SECURE
Cyber Resilience for SMEs

CRA101: Comprendere gli obblighi previsti dal CRA

31/03/2026

Funded by the European Union

Dichiarazione sui finanziamenti UE: Finanziato dall'Unione Europea nell'ambito del GA n. 101190325.
I punti di vista e le opinioni espressi sono tuttavia esclusivamente degli autori e non riflettono necessariamente quelle dell'Unione Europea o del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza.
Né l'Unione Europea né l'autorità che eroga il finanziamento possono essere ritenute responsabili per tali opinioni.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Nota ECCC: Il progetto è sostenuto dal Centro europeo di competenza per la cibersicurezza e dai suoi membri

DICHIARAZIONE DI NON RESPONSABILITÀ

Il presente documento fa parte del Deliverable D4.1 "Linee guida e materiali per la conformità delle PMI al CRA" del progetto SECURE. È stato pubblicato per la prima volta nell'ottobre del 2025 e aggiornato nel marzo del 2026.

Questa versione è una traduzione del documento originale in lingua inglese; in caso di discrepanze o ambiguità interpretative, prevale la versione originale in inglese.

Primo autore: *Centre for Cybersecurity Belgium (CCB)*

Secondo autore: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Indice

Elenco delle tabelle e delle figure

Abbreviazioni

CE - Conformité Européenne, ovvero Conformità Europea

CRA – Cyber Resilience Act

CSIRT – Computer Security Incident Response Team

CVD – Coordinated Vulnerability Disclosure

ENISA – European Union Agency for Cybersecurity

UE – Unione Europea

DoC UE – Declaration of Conformity dell'Unione Europea

NB – Notified Body

PED – Prodotto con elementi digitali

SBOM – Software Bill of Materials (Distinta base del software)

PMI – Piccole e medie imprese

SPOC – Single Point of Contact

Introduzione

Il Cyber Resilience Act (CRA) dell'Unione Europea (UE), Regolamento (UE) 2024/2847, è stato adottato con l'obiettivo di migliorare la preparazione e la resilienza in materia di cibersicurezza del mercato digitale dell'UE alla luce delle crescenti sfide in questo ambito. Introducendo norme armonizzate e chiari requisiti minimi di cibersicurezza, il CRA intende ridurre le vulnerabilità e tutelare sia i consumatori che le imprese. Sebbene questo regolamento fondamentale sia entrato in vigore nel dicembre 2024, la sua attuazione è graduale, prevedendo un periodo di transizione e di adattamento dal 2024 al 2027. Concretamente, il CRA elenca gli obblighi a carico dei fabbricanti, degli importatori e dei distributori di prodotti con elementi digitali (PED). **L'articolo 13 e l'Allegato I** del CRA elencano i requisiti essenziali di cibersicurezza che i fabbricanti devono rispettare, sia quando immettono i loro PED sul mercato UE sia durante l'intero ciclo di vita del PED. La parte I dei requisiti dell'Allegato I si concentra sulle proprietà dei PED, mentre la parte II si concentra sulla gestione delle vulnerabilità. Oltre ai requisiti previsti dall'articolo 13 e dall'Allegato I, il CRA impone ulteriori requisiti fra cui, ad esempio, requisiti in materia di informazioni e istruzioni per l'uso (Allegato II), obblighi di segnalazione (articoli 14-17) e conformità (articoli 27-32). In uno sforzo preliminare volto a tradurre gli obblighi giuridici chiave in orientamenti concreti, **le presenti linee guida offrono una panoramica semplificata[1] degli obblighi**, articolati in **cinque sezioni**, da considerare **come requisiti minimi**. L'obiettivo è quello di migliorare l'accessibilità del regolamento e aumentare la consapevolezza e la comprensione a livello di base, in particolare per le piccole e medie imprese (PMI), in linea con gli obiettivi **del progetto SECURE**[2] . Per indicazioni tecniche e strumenti sull'attuazione pratica di queste disposizioni, ulteriori materiali vengono resi disponibili su base continuativa **nell'archivio aperto di SECURE**.

Timeline del CRA:

- Entrata in vigore: 10 dicembre 2024
- Obblighi di segnalazione: 11 settembre 2026
- Piena applicazione dei requisiti del CRA: 11 dicembre 2027

[1] Si tratta di un elenco non esaustivo volto a semplificare gli obblighi previsti dal CRA e non include le eccezioni previste dalla normativa. Per fornire una panoramica generale, sono stati inclusi solo gli obblighi principali, selezionati sulla base di un'attenta lettura del testo normativo del CRA.

[2] Il progetto "Strengthening EU SMEs Cyber Resilience" (SECURE) offre sostegno finanziario e orientamento alle PMI per adeguarsi agli obblighi previsti dal CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Comprendere gli obblighi del CRA - CRA 101

1. Valutazione dei rischi di cibersicurezza

Al fine di ottemperare all'obbligo di garantire che il proprio PED «sia stato progettato, sviluppato e prodotto in conformità ai requisiti essenziali di cibersicurezza di cui alla parte I dell'allegato I»[3] – ovvero di garantire «un livello adeguato di cibersicurezza basato sui rischi»[4] – *è* necessario effettuare una valutazione dei rischi di cibersicurezza. Tale valutazione deve essere **documentata**[5] e **aggiornata regolarmente** per tutta la durata del cosiddetto «periodo di assistenza»[6] .

In concreto, la valutazione dei rischi dovrebbe includere, almeno,[7] :

1) **Un'analisi dei rischi di cibersicurezza** che tenga conto di:
   - La finalità prevista e l'uso ragionevolmente prevedibile del PED;
   - Le condizioni d'uso (ad es. ambiente operativo, attivi da proteggere).
2) **Un chiarimento, una spiegazione e/o una giustificazione** su:
   - L'applicazione del requisito di "cibersicurezza fin dalla progettazione" ([8]) – ossia, come viene applicato?
   - L'applicabilità (o non applicabilità) dei requisiti di cui all'allegato I, parte I, al PED – ossia, i requisiti di sicurezza sono applicabili e in che modo?
   - L'applicazione e l'attuazione dei requisiti di gestione delle vulnerabilità[9] – ossia, come vengono applicati?

Quando un PED contiene componenti provenienti da terzi, il CRA prevede che venga applicata **la dovuta diligenza** per salvaguardare la cibersicurezza del prodotto finale. Ciò può significare, ad esempio, segnalare al fabbricante una vulnerabilità identificata in una componente e, in seguito, occuparsi di trovare una soluzione rispetto a tale vulnerabilità. A

[3] Art. 13, paragrafo 1, CRA.
[4] Allegato I, Parte I, punto 1, CRA.
[5] Documentazione tecnica: chiarita al punto 5.
[6] Periodo di assistenza: chiarito al punto 2.
[7] Art. 13, paragrafo 3, CRA.
[8] Allegato I, Parte I, punto 1, CRA.
[9] Allegato I, Parte II, CRA.

tal fine, è necessario mantenere una "Software Bill of Materials" (SBOM)[10] e una politica di "divulgazione coordinata delle vulnerabilità" (o Coordinated Vulnerability Disclosure - CVD) da applicare ai fornitori, che, su richiesta, devono essere messe a disposizione delle autorità di vigilanza del mercato.

2. Gestione delle vulnerabilità e aggiornamenti di sicurezza

Come indicato all'articolo 13, paragrafo 8, i fabbricanti devono garantire che le vulnerabilità del PED e dei suoi componenti siano "gestite in modo efficace e in conformità con i requisiti essenziali di cui all'allegato I, parte II"[11] per tutto il periodo di assistenza. Ciò significa, tra le altre cose[12] :

1) **Identificare e documentare le vulnerabilità** – ossia redigere la SBOM (almeno per le dipendenze di primo livello) e tenerla a disposizione per fornirla, su richiesta, alle autorità di vigilanza del mercato[13] ;
2) Affrontare e correggere le vulnerabilità senza indugio – ossia **fornire aggiornamenti di sicurezza** senza indebiti ritardi e a titolo gratuito (con messaggi di avviso per gli utilizzatori):
    - Ogni aggiornamento di sicurezza rilasciato durante il periodo di assistenza deve rimanere disponibile per almeno 10 anni dopo il rilascio, o per il resto del periodo di assistenza, a seconda di quale dei due periodi sia più lungo[14] .
3) **Rivedere e testare** regolarmente la sicurezza del prodotto;
4) **Condividere le informazioni** relative alle vulnerabilità (risolte e potenziali), al loro impatto e gravità, alle istruzioni per gli utilizzatori per la correzione, agli indirizzi di contatto per la segnalazione delle vulnerabilità, nonché definire e applicare una politica CVD.

[10] Per SBOM si intende una „distinta base del software", ossia una registrazione formale dei dettagli e delle relazioni nella catena di approvvigionamento dei componenti inclusi negli elementi software dei PED (Art. 3(39), CRA).
[11] Art. 13, paragrafo 8, CRA.
[12] Allegato I, Parte II, CRA.
[13] La condivisione con gli utilizzatori è facoltativa.
[14] Art. 13, paragrafo 9, CRA.

Il «periodo di assistenza» di cui sopra «riflette il periodo di tempo durante il quale si prevede che il prodotto sia in uso»[15] e dovrebbe tenere conto in modo proporzionato delle aspettative degli utilizzatori, della natura (finalità) del PED e della normativa dell'Unione pertinente.
In concreto, quando si definisce il periodo di assistenza, è necessario tenere in considerazione che questo dovrebbe:

- avere una durata di almeno cinque anni (a meno che la durata di vita del prodotto non sia inferiore a tale soglia, nel qual caso il periodo di assistenza è pari alla durata di vita del prodotto);
- avere una chiara data di scadenza (mese e anno) che deve essere specificata al momento dell'acquisto/sulla confezione/in formato digitale (il raggiungimento della scadenza dovrebbe essere idealmente notificato agli utilizzatori)[16] .

La determinazione e la definizione del periodo di assistenza devono essere incluse nella Documentazione Tecnica[17].

3. Informazioni per l'utilizzatore, istruzioni e punto di contatto unico

Ai sensi dell'articolo 13, paragrafi 14-18, e dell'allegato II, i fabbricanti *devono*, come minimo, **informare chiaramente gli utilizzatori** includendo su supporto cartaceo/digitale le seguenti informazioni:

- Dettagli del fabbricante (nome, denominazione commerciale registrata o marchio, indirizzo postale, indirizzo e-mail o contatto digitale, sito web);
- Dettagli del PED (nome, tipo, finalità prevista, ambiente di sicurezza e proprietà di sicurezza, funzionalità essenziali, possibili rischi per la cibersicurezza, assistenza tecnica di sicurezza fornito, data di scadenza del periodo di assistenza);
- Istruzioni dettagliate o link alle stesse (riguardanti le misure per un utilizzo sicuro, i possibili effetti sulla sicurezza dei dati dovuti a modifiche del prodotto, l'installazione di aggiornamenti di sicurezza, la dismissione sicura e la rimozione dei dati degli utilizzatori, le impostazioni predefinite per l'installazione degli aggiornamenti di sicurezza);

[15] Art. 13, paragrafo 8, CRA.
[16] Art. 13(19), CRA.
[17] Documentazione tecnica: chiarita al punto 5.

- Nominativo del punto di contatto unico (Single Point of Contact - SPOC) per consentire agli utilizzatori di:
    - Comunicare in modo diretto e rapido con il fabbricante tramite i mezzi di comunicazione preferiti dagli utilizzatori, senza limitarsi agli strumenti automatizzati;
    - Segnalare le vulnerabilità;
    - Identificare la politica CVD.
- Collegamenti web (se applicabili) alla politica CVD, alla Dichiarazione di conformità UE (EU DoC)[18] e alla SBOM (se resa disponibile agli utilizzatori).

Le istruzioni per gli utilizzatori devono essere disponibili in un linguaggio facilmente comprensibile, online o su carta, per almeno dieci anni o per il periodo di assistenza (a seconda di quale sia più lungo).

4. Obblighi di segnalazione: segnalazione di vulnerabilità e incidenti

Per quanto riguarda le segnalazioni[19] , la tabella sottostante fornisce una panoramica dei principali obblighi. Si riportano a seguire ulteriori chiarimenti.

Tabella1 :
Segnalazioni di vulnerabilità e incidenti

Segnalazione	Vulnerabilità	Incidenti
COSA	*Obbligatoria: "*vulnerabilità attivamente sfruttate" *Facoltativa:* vulnerabilità (non attivamente sfruttate); minacce informatiche	*Obbligatoria*: "incidenti gravi" *Facoltativa*: incidenti (non gravi); quasi incidenti

[18] DoC UE: chiarito al punto 5.
[19] Art. 14-17, CRA.

A CHI	CSIRT[20] Piattaforma unica di segnalazione (ENISA) Utilizzatori interessati	
COME	1) Notifica di preallarme (24 ore) 2) Notifica della vulnerabilità (72 ore) 3) Relazione finale (14 giorni)	1) Notifica di preallarme (24 ore) 2) Notifica dell'incidente (72 ore) 3) Relazione finale (1 mese)

4.1. Cosa

Secondo le definizioni di cui all'articolo 3 del CRA,

- Una «vulnerabilità attivamente sfruttata» per essere considerata tale richiede prove attendibili che un soggetto malintenzionato l'ha sfruttata in un sistema senza l'autorizzazione del proprietario del sistema [21] ;
- Un incidente è considerato "grave" quando[22] :
    - Influisce o può influire negativamente sulla capacità del PED di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o delle funzioni; oppure
    - Ha portato o può portare all'introduzione/esecuzione di codici dannosi nel prodotto o nella rete e nei sistemi informativi di un utilizzatore.

4.2. A chi

Il Computer Security Incident Response Team (CSIRT) a cui effettuare la segnalazione è quello dello Stato membro in cui il fabbricante[23] :

- ha lo stabilimento principale; oppure, se non determinabile,

[20] Art. 3, paragrafo 51, CRA: per «CSIRT designato come coordinatore» si intende un team di risposta agli incidenti di cibersicurezza (CSIRT) designato come coordinatore ai sensi dell'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555.

[21] Art. 3, paragrafo 42, CRA.

[22] Art. 3, paragrafo 44, CRA; art. 14, paragrafo 5, CRA.

[23] Il CSIRT è in genere il CERT nazionale: Computer Emergency Response Team.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- ha lo stabilimento con il maggior numero di dipendenti.

Se il fabbricante è stabilito al di fuori dell'UE, è possibile identificare lo Stato membro rilevante, considerando nell'ordine: la sede del rappresentante autorizzato del fabbricante → la sede dell'importatore → la sede del distributore → dove si trova il maggior numero di PED o di utilizzatori.

Fatte salve alcune eccezioni, tutte le notifiche dovranno passare attraverso un'unica piattaforma di segnalazione, che verrà istituita e gestita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), e saranno diffuse ad altri CSIRT e alle autorità di vigilanza del mercato tramite un punto di contatto elettronico.

Gli utilizzatori interessati (e, se del caso, tutti gli utilizzatori) devono inoltre essere informati in merito alle vulnerabilità/agli incidenti e alle azioni da intraprendere, preferibilmente in un formato leggibile da un computer. I CSIRT possono informare gli utilizzatori qualora il fabbricante non lo faccia[24] .

4.3. Come

Esistono diverse differenze nella segnalazione di vulnerabilità e incidenti.

Vulnerabilità

1) **Notifica di preallarme**: deve essere presentata al più tardi entro 24 ore dal momento in cui se ne viene a conoscenza e deve indicare, se del caso, gli Stati membri in cui è disponibile il PED.
2) **Notifica di vulnerabilità**: deve essere presentata entro e non oltre 72 ore dal momento in cui se ne viene a conoscenza e deve includere:
    - Informazioni generali sul PED;
    - Natura generale della vulnerabilità;
    - Misure correttive o di mitigazione adottate o che possono essere adottate dagli utilizzatori;
    - Sensibilità delle informazioni segnalate.
3) **Relazione finale**: deve essere presentata entro e non oltre **14 giorni** dall'adozione delle misure correttive/di mitigazione e deve includere:
    - Descrizione: gravità e impatto;

[24] Art. 14, paragrafo 8, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Informazioni sull'autore dell'attacco, se applicabile;
- Dettagli sull'aggiornamento di sicurezza o su altre misure correttive disponibili.

Incidenti

1) **Notifica di preallarme**: deve essere presentata al più tardi entro 24 ore dal momento in cui se ne viene a conoscenza e deve indicare,
    - Se applicabile, gli Stati membri in cui è disponibile il PED;
    - Se si sospetta che sia stato causato da atti illeciti o dolosi.
2) **Notifica dell'incidente**: deve essere presentata entro e non oltre 72 ore dal momento in cui se ne viene a conoscenza e deve includere:
    - Informazioni generali sulla natura dell'incidente;
    - Valutazione iniziale dell'incidente;
    - Misure correttive o di mitigazione adottate o che possono essere adottate dagli utilizzatori;
    - Sensibilità delle informazioni notificate.
3) **Relazione finale**: deve essere presentata entro un mese dall'invio della notifica dell'incidente e deve includere:
    - Descrizione: gravità e impatto;
    - Tipo di minaccia o causa principale che potrebbe aver causato l'incidente;
    - Misure di mitigazione applicate e in corso.

5. Valutazione della conformità

Prima che un PED sia immesso sul mercato, il fabbricante deve dimostrare che esso è conforme ai requisiti essenziali di cibersicurezza di cui all'allegato I del CRA. Ciò avviene attraverso la **procedura di valutazione della conformità** applicabile alla categoria di prodotto pertinente.

5.1. Procedure di valutazione della conformità

Il CRA prevede, tra l'altro:

- Controllo interno (Modulo A);

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Esame UE del tipo seguito dalla verifica della conformità al tipo (Moduli B + C);
- Garanzia di qualità totale (Modulo H);
- Valutazione nell'ambito di un sistema europeo di certificazione della cibersicurezza, ove applicabile.

Le norme armonizzate e le specifiche comuni non costituiscono procedure di conformità. Tuttavia, possono supportare la dimostrazione della conformità.

5.2. Presunzione di conformità

Un prodotto conforme

- alle norme armonizzate i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale, oppure
- alle specifiche comuni adottate dalla Commissione europea

si **presume conforme**[25] ai requisiti essenziali contemplati da tali norme o specifiche.

Qualora tali norme o specifiche non siano (pienamente) applicate, il fabbricante deve dimostrare direttamente la conformità ai requisiti dell'Allegato I attraverso la procedura di valutazione della conformità applicabile. Ove pertinente, può essere utilizzato anche un certificato europeo di cibersicurezza per dimostrare la conformità, entro i limiti previsti dal CRA.

5.3. Categorie di prodotti

La procedura di valutazione della conformità da applicare dipende dalla classificazione del PED ai sensi del CRA, specificata negli allegati III e IV del CRA[26] . Il CRA distingue tra prodotti ordinari, importanti (Classe I e II) e critici.

A seconda della categoria:

- il controllo interno può essere sufficiente;
- può essere richiesto il coinvolgimento di un organismo notificato (ON); oppure
- La valutazione nell'ambito di uno schema di certificazione europeo può essere obbligatoria o consentita.

La **corretta classificazione** è quindi determinante per stabilire la procedura applicabile.

[25] Art. 27, CRA.

[26] Art. 32, CRA; Allegato VIII, CRA.

Una panoramica delle procedure applicabili per ciascuna classe di prodotti è riportata nella tabella 2 alla pagina seguente.

Tabella2 :
Procedure di valutazione della conformità

	Controllo interno (modulo A)	Esame UE del tipo seguito dalla verifica della conformità al tipo (moduli B + C)	Garanzia di qualità totale (modulo H)	Sistema europeo di certificazione della cibersicurezza	Norme armonizzate/ Specifiche comuni[27]
Prodotti ordinari	X	X	X	X	X Può fornire supporto per la conformità ai requisiti coperti
Prodotti importanti di Classe I	X[28]	X	X	X Livello: sostanziale[29]	X Può fornire supporto di conformità per i requisiti coperti
Prodotti importanti di Classe II		X	X	X Livello: sostanziale[30]	X Può fornire supporto di conformità per i requisiti coperti
Prodotti critici				X Livello: sostanziale	X Può fornire supporto alla conformità per i requisiti coperti

[27] Le norme armonizzate e le specifiche comuni non sono procedure, ma possono supportare la dimostrazione della conformità.

[28] Il controllo interno (modulo A) può essere utilizzato solo quando vengono applicate norme armonizzate, specifiche comuni o, se del caso, un sistema di certificazione pertinente. In caso contrario, le vie applicabili sono l'esame UE del tipo seguito dalla conformità al tipo (moduli B+C) o la garanzia di qualità totale (modulo H).

[29] Se, ai sensi dell'art. 8, paragrafo 1, del CRA, viene adottato un atto delegato, è possibile ricorrere allo schema di certificazione informatica dell'UE. In caso contrario, si ricorre alle norme relative ai prodotti importanti di Classe II.

[30] Si applica la nota 29.

5.4. Dichiarazione di conformità UE (EU DoC)

A seguito di una valutazione della conformità positiva, il fabbricante redige una **Dichiarazione di Conformità UE** (EU DoC)[31] .

In questa dichiarazione, si conferma che il PED è conforme ai requisiti essenziali applicabili e include gli elementi richiesti come previsto dal CRA. La struttura del modello è disponibile nell'Allegato V del CRA. La EU DoC semplificata è disponibile nell'Allegato VI. Deve essere resa disponibile nelle lingue richieste dallo Stato membro in cui il PED è immesso sul mercato e deve rimanere disponibile per il periodo prescritto dalla legge.

5.5. Marcatura CE

Per consentire ai consumatori di identificare i PED che soddisfano i requisiti del regolamento CRA e di prendere decisioni informate al momento dell'acquisto e dell'utilizzo, la **marcatura CE**[32] deve essere «apposta in modo visibile, leggibile e indelebile»[33] prima dell'immissione dei PED sul mercato. Ciò deve avvenire sul prodotto stesso. Qualora ciò non sia possibile a causa della natura del prodotto, la marcatura deve essere apposta sull'imballaggio e inclusa nella dichiarazione di conformità UE (EU DoC) di accompagnamento[34] [35] . La marcatura CE indica che il prodotto è conforme a tutta la legislazione dell'Unione applicabile che richiede la marcatura CE, compreso il CRA.

5.6. Dimostrazione della conformità tramite la documentazione tecnica

Un elemento chiave per la valutazione della conformità è la **documentazione tecnica.** Prevista dall'articolo 31 del CRA e dall'Allegato VII, la documentazione tecnica è rilevante per tutti i punti discussi in precedenza, in quanto deve essere redatta prima che il PED sia immesso sul mercato e aggiornata continuamente per tutto il periodo di assistenza[36] . Rispondendo alla maggior parte degli obblighi del CRA, la documentazione tecnica dovrebbe quindi includere[37] :

[31] Art. 28, CRA; Allegati V-VI, CRA.
[32] Conformité Européenne (Conformità Europea).
[33] Art. 30, paragrafo 1, CRA.
[34] Art. 29-30, CRA.
[35] Si applicano norme aggiuntive qualora un organismo notificato partecipi alla valutazione della conformità.
[36] Art. 31, par. 2, CRA.
[37] Allegato VII, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Descrizione generale del PED (destinazione d'uso, versioni software che incidono sulla conformità, prove delle caratteristiche esterne, marcatura e layout interno per i prodotti hardware, informazioni e istruzioni per l'utilizzatore);
- Descrizione dei processi di progettazione, sviluppo e produzione del PED, nonché di gestione delle vulnerabilità (ad es. descrizione dell'architettura di sistema, SBOM, politica CVD, processi di monitoraggio, ecc.);
- Valutazione dei rischi di cibersicurezza;
- Definizione e chiarimento del periodo di assistenza;
- Norme armonizzate applicate (o parti di esse);
- Rapporti sui test di conformità e rapporti sulla gestione delle vulnerabilità;
- Copia della Dichiarazione di conformità UE.

La Commissione europea sta elaborando un modulo **semplificato di documentazione tecnica** per le microimprese e le piccole imprese[38] . Inoltre, l'articolo 33 stabilisce che sia gli Stati membri che la Commissione europea devono fornire **sostegno alle PMI,** tra l'altro, sotto forma di orientamenti[39] e opportunità di sostegno finanziario.

Il **progetto SECURE offre sostegno finanziario alle PMI tenute a conformarsi al CRA e fornisce linee guida e materiali su base continuativa volti ad assistere le PMI nell'attuazione del CRA**, come la presente linea guida CRA101.

[38] Art. 33, par. 5, CRA.

[39] Art. 26, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusioni

Nel tentativo di fornire una **panoramica accessibile degli obblighi chiave stabiliti dal CRA**, questa linea guida si concentra su **cinque componenti** del CRA, da considerare come contenuti essenziali: (1) Valutazione dei rischi di cibersicurezza; (2) Gestione delle vulnerabilità e aggiornamenti di sicurezza; (3) Informazioni per gli utilizzatori, istruzioni e Punto Unico di Contatto; (4) Obblighi di segnalazione: segnalazione di vulnerabilità e incidenti; (5) Valutazione della conformità. Chiarisce elementi quali il periodo di assistenza, la Dichiarazione di conformità UE e la marcatura CE, nonché la documentazione tecnica. Con l'obiettivo di **aiutare le PMI a orientarsi nel complesso quadro giuridico**, questa linea guida offre una sintesi dei principali obblighi legali che devono essere compresi prima della loro attuazione. Per ulteriori indicazioni pratiche su come affrontare e attuare le disposizioni legali rilevanti, nonché su elementi specifici del CRA (ad esempio, SBOM, gestione delle vulnerabilità, ecc.), nuove linee guida tecniche e altri strumenti saranno resi disponibili su base continuativa **nell'archivio centrale SECURE**, di pari passo con l'evoluzione dell'attuazione del CRA. Come prossimi passi per le PMI, si raccomanda di consultare le altre linee guida disponibili nell'archivio SECURE, quali "**Requisiti essenziali di cibersicurezza del CRA: Allegato I, Parte I",** dove è possibile trovare suggerimenti pratici e raccomandazioni su ciascuna delle disposizioni dell'Allegato I, nonché il "**Quadro metodologico di valutazione della conformità al CRA"** che fornisce un kit di strumenti e una checklist sulla conformità al CRA oltre l'Allegato I.