sono riassunti nella tabella 3 riportata di seguito:

Obbligo	Attività	Soggetto	
		Importatore	Distributore
Immettere sul mercato dell'UE solo prodotti conformi al CRA	Astenersi dall'immissione sul mercato dell'UE di prodotti non conformi al CRA;	✅	✅
Gestire i prodotti non conformi	Garantire la correzione o il ritiro/richiamo se si sospetta la non conformità del prodotto al CRA o al suo Allegato I - Requisiti essenziali di sicurezza informatica;	✅	✅
Segnalare	Informare il fabbricante e le autorità di vigilanza del mercato, senza indebito ritardo, in caso di rischio significativo per la sicurezza informatica posto dal PDE;	✅	✅
	Informare il fabbricante di eventuali vulnerabilità del prodotto;	✅	✅
	Informare le autorità di vigilanza del mercato e, nella misura del possibile, gli utenti, nel caso in cui il fabbricante di tale prodotto abbia cessato la propria attività e, di conseguenza, non sia in grado di adempiere agli obblighi previsti dal CRA.	✅	✅
Autoidentificazione	*Inserire i propri dati di contatto sul PDE o sulla documentazione*	✅	

	che accompagna il prodotto, in una lingua facilmente comprensibile dagli utenti e dalle autorità di vigilanza del mercato.		
Conservare i documenti di conformità	*Conservare una copia della dichiarazione di conformità UE a disposizione delle autorità di vigilanza del mercato per almeno 10 anni.*	✅	
Assicurarsi	Prima di immettere un prodotto sul mercato assicurarsi che:		
	(a) siano state eseguite le procedure di valutazione della conformità appropriate[10] *;*	✅	
	(b) il fabbricante abbia redatto la documentazione tecnica;	✅	
	(c) il PDE rechi il marchio CE e sia accompagnato dalla dichiarazione di conformità UE e dalle informazioni e istruzioni per l'utente di cui all'allegato II in una lingua facilmente comprensibile dagli utenti e dalle autorità di vigilanza del mercato[11] *;*	✅	
	(d) il PDE o la sua documentazione rechino l'identificazione del prodotto, del fabbricante e del periodo di assistenza[12] *.*	✅	
	Il fabbricante e l'importatore abbiano adempiuto agli obblighi e fornito tutti i documenti necessari al distributore.		✅

Tabella 3: Obblighi degli importatori e dei distributori

Inoltre, l'articolo 21 definisce le circostanze in cui gli obblighi previsti per i fabbricanti si estendono anche agli importatori e ai distributori. Ciò si verifica quando l'importatore o il distributore immette sul mercato un PDE con il proprio nome o marchio commerciale o apporta una modifica sostanziale a un PDE già immesso sul mercato.

3.4 Altre persone fisiche o giuridiche (articolo 22)

L'articolo 22 riguarda il caso in cui una persona fisica o giuridica (diversa dal fabbricante, dall'importatore o dal distributore) apporti una modifica sostanziale a un PDE e lo metta a disposizione sul mercato. In questo caso, l'entità interessata è considerata un fabbricante.

3.5 Rappresentanti autorizzati nell'UE

Un altro ruolo in cui la PMI può essere riconosciuta è quello di rappresentante autorizzato del fabbricante. Si tratta di un ruolo derivato da quello del fabbricante ed è definito in un mandato speciale con cui il fabbricante nomina il rappresentante autorizzato. Il mandato può includere qualsiasi obbligo del fabbricante, ad eccezione di

[10] *Come stabilito dall'articolo 32*
[11] *Come stabilito dall'articolo 30 e dall'articolo 13, paragrafo 20, di conseguenza*
[12] *Come stabilito all'articolo 13, paragrafi 15, 16 e 19*

quelli specificati esplicitamente dal CRA nell'articolo 18, che riguardano principalmente la sicurezza informatica durante le fasi di progettazione, sviluppo e produzione. Tuttavia, per quanto riguarda i requisiti del CRA relativi alla conformità alla sicurezza informatica del prodotto immesso sul mercato, il rappresentante è tenuto a cooperare con le autorità competenti che vigilano sul PDE che rappresenta.

I fabbricanti possono scegliere di nominare un rappresentante autorizzato che svolga compiti per loro conto, conferendogli un mandato. Il rappresentante autorizzato è tenuto a fornire una copia di tale mandato alle autorità di vigilanza del mercato, se richiesto.

Quando il fabbricante sceglie di procedere in tal senso, il mandato deve consentire al rappresentante autorizzato di svolgere almeno le seguenti attività:

- Conservare la dichiarazione di conformità UE e la documentazione tecnica (cfr. sezione 4 delle presenti linee guida) a disposizione delle autorità di vigilanza del mercato per almeno 10 anni dopo l'immissione sul mercato del PDE o per il periodo di assistenza, a seconda di quale dei due sia più lungo;
- Su richiesta, fornire alle autorità di vigilanza del mercato tutte le informazioni e la documentazione necessarie per dimostrare la conformità del PDE;
- Cooperare con le autorità di vigilanza del mercato.

3.6 Organismi di valutazione della conformità

Le PMI potrebbero anche assumere il ruolo di organismi di valutazione della conformità (Conformity Assessment Bodies - CAB), che nel CRA sono anche definiti organismi notificati. Si tratta di organismi indipendenti, designati dagli Stati membri dell'UE e notificati alla Commissione europea, incaricati di svolgere le valutazioni di conformità di terza parte. Essi valutano se determinati prodotti digitali sono conformi ai requisiti di sicurezza informatica prima che possa essere richiesta la marcatura CE.

I CAB sono principalmente responsabili di effettuare valutazioni di conformità in linea con i requisiti CRA (moduli B, C e H) e di verificare la documentazione tecnica corrispondente. In caso di esito positivo della valutazione, l'organismo notificato rilascia una dichiarazione di conformità, necessaria per ottenere il marchio CE.

Di conseguenza, gli organismi di valutazione della conformità devono essere:

- Accreditati e designati secondo le norme UE[13]
- Tecnicamente competenti in materia di sicurezza informatica e valutazione dei prodotti

[13] Sistema informativo NANDO (New Approach Notified and Designated Organisations) https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

Essi sono soggetti alla supervisione nazionale e al coordinamento a livello UE.

4. Requisiti essenziali di sicurezza informatica

4.1 Relativi alle proprietà dei prodotti

4.1.1 Principi di sicurezza fin dalla progettazione e sicurezza predefinita

I requisiti CRA per l'adozione del principio di sicurezza fin dalla progettazione e sicurezza predefinita, citato in diversi punti del testo:

- Il considerando 32 del CRA riconosce che "*La protezione dei dati fin dalla progettazione e per impostazione predefinita e la cibersicurezza in generale sono elementi fondamentali del regolamento (UE) 2016/679*"[14] .
- Il considerando 34 afferma che *"Quando integrano componenti provenienti da terzi in prodotti con elementi digitali durante la fase di progettazione e sviluppo, i fabbricanti dovrebbero, al fine di garantire che i prodotti siano progettati, sviluppati e fabbricati conformemente ai requisiti essenziali di cibersicurezza di cui al presente regolamento, esercitare la dovuta diligenza per quanto riguarda tali componenti"*,
- L'articolo 13, paragrafo 1, che specifica gli obblighi dei fabbricanti, richiede che *"All'atto dell'immissione sul mercato di un prodotto con elementi digitali, i fabbricanti assicurano che esso sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cibersicurezza di cui all'allegato I, parte I.*".
- L'allegato I, che specifica i requisiti essenziali di cibersicurezza, richiede che *«(1) I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi».*

Come prova della conformità al principio della sicurezza fin dalla progettazione, le PMI possono utilizzare il piano di gestione dei rischi per lo sviluppo dei prodotti, che

14Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)

comprende l'identificazione dei rischi, l'analisi e le strategie di mitigazione per ciascuna fase di sviluppo.

Più esplicitamente, l'allegato I, punto 2, lettera b), prevede un requisito esplicito per una configurazione sicura per impostazione predefinita: *«I prodotti con elementi digitali: 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».*

Questi concetti non sono definiti nel testo e il loro significato è dato per scontato. Ad esempio, l'autorità di regolamentazione tedesca - l'Ufficio federale per la sicurezza informatica in Germania (BSI)[15] - amplia la spiegazione affermando che, secondo il CRA:

- il principio di sicurezza fin dalla progettazione (*secure-by-design*) significa che *«i prodotti connessi devono essere progettati tenendo conto della sicurezza informatica, ad esempio garantendo che i dati memorizzati o trasmessi con il prodotto siano crittografati e che la superficie di attacco sia la più piccola possibile»*
- il principio di sicurezza predefinita (*secure-by-default*) significa che *"le impostazioni predefinite dei prodotti collegati in rete devono contribuire ad aumentarne la sicurezza, ad esempio vietando password predefinite deboli, installando automaticamente aggiornamenti di sicurezza, ecc.".*

Per quanto riguarda le prove accettabili di conformità al principio di sicurezza predefinita, le PMI dovrebbero prendere in considerazione la possibilità di documentare le regole di configurazione sicura applicate e, se il prodotto è personalizzato, di offrire un accordo adeguato con i propri utenti aziendali con clausole pertinenti.

In pratica, l'interpretazione di questi requisiti deve basarsi sulla valutazione dei rischi e sarà a discrezione del produttore, riflettendo la natura del prodotto e il contesto in cui sarà utilizzato.

4.1.2 Gestione dei rischi di sicurezza informatica

La valutazione dei rischi di sicurezza informatica costituisce il fondamento dell'intero approccio alla sicurezza previsto dal CRA, promuovendo una gestione proattiva dei rischi e giustificando le misure di sicurezza informatica rispetto a un semplice approccio

[15] BSI - Ufficio federale per la sicurezza informatica in Germania (2025) Legge sulla resilienza informatica, disponibile all'indirizzo: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html#:~:text=Take%20cybersecurity%20into%20account,not%20have%20to%20be%20published., consultato il 21 luglio 2025

basato sulla conformità.[16] . La valutazione dei rischi è un elemento fondamentale della sicurezza dei prodotti, in quanto fornisce un metodo sistematico per identificare, valutare e dare priorità alle potenziali minacce sin dalle prime fasi di sviluppo e per tutto il ciclo di vita del prodotto. Aggiornando continuamente la valutazione dei rischi man mano che il prodotto evolve, le organizzazioni garantiscono che le misure di sicurezza rimangano solide e pertinenti, proteggendo efficacemente sia il prodotto che i suoi utenti. Questo processo non solo guida la selezione e il rigore dei controlli di sicurezza, ma funge anche da base per tutte le successive valutazioni e decisioni in materia di sicurezza. L'adesione alle buone pratiche consolidate, come quelle descritte nelle norme ISO 31000 o ISO 14971, garantisce un approccio completo e ripetibile. In definitiva, la valutazione dei rischi non solo è essenziale per la realizzazione di prodotti sicuri, ma è anche un prerequisito obbligatorio per la conformità normativa al CRA e a qualsiasi altra normativa dell'UE in materia di sicurezza informatica o di sicurezza dei prodotti. Infatti, lo stesso CRA utilizza tecniche di valutazione dei rischi per definire diverse classi di prodotti e stabilire requisiti di sicurezza proporzionati al livello di rischio associato a ciascuna classe Un modello di valutazione dei rischi è disponibile nell'appendice B del presente documento.

Inoltre, la valutazione del rischio per i PDE ai sensi del CRA è specifica per ciascun prodotto, andando oltre la semplice valutazione dei rischi a livello di progetto o organizzazione. Per rispettare i requisiti del CRA, la valutazione deve considerare in modo dettagliato la sicurezza di:

- **utenti finali**: informazioni e istruzioni da fornire per un utilizzo sicuro del prodotto;
- **catena di approvvigionamento**, comprese le vulnerabilità identificate attraverso la Software Bill of Materials (SBOM), redatta in un formato comunemente utilizzato e leggibile da macchina, che copra almeno le dipendenze di primo livello del prodotto, e integrata nei requisiti di gestione delle vulnerabilità discussi di seguito
- **Interazioni con altri sistemi:** come il PDE o i suoi dispositivi collegati potrebbero influire su altre reti e prodotti, ossia i requisiti di progettazione del prodotto discussi più avanti.

Questa prospettiva globale assicura che non solo il prodotto, ma anche il suo ecosistema e gli utenti siano protetti dalle minacce in continua evoluzione, con controlli di sicurezza proporzionati ai rischi interconnessi del mondo reale

Riferimenti chiave nel testo CRA:

➔ L'articolo 3, paragrafi 37 e 38, definisce rispettivamente i concetti di "rischio di sicurezza informatica" e "rischio significativo di sicurezza informatica".

[16] Si fa riferimento alla gestione dei rischi anche nei considerando 37, 38, 39, 48 e 52 (in riferimento alla valutazione coordinata a livello dell'Unione dei rischi per la sicurezza delle catene di approvvigionamento critiche), 53, 55, 58, 114.

- ➔ L'articolo 13 stabilisce requisiti espliciti su come i fabbricanti devono gestire i rischi per garantire un adeguato livello di sicurezza dei loro prodotti. In particolare, il paragrafo 3 elenca i componenti minimi che la gestione dei rischi deve includere, come l'analisi dei rischi basata sulla destinazione d'uso del PDE e sull'uso ragionevolmente prevedibile, le condizioni d'uso (ad esempio l'ambiente operativo o le risorse da proteggere) e altri elementi rilevanti.
- ➔ L'allegato I (punto 2) stabilisce una serie di requisiti essenziali in materia di sicurezza informatica *sulla base della valutazione dei rischi di cibersicurezza di cui all'articolo 13, paragrafo 2,.*

4.1.3 Obiettivi di sicurezza

La sicurezza dei prodotti rappresenta un elemento centrale del Cyber Resilience Act (CRA), che obbliga le organizzazioni a integrare misure di sicurezza robuste lungo l'intero ciclo di vita dei prodotti, dalla progettazione e sviluppo fino alla distribuzione e manutenzione. Le aree chiave includono:

- **Gestione delle identità e degli accessi**: garantire che solo utenti e sistemi autorizzati possano accedere a funzioni e dati sensibili, riducendo il rischio di accessi non autorizzati e usi impropri;
- **Registrazione (logging)**: implementare una registrazione completa per monitorare le attività, rilevare anomalie e supportare le indagini forensi in caso di incidenti;
- **Sicurezza e minimizzazione dei dati**: proteggere i dati in ogni fase e raccogliere solo quelli strettamente necessari, limitando l'esposizione e riducendo i rischi di non conformità;
- **Backup e cancellazione sicura**: eseguire regolarmente il backup dei dati critici e garantire la cancellazione sicura quando i dati non sono più necessari, prevenendo la perdita di dati e il recupero non autorizzato;
- **Crittografia**: salvaguardia delle informazioni in transito e inattive, rendendo i dati illeggibili a soggetti non autorizzati e mantenendo così la riservatezza.

Integrando questi controlli nel ciclo di vita del prodotto, le organizzazioni possono soddisfare i requisiti del CRA, aumentare la fiducia degli utenti e proteggerli dalle minacce informatiche in continua evoluzione.

L'allegato I del CRA, punto (2), elenca gli obiettivi di sicurezza specifici che devono essere implementati dal produttore, precisando però che i dettagli sull'implementazione di tali meccanismi devono riflettere la valutazione dei rischi effettuata per il prodotto. Questi meccanismi di controllo includono pratiche, procedure e misure tecniche: i meccanismi più importanti sono brevemente discussi di seguito.

Requisiti relativi alla progettazione del prodotto
I prodotti devono:
(j) essere progettati, sviluppati e prodotti in modo da limitare le superfici di attacco, comprese le interfacce esterne;
(k) essere progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;
Questi requisiti di progettazione devono essere considerati insieme al requisito di configurazione sicura per impostazione predefinita.

A dimostrazione della conformità ai requisiti sopra citati, le PMI devono incorporare, implementare e monitorare valutazioni complete dei rischi dei prodotti, mappare i rischi rispetto ai servizi e ai controlli, valutare la documentazione di progettazione e rivedere il codice, garantire ambienti di produzione e sviluppo separati, stabilire e monitorare linee guida di sicurezza per individuare anomalie, ed eseguire regolarmente backup di software e dati.

Misure per individuare ed eliminare le vulnerabilità durante tutto il ciclo di vita del prodotto
L'individuazione e l'eliminazione delle vulnerabilità prima del rilascio del software è un requisito fondamentale del CRA
I prodotti con elementi digitali devono:

(a) essere immessi sul mercato senza vulnerabilità sfruttabili note;
Le vulnerabilità note sono registrate in banche dati pubbliche, come la banca dati sulle vulnerabilità dell'UE[17] o la banca dati nazionale sulle vulnerabilità degli Stati Uniti[18] oppure sono rilevate dagli strumenti di scansione delle vulnerabilità (per ulteriori dettagli sulla scansione e sulla gestione delle vulnerabilità, si rimanda alla metodologia di pentesting di Confirmate).
Quando viene rilevato che una vulnerabilità è già stata sfruttata in un attacco informatico, il fabbricante deve adottare le misure necessarie per prevenirne lo sfruttamento con successo sul PDE, sia prima sia dopo l'immissione sul mercato. Molti hacker, anche senza competenze avanzate, sfruttano vulnerabilità note e non corrette attraverso attacchi zero-day.

(c) garantire 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;

[17] Disponibile all'indirizzo: https://euvd.enisa.europa.eu/
[18] Disponibile all'indirizzo: https://nvd.nist.gov/

La seconda parte dei requisiti essenziali di sicurezza è interamente dedicata alla gestione delle vulnerabilità.

Una volta identificata una vulnerabilità, è importante valutarne la gravità secondo un quadro accettato come il CVSS (Common Vulnerability Scoring System). La priorità viene assegnata in base a questo punteggio, in modo che le vulnerabilità critiche e attivamente sfruttate siano affrontate con urgenza. La correzione viene tipicamente effettuata mediante il rilascio di una patch o la modifica della configurazione.

«Ai sensi del CRA, i produttori hanno l'obbligo chiaro di fornire tempestivamente aggiornamenti di sicurezza agli utenti, utilizzando meccanismi sicuri e separati dagli aggiornamenti delle funzionalità. Tali aggiornamenti devono essere gratuiti, accompagnati da messaggi di avviso chiari e, ove possibile, configurati per l'installazione automatica di default. Questo garantisce che gli utenti siano protetti in tempi rapidi, anche se non intervengono in modo proattivo. Le migliori pratiche del settore consigliano inoltre di stabilire accordi sul livello di servizio (SLA) per la gestione delle patch. Ad esempio:

- da 24 a 48 ore per correggere le vulnerabilità critiche
- 7 giorni per le vulnerabilità elevate
- 30 giorni per le vulnerabilità medie
- 90 giorni per le vulnerabilità basse

Dopo la correzione, è essenziale un monitoraggio continuo. I produttori devono garantire che le patch siano state applicate in modo efficace e monitorare eventuali tentativi di sfruttare le vulnerabilità residue, analizzando i log di sistema e prestando attenzione agli avvisi di rilevamento delle intrusioni.

Insidie da evitare:

- Ritardare la correzione fino agli aggiornamenti delle funzionalità
- Sottovalutare la gravità delle vulnerabilità
- Mancata comunicazione tempestiva e comprensibile agli utenti.

Anche l'applicazione frettolosa di patch senza un adeguato test può introdurre nuovi problemi o rischi. Pertanto, combinando correzioni tempestive, implementazione delle patch e monitoraggio continuo, le PMI possono instaurare un solido processo di gestione delle vulnerabilità che soddisfi i requisiti essenziali di sicurezza informatica previsti dal CRA..

Le prove raccomandate per dimostrare la conformità ai requisiti sopra citati, oltre allo sviluppo e all'applicazione di politiche e procedure pertinenti, possono includere test di penetrazione (interni e da parte di terzi), meccanismi di aggiornamento automatico della sicurezza, revisioni del codice e, soprattutto, aggiornamenti tempestivi e pertinenti (anche proattivi) in caso di individuazione di nuove minacce o vulnerabilità, anche se non ancora sfruttate.

Requisiti tecnici

Esempi di misure tipiche per soddisfare i requisiti tecnici del CRA sono riportati in diversi standard di sicurezza delle informazioni, tra cui il NIST SP800 e il Cyber Fundamentals (CyFun), nella rispettiva sezione dedicata alla Protezione. Di seguito vengono illustrati alcuni esempi di misure specifiche.

(d) garantire 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;

Le misure raccomandate dal NIST Cybersecurity Framework includono:

- Richiedere l'autenticazione a più fattori;
- Applicare politiche relative alla forza minima di password, PIN e autenticatori simili;
- Riautenticare periodicamente utenti, servizi e dispositivi hardware in base al livello di rischio (ad esempio, nelle architetture zero trust);
- Garantire che il personale autorizzato possa accedere agli account essenziali per proteggere la sicurezza in condizioni di emergenza.

(e) proteggere 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;

Le linee guida pertinenti sui fondamenti informatici, come misure, includono:

- l'uso di tecniche di crittografia per l'archiviazione, la trasmissione o il trasporto dei dati (ad esempio, laptop, USB);
  meccanismi di controllo dell'integrità avanzati (ad esempio, controlli di parità, controlli di ridondanza ciclica, hash crittografici) e strumenti associati, che possono monitorare automaticamente l'integrità dei sistemi informativi e delle applicazioni ospitate.

Indicazioni simili sono riportate anche in altri punti:

(f) 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) 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) proteggere 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);

È importante notare che il CRA identifica COSA deve essere fatto, ma non COME deve essere fatto. Il modo in cui questi requisiti vengono implementati è interamente a discrezione del produttore, anche se vi è una chiara aspettativa che i metodi adottati siano commisurati al livello di rischio associato al prodotto.

Le PMI potrebbero dimostrare la conformità ai requisiti di cui sopra dotando i propri prodotti di elementi digitali con funzionalità di registrazione che consentano loro di essere integrati nell'ambiente di sicurezza informatica dei propri utenti aziendali. L'integrazione dovrebbe anche tenere conto della compatibilità con il controllo centralizzato degli accessi, regolarmente testato, compresi i test di penetrazione, e, non da ultimo, della crittografia avanzata.

Le misure di sicurezza specifiche che le PMI devono prendere in considerazione, almeno come minimo, per soddisfare i requisiti sopra indicati, includono:

- Adottare politiche e procedure di identità, controllo degli accessi, autorizzazione e gestione degli incidenti.
- Implementare misure di sicurezza dedicate per impedire l'accesso non autorizzato, la distorsione o la modifica dei dati di sistema e dei registri di audit (ad esempio, diritti di accesso limitati, backup giornalieri, crittografia dei dati, installazione di firewall).
- Implementare meccanismi di rilevamento dell'integrità e di segnalazione.
- Attivare l'autenticazione a più fattori.
- Applicare politiche relative alla forza minima di password, PIN e autenticatori simili.
- Implementare meccanismi di rilevamento e risposta DDoS.

Misure per mitigare l'impatto sull'ambiente IT
Esistono due requisiti volti a ridurre al minimo l'impatto di un incidente o di un malfunzionamento del prodotto sul suo ambiente, indicati ai punti (i) e (k) di seguito:

(i) ridurre al minimo l'impatto negativo dei prodotti stessi o dei dispositivi connessi sulla disponibilità dei servizi forniti da altri dispositivi o reti;

Questo requisito impone che i PDE non solo siano sicuri per il proprio account, ma non rappresentino anche una minaccia per la disponibilità di altri dispositivi o reti. È simile alla direttiva sulle apparecchiature radio, in base alla quale i dispositivi non devono "interferire con altri dispositivi o reti", richiedendo che le apparecchiature utilizzino in modo efficiente lo spettro radio e soddisfino gli standard di compatibilità elettromagnetica, prevenendo interferenze dannose. Applicato alla sicurezza informatica, potremmo consigliare che i PDE siano progettati con attenzione per evitare un consumo eccessivo di dati, CPU o rete, ad esempio, e che dispongano di punti di controllo per evitare di essere utilizzati per un attacco denial of service. In un attacco denial of service, i PDE compromessi potrebbero entrare a far parte di un esercito di bot (dispositivi compromessi), attaccando simultaneamente una rete, un sito web o un'applicazione, mettendo fuori uso il prodotto o la rete sotto attacco.

(k) essere progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;

Le misure di sicurezza specifiche che le PMI devono prendere in considerazione, almeno come minimo, per soddisfare i requisiti sopra citati includono:

- Condurre una valutazione completa dei rischi del prodotto sin dalla fase iniziale, considerando i potenziali rischi relativi alla disponibilità dei servizi forniti da altri dispositivi o reti a causa del PDE o dei dispositivi collegati, e identificando misure di mitigazione per ridurre impatto e probabilità dei rischi;
- Implementare misure di sicurezza dedicate per prevenire accessi non autorizzati, alterazioni o modifiche dei dati di sistema e dei registri di audit (ad esempio, diritti di accesso limitati, backup giornalieri, crittografia dei dati, installazione di firewall);
- Implementare meccanismi di rilevamento e risposta agli attacchi DDoS.

Controlli relativi agli utenti

Altre due misure mirano a consentire all'utente di gestire la propria sicurezza e i propri dati:

(l) fornire informazioni sulla sicurezza registrando e monitorando le attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi, con un meccanismo di disattivazione per l'utilizzatore;

Le tecniche di rilevamento di comportamenti anomali indicativi di un attacco informatico si basano principalmente sulla revisione e l'analisi dei registri dei prodotti con elementi digitali al fine di determinare il tipo e il vettore dell'attacco e adottare misure adeguate per rispondere. Ciò avviene solitamente con strumenti automatizzati per la raccolta e la correlazione dei registri, per i quali i prodotti con elementi digitali devono disporre della funzionalità di supporto per la registrazione e il monitoraggio delle proprie attività.

(m) offrire agli utenti la possibilità di rimuovere in modo sicuro e agevole, su base permanente, tutti i dati e tutte le impostazioni e, qualora tali dati possano essere trasferiti ad altri prodotti o sistemi, garantiscono che ciò avvenga in modo sicuro..

Le tecniche di rimozione sicura dei dati sono diverse, a seconda del tipo di supporto (carta, disco rigido, cloud) o del livello di sensibilità (dai dati generici alla cronologia dei clienti).

Le misure di sicurezza specifiche che le PMI devono prendere in considerazione, come minimo, per soddisfare i requisiti di cui sopra, includono:

- Integrare funzionalità di supporto per la registrazione e il monitoraggio delle attività dei PDE.
- Integrare funzionalità di cancellazione sicura e trasferimento dei dati e dare all'utente la possibilità di avviare il processo in modo semplice.
- Utilizzare metodi come la sovrascrittura completa della memoria, la cancellazione basata sulla crittografia, lo zero-fill, la cancellazione a livello hardware o persino la distruzione fisica per garantire che i dati siano realmente irrecuperabili. È fondamentale identificare tutti i segreti memorizzati prima della cancellazione, verificare che i dati siano stati eliminati e revocare i certificati dei dispositivi durante il processo.

Il CRA presume che gli hacker possano ottenere informazioni importanti, o persino riservate, dai PDE a cui hanno accesso dopo che questi sono stati dismessi o sostituiti, a meno che non sia presente un meccanismo affidabile per eliminare i vecchi dati e ripulire l'archivio residuo.

4.2 Sicurezza delle catene di approvvigionamento e delle terze parti

I produttori sono responsabili della sicurezza informatica dell'intero prodotto che realizzano, inclusi eventuali componenti di terze parti incorporati o integrati, come librerie software, moduli open source e firmware. In particolare, devono valutare e gestire i rischi derivanti dalla catena di fornitura e assicurarsi che il software di terze parti sia conforme ai requisiti del CRA.

In pratica, ciò significa che qualsiasi responsabilità attribuita al produttore deve essere estesa anche alla corrispondente catena di fornitura, se ha un impatto sul prodotto finale. Esempi di tali aspettative includono, ma non sono limitati a:

- sicurezza fin dalla progettazione e per impostazione predefinita;
- periodo di assistenza prolungato (compatibile con quello del prodotto finale);

- gestione e divulgazione delle vulnerabilità;
- gestione degli incidenti (nella misura in cui incidono sul prodotto del produttore).

Di conseguenza, i produttori saranno tenuti a esercitare la dovuta diligenza nella selezione dei fornitori e di altri terzi che contribuiscono ai loro prodotti

Nell'ambito di questa attività, i produttori devono mantenere e fornire una distinta dei materiali software (SBOM), che elenchi tutti i componenti software utilizzati, comprese le dipendenze di terze parti e open source. La SBOM deve essere:

- Disponibile in formato leggibile da computer su richiesta dei clienti e delle autorità di vigilanza del mercato;
- Aggiornata e riflettere tutte le modifiche apportate durante il ciclo di vita del prodotto.

Ulteriori dettagli sul formato (ad esempio JSON) e sugli elementi (informazioni) della SBOM potranno essere forniti dalla Commissione europea sotto forma di atto di esecuzione.

Parallelamente, l'Agenzia statunitense per la sicurezza informatica e delle infrastrutture (CISA) fornisce una panoramica delle migliori pratiche e dei requisiti minimi nella sua bozza dell'agosto 2025 intitolata "Elementi minimi per una distinta dei materiali software (SBOM)".

Per le PMI che producono prodotti soggetti al CRA, questi requisiti SBOM in evoluzione della CISA chiariscono gli aspetti tecnici e gli standard per la gestione dell'SBOM. Tuttavia, i dettagli forniti dalla CISA comportano anche una complessità operativa non trascurabile.

4.3 Gestione delle vulnerabilità

La parte II dei requisiti essenziali di sicurezza (allegato I del CRA) riguarda i requisiti relativi alla gestione delle vulnerabilità. In questo caso vi è una certa sovrapposizione con i requisiti della parte I (ad esempio il requisito che i prodotti con elementi digitali siano immessi sul mercato senza vulnerabilità note sfruttabili). Tuttavia, la maggior parte dei requisiti elencati in questa parte dell'allegato sono orientati alle politiche e alle procedure e mirano esplicitamente alla gestione delle vulnerabilità.

4.3.1 Identificazione e documentazione

(1) identificare e documentare le vulnerabilità e i componenti contenuti nel prodotto con elementi digitali, redigendo anche una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del prodotto;

Il requisito di produrre una distinta dei materiali software (SBOM) è obbligatorio. Ulteriori informazioni sul rapporto tra il concetto di SBOM e il CRA sono disponibili nei considerando 77 e 118 e nell'articolo 13, paragrafo 24, del CRA.
Come discusso in precedenza, al momento della stesura del presente documento non esiste un formato imposto per tale documento, né esiste un formato standard accettato, sebbene l'articolo 13, paragrafo 24, consenta alla Commissione, mediante atti di esecuzione che tengono conto delle norme e delle migliori pratiche europee o internazionali, di specificare il formato e gli elementi della SBOM.
Inoltre, i fabbricanti devono *(3) effettuare prove e riesami efficaci e periodici della sicurezza del prodotto con elementi digitali;*
È importante notare che il requisito (3) consiste nell'istituire un processo completo e periodico di test e revisioni, sia per le vulnerabilità tecniche e organizzative che per le configurazioni errate, indipendentemente dal fatto che sia stata scoperta o meno una vulnerabilità.

4.3.2 Rimedio

Le vulnerabilità PDE devono essere affrontate o risolte senza indugio. Ciò è necessario per garantire che il prodotto rimanga sicuro mentre è presente sul mercato dell'UE. Inoltre, il CRA ha specificato che, ove possibile, i nuovi aggiornamenti di sicurezza devono essere forniti separatamente dagli aggiornamenti di funzionalità. Ciò potrebbe contribuire a colmare la differenza di tempistica tra lo sviluppo del prodotto e la manutenzione della sicurezza.

4.3.3 Divulgazione delle vulnerabilità e condivisione delle informazioni

In questo ambito vi sono tre requisiti fondamentali:
(4) una volta reso disponibile un aggiornamento di sicurezza, condividono e divulgano pubblicamente informazioni sulle vulnerabilità risolte, compresi una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritengano che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, i fabbricanti possono ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità di applicare la pertinente patch;;
(5) mettere in atto e applicare una politica di divulgazione coordinata delle vulnerabilità;
(6) adottare misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilità nel loro prodotto con elementi digitali e nei componenti di terzi contenuti in

tale prodotto, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate nel prodotto con elementi digitali;

Il requisito (5) si riferisce alla divulgazione coordinata delle vulnerabilità, che ha un significato specifico in questo contesto. L'idea alla base della divulgazione coordinata delle vulnerabilità (CVD) è descritta in modo esauriente dall'ENISA[19] . In sostanza, la CVD è un insieme di regole (ad esempio una politica) pubblicate da un produttore che consente agli esperti di sicurezza esterni con buone intenzioni (che potrebbero essere "hacker etici" o servizi di scansione delle vulnerabilità) di identificare potenziali vulnerabilità nei suoi sistemi o prodotti e fornisce una procedura (modulo, canale, contatti) per segnalare al produttore le debolezze di sicurezza individuate. La CVD di solito definisce quali sistemi rientrano nel campo di applicazione e a quali condizioni può essere effettuata l'identificazione (nessuna violazione della legge, nessun danno, nessuna fuga di dati).

4.3.4 Gestione degli aggiornamenti di sicurezza

I requisiti finali della parte II riguardano la gestione degli aggiornamenti di sicurezza, garantendo che la correzione (aggiornamenti di sicurezza) discussa sopra sia fattibile attraverso *meccanismi per distribuire in modo sicuro gli aggiornamenti* per i PDE.

Inoltre, gli aggiornamenti di sicurezza devono essere gratuiti e accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare. Tutto ciò con l'obiettivo di consentire agli utenti dei PDE di mantenere i loro prodotti sicuri e di adottare le necessarie misure di mitigazione del rischio, quando necessario.

[19] https://www.enisa.europa.eu/topics/vulnerability-disclosure

5. Valutazione della conformità

5.1 Procedure di valutazione della conformità

Le procedure di valutazione della conformità adottate dalla CRA si basano sul NLF[20] e ruotano attorno al principio "alto rischio = alta garanzia". In particolare, le categorie predefinite (non specificatamente menzionate nel regolamento) sono soggette a procedure di autovalutazione, la classe I importante si basa su norme armonizzate o valutazioni di terzi, la classe II importante e i prodotti critici sono soggetti a valutazioni e certificazioni di terzi. I requisiti specifici per le classi di prodotti sono riassunti nella tabella seguente. Una descrizione dettagliata delle procedure di valutazione della conformità è disponibile nel capitolo "Processo di conformità CRA" del documento **CONFIRMATE D3.1 – Architecture for Automated CRA Conformance Assessment,** nel processo di conformità CRA. I requisiti sono stabiliti nell'articolo 32 della legge. L'allegato VIII fornisce una descrizione dettagliata delle procedure di valutazione della conformità.

Il CRA riconosce e si affida alle procedure di conformità presentate di seguito.

5.1.1 Norme armonizzate. Si tratta di norme europee ufficialmente riconosciute che danno presunzione di conformità a specifici requisiti legali nella legislazione dell'UE. Esse fungono da linee guida prescrittive e verificabili per la gestione dei rischi, lo sviluppo sicuro e la sicurezza operativa.

Tali norme devono ancora essere sviluppate e riconosciute ufficialmente per presumere la conformità ai requisiti essenziali di sicurezza informatica. Nel febbraio 2025, la Commissione europea ha incaricato gli organismi europei di normazione (CEN, CENELEC, ETSI) di sviluppare 41 norme: 15 orizzontali, che si applicano in modo generale a tutti i PDE, e 25 verticali, che sono adattate a tipi di prodotti e classi di rischio specifici. Gli standard orizzontali riguardano la sicurezza generale (tipo A) e i requisiti di vulnerabilità (tipo B), mentre gli standard verticali forniscono indicazioni dettagliate per prodotti specifici, ad esempio browser, dispositivi IoT (tipo C), influenzando la possibilità

[20] Il NLF (Nuovo Quadro Legislativo) chiarisce l'uso del marchio CE e crea una serie di misure da utilizzare nella legislazione sui prodotti. Il NLF è composto da: Regolamento (CE) 765/2008 che stabilisce i requisiti per l'accreditamento e la sorveglianza del mercato dei prodotti, Decisione 768/2008 su un quadro comune per la commercializzazione dei prodotti, che include disposizioni di riferimento da incorporare nelle revisioni della legislazione sui prodotti. In effetti, si tratta di un modello per la futura legislazione in materia di armonizzazione dei prodotti, il regolamento (UE) 2019/1020 sulla sorveglianza del mercato e la conformità dei prodotti. Per ulteriori dettagli, consultare il sito web della Commissione europea: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

per i produttori di effettuare un'autovalutazione o di richiedere la conformità da parte di terzi, con gli standard più sensibili sviluppati in condizioni limitate. Un elenco completo degli standard è disponibile sul sito web del CEN/CENELEC[21] .

La pianificazione per la consegna di questi standard prevede la consegna degli standard di tipo A e di tipo B per la gestione delle vulnerabilità entro il 30.08.26, di tutti gli standard di tipo C entro il 30.10.26 e dei restanti standard di tipo B entro il 30.10.27.

Oltre alle norme armonizzate che supportano direttamente la conformità al CRA, i produttori sono incoraggiati a utilizzare le principali norme industriali nell'attuazione dei requisiti del CRA. Esempi significativi sono elencati nell'appendice C.

5.1.2 Le specifiche comuni (adottate dall'atto di esecuzione della CE) sono linee guida dettagliate e pratiche della Commissione europea volte ad aiutare i fabbricanti a soddisfare requisiti specifici in materia di sicurezza informatica, in assenza di norme armonizzate o per settori non sufficientemente trattati in una norma armonizzata pubblicata, fungendo da opzione di ripiego in tali casi.

5.1.3 Certificati rilasciati nell'ambito di un sistema europeo di certificazione della sicurezza informatica.
Il principale sistema di certificazione dell'UE che supporterà la conformità al CRA è l'EUCC (European Common Criteria). L'EUCC è un sistema di certificazione della sicurezza informatica su base volontaria a livello europeo che consente la certificazione di prodotti ICT quali componenti tecnologici (chip, smart card), hardware e software. Basandosi sull'attuale quadro di valutazione dei criteri comuni SOG-IS, che esiste da oltre vent'anni, esso funge da continuazione ed espansione (da 17 Stati membri dell'UE attualmente a tutti i 27 che lo adotteranno). Propone due livelli di garanzia basati sul livello di rischio associato all'uso previsto del prodotto, del servizio o del processo, in termini di probabilità e impatto di un incidente.
La Commissione europea ha centralizzato tutti i documenti e le linee guida relativi all'EUCC[22] . La scelta di una certificazione UE in materia di sicurezza informatica come procedura di valutazione della conformità offre il vantaggio della presunzione di conformità con il CRA, anche per le categorie ad alto rischio, e rafforza la credibilità del mercato e la fiducia dei clienti.

Il regolamento UE sulla sicurezza informatica (UE 2019/881) istituisce un quadro comune per la certificazione della sicurezza informatica in tutta l'UE. Ai sensi del regolamento CRA, tale quadro assume particolare importanza per i prodotti che

[21] Disponibile all'indirizzo: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf
[22] Disponibile qui: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

comportano rischi più elevati, quelli classificati come **importanti di classe II** o **critici** nell'allegato VIII. Per queste classi di prodotti, la certificazione può servire come prova formale del raggiungimento di livelli di garanzia "sostanziali" o "elevati".

5.2 Procedure minime richieste per la valutazione della conformità

Le PMI dovrebbero soddisfare almeno le procedure minime richieste stabilite nel CRA per la loro categoria di prodotti, come spiegato nel documento Confirmate D3.1 – Architecture for Automated CRA Conformance Assessment (Architettura per la valutazione automatizzata della conformità al CRA)[23] **OPPURE** qualsiasi altra procedura più rigorosa. Più rigorosa è la procedura di valutazione scelta, più sicuro e affidabile appare il PDE sul mercato, il che potrebbe rappresentare un vantaggio competitivo significativo. Ad esempio, se il PDE rientra nella categoria Default, la procedura minima richiesta è il Modulo A, ma la PMI può scegliere una qualsiasi delle altre procedure più rigorose riportate di seguito. Se un PDE rientra nella Classe I importante, la PMI che lo produce può effettuare un'autovalutazione rispetto alle norme armonizzate per il suo tipo di prodotto, se disponibili, oppure, se non disponibili, scegliere la procedura più rigorosa successiva: Modulo B+C o Modulo H. Se un PDE è elencato nella Classe II importante, le procedure minime richieste sono due: "Modulo B+C" o Modulo H, entrambe prevedono una valutazione da parte di terzi.

Le opzioni procedurali per prodotti specifici sono riassunte nella tabella sottostante, dove ogni segno di spunta indica un'opzione per la categoria specificata:

Tipo / categoria di prodotto	Default	Classe importante I	Classe importante II	Critico
Autovalutazione (Modulo A – Controllo interno)	✅			
Autovalutazione rispetto allo standard armonizzato UE, specifiche comuni (Modulo A – Controllo interno)	✅	✅		
Valutazione CAB della progettazione + Autovalutazione della produzione (Modulo B+C)	✅	✅	✅	
Garanzia di qualità CAB completa (Modulo H)	✅	✅	✅	
Certificato UE di sicurezza informatica (CSA) di livello "sostanziale" o "elevato"	✅	✅	✅	✅

[23] Disponibile all'indirizzo https://confirmate-project.eu/materials/

È prevista un'eccezione per i prodotti open source: *"I fabbricanti di prodotti con elementi digitali importanti che si qualificano come software liberi e open source dovrebbero essere poter seguire la procedura di controllo interno basata sul modulo A, a condizione che mettano la documentazione tecnica a disposizione del pubblico"* (considerando 91 del CRA).

5.3 Marchio CE e documentazione tecnica

5.3.1 Marchio CE

Il marchio CE è definito nel CRA come: *«marchio con cui un fabbricante indica che un prodotto con elementi digitali e i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di sicurezza informatica di cui all'allegato I e ad altre normative di armonizzazione dell'Unione applicabili che ne prevedono l'apposizione».*
In generale, il marchio CE è necessario per attestare che un prodotto soddisfa tutti i requisiti applicabili dell'UE in materia di sicurezza informatica e sicurezza. Nel contesto del CRA, il marchio CE dovrebbe essere apposto solo dopo (a) aver completato la procedura di valutazione della conformità pertinente e (b) aver redatto e firmato la dichiarazione di conformità UE.
Il marchio CE è soggetto ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008. Il marchio CE deve essere apposto in modo visibile, leggibile e indelebile sul prodotto e sull'imballaggio o sulla documentazione di accompagnamento (se non è possibile apporre il marchio fisico).

Nota importante: *Non tutti i prodotti devono recare il marchio CE. Esso è obbligatorio solo per la maggior parte dei prodotti coperti dalle direttive del "Nuovo Approccio" ed è vietato apporlo su altri prodotti. Si segnala che il marchio CE non indica che un prodotto sia stato approvato come sicuro dall'UE o da altre autorità, né ne attesta l'origine*[24] *.*

[24] *Il testo completo e tutte le opzioni di formato del marchio CE sono disponibili sul sito web della Commissione europea: https://single-market-economy.ec.europa.eu/single-market/goods/ce-marking_en*

5.3.2 Documentazione tecnica

I fabbricanti sono tenuti a preparare e conservare la documentazione tecnica (come stabilito nell'allegato VII del CRA), che dimostri la conformità del prodotto. Ciò è obbligatorio sia per l'autovalutazione che per la valutazione da parte di terzi.

Tale documentazione deve includere:

- Descrizione generale del prodotto
- Una descrizione della progettazione, dello sviluppo e della produzione del prodotto
- Valutazioni dei rischi iniziali e aggiornate
- Informazioni rilevanti che sono state prese in considerazione per determinare il periodo di assistenza
- Un elenco delle norme armonizzate applicate in tutto o in parte al prodotto
- Rapporti di prova, risultati delle ispezioni e norme applicate
- Descrizione della procedura di valutazione della conformità utilizzata
- Una copia della dichiarazione di conformità UE
- Se del caso, la distinta dei materiali software

Per le PMI, un'opzione per una forma semplificata della documentazione tecnica sarà resa disponibile in un regolamento di esecuzione della Commissione che deve ancora essere pubblicato al momento della stesura della presente guida.

5.4 Dichiarazione di conformità

La dichiarazione di conformità (DICO) è un documento legale che attesta che un prodotto soddisfa i requisiti essenziali di sicurezza informatica applicabili di cui all'allegato I del CRA. È redatta dal fabbricante dopo aver completato con successo le procedure appropriate di valutazione della conformità. La DICO deve essere firmata da un rappresentante autorizzato e messa a disposizione delle autorità nazionali di vigilanza del mercato.

La DICO deve contenere:

- Nome e indirizzo del produttore
- Identificazione del prodotto
- Una dichiarazione di conformità al CRA
- Un elenco delle norme pertinenti e delle procedure di conformità utilizzate
- Riferimento all'esame UE del tipo (se applicabile)
- Firma, data e recapiti della persona responsabile

Il contenuto della dichiarazione di conformità è riportato negli allegati V e VI del CRA.

6. Obblighi di segnalazione e post-commercializzazione

6.1 Obblighi di segnalazione

In conformità con l'articolo 14, le PMI sono tenute a segnalare sia le "vulnerabilità attivamente sfruttate" che gli "incidenti gravi". Questi sono definiti come segue:

- Una vulnerabilità attivamente sfruttata è una falla di sicurezza già utilizzata o oggetto di un attacco dannoso attivo.
- Un incidente grave è un evento che incide sulla riservatezza, l'integrità e la disponibilità del prodotto, compresa l'introduzione di malware.

L'articolo 14 del CRA descrive inoltre un incidente grave come un incidente che (a) influisce negativamente o è in grado di influire negativamente sulla capacità di un PDE di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati o funzioni sensibili o importanti, OPPURE (b) ha portato o è in grado di portare all'introduzione o all'esecuzione di codice dannoso in un PDE o nella rete e nei sistemi informativi di un utente del prodotto.
I requisiti di segnalazione per questi due tipi di eventi differiscono, come spiegato nelle sezioni seguenti. I dettagli sono disponibili nell'articolo 14 del CRA.

Oltre alla segnalazione obbligatoria di qualsiasi vulnerabilità attivamente sfruttata e di incidenti gravi, il CRA prevede anche la segnalazione volontaria di altri incidenti o minacce al PDE. La stessa procedura di segnalazione simultanea al CSIRT e all'ENISA, tramite la piattaforma di segnalazione unica, si applica anche a questi casi

6.2 Procedura di segnalazione

Tutte le notifiche obbligatorie devono essere presentate tramite la futura piattaforma unica di segnalazione[25] all'ENISA e contemporaneamente al CSIRT della sede principale del produttore nell'UE. Una volta che la piattaforma unica di segnalazione (vedi sotto) sarà disponibile, ciò avverrà tramite un'unica notifica alla piattaforma.

Vulnerabilità attivamente sfruttate

La segnalazione delle vulnerabilità attivamente sfruttate avviene in tre fasi distinte:

- Fase 1: allerta precoce entro **24 ore** dalla presa di coscienza. Se del caso, in questa fase devono essere identificati gli Stati membri in cui il prodotto è stato messo a disposizione.
- Fase 2: segnalazione iniziale della vulnerabilità entro **72 ore** dalla sua individuazione, comprendente:

[25] Cfr. articolo 16 del CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

- informazioni generali sul prodotto, la natura dell'exploit e la vulnerabilità in questione.
- Eventuali misure correttive o di mitigazione adottate e misure correttive o di mitigazione che gli utenti possono adottare.
- Una valutazione da parte del fabbricante del livello di sensibilità delle informazioni notificate.

- Fase 3: segnalazione finale entro **14 giorni** dalla disponibilità di una correzione, comprendente:
  - Una descrizione della vulnerabilità, compresa la sua gravità e il suo impatto;
  - Se disponibili, informazioni relative a eventuali soggetti malintenzionati che hanno sfruttato o stanno sfruttando la vulnerabilità;
  - Dettagli sull'aggiornamento di sicurezza o altre misure correttive che sono state rese disponibili per porre rimedio alla vulnerabilità.

Incidenti di sicurezza gravi

Anche la segnalazione di incidenti di sicurezza gravi avviene in tre fasi distinte, con una differenza sostanziale nell'ultima fase.

- Fase 1: Allerta precoce entro **24 ore** dalla scoperta, che include:
  - Un parere sul fatto che l'incidente sia sospettato di essere causato da atti illeciti o dolosi, che indichi anche.
  - Se del caso, gli Stati membri in cui il prodotto è stato messo a disposizione.
- Fase 2: segnalazione dell'incidente entro **72 ore** dalla sua individuazione, che include:
  - La natura dell'incidente
  - Una valutazione iniziale dell'incidente
  - Eventuali misure correttive o attenuanti adottate e misure correttive o attenuanti che gli utenti possono adottare
  - Una valutazione da parte del fabbricante del livello di sensibilità delle informazioni comunicate.
- Fase 3: Segnalazione definitiva entro **un mese** dalla notifica entro 72 ore, comprendente:
  - Una descrizione dettagliata dell'incidente, compresa la sua gravità e il suo impatto;
  - Il tipo di minaccia o la causa principale che potrebbe aver provocato l'incidente;
  - Misure di mitigazione applicate e in corso.

Notifica agli utenti

Per entrambi i tipi di incidente, una volta venuti a conoscenza della vulnerabilità o dell'evento, i produttori devono informare senza indugio gli utenti interessati (e, se del caso, tutti gli utenti), fornendo indicazioni per la mitigazione dei rischi in un formato facilmente automatizzabile e leggibile da dispositivi elettronici. Qualora i produttori non provvedano alla notifica, il CSIRT può intervenire per informare gli utenti.

Segnalazione volontaria

Al di fuori dell'ambito dei loro obblighi di notifica, ai sensi dell'articolo 15, i fabbricanti sono incoraggiati a segnalare volontariamente qualsiasi vulnerabilità e minaccia che possa influire sulla sicurezza informatica di un PDE. Anche la notifica di incidenti non gravi è volontaria.

Questo meccanismo di segnalazione volontaria potrebbe introdurre una buona pratica per le PMI con un effetto positivo indiretto per il fabbricante e i suoi clienti, aumentando la visibilità della minaccia e prevenendo così ulteriori incidenti. Inoltre, laddove sia difficile valutare con esattezza se una particolare vulnerabilità sia attivamente sfruttata o se un incidente sia grave, la segnalazione volontaria sembra essere l'opzione più sicura.

6.3 Cooperazione con le autorità dell'UE e nazionali

6.3.1 ENISA e CSIRT sulla gestione delle vulnerabilità

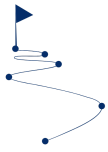
I produttori segnalano le vulnerabilità attivamente sfruttate e gli incidenti gravi all'ENISA e al CSIRT nazionale secondo le disposizioni di cui all'articolo 14 della legge. I requisiti a carico del produttore sono presentati nella sezione 5.2 delle presenti linee guida.

6.3.2 Autorità nazionali di vigilanza del mercato

Le autorità di vigilanza del mercato (MSA) sono responsabili dell'applicazione degli obblighi previsti dal CRA in ciascuno Stato Membro. Le modalità di applicazione sono illustrate nel capitolo V del CRA.

Le conseguenze per i fabbricanti comportano l'obbligo di:

- Cooperare durante le indagini, gli audit e le ispezioni;
- Fornire la documentazione (ad esempio SBOM, valutazioni dei rischi, fascicoli tecnici) su richiesta;
- Informare le MSA di eventuali casi di non conformità e misure correttive, se applicabile.



7. Le fasi per l'attuazione del CRA da parte delle PMI

7.1 Valutazione iniziale dell'ambito di applicazione e delle lacune

Il primo passo per conformarsi al CRA consiste nello sviluppare una chiara comprensione di quali prodotti rientrano nel suo ambito di applicazione, quale ruolo riveste l'organizzazione rispetto a tali prodotti e quali requisiti i prodotti rispettano o non rispettano. Tale comprensione si ottiene attraverso una valutazione dell'ambito di applicazione e delle eventuali lacune.

Il presente documento, insieme agli strumenti forniti dal progetto CONFIRMATE, ha lo scopo di supportare l'analisi iniziale, comprendente l'ambito di applicazione, l'identificazione dei ruoli, la valutazione delle lacune e il monitoraggio dei progressi nel tempo, man mano che l'organizzazione affronta i requisiti non conformi. In questo contesto, la valutazione delle lacune dovrebbe essere considerata un "documento vivo", aggiornato regolarmente per riflettere i progressi compiuti. In tal modo, la valutazione rappresenterà accuratamente lo stato dell'organizzazione rispetto alla conformità in ogni momento.

7.2 Sviluppo di un piano di implementazione

Il piano di implementazione può essere sviluppato una volta completata la valutazione iniziale delle lacune. Analogamente alla valutazione stessa, il piano dovrebbe essere considerato un documento in evoluzione, che integra le lezioni apprese man mano che il progetto di implementazione procede.

Per quanto riguarda la pianificazione, si raccomanda di adottare un approccio "a ondate successive": le attività previste per i tre mesi successivi dovrebbero essere pianificate in modo molto dettagliato, mentre quelle più lontane nel tempo possono essere stimate sulla base dello sforzo massimo previsto. Inserire un livello eccessivo di dettaglio nelle fasi future può risultare controproducente, poiché le attività a lungo termine tendono a essere riviste per riflettere le lezioni apprese nelle prime fasi del progetto.

In ogni caso, qualora non fosse già presente, la valutazione dei rischi dovrebbe essere considerata una priorità. I risultati di tale valutazione giustificheranno le misure pianificate e adottate e permetteranno all'organizzazione di stabilire le priorità di intervento nel modo più efficiente possibile.

Per la pianificazione a breve termine si raccomanda di mantenere le attività semplici, definire risultati chiari per ogni compito e assegnare il minor tempo possibile a ciascuna attività. Questo approccio aiuta a evitare la tipica situazione in cui i compiti sembrano rimanere indefinitamente "al 90%", senza mai essere completati del tutto.

Infine, le PMI possono sfruttare appieno le risorse sviluppate appositamente per supportarle nel percorso di conformità al CRA nell'ambito del programma Europa digitale: gli strumenti del progetto CONFIRMATE, elencati nell'appendice E, altri progetti pertinenti riportati nell'appendice F, e le risorse di supporto europee e nazionali per le PMI indicate nell'appendice D.

7.3 Formazione e sensibilizzazione del personale

I programmi di formazione e sensibilizzazione del personale rappresentano una componente essenziale del percorso verso la conformità. Sebbene queste linee guida e gli strumenti correlati mirino a semplificare i requisiti del CRA, è fondamentale che il personale sviluppi e mantenga una conoscenza approfondita del regolamento e delle politiche ad esso collegate.

Indicazioni aggiuntive, strumenti e modelli utili alle PMI per implementare i requisiti essenziali di sicurezza e soddisfare gli obblighi documentali sono riportati negli allegati. L'utilizzo di tali risorse non è obbligatorio, fatta eccezione per il modello di dichiarazione di conformità, ma dovrebbe essere valutato nell'ambito di una pianificazione strutturata a livello organizzativo.

8. Tempistiche e periodi di transizione

Le date chiave nel calendario di attuazione del CRA sono le seguenti:

Data	Evento
11.12.24	Entrata in vigore del CRA
11.06.26	Obblighi di notifica degli organismi di valutazione della conformità applicabili[26]
30.08.26	Scadenza per le norme di tipo A e le norme armonizzate di tipo B relative alla gestione delle vulnerabilità

[26] Si tratta di un obbligo a carico degli Stati membri e non dei fabbricanti

11.09.26	Entrano in vigore gli obblighi di segnalazione delle vulnerabilità e degli incidenti di sicurezza.
30.10.27	Scadenza per le restanti norme armonizzate di tipo B.
11.12.27	Piena applicazione del CRA

Appendice A: Dichiarazione di conformità UE semplificata

Con la presente, ... [nome del fabbricante] dichiara che il prodotto con elementi digitali di tipo ... [designazione del tipo di prodotto con elemento digitale] è conforme al regolamento (UE) 2024/2847 (1).

Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: ...

Appendice B: Modello di valutazione dei rischi

Il toolbox interoperabile dell'ENISA per la gestione dei rischi nell'UE fornisce una metodologia armonizzata e riconosciuta a livello europeo. È stato progettato per supportare un'applicazione coerente delle pratiche di gestione dei rischi in tutta l'UE, integrando elementi di ISO/IEC 27005, della direttiva NIS2 e delle migliori pratiche settoriali. È importante notare, tuttavia, che il toolbox non è stato sviluppato specificamente per soddisfare i requisiti del CRA, bensì come strumento generale destinato a numerosi ambiti applicativi.

Il toolbox include modelli standardizzati e linee guida per:

- Identificazione e valutazione delle risorse
- Analisi delle minacce e delle vulnerabilità
- Stima e valutazione dei rischi
- Definizione delle azioni di trattamento e mitigazione dei rischi
- Integrazione con i controlli di sicurezza richiesti dall'allegato I del CRA[27]

Supporta valutazioni qualitative e semiquantitative ed è interoperabile con metodologie nazionali e internazionali. L'impiego di questo toolbox assicura coerenza, verificabilità e completa tracciabilità delle decisioni in materia di sicurezza, facilitando le valutazioni di conformità e la preparazione della documentazione tecnica richiesta dal CRA.

[27] Si noti che non si tratta di una mappatura esplicita dei controlli del CRA.

Appendice C: Norme pertinenti

- ETSI TS 103 701, Allegati B e C possono essere utilizzati per strutturare la documentazione tecnica pronta per la revisione utilizzando i modelli ICS/IXIT
- **ISO/IEC 27001** - Sistema di gestione della sicurezza delle informazioni (ISMS)
- **ISO/IEC 27701** - Sistema di gestione delle informazioni sulla privacy (PIMS)
- ETSI EN 303 645 - Requisiti di sicurezza di base per l'IoT consumer, dove le clausole 4-5 possono essere utilizzate per definire i requisiti di sicurezza di base
- **OWASP ASVS** - Standard di verifica della sicurezza delle applicazioni
- **CIS Benchmarks** - Linee guida per la configurazione sicura
- **Linee guida della IoT Security Foundation** - Best practice per la sicurezza dei dispositivi IoT
- **NIST SP 800-53** - **Controlli di sicurezza e privacy per sistemi informativi e organizzazioni.**
- **NIST SP 800-37** - Quadro di gestione dei rischi (RMF), che fornisce un processo che integra le attività di gestione dei rischi relativi alla sicurezza, alla privacy e alla catena di approvvigionamento informatica nel ciclo di vita dello sviluppo del sistema.
- **Il quadro di riferimento per la sicurezza informatica (CSF) del NIST**, che fornisce indicazioni sulla gestione dei rischi legati alla sicurezza informatica
- **IEC 62443 / ISA-62443** - Standard di sicurezza per i sistemi di automazione e controllo industriale
- **ISO 9001** - Sistema di gestione della qualità
- **CMMC** - Certificazione del modello di maturità della sicurezza informatica
- **GDPR** - Regolamento generale sulla protezione dei dati

Appendice D: Risorse europee e nazionali di supporto per le PMI

La Commissione europea, l'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) e il Centro europeo di competenza per la sicurezza informatica (ECCC) pubblicano regolarmente rapporti sulla sicurezza informatica, molti dei quali contengono linee guida utili alle PMI che devono implementare il CRA.

In particolare, le Linee guida ENISA per la sicurezza dell'Internet of Things (IoT)[28] efiniscono requisiti di sicurezza completi lungo l'intero ciclo di vita del prodotto: dalla definizione dei requisiti e dalla progettazione, fino alla consegna all'utente finale, alla manutenzione e allo smaltimento. Lo studio è stato sviluppato specificamente per supportare produttori, sviluppatori, integratori e altri stakeholder della catena di fornitura IoT nel prendere decisioni informate in materia di sicurezza durante la creazione, l'implementazione o la valutazione di tecnologie IoT.

Inoltre, la Guida ENISA alla sicurezza informatica per le PMI è un documento specificamente pensato per migliorare la postura di sicurezza delle piccole organizzazioni, inclusi i produttori di tecnologie digitali.

A livello nazionale, la missione dei Centri nazionali di competenza per la sicurezza informatica è promuovere l'eccellenza nella ricerca e la competitività dell'Unione nel campo della cybersecurity. Un elenco aggiornato dei centri è stato pubblicato dall'ECCC.[29] .

Oltre ai centri di competenza, molti Stati membri hanno istituito un'agenzia nazionale per la cybersecurity. Mentre i centri di competenza si concentrano principalmente su ricerca e innovazione, le agenzie nazionali tendono a coprire una più ampia gamma di aspetti operativi, regolatori e di supporto (con mandati specifici che variano tra i Paesi). Alcuni esempi includono:

- **Belgio**: CCB - Centro per la sicurezza informatica del Belgio
- **Germania**: BSI – Ufficio federale per la sicurezza informatica
- **Francia**: ANSSI – Agence nationale de la sécurité des systèmes d'information
- **Italia**: ACN – Agenzia per la Cybersicurezza Nazionale
- **Romania**: DNSC – Directoratul Național de Securitate Cibernetică

Infine, anche organizzazioni industriali e professionali mettono a disposizione risorse per aiutare i propri membri a comprendere e rispettare il CRA. Tra queste, ad esempio, la Digital SME Alliance, l'ECSO (a livello UE) e Agoria.

[28]Disponibile all'indirizzo: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
[29]Disponibile all'indirizzo: https://cybersecurity-centre.europa.eu/nccs-0_en

Appendice E: Strumenti CONFIRMATE

Di seguito è riportata una breve panoramica delle altre linee guida, corsi di formazione, strumenti e documentazione che accompagnano il presente documento. Tutti i materiali del progetto sono disponibili su www.confirmate-project.eu/materials .

Parte 1 Linee guida e metodologie

Metodologia di pentesting: documento sviluppato e sottoposto a revisione paritaria che mira a supportare le PMI nella preparazione e nell'esecuzione di test di penetrazione sui PDE, in linea con i requisiti del Cyber Resilience Act (CRA). Basato sugli standard di settore, il documento sintetizza e fornisce una guida essenziale su ciò che è necessario per condurre un pentest di prodotto efficace e su quali risultati ci si può ragionevolmente attendere, tenendo conto delle caratteristiche dei prodotti che rientrano nelle diverse categorie previste dal CRA.

D3.1 - Architettura per la valutazione automatizzata della conformità al CRA: Panoramica dettagliata e completa del framework CONFIRMATE, che ne illustra in modo chiaro e metodico le funzionalità e la struttura prevista. Il documento introduce e definisce il processo di valutazione della conformità previsto dal CRA, fornendo ai lettori il contesto normativo essenziale. Successivamente, descrive con precisione come gli utenti finali interagiranno con il framework CONFIRMATE e in che modo potranno trarne beneficio nell'ambito dei loro processi di valutazione della conformità al CRA.
Dopo questa parte orientata all'utente, il documento presenta l'architettura software prevista, descrivendo in dettaglio gli elementi fondamentali, tra cui i componenti principali, la suddivisione modulare e le interazioni tra i vari moduli.

D2.2 - Modello di dati probatori: rappresenta una base per la raccolta e la valutazione automatizzata delle prove tecniche relative alle diverse tecnologie, garantendo un'acquisizione e un'organizzazione efficienti delle informazioni necessarie. Grazie all'uso di formati leggibili da macchina, il modello facilita l'integrazione delle prove in strumenti di conformità automatizzati, riducendo lo sforzo manuale richiesto per la documentazione e migliorando l'accuratezza delle valutazioni di conformità. Si segnala tuttavia che questo approccio non assicura la piena conformità al CRA, poiché alcuni requisiti non sono totalmente trasponibili in metodi automatizzati di raccolta dati. Il modello di dati probatori supporta inoltre la definizione di metriche specifiche derivate dai requisiti essenziali del CRA, fornendo misure quantificabili della conformità.

Parte 2 Strumento open source per la valutazione automatizzata della conformità

CONFIRMATE propone uno strumento di automazione open source che semplifica la valutazione della conformità ai requisiti essenziali di sicurezza informatica del CRA. Lo strumento elenca tutti i requisiti e le metriche essenziali di sicurezza, confronta automaticamente le impostazioni di sicurezza con le specifiche del CRA e individua le singole esigenze di intervento. I dashboard intuitivi e le funzionalità strutturate aiutano le organizzazioni a identificare rapidamente quali requisiti essenziali di sicurezza sono già implementati e quali devono ancora essere valutati o adottati, risparmiando tempo prezioso nei controlli di conformità e fornendo informazioni chiare e operative per garantire miglioramenti continui.

Inoltre, strumenti di documentazione complementari includono:

- D2.2 – Evidence Data Model, che supporta l'automazione della verifica della conformità attraverso un approccio strutturato alla raccolta e alla valutazione delle prove.
- D3.1 – Architecture for Automated CRA Conformance Assessment, un documento che offre una panoramica dettagliata e completa del framework CONFIRMATE, ne illustra le funzionalità e la struttura, introduce il processo di valutazione della conformità e mostra come gli utenti finali interagiranno con il framework, traendo vantaggio nel processo di valutazione della conformità al CRA.

Parte 3 Formazione e workshop CONFIRMATE

L'elenco è un documento in continua evoluzione, con una serie di corsi di formazione e workshop in programma fino a luglio 2026.

Introduzione alla conformità CRA: tutto quello che c'è da sapere sul Cyber Resilience Act (CRA) dell'UE[30] fornisce una panoramica completa dei principi e degli obblighi fondamentali del CRA. Il video illustra come il CRA impatti produttori, importatori, distributori e gestori di software open source, delineando ruoli e responsabilità, classificazioni dei prodotti basate sul rischio (predefinito, importante e critico), nonché requisiti di sicurezza, marcatura CE e procedure di valutazione della conformità. Vengono inoltre trattati temi cruciali quali la divulgazione delle vulnerabilità, la segnalazione degli incidenti, la Software Bill of Materials (SBOM), i tempi di applicazione e le sanzioni previste in caso di non conformità.

[30] Disponibile su YouTubehttps://youtu.be/-QbPIFVobNw

Spiegazione della metodologia di pentesting[31]

Nell'ambito della serie di corsi di formazione sulla conformità al Cyber Resilience Act (CRA), questo modulo fornisce una guida completa e dettagliata alla metodologia di penetration testing per i prodotti con elementi digitali. È progettato per produttori, PMI e team di sicurezza informatica che desiderano soddisfare i requisiti CRA in modo efficace ed efficiente. La formazione copre le cinque fasi chiave dei test di penetrazione in linea con il CRA e spiega come pianificare, condurre e segnalare i test in conformità con gli standard CRA. Chiarisce inoltre i requisiti di conformità per i prodotti di classe I importante, classe II importante e categoria default.

Appendice F: Strumenti di altri progetti europei

In parallelo a CONFIRMATE, è stata avviata una serie di progetti europei volti a supportare le PMI nella conformità al CRA. Ogni progetto adotta un approccio differente, coinvolge gruppi di paesi diversi e sviluppa risorse e strumenti complementari. L'elenco dei progetti attivi nel periodo 2025-2026, raccolti da CyberStandEU[32] è il seguente:

1. CRA-AI sviluppa una piattaforma basata sull'intelligenza artificiale per aiutare le PMI a raggiungere e mantenere la conformità al Cyber Resilience Act dell'UE, riunendo esperti di sicurezza informatica di sei paesi europei.
2. CURIUM sviluppa il Compliance Continuum, una serie di strumenti per automatizzare e semplificare la conformità al CRA. Offrendo valutazioni di sicurezza informatica, gestione dei rischi e test di vulnerabilità, aiuta le PMI a ridurre i costi, accelerare la certificazione e rafforzare l'ecosistema di sicurezza digitale europeo.
3. OSCRAT sviluppa strumenti gratuiti e open source per aiutare le PMI europee, i responsabili politici e le associazioni industriali a raggiungere la conformità al CRA e rafforzare le pratiche di sicurezza informatica.
4. OCCTET sviluppa un toolkit open source progettato per aiutare le PMI ad automatizzare la conformità al CRA per il software open source. Il toolkit comprende una checklist di conformità, strumenti di valutazione automatizzati, un database federato, strumenti per l'analisi delle dipendenze e risorse per il reporting.
5. CYBERFORT aiuta le PMI a soddisfare i requisiti del CRA offrendo strumenti su misura, guida di esperti e formazione. Attraverso una piattaforma aperta e la collaborazione con aziende di sicurezza informatica, autorità e parti interessate del settore, rafforza la resilienza informatica e la consapevolezza in tutta Europa.
6. TRUSTBOOST rafforza la sicurezza informatica, la resilienza e la conformità in tutta l'UE promuovendo la collaborazione in materia di certificazione e il rispetto delle principali normative europee.
7. CRACoWi (Cyber Resilience Act Compliance Wizard) crea un assistente digitale per aiutare le PMI, i produttori, i distributori e gli importatori a soddisfare gli standard del

[31] Disponibile su YouTube: https://youtu.be/wpJluHL9IIQ
[32] Disponibile all'indirizzo: https://cyberstand.eu/events/impacting-cra-defining-standards-future

CRA, garantendo la sicurezza dei prodotti dalla progettazione alla fase post-commercializzazione.

8. CRACY: (CRA made Easy) aiuta le PMI europee a soddisfare i requisiti del CRA semplificando la conformità dei prodotti con elementi digitali, promuovendo le migliori pratiche e prodotti e servizi più sicuri.

Appendice G: Relazione con altre normative UE

Pur non essendo possibile fornire in questo documento un'analisi completa del rapporto tra il CRA e le altre normative UE, di seguito sono riportati alcuni dei collegamenti più rilevanti:

1. *Il nuovo quadro legislativo (CE/2008/765 e CE:2008/768):* il CRA si basa sul NLF e ne estende essenzialmente il campo di applicazione ai prodotti con elementi digitali. Ciò è descritto in dettaglio nella sezione 4.1 delle presenti linee guida.
2. *Resilienza informatica:* sia la direttiva NIS2 che il regolamento DORA mirano a migliorare la resilienza informatica in tutta l'UE. Essi stabiliscono la gestione dei rischi di sicurezza informatica e la segnalazione degli incidenti da parte delle entità in relazione ai loro servizi essenziali. Il CRA integra queste iniziative imponendo requisiti di sicurezza relativi ai prodotti con elementi digitali, che confluiscono nel quadro normativo dell'UE sui prodotti.
3. *La direttiva sulle apparecchiature radio (RED) (direttiva 2014/53/UE)* si concentra sulla sicurezza, la compatibilità elettromagnetica e l'interoperabilità dei prodotti dotati di apparecchiature radio. Il CRA si concentra sulla sicurezza informatica e ha un ambito di applicazione più ampio (che include il software, non solo l'IoT). Sostituisce l'atto delegato RED per la sicurezza informatica.
4. *Il regolamento sulle macchine (regolamento (UE) 2023/1230)* riguarda la salute e la sicurezza nell'uso delle macchine. Esso è complementare al CRA, che si applica ai componenti digitali delle macchine. Entrambi i regolamenti si applicano contemporaneamente.
5. *GDPR dell'UE:* il CRA si basa sul GDPR che richiede la protezione e la minimizzazione di tutti i dati (personali e non) trattati da prodotti con elementi digitali immessi sul mercato dell'UE.
6. *L'AI Act* (Regolamento (UE) 2024/1689) disciplina l'affidabilità e la sicurezza dei sistemi (AI). Si applica alle funzionalità AI ad alto rischio, mentre il CRA si applica alla sicurezza informatica del prodotto stesso. Un sistema AI ad alto rischio deve essere conforme sia all'AI Act che ai requisiti di sicurezza informatica del CRA.
7. *Il Digital Services Act (DSA) e il Digital Markets Act (DMA) dell'UE* impongono la responsabilità delle piattaforme e la moderazione dei contenuti (DSA) nonché l'equità di mercato per i gatekeeper (DMA). Il CRA non si sovrappone direttamente a queste normative, ma si applica al software utilizzato dalle piattaforme e dai sistemi di backend.
8. *Legge sulla sicurezza informatica (CSA)* (Regolamento (UE) 2019/881): il CRA fa riferimento ai sistemi di certificazione sviluppati nell'ambito della CSA in base ai requisiti di valutazione della conformità (per i dettagli, cfr. la sezione 4 delle presenti linee guida).