WHITEPAPER CRA EVIDENCE

Il regolamento sulla ciberresilienza dell'UE: guida pratica alla conformità

Libro bianco per fabbricanti, importatori e distributori di prodotti con elementi digitali.

Versione	1.0
Stato	Documento in aggiornamento continuo
Base	Regolamento (UE) 2024/2847

Cronologia delle modifiche

Questa guida viene aggiornata man mano che evolvono gli orientamenti della Commissione, le norme armonizzate e la prassi di mercato in materia di CRA.

Versione	Data	Descrizione
1.0	17 maggio 2026	Prima pubblicazione. Copre ambito, classificazione, modifica sostanziale, requisiti essenziali, gestione delle vulnerabilità, documentazione tecnica, percorsi di valutazione della conformità e interazione con AI Act, Data Act, ESPR e responsabilità per danno da prodotti difettosi.

Indice

Sintesi

IN 60 SECONDI

Ambito coperto: prodotti hardware e software connessi immessi sul mercato dell'UE, con la sicurezza trattata come requisito di conformità del prodotto, non come buona pratica.

Da quando incide: segnalazioni dell'articolo 14 dall'11 settembre 2026; obblighi tecnici, documentali e di marcatura CE completi dall'11 dicembre 2027.

Cosa deve produrre: valutazione dei rischi di cibersicurezza, SBOM, documentazione tecnica, istruzioni per gli utenti, dichiarazione UE di conformità, marcatura CE e segnalazioni di incidenti e vulnerabilità dell'articolo 14.

Chi deve agire

I fabbricanti hanno l'onere principale. Importatori e distributori devono svolgere controlli di diligenza prima di mettere i prodotti a disposizione.

Cosa cambia

La cibersicurezza entra nella conformità di prodotto: progettazione sicura, gestione delle vulnerabilità, documentazione, marcatura CE e attività post-mercato.

Prima scadenza

Le segnalazioni dell'articolo 14 iniziano l'**11 settembre 2026** per vulnerabilità attivamente sfruttate e incidenti gravi.

Applicazione completa

La conformità tecnica completa si applica dall'**11 dicembre 2027**. I prodotti precedenti rientrano dopo una modifica sostanziale, ma la segnalazione resta applicabile.

Spina dorsale delle prove

La documentazione tecnica richiede la valutazione dei rischi, la SBOM, la motivazione del periodo di supporto, le prove di test, le istruzioni per gli utenti, la dichiarazione e le prove di conformità ai requisiti essenziali di cibersicurezza.

Percorso di conformità

La maggior parte dei prodotti può usare il modulo A. I prodotti importanti e critici possono richiedere un organismo notificato o una certificazione europea di cibersicurezza.

Che cos'è il regolamento sulla ciberresilienza?

Il Regolamento (UE) 2024/2847, il Cyber Resilience Act (CRA), è il primo quadro valido in tutta l'UE che rende la cibersicurezza un requisito vincolante per i prodotti con elementi digitali immessi sul mercato dell'UE. Il testo autorevole è disponibile su EUR-Lex.

Il CRA si applica a fabbricanti, importatori e distributori di hardware e software connessi. Copre prodotti che vanno dai dispositivi IoT di consumo ai sistemi di controllo industriale. Il cambiamento pratico è semplice: la cibersicurezza deve essere progettata, provata, mantenuta e monitorata come parte della conformità di prodotto.

La mancata conformità ai requisiti essenziali di cibersicurezza o agli obblighi degli articoli 13 e 14 può comportare sanzioni fino a 15 milioni di euro o al 2,5% del fatturato annuo mondiale, a seconda di quale importo sia superiore. Si applicano fasce inferiori: fino a 10 milioni di euro o al 2% per la violazione di altri obblighi specificati, e fino a 5 milioni di euro o all'1% per la trasmissione di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità di vigilanza del mercato. Le autorità di vigilanza del mercato possono anche richiedere azioni correttive, limitare la disponibilità, ritirare prodotti o imporre richiami.

Date chiave per pianificare la conformità

Il CRA è entrato in vigore il **10 dicembre 2024**. Il lavoro pratico di conformità si concentra su tre tappe: organismi notificati a **giugno 2026**, segnalazioni a **settembre 2026** e conformità tecnica completa a **dicembre 2027**.

NOTA

Stato degli orientamenti della Commissione: La Commissione europea ha pubblicato il progetto di orientamenti CRA il 3 marzo 2026. La consultazione si è chiusa il 13 aprile 2026. Gli orientamenti non sono definitivi, ma sono utili per pianificare immissione sul mercato, software libero e open source, periodi di supporto, modifiche sostanziali, classificazione dei prodotti, due diligence sui componenti, trattamento dati da remoto, gestione delle vulnerabilità e sovrapposizioni con altre norme UE. Alcune questioni di confine, incluse quelle con AI Act e DORA, potrebbero richiedere ulteriori chiarimenti.

10 dicembre 2024

Entrata in vigore

Inizia il periodo transitorio

11 giugno 2026

Organismi notificati

Si applica il capo IV

11 settembre 2026

Segnalazione

Iniziano le segnalazioni dell'articolo 14

11 dicembre 2027

Applicazione completa

Requisiti tecnici, marcatura CE, documentazione e valutazione della conformità

DA FARE PER PRIMA COSA

Parta dalla preparazione alla segnalazione. La scadenza dell'articolo 14 arriva prima della conformità tecnica completa e si applica ai prodotti già presenti sul mercato dell'UE.

Poiché le segnalazioni iniziano l'**11 settembre 2026**, la preparazione alla segnalazione dovrebbe essere il primo filone di attuazione: **rilevamento, triage, informazione degli utenti e segnalazione alle autorità** devono funzionare prima della scadenza della conformità tecnica completa.

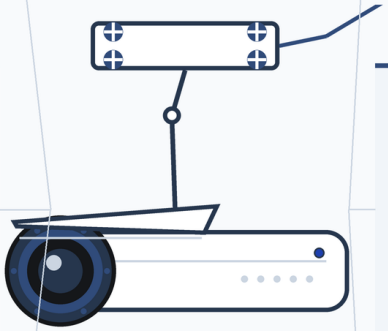
I prodotti immessi sul mercato prima dell'**11 dicembre 2027** sono soggetti ai requisiti tecnici del CRA solo se subiscono una **modifica sostanziale** da tale data. Per la segnalazione vale una regola diversa: l'articolo 14 si applica a **tutti i prodotti che rientrano nell'ambito**, inclusi quelli già presenti sul mercato dell'UE.

Il CRA lungo il ciclo di vita del prodotto

PASSO 01
Definire l’ambito
Ambito, classificazione, periodo di supporto e valutazione dei rischi

PASSO 02
Sviluppare in sicurezza
Impostazioni sicure predefinite, analisi del codice, SBOM e controllo delle dipendenze

PASSO 03
Validare e documentare
Test di sicurezza, triage delle vulnerabilità, fascicolo tecnico e istruzioni utente



PASSO 04
Immettere sul mercato
Dichiarazione UE di conformità, marcatura CE e decisione di rilascio

PASSO 05
Monitorare e aggiornare
CVE, avvisi, attività di exploit, aggiornamenti di sicurezza e divulgazione

PASSO 06
Supportare e cooperare
Segnalazioni articolo 14, avvisi agli utenti, richieste delle autorità e fine supporto

Telecamera IP connessa, dalla pianificazione del prodotto al supporto post-commercializzazione secondo il CRA

Quali prodotti rientrano nell'ambito

Ambito ed esclusioni

Il CRA si applica ai prodotti hardware e software il cui uso previsto o ragionevolmente prevedibile include una connessione dati diretta o indiretta a un dispositivo o a una rete. Sono inclusi computer, smartphone, apparecchiature di rete, dispositivi IoT, sistemi di controllo industriale e applicazioni di trattamento dei dati.

Le categorie seguenti sono escluse in modo esplicito:

- Dispositivi medici e dispositivi medico-diagnostici in vitro disciplinati dai regolamenti (UE) 2017/745 e 2017/746
- Sistemi automobilistici disciplinati dal regolamento (UE) 2019/2144
- Apparecchiature aeronautiche disciplinate dal regolamento (UE) 2018/1139
- Equipaggiamento marittimo disciplinato dalla direttiva 2014/90/UE
- Prodotti sviluppati esclusivamente per finalità di sicurezza nazionale o difesa
- Prodotti puramente meccanici senza elementi digitali o connettività di rete

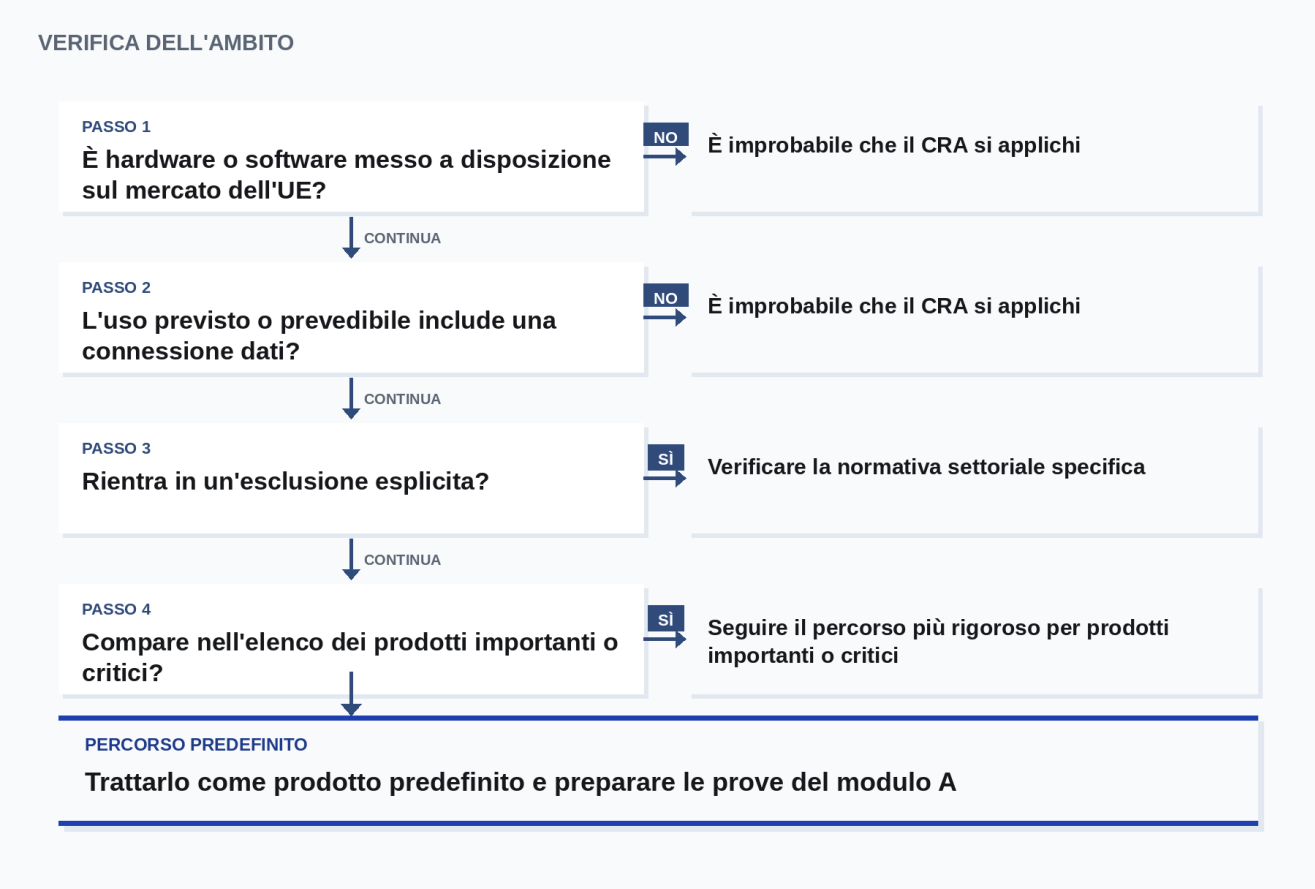
In assenza di un'esclusione chiara, tratti il prodotto connesso come rientrante nell'ambito.

NOTA

Prodotti su misura: una deroga ristretta. Se sviluppa un prodotto adattato a un singolo utente commerciale, sulla base di un accordo scritto con quell'utente, può derogare a due soli requisiti: la configurazione sicura per impostazione predefinita (deve comunque restare disponibile un percorso di ritorno allo stato originale sicuro) e gli aggiornamenti di sicurezza gratuiti (l'accordo può fissare una base commerciale diversa). Tutto il resto si applica integralmente: trattamento delle vulnerabilità, gli altri requisiti di sicurezza del prodotto, segnalazioni dell'articolo 14, documentazione tecnica, marcatura CE, valutazione della conformità e periodo di supporto. Non è una deroga B2B generica e non copre i prodotti standard venduti alle imprese.

RESPONSABILITÀ DEGLI OPERATORI ECONOMICI

Fabbricante	Progettare prodotti sicuri, valutare il rischio, predisporre la documentazione tecnica, svolgere la valutazione della conformità, trattare le vulnerabilità, segnalare gli eventi dell'articolo 14.
Importatore	Verificare la conformità del fabbricante, controllare marcatura CE e documentazione, tenere disponibile la dichiarazione, agire sulle vulnerabilità note.
Distributore	Verificare gli indicatori di diligenza prima della fornitura, controllare informazioni e istruzioni richieste, evitare di mettere a disposizione prodotti non conformi.



La classificazione del prodotto determina il percorso di valutazione

La categoria del prodotto determina come dimostrare la conformità.

Categoria	Esempi	Valutazione della conformità
Predefinita, non classificata	Software generale e prodotti di consumo connessi che non rientrano nelle categorie importanti o critiche	Modulo A: autovalutazione
Importante, classe I	Identità, browser, gestore di password, antivirus, VPN, gestione di rete, router, serratura intelligente, telecamera di sicurezza e prodotti simili	Modulo A solo quando sono applicati, come richiesto, norme armonizzate, specifiche comuni o schemi di certificazione applicabili; altrimenti modulo B+C o modulo H
Importante, classe II	Hypervisor, runtime per container, firewall, IDS/IPS e microprocessori resistenti alla manomissione	Modulo B+C, modulo H o uno schema europeo di certificazione della cibersicurezza applicabile almeno al livello di affidabilità «sostanziale»
Prodotti critici	Elementi sicuri, smart card, gateway per contatori intelligenti e dispositivi hardware con security box	Certificazione europea di cibersicurezza quando richiesta e disponibile; altrimenti si applicano i percorsi di classe II

Le quattro categorie di prodotto

La tabella sopra mostra gli esempi. Il riferimento completo, con cui confrontare la funzionalità principale del prodotto, è esposto qui di seguito.

Prodotti predefiniti

La maggior parte dei prodotti finisce qui. Qualsiasi prodotto con elementi digitali la cui funzionalità principale non corrisponde a una voce degli elenchi importanti o critici riportati sotto è trattato come predefinito. Il percorso di conformità è l'autovalutazione del modulo A.

Esempi comuni:

- Smart TV e dispositivi di streaming.
- Stampanti di rete e dispositivi multifunzione per ufficio.
- Casse Bluetooth e prodotti audio di consumo.
- Applicazioni software per la riproduzione di contenuti multimediali.
- Console di gioco, e-reader e elettronica di consumo simile.
- Elettrodomestici intelligenti da cucina come forni, frigoriferi e lavastoviglie senza funzioni di sicurezza.
- Lampadine intelligenti e illuminazione connessa senza funzioni di sicurezza.
- Fitness tracker che non hanno finalità di monitoraggio della salute.
- Applicazioni mobili di uso generale che non sono browser, gestori di password o app VPN.
- Software di produttività da ufficio come elaboratori di testo e fogli di calcolo.

L'elenco sopra è illustrativo. Gli elenchi dei prodotti importanti e critici sotto sono esaustivi.

Prodotti importanti (classe I)

Valutazione obbligatoria da parte di terzi, salvo quando sono applicate, come richiesto, norme armonizzate, specifiche comuni o schemi di certificazione applicabili.

1. Software e hardware di gestione delle identità e degli accessi privilegiati, inclusi i lettori di autenticazione e di controllo degli accessi (anche i lettori biometrici).
2. Browser standalone e integrati.
3. Gestori di password.
4. Software che cerca, rimuove o mette in quarantena software malevolo.
5. Prodotti VPN.
6. Sistemi di gestione di rete.
7. Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM).
8. Boot manager.
9. Software per infrastrutture a chiave pubblica e per l'emissione di certificati digitali.
10. Interfacce di rete fisiche e virtuali.
11. Sistemi operativi.
12. Router, modem destinati alla connessione a Internet e switch.
13. Microprocessori con funzionalità connesse alla sicurezza.

14. Microcontrollori con funzionalità connesse alla sicurezza.
15. ASIC e FPGA con funzionalità connesse alla sicurezza.
16. Assistenti virtuali di uso generale per la casa intelligente.
17. Prodotti smart-home con funzionalità di sicurezza (serrature intelligenti, telecamere di sicurezza, baby monitor, sistemi di allarme).
18. Giocattoli connessi a Internet con funzioni interattive (parlare, riprendere, tracciamento della posizione).
19. Dispositivi indossabili personali con finalità di monitoraggio della salute (quando i regolamenti (UE) 2017/745 o 2017/746 non si applicano), o dispositivi indossabili destinati a essere usati dai bambini.

Prodotti importanti (classe II)

Valutazione obbligatoria da parte di terzi, percorso più rigoroso. L'autovalutazione non è disponibile nemmeno in presenza di norme armonizzate.

1. Hypervisor e sistemi di runtime per container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti analoghi.
2. Firewall, sistemi di rilevamento e prevenzione delle intrusioni.
3. Microprocessori resistenti alla manomissione.
4. Microcontrollori resistenti alla manomissione.

Prodotti critici

Certificazione europea di cibersicurezza richiesta quando lo schema è disponibile. Altrimenti si applica il percorso di classe II.

1. Dispositivi hardware con cassette di sicurezza.
2. Gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23, della direttiva (UE) 2019/944, e altri dispositivi a fini di sicurezza avanzata, inclusa la criptoelaborazione sicura.
3. Smart card e dispositivi analoghi, inclusi gli elementi sicuri.

Se la funzionalità principale del prodotto corrisponde a una voce degli elenchi importanti o critici, il prodotto appartiene a quella classe. Se il prodotto integra una di quelle voci come componente ma la propria funzionalità principale è altro, l'integrazione non cambia la classe.

Come classificare: la funzionalità principale, non l'integrazione

Gli elenchi sopra dicono quali sono le categorie. Non dicono come applicarle al prodotto. La risposta del CRA sta in una sola espressione: **funzionalità principale**.

La classe del prodotto è determinata dalla sua funzionalità principale, non dai componenti che integra. Confronta la funzionalità principale con gli elenchi importanti e il prodotto è importante (classe I o II). La confronta con l'elenco dei critici e il prodotto è critico. Nessuna corrispondenza, e il prodotto è predefinito. È tutto il test.

La tutela pratica sta nella seconda frase dell'articolo 7, paragrafo 1. L'integrazione di un componente importante non spinge il prodotto integrante nella classe importante. Incorporare una libreria firewall in un hub smart-home non rende l'hub un firewall. Il considerando 45 lo dice in parole semplici: firewall e sistemi di rilevamento delle intrusioni sono importanti di classe II, ma gli altri prodotti che li integrano non lo sono.

Usi questa sequenza per autoclassificare.

1. **Nomi la funzionalità principale del prodotto in una frase.** Se non ci riesce, il resto dell'analisi non regge. Si concentri su ciò senza cui il prodotto non funzionerebbe.
2. **Verifichi gli elenchi importanti qui sopra.** Una corrispondenza in classe I o II rende il prodotto importante.
3. **Verifichi l'elenco dei critici qui sopra.** Una corrispondenza rende il prodotto critico. Un percorso di certificazione europea di cibersicurezza si applica quando lo schema è disponibile; altrimenti si applica il percorso di classe II.
4. **Nessuna corrispondenza in nessun elenco.** Il prodotto è predefinito. Il percorso è l'autovalutazione del modulo A.
5. **Documenti il ragionamento.** Un promemoria di una pagina con la dichiarazione della funzionalità principale, il controllo degli elenchi e il percorso scelto va nella documentazione tecnica.

Due esempi pratici.

Hub smart-home con un gestore di password integrato. Funzionalità principale: orchestrazione di routine fra i dispositivi IoT di consumo in casa. Il componente gestore di password, venduto separatamente dal suo fabbricante, è un prodotto importante di classe I a sé stante. La funzionalità principale dell'hub è l'automazione domestica, non la gestione delle credenziali. L'hub resta predefinito.

Sistema operativo per insieme di funzioni. Un prodotto è commercializzato come elettrodomestico smart-home, ma le sue funzioni principali sono l'inizializzazione dell'hardware e delle periferiche, la pianificazione dei processi, la gestione della memoria e un'interfaccia per chiamate di sistema. Quella è la funzionalità principale di un sistema operativo. I sistemi operativi sono un prodotto importante di classe I. Il prodotto è importante di classe I, a prescindere dal marketing.

Se la classificazione finisce su una classe che sorprende il resto del team, la dichiarazione di funzionalità principale ha bisogno di un'altra revisione prima del rilascio.

Quando il cloud è parte del prodotto

La maggior parte dei prodotti con elementi digitali si appoggia a qualcosa al di fuori del dispositivo: un backend cloud, un'app mobile complementare, un server di aggiornamento over-the-air, un portale di autenticazione, un sistema di gestione dei dispositivi. Il CRA non tratta tutti questi elementi come parte del prodotto. Li tratta come parte del prodotto solo quando sono vere **entrambe** queste due condizioni:

- Il software è stato **progettato e sviluppato dal suo team, o sotto la sua responsabilità**.
- Il prodotto **non eseguirebbe una delle sue funzioni** senza di esso.

Se una delle due condizioni non è soddisfatta, il servizio remoto sta fuori dal perimetro del prodotto per il CRA. Un SaaS di terzi che non possiede, anche se il prodotto vi si collega, non è parte del prodotto. Un sito che promuove il prodotto ma non ne supporta le funzioni non è parte del prodotto.

Quando un componente remoto rientra nell'ambito, vi rientra **come parte del prodotto**. Documentazione tecnica, valutazione della conformità, dichiarazione UE di conformità, trattamento delle vulnerabilità e tempistiche di segnalazione dell'articolo 14 coprono il componente cloud insieme al dispositivo.

Usi questa matrice per chiudere rapidamente la questione.

Componente	Rientra nell'ambito come parte del prodotto?
App mobile complementare che si abbina al dispositivo	**Sì.** L'ha progettata Lei, e il dispositivo non può essere configurato o usato senza di essa.
Backend cloud che conserva e tratta i dati del dispositivo	**Sì.** L'ha progettato Lei, e la dashboard o la funzione principale non funziona senza.
Server di aggiornamento over-the-air	**Sì.** L'ha progettato Lei, e il dispositivo non può ricevere aggiornamenti di sicurezza senza.
Portale di autenticazione che controlla l'accesso al dispositivo	**Sì.** L'ha progettato Lei, e gli utenti non possono accedere senza.
Sito di marketing del prodotto	**No.** Non supporta una funzione del prodotto.
SaaS di terzi con cui il prodotto si integra (non lo possiede)	**No.** Non l'ha progettato Lei. Il fornitore terzo ha i suoi obblighi sotto NIS 2.
Infrastruttura cloud generica su cui gira il servizio (IaaS o PaaS)	**No.** Non l'ha progettata Lei. Il fornitore di infrastruttura rientra in NIS 2.

Uno schema comune: un dispositivo smart-home con un'app mobile, un server di aggiornamento e un backend cloud. Tutti e tre sono progettati dal fabbricante, e il dispositivo non può eseguire le funzioni pubblicizzate senza di essi. Tutti e tre sono parte del prodotto. Gli obblighi CRA si applicano all'intero bundle. Se poi il backend cloud parla con un SaaS di analisi di terzi, quel SaaS non è parte del prodotto. Il fornitore terzo ha i suoi obblighi sotto NIS 2.

Il CRA non richiede misure di sicurezza per le reti e i sistemi informativi del fabbricante nel loro complesso. Richiede sicurezza per i servizi remoti che sono parte del prodotto. La linea è il perimetro del prodotto, non quello dell'azienda.

La sua catena di fornitura: chi fa che cosa sotto il CRA

Il CRA mette gli obblighi principali su di Lei come fabbricante, ma anche importatori e distributori hanno doveri che incidono su come il prodotto arriva al mercato. Tre cose contano per Lei.

Chi	Cosa verifica prima della fornitura	Cosa fa in caso di vulnerabilità	Quando subentra nei suoi doveri
Importatore	Marcatura CE, dichiarazione UE di conformità, istruzioni per gli utenti nella lingua corretta, suoi dati di contatto sul prodotto o con il prodotto	La avvisa senza ritardi indebiti; avvisa direttamente le autorità di vigilanza del mercato se il prodotto presenta un rischio significativo di cibersicurezza	Quando immette il suo prodotto con il proprio nome o marchio, o lo modifica sostanzialmente
Distributore	Marcatura CE, che Lei e l'importatore abbiate fatto la vostra parte, che la documentazione richiesta accompagni il prodotto	La avvisa senza ritardi indebiti; avvisa direttamente le autorità di vigilanza del mercato se il prodotto presenta un rischio significativo di cibersicurezza; può smettere di mettere il prodotto a disposizione	Stesso innesco degli importatori

Per un fabbricante questo significa tre cose pratiche:

- Marcatura CE, dichiarazione UE di conformità e istruzioni per gli utenti devono essere corrette e nella lingua giusta nel momento in cui un distributore le verifica. I partner di canale sono tenuti a verificarle e possono rifiutarsi di mettere a disposizione il prodotto se mancano o sono errate.
- Serve un percorso di contatto chiaro e a basso attrito che importatori e distributori possano usare per segnalare vulnerabilità nel suo processo di trattamento. Lo useranno.
- Qualsiasi partner che riprenda il marchio, immetta il prodotto con il proprio nome o marchio, o lo modifichi sostanzialmente diventa il fabbricante per quella variante. Gli obblighi pieni di documentazione tecnica, valutazione della conformità, segnalazione e periodo di supporto si trasferiscono a loro per quella versione. Si veda *Quando qualcun altro diventa il fabbricante* nella prossima sezione per la regola della modifica sostanziale.

Modifica sostanziale: quando si rifà la conformità

Dopo che il prodotto è sul mercato, il CRA divide le modifiche successive in due campi. La maggior parte è di routine e non richiede nulla in più. Alcune sono sostanziali. Una modifica sostanziale è trattata, ai fini del CRA, come un nuovo prodotto immesso sul mercato. Significa una nuova valutazione della conformità, una documentazione tecnica aggiornata, una nuova dichiarazione UE di conformità e la marcatura CE sulla nuova versione.

Il test è breve e sta nella definizione di modifica sostanziale. Una modifica è sostanziale se è vera una delle due condizioni:

- **Incide sulla conformità** ai requisiti essenziali di cibersicurezza.
- **Modifica la finalità prevista** per la quale il prodotto è stato valutato.

Se non si applica nessuna delle due, la modifica non è sostanziale. Documenti comunque il ragionamento e lo tenga agli atti. L'analisi è parte della catena di prove.

Cosa non conta come sostanziale

Due deroghe fanno la maggior parte del lavoro in pratica.

Gli aggiornamenti di sicurezza e le correzioni di bug che riducono il rischio di cibersicurezza senza cambiare la finalità prevista non sono sostanziali. Correggere una vulnerabilità nota, modificare la validazione degli input per chiudere una falla o ricompilare un componente per affrontare un CVE stanno tutti su questo lato della linea.

Anche il ricondizionamento, la manutenzione e le riparazioni non sono automaticamente sostanziali. Lo diventano solo se alterano la finalità prevista o incidono sulla conformità ai requisiti essenziali di cibersicurezza.

Anche le piccole modifiche all'interfaccia utente restano sul lato sicuro. Aggiungere una lingua, sostituire un'icona o rifinire il layout di una schermata non è di per sé una modifica sostanziale. Aggiungere un nuovo elemento di input che richiede una validazione adeguata può esserlo.

Pezzi di ricambio

Il CRA esenta i pezzi di ricambio in modo ristretto e specifico. **I pezzi di ricambio identici**, fabbricati secondo le stesse specifiche dei componenti che sostituiscono, sono del tutto fuori dall'ambito del regolamento. I sostituti funzionali no.

Usi questa matrice per chiudere rapidamente la questione.

Sostituto	Prodotto ospitante immesso prima dell'11 dicembre 2027	Prodotto ospitante immesso l'11 dicembre 2027 o dopo
Identico al componente originale, stesse specifiche	Pezzo di ricambio fuori dall'ambito CRA. Nessun obbligo innescato dalla sostituzione.	Pezzo di ricambio fuori dall'ambito CRA. Nessun obbligo innescato dalla sostituzione.
Funzionalmente equivalente, progettazione o specifica diversa	Il sostituto è un prodotto CRA a sé stante. L'ospitante non ha obblighi CRA, perché precede la data di applicazione.	Il sostituto è un prodotto CRA. Valuti se la sostituzione nell'ospitante è una modifica sostanziale dell'ospitante usando il test a due rami qui sopra.

Due conseguenze pratiche. Primo, l'esenzione dipende dalla specifica identica. Un modulo wireless ricostruito su un chipset diverso non è un ricambio identico, anche se il cliente non riesce a distinguerlo. Secondo, il fabbricante che fornisce un sostituto funzionale porta gli obblighi CRA per quel pezzo, indipendentemente da chi ha fatto l'ospitante.

Aggiornamenti software e feature flag

I rilasci software sono la fonte più frequente di domande sulla modifica sostanziale. Il test a due rami le risolve comunque.

Una patch che corregge una vulnerabilità non è sostanziale. Un feature toggle che attiva una funzionalità per cui il prodotto non è stato mai valutato lo è. Un aggiornamento del modello che permette al prodotto di decidere su nuove categorie di input lo è anche. Se un rilascio porta sia una correzione sia una nuova funzionalità, valuti la funzionalità.

Il pacchetto conta meno della sostanza. Che un aggiornamento di funzionalità arrivi da solo o nello stesso rilascio di una patch di sicurezza è irrilevante ai fini della valutazione.

Se usa feature flag o rollout graduali, il momento che conta è l'abilitazione per gli utenti finali in produzione, non la spedizione del binario che contiene il flag.

La decisione in pratica

Usi questa sequenza su ogni modifica prima del rilascio.

1. **La modifica cambia la finalità prevista del prodotto?** Se sì: sostanziale. Rifaccia la valutazione della conformità per la nuova versione.
2. **La modifica incide sulla conformità ai requisiti essenziali di cibersicurezza?** Se sì: sostanziale. Rifaccia la valutazione della conformità per la nuova versione.
3. **In caso contrario:** non sostanziale. Documenti l'analisi e continui sotto la documentazione tecnica esistente.

Se il prodotto è in classe importante o critica e il percorso richiedeva una valutazione di terza parte la prima volta, una modifica sostanziale la rimette sullo stesso percorso. Avvisi la terza parte in anticipo di qualsiasi modifica che possa essere sostanziale. L'autovalutazione non è una scorciatoia per riclassificare a posteriori un prodotto importante.

Conseguenze quando una modifica è sostanziale

Una modifica sostanziale è trattata come un nuovo prodotto immesso sul mercato. Per il fabbricante significa:

- Aggiornare la documentazione tecnica per la versione modificata.
- Rifare la valutazione della conformità lungo il percorso richiesto dalla classe del prodotto.
- Emettere una nuova dichiarazione UE di conformità per la versione modificata.
- Riapporre la marcatura CE, con la nuova dichiarazione agli atti.
- Conservare la documentazione della versione precedente per l'intero periodo di conservazione. La nuova versione non la cancella.

Per i prodotti software in particolare, può limitare gli aggiornamenti di sicurezza durante il periodo di supporto alla versione più recente immessa sul mercato, a condizione che gli utenti delle versioni precedenti possano passare a quella più recente gratuitamente e senza nuovo hardware.

Le unità sul campo già vendute con la conformità precedente non sono toccate. L'obbligo si attacca alla versione modificata che viene messa a disposizione, non alle unità identiche che la precedono.

Quando qualcun altro diventa il fabbricante

Se non è il fabbricante originale ed effettua una modifica sostanziale, il CRA La tratta come il fabbricante per quella versione. Gli obblighi pieni degli articoli 13 e 14 ricadono su di Lei. La stessa regola si applica se immette il prodotto sul mercato con il proprio nome o marchio.

Questo cattura più situazioni di quanto i team si aspettino:

- Un integratore di sistemi che spedisce una build firmware specifica per il cliente con nuove funzionalità.
- Un rivenditore che fa white-label di un prodotto e cambia la finalità prevista commercializzata.
- Un fornitore di servizi che pacchettizza un dispositivo di terzi con il proprio firmware.

In ciascun caso l'attore che ha fatto la modifica eredita gli obblighi del fabbricante per quella versione: documentazione tecnica, valutazione della conformità, segnalazione, trattamento delle vulnerabilità e il resto. L'etichetta «importatore» o «distributore» smette di proteggerli nel momento in cui superano una delle due linee.

Cosa serve avere

Usi questa sezione come checklist operativa. La guida dettagliata requisito per requisito segue nelle sezioni successive.

Valutazione dei rischi di cibersicurezza

Prima di immettere un prodotto sul mercato, serve una valutazione dei rischi di cibersicurezza agli atti. È il documento che spiega, con le sue parole, perché il prodotto è sicuro da spedire e da tenere sul mercato.

La valutazione deve coprire:

- La finalità prevista del prodotto e i casi d'uso ragionevolmente prevedibili
- Le condizioni e l'ambiente in cui il prodotto opererà
- I dati e le funzioni da proteggere
- Le minacce applicabili e i controlli su cui si affida per gestirle
- La durata di vita prevista per il prodotto

Come la struttura la maggior parte dei team. Le metodologie credibili convergono sulle stesse mosse: identificare gli asset (dati che il prodotto tratta, materiale di sicurezza come chiavi e credenziali, funzioni la cui perdita danneggerebbe gli utenti), mappare dove ciascun asset risiede o si sposta, modellare le minacce per asset e ambiente usando riservatezza, integrità e disponibilità come dimensioni, attribuire impatto e probabilità, decidere quali rischi residui accettare e quali mitigare, poi rivalutare dopo ogni ciclo di controlli (ogni nuova chiave, certificato o funzione di autenticazione è a sua volta un nuovo asset da analizzare).

Modellazione delle minacce. Il terzo passo sopra è quello più tecnico e ha tecniche consolidate proprie. STRIDE classifica le minacce come spoofing, tampering, repudiation, information disclosure, denial of service ed elevation of privilege; ampiamente usato, si adatta alla maggior parte dei prodotti connessi. LINDDUN estende il quadro per i prodotti che trattano dati personali, aggiungendo linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness e non-compliance; utile quando il regime di protezione dei dati si sovrappone ai doveri CRA. PASTA percorre un processo in sette fasi dagli obiettivi di business fino all'accettazione del rischio residuo; utile per sistemi complessi in cui il quadro d'attacco guida il design. Nessuna di queste è specifica per il CRA, e il CRA non ne richiede alcuna in particolare. Scelga quella che corrisponde al profilo di esposizione del suo prodotto.

Dove trovare una metodologia elaborata. Il CRA non prescrive un metodo. L'Ufficio federale tedesco per la sicurezza informatica (BSI) pubblica la Technical Guideline TR-03183, la metodologia di valutazione dei rischi allineata al CRA più dettagliata in circolazione pubblica. ENISA pubblica orientamenti più ampi sull'attuazione del CRA.

Tenga la valutazione aggiornata per tutto il periodo di supporto. Quando il quadro delle minacce, i componenti o il caso d'uso cambiano, anche la valutazione deve cambiare.

Determinazione del periodo di supporto

Ogni prodotto necessita di un periodo di supporto definito, e la data di fine deve essere pubblicata al momento dell'acquisto. Il periodo di supporto è la finestra durante la quale tratta le vulnerabilità, spedisce gli aggiornamenti di sicurezza e tiene aggiornata la documentazione tecnica.

Quanto deve durare

Almeno cinque anni. Se il prodotto è previsto in uso per meno di cinque anni, il periodo di supporto deve corrispondere alla durata d'uso prevista. Se è previsto in uso più a lungo, il periodo di supporto deve riflettere quella durata maggiore; prodotti come router, sistemi operativi e controllori industriali giustificano abitualmente più di cinque anni.

Fattori da pesare

Nel fissare il periodo, tenga conto, in modo proporzionato, di:

- Aspettative ragionevoli degli utenti per il prodotto
- Natura del prodotto, inclusa la sua finalità prevista
- Qualsiasi normativa UE che fissi già una durata di vita per questa categoria di prodotti
- Periodi di supporto di prodotti comparabili sul mercato
- Disponibilità dell'ambiente operativo da cui il prodotto dipende
- Periodi di supporto dei componenti integrati che forniscono funzioni principali
- Eventuali orientamenti di ADCO o della Commissione per la categoria di prodotto

Il ragionamento dietro il periodo scelto deve essere nella documentazione tecnica. Le autorità di vigilanza del mercato possono chiederlo.

Cosa deve pubblicare

Indichi la fine del periodo di supporto al momento dell'acquisto, almeno con mese e anno, in un luogo facilmente accessibile. Quando il prodotto ha un'interfaccia utente, mostri una notifica quando raggiunge la fine del periodo di supporto.

Conservazione degli aggiornamenti

Ogni aggiornamento di sicurezza messo a disposizione degli utenti durante il periodo di supporto deve restare disponibile per almeno 10 anni dopo la sua emissione, o per il resto del periodo di supporto, se questo è più lungo.

Diligenza sui componenti

Un prodotto è fatto di componenti. Alcuni li ha scritti Lei, altri li ha acquistati, altri ancora li ha presi da un repository open source. Il CRA tratta il prodotto come un tutto ai fini della conformità, quindi anche i componenti contano. Se una vulnerabilità sta in un componente, sta nel suo prodotto. Se un componente non riceve aggiornamenti di sicurezza, neppure il suo prodotto li riceve.

I fabbricanti devono esercitare la dovuta diligenza sui componenti di terzi, compresi quelli liberi e open source. I componenti non devono compromettere la cibersicurezza del prodotto.

Quanta diligenza basta dipende dal rischio di cibersicurezza che il componente porta. Una libreria che gestisce l'autenticazione non è come una libreria per il rendering dei font. Usi uno o più di questi controlli, in proporzione al rischio:

1. **Verifichi la marcatura CE sul componente.** Se il componente è a sua volta un prodotto CRA e il fornitore ne ha dimostrato la conformità, la marcatura CE è sul componente. Questo dimostra il lavoro CRA del fornitore.
2. **Verifichi lo storico degli aggiornamenti di sicurezza.** Un componente che spedisce aggiornamenti di sicurezza regolari è un rischio migliore di uno silenzioso da anni. Cerchi una cadenza di rilascio e una traccia recente di avvisi di sicurezza.
3. **Verifichi il componente nelle banche dati di vulnerabilità.** La banca dati europea delle vulnerabilità e le banche dati CVE pubbliche dicono cosa è noto del componente. Un CVE noto senza patch è una bandiera rossa.
4. **Esegua test di sicurezza aggiuntivi.** Quando i punti sopra non bastano, testi il componente nel suo contesto di integrazione: analisi statica, analisi dinamica, fuzzing o una revisione di sicurezza mirata.

Per i componenti integrati prima che il loro fornitore sia pienamente sotto il CRA (e quindi ancora senza marcatura CE), usi gli altri tre controlli. L'obbligo di diligenza non si ferma solo perché la catena di fornitura sta ancora recuperando.

Prove da tenere agli atti

La documentazione tecnica deve mostrare la sua diligenza, non solo dichiararla. Conservi:

- Un elenco dei componenti di terzi nel prodotto, tracciabili per versione, compresi quelli open source. La SBOM è il luogo naturale.
- La documentazione di sicurezza del fornitore che ha esaminato: politiche di sicurezza, programmi di disclosure delle vulnerabilità, impegni sul periodo di supporto.
- Rapporti di test di integrazione che mostrano il comportamento sicuro del componente nel suo prodotto.
- Clausole di sicurezza nei contratti o negli SLA con fornitori commerciali: tempi di notifica delle vulnerabilità, impegni sul periodo di supporto, regole di escalation.
- Una registrazione delle mitigazioni a livello di prodotto che ha aggiunto quando la diligenza sui componenti ha rivelato limiti: sandboxing, permessi limitati, validazione degli input, segmentazione di rete.

Quando trova una vulnerabilità in un componente

Se la sua diligenza o il monitoraggio post-mercato individuano una vulnerabilità in un componente, deve fare due cose. Primo, avvisare la persona o l'ente che mantiene il componente. Se il componente è open source, è il progetto upstream. Secondo, affrontare e correggere la vulnerabilità nel suo prodotto entro gli stessi tempi di qualsiasi altra vulnerabilità rilevata. Se ha sviluppato una correzione, condivida il codice o la documentazione con il manutentore, in formato leggibile da macchina ove applicabile.

Il CRA non Le permette di aspettare che il manutentore del componente agisca prima di proteggere i propri utenti. La tempistica di trattamento delle vulnerabilità del suo prodotto corre indipendentemente da quella dell'upstream.

I 13 requisiti di sicurezza del prodotto

Ogni prodotto con elementi digitali deve soddisfare tredici requisiti di sicurezza di base quando è immesso sul mercato, e continuare a soddisfarli per tutto il periodo di supporto. Sono la base di ciò che la cibersicurezza significa in termini di prodotto sotto il CRA.

I tredici requisiti sono:

- Nessuna vulnerabilità sfruttabile nota al momento dell'immissione sul mercato
- Configurazione sicura per impostazione predefinita fin dal primo avvio
- Aggiornamenti di sicurezza, inclusi aggiornamenti automatici con possibilità di rifiuto
- Protezione contro gli accessi non autorizzati
- Riservatezza dei dati conservati, trasmessi e trattati
- Integrità di dati, firmware e configurazione
- Minimizzazione dei dati
- Disponibilità e resilienza, anche contro gli attacchi di negazione del servizio
- Nessun impatto negativo su altri dispositivi o reti connessi
- Superficie di attacco limitata, incluse le interfacce esterne
- Riduzione dell'impatto degli incidenti tramite misure di mitigazione dello sfruttamento
- Registrazione delle attività rilevanti per la sicurezza, con possibilità di rifiuto da parte dell'utente
- Cancellazione sicura e permanente dei dati e portabilità

Ciascun requisito è approfondito nel dettaglio più avanti nella guida, con il significato pratico e le prove da tenere agli atti.

Gli 8 requisiti di trattamento delle vulnerabilità

I fabbricanti devono anche disporre di processi di trattamento delle vulnerabilità attivi per tutto il periodo di supporto del prodotto:

1. Identificare e documentare le vulnerabilità (inclusa la distinta base del software, SBOM)
2. Gestione del rischio e aggiornamenti di sicurezza tempestivi
3. Test di sicurezza regolari
4. Notifica degli aggiornamenti di sicurezza e divulgazione delle vulnerabilità
5. Politica di divulgazione coordinata delle vulnerabilità (CVD)
6. Contatto per la condivisione e la segnalazione delle vulnerabilità
7. Meccanismi sicuri di distribuzione degli aggiornamenti
8. Aggiornamenti di sicurezza gratuiti con messaggi di avviso

Tempistiche di segnalazione dell'articolo 14

Questi obblighi si applicano dall'**11 settembre 2026**. Riguardano i fabbricanti di prodotti con elementi digitali che rientrano nell'ambito, inclusi i prodotti immessi sul mercato prima dell'**11 dicembre 2027**. Le microimprese e le piccole imprese non sono esentate in via generale dalla segnalazione. L'agevolazione sanzionatoria per le piccole imprese è limitata: riguarda solo il primo termine di **24 ore per l'allerta precoce**.

Il CRA distingue tre livelli di stato della vulnerabilità:

- **Vulnerabilità:** qualsiasi debolezza che potrebbe essere sfruttata
- **Vulnerabilità sfruttabile:** debolezza utilizzabile in condizioni reali
- **Vulnerabilità attivamente sfruttata:** vulnerabilità di cui è stato confermato l'uso in un attacco

Quando parte l'orologio

Non è sull'orologio nel momento in cui arriva un segnale. L'orologio parte una volta che ha svolto una valutazione iniziale e ha un ragionevole grado di certezza che una vulnerabilità nel suo prodotto è attivamente sfruttata, o che un incidente grave ha compromesso la sicurezza del prodotto. L'accento è sulla valutazione iniziale tempestiva, non sull'attesa che si chiuda l'indagine completa. Se un cliente, un ricercatore, un'autorità o un altro terzo Le porta all'attenzione un possibile problema, lo valuti senza ritardo e faccia partire l'orologio appena quella valutazione Le dà la ragionevole certezza.

Quando rileva una **vulnerabilità attivamente sfruttata**, si applica la seguente tempistica di segnalazione:

Tempistica	Cosa è richiesto	Dove segnalare
Entro 24 ore	Allerta precoce dello sfruttamento attivo	ENISA tramite CSIRT nazionale
Entro 72 ore	Notifica di vulnerabilità: prodotto interessato, natura generale dello sfruttamento e della vulnerabilità, misure di mitigazione, misure correttive che gli utenti possono adottare e marcatura di sensibilità, se applicabile	ENISA tramite CSIRT nazionale
Non oltre 14 giorni dalla disponibilità di una misura correttiva o di mitigazione	Relazione finale: descrizione della vulnerabilità, gravità, impatto, informazioni disponibili sugli attori malevoli e dettagli dell'aggiornamento di sicurezza o di altre misure correttive	ENISA tramite CSIRT nazionale

Quando rileva un **incidente grave** che incide sulla sicurezza del prodotto, si applica la seguente tempistica di segnalazione:

Tempistica	Cosa è richiesto	Dove segnalare
Entro 24 ore	Allerta precoce, inclusa l'indicazione se si sospetta che l'incidente sia causato da atti illeciti o dolosi	ENISA tramite CSIRT nazionale
Entro 72 ore	Notifica di incidente: natura dell'incidente, valutazione iniziale, misure di mitigazione, misure correttive che gli utenti possono adottare e marcatura di sensibilità, se applicabile	ENISA tramite CSIRT nazionale
Entro un mese dalla notifica di incidente a 72 ore	Relazione finale: descrizione dettagliata dell'incidente, gravità, impatto, minaccia probabile o causa principale e misure di mitigazione applicate o in corso	ENISA tramite CSIRT nazionale

Le notifiche si aggiornano man mano che si scoprono nuove informazioni

Le segnalazioni a 24 ore, 72 ore e 14 giorni (o un mese) sono fasi della stessa notifica, non depositi separati. Ogni fase aggiunge le informazioni non ancora disponibili nella precedente. Il CSIRT designato come coordinatore può anche chiedere un aggiornamento intermedio in qualsiasi momento. Non serve ripetere informazioni già fornite.

Le segnalazioni sono depositate tramite la **piattaforma unica di segnalazione del CRA**, instradate attraverso il Computer Security Incident Response Team (CSIRT) nazionale dello Stato membro principale del fabbricante, con accesso simultaneo per ENISA.

Informare gli utenti

Dopo essere venuto a conoscenza, deve informare gli utenti impattati della vulnerabilità o dell'incidente, e quando opportuno tutti gli utenti, di qualsiasi misura di riduzione del rischio e misura correttiva che possono adottare. Non è la stessa cosa della divulgazione pubblica. Il dovere è far arrivare l'informazione agli utenti che ne hanno bisogno per proteggersi, in proporzione al rischio. Per i prodotti usati in ambienti sensibili o essenziali, limiti le informazioni tecniche di dettaglio ai clienti interessati finché la vulnerabilità non è mitigata; un dettaglio pubblico prematuro può rendere più facile lo sfruttamento.

Una volta che la vulnerabilità è stata rimediata o mitigata, una divulgazione più ampia può diventare opportuna per aiutare gli utenti a verificare che i prodotti non siano più colpiti e per aumentare la consapevolezza generale. Tenga il livello di dettaglio e i tempi proporzionati al rischio residuo. Se non informa gli utenti tempestivamente, il CSIRT può intervenire e fornire l'informazione esso stesso quando lo ritenga proporzionato e necessario.

Vulnerabilità attivamente sfruttata	
24 ore	allerta precoce
72 ore	notifica di vulnerabilità
14 giorni dopo la misura correttiva	relazione finale

Incidente grave	
24 ore	allerta precoce
72 ore	notifica di incidente
un mese dopo la notifica a 72 ore	relazione finale

Azione correttiva quando un prodotto non è conforme

Se sa, o ha motivo di credere, che un prodotto immesso sul mercato, o uno dei suoi processi, non è conforme ai requisiti essenziali di cibersicurezza del CRA, deve agire immediatamente. Il dovere corre dall'immissione sul mercato e per tutto il periodo di supporto.

Le tre opzioni

1. **Rendere conforme.** Correggere il prodotto o il processo. Per i prodotti software in genere è un aggiornamento di sicurezza o una modifica di processo. Applichi la correzione alle versioni supportate.
2. **Ritiro.** Smettere di mettere il prodotto a disposizione sul mercato. Lo ritiri dalla catena di fornitura e da qualsiasi rivenditore, integratore o distributore che lo abbia a magazzino.
3. **Richiamo.** Recuperare il prodotto dagli utenti che già lo hanno. Lo usi quando il rischio di cibersicurezza per gli utenti è significativo e una correzione o un ritiro da soli non bastano.

La scelta è proporzionata al rischio, non una sequenza fissa. Una vulnerabilità correggibile con una patch funzionante in genere significa *rendere conforme*. Un prodotto che non può essere corretto in modo sicuro sul campo in genere significa *ritiro* e, se è in uso attivo con un rischio significativo, *richiamo*.

Cosa deve fare in aggiunta

- **Segnalare nella catena dell'articolo 14** quando la non conformità è una vulnerabilità attivamente sfruttata o un incidente grave. La tempistica di segnalazione è indicata sopra.
- **Informare gli utenti** della non conformità e di qualsiasi misura correttiva che possono applicare da soli. Si veda *Informare gli utenti* sopra per le regole di proporzionalità.
- **Cooperare** con qualsiasi richiesta motivata di un'autorità di vigilanza del mercato, anche fornendo la documentazione tecnica in una lingua che possono leggere.
- **Conservare le prove.** Tenga le registrazioni che mostrano cosa ha trovato, quando lo ha trovato, cosa ha fatto al riguardo e come ha comunicato con utenti e autorità. La documentazione tecnica e la dichiarazione UE di conformità devono restare disponibili per almeno 10 anni dopo l'immissione sul mercato, o per l'intero periodo di supporto, se questo è più lungo.

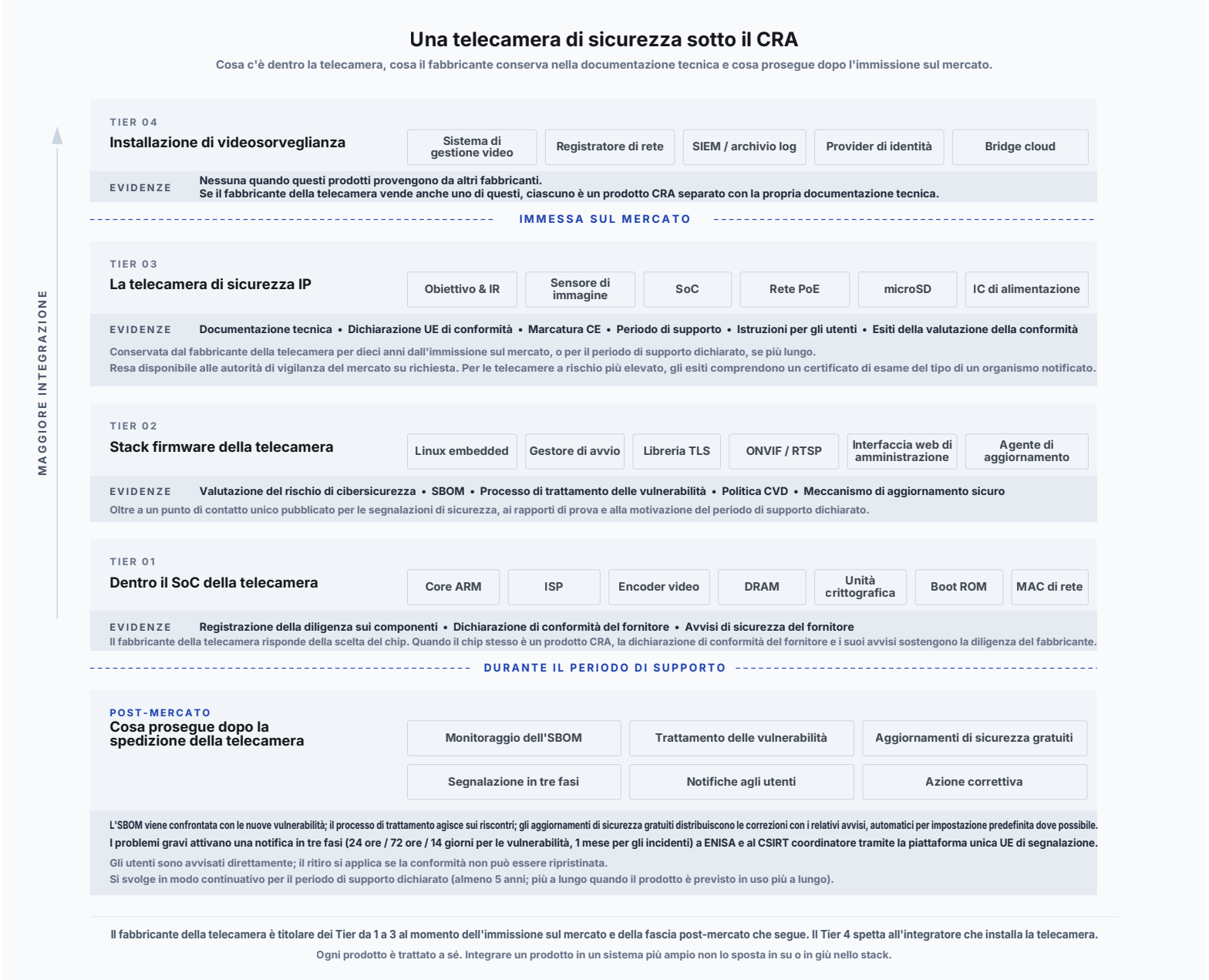
Requisiti di documentazione del prodotto

La documentazione deve essere conservata per **almeno 10 anni** dopo l'immissione sul mercato del prodotto, o per l'**intero periodo di supporto**, se questo è più lungo. A livello sintetico, la documentazione tecnica necessita di otto famiglie di prove:

1. Descrizione generale del prodotto
2. Dettagli di progettazione, sviluppo e produzione (inclusa la SBOM)
3. Valutazione dei rischi di cibersicurezza
4. Determinazione del periodo di supporto
5. Norme armonizzate e specifiche applicate
6. Rapporti di prova
7. Dichiarazione UE di conformità
8. SBOM completa (su richiesta delle autorità di vigilanza del mercato)

Checklist del percorso di valutazione della conformità

Usi la tabella di classificazione sopra per identificare il percorso. Conservi poi la decisione sul percorso nella documentazione tecnica insieme a norme, specifiche, schema di certificazione o prove dell'organismo notificato usate per giustificarla.



Un esempio elaborato. La stessa struttura a livelli si applica a ogni prodotto con elementi digitali, non solo alle telecamere di sicurezza.

Requisiti di sicurezza del prodotto

a. Nessuna vulnerabilità sfruttabile nota al momento dell'immissione sul mercato

Non immetta sul mercato un prodotto che contiene vulnerabilità sfruttabili note al pubblico e non ancora trattate. Una vulnerabilità nota può provenire da una banca dati pubblica, da un avviso del fornitore, da una segnalazione del cliente o dal monitoraggio interno.

Per soddisfare questo requisito:

- Verifichi le banche dati di vulnerabilità, incluse le Common Vulnerabilities and Exposures, CVE, prima di ogni release
- Usi test statici e dinamici di sicurezza applicativa (SAST/DAST) nella pipeline di build
- Analizzi le dipendenze di tutti i componenti di terzi e open source
- Documenti la decisione di accettazione o mitigazione del rischio per ogni problema individuato

b. Configurazione sicura per impostazione predefinita

Il prodotto deve essere sicuro nello stato predefinito. Disattivi i servizi non necessari, eviti credenziali predefinite deboli e limiti qualsiasi modalità di provisioning non sicura per durata e ambito. L'obbligo di configurazione sicura per impostazione predefinita può essere modificato per prodotti su misura forniti a utenti commerciali con accordo scritto, purché resti possibile ripristinare il prodotto allo stato originale sicuro.

Per soddisfare questo requisito:

- Disattivi porte di accesso remoto e interfacce di debug nelle build predefinite
- Imponga meccanismi di autenticazione robusti per impostazione predefinita
- Riservi le funzioni di amministrazione ai soli utenti autorizzati
- Predisponga un ripristino di fabbrica sicuro che riporti tutte le impostazioni e il firmware a uno stato sicuro noto, eliminando i dati dell'utente

c. Aggiornamenti di sicurezza, inclusi aggiornamenti automatici con possibilità di rifiuto

Il prodotto ha bisogno di un meccanismo di correzione capace di trattare i problemi di sicurezza dopo il rilascio. Quando gli aggiornamenti automatici sono adatti al contesto, li abiliti per impostazione predefinita e offra agli utenti un modo chiaro per rinviarli o disattivarli.

Per soddisfare questo requisito:

- Applichi firma crittografica e verifica di integrità ai pacchetti di aggiornamento
- Preveda prevenzione del rollback e registrazione degli eventi di aggiornamento
- Crei sistemi di notifica che avvisino gli utenti degli aggiornamenti in attesa
- Consenta agli utenti di rinviare o disattivare gli aggiornamenti automatici tramite un'interfaccia di configurazione chiara

d. Protezione contro gli accessi non autorizzati

I controlli di accesso devono proteggere sia le interfacce locali sia quelle remote. L'obiettivo è impedire agli utenti non autorizzati di accedere a funzioni, dati, configurazioni o superfici di amministrazione.

Per soddisfare questo requisito:

- Imponga policy robuste per password e credenziali predefinite
- Metta in atto l'autenticazione a più fattori (MFA) quando il contesto lo richiede
- Applichi il controllo degli accessi basato sui ruoli (RBAC) e la gestione della scadenza delle sessioni
- Registri i tentativi di accesso non riusciti, usi il rilevamento delle anomalie per segnalare attività non autorizzate e renda disponibili questi eventi per esame e segnalazione

e. Riservatezza dei dati conservati, trasmessi e trattati

I dati sensibili devono essere protetti a riposo, in transito e durante il trattamento.

Per soddisfare questo requisito:

- Usi algoritmi di cifratura standardizzati, per esempio AES-256 per i dati a riposo e TLS per i dati in transito
- Applichi pratiche sicure di gestione delle chiavi
- Separi i dati riservati dai componenti di sistema non critici
- Conservi log di audit per tutti gli eventi di accesso ai dati

f. Integrità di dati, firmware e configurazione

Questo requisito copre il sistema stesso, cioè firmware, software e file di configurazione, oltre ai dati che tratta, come misure, comandi di controllo e input dell'utente.

Per soddisfare questo requisito:

- Metta in atto avvio sicuro e firmware firmato, così che venga eseguito solo codice attendibile
- Usi verifiche in runtime per rilevare e segnalare tentativi di alterazione
- Applichi hashing crittografico e firme digitali per proteggere l'integrità dei dati
- Crei un'infrastruttura in grado di generare, distribuire e verificare chiavi crittografiche tra sistemi o organizzazioni

g. Minimizzazione dei dati

Raccolga e tratti solo i dati necessari alla finalità prevista del prodotto. Vale per i dati personali e per i dati tecnici.

Per soddisfare questo requisito:

- Svolga valutazioni d'impatto sulla protezione dei dati o esercizi di protezione dei dati fin dalla progettazione per identificare flussi non necessari
- Elimini o renda opzionali telemetria, diagnostica o raccolte dati in background non usate
- Preveda impostazioni configurabili di raccolta dei dati, così che la raccolta estesa possa essere abilitata o disabilitata secondo il contesto

h. Disponibilità e resilienza, anche contro gli attacchi di negazione del servizio

Durante un incidente o un attacco, le funzioni chiave del prodotto devono restare disponibili o degradare in modo controllato.

Per soddisfare questo requisito:

- Metta in atto circuit breaker software, logiche di nuovo tentativo, meccanismi di fallback e watchdog timer
- Applichi limiti di risorse per evitarne l'esaurimento
- Usi limitazione del tasso e validazione degli input per proteggersi dagli scenari di negazione del servizio
- Applichi filtraggio a livello di rete per bloccare i tentativi di sovraccarico

i. Nessun impatto negativo su altri dispositivi o reti connessi

Il prodotto non deve disturbare gli altri sistemi nello stesso ambiente. Deve avere un comportamento prevedibile ed evitare un consumo eccessivo delle risorse condivise.

Per soddisfare questo requisito:

- Metta in atto gestione del traffico e limiti l'uso di broadcast o multicast
- Assicuri la conformità alle specifiche dei protocolli di comunicazione
- Usi l'automonitoraggio per rilevare e prevenire comportamenti disturbanti, come flood di rete o esaurimento delle risorse

j. Superficie di attacco limitata, incluse le interfacce esterne

Riduca al minimo i punti di ingresso e le funzionalità esposte. Questo include porte fisiche, interfacce wireless, API, servizi di debug e componenti software non necessari.

Per soddisfare questo requisito:

- Disattivi servizi, porte e interfacce non utilizzati nelle build di produzione
- Irrigidisca le impostazioni predefinite del sistema e limiti i privilegi degli utenti
- Modularizzi le architetture software per isolare i componenti tra loro
- Applichi principi di progettazione software sicura e conduca modellazione delle minacce per identificare ed eliminare esposizioni non necessarie

k. Riduzione dell'impatto degli incidenti tramite misure di mitigazione dello sfruttamento

Parta dal presupposto che alcuni attacchi avranno successo. La progettazione del prodotto deve limitare l'entità del danno.

Per soddisfare questo requisito:

- Separi i componenti di sistema ed esegua i processi in ambienti isolati tramite sandboxing o containerizzazione
- Imponga la separazione dei privilegi, così che le funzioni critiche operino con i soli diritti necessari
- Progetti il prodotto in modo che la compromissione di un componente non consenta a un attaccante di prendere il controllo dell'intero sistema

l. Registrazione delle attività rilevanti per la sicurezza, con possibilità di rifiuto da parte dell'utente

Registri le attività rilevanti per la sicurezza, come tentativi di accesso e modifiche ai dati, così che possano essere monitorate e sottoposte ad audit. Gli utenti devono disporre di un meccanismo di disattivazione quando il CRA lo richiede.

Per soddisfare questo requisito:

- Predisponga logging strutturato, per esempio log JSON con timestamp
- Preveda conservazione locale dei log con rotazione e opzioni di inoltro remoto
- Monitori eventi come tentativi di login, modifiche di configurazione e aggiornamenti software per rilevare anomalie
- Fornisca un meccanismo chiaro lato utente per disattivare la registrazione quando ciò è consentito

m. Cancellazione sicura e permanente dei dati e portabilità

Gli utenti hanno bisogno di un modo pratico per cancellare definitivamente dati e impostazioni. Quando i dati possono essere trasferiti a un altro prodotto o sistema, il trasferimento deve essere sicuro.

Per soddisfare questo requisito:

- Predisponga una funzione di cancellazione sicura che sovrascriva le aree di archiviazione o elimini le chiavi con mezzi crittografici
- Usi canali autenticati e cifrati per i trasferimenti legati alla portabilità dei dati, così da evitare esposizioni durante il trasferimento

Requisiti di trattamento delle vulnerabilità

1. Identificare e documentare le vulnerabilità

Deve sapere quali componenti software si trovano nel prodotto e quali vulnerabilità note li riguardano. Una distinta base del software, SBOM, fornisce questo inventario leggibile da macchina.

Per soddisfare questo requisito:

- Integri la generazione della SBOM direttamente nella pipeline CI/CD, così che ogni build produca un inventario aggiornato dei componenti
- Usi formati consolidati come CycloneDX, SPDX o SWID per l'interoperabilità
- Esegua analisi automatizzate delle vulnerabilità a partire dagli elenchi CVE e da basi come CISA KEV ed ENISA EUVD
- Conservi la SBOM nella documentazione tecnica per tutto il periodo di supporto e la fornisca alle autorità di vigilanza del mercato su richiesta

2. Gestione del rischio e aggiornamenti di sicurezza tempestivi

Quando vengono scoperte vulnerabilità, le corregga rapidamente e fornisca aggiornamenti di sicurezza. Quando possibile, separi le correzioni di sicurezza dagli aggiornamenti funzionali, così che le correzioni critiche possano essere installate senza attendere.

Per soddisfare questo requisito:

- Progetti il meccanismo di aggiornamento in modo che le correzioni di sicurezza possano essere distribuite senza richiedere un aggiornamento completo del sistema
- Strutturi software e firmware affinché i componenti critici possano essere corretti in modo indipendente
- Distribuisca gli aggiornamenti tramite canali sicuri con controlli di integrità
- Conservi le registrazioni delle attività di aggiornamento per garantire tracciabilità e dimostrare la conformità

3. Test di sicurezza regolari

I test di sicurezza non sono un'attività una tantum. Verifichi i prodotti lungo tutto il ciclo di vita, mentre minacce, dipendenze e comportamento del prodotto cambiano. La valutazione del rischio deve determinare tipo e frequenza dei test.

Per soddisfare questo requisito:

- Svolga penetration test per simulare attacchi reali
- Applichi analisi statica e dinamica del codice per individuare debolezze di sicurezza
- Usi fuzzing per far emergere difetti nel trattamento degli input
- Pianifichi e documenti formalmente revisioni di sicurezza del codice e dell'architettura, soprattutto dopo modifiche rilevanti di progettazione o funzionalità

4. Ricezione delle vulnerabilità, politica CVD e advisory

Copre i doveri di intake, divulgazione coordinata e advisory (voci 4, 5 e 6 della sintesi sopra) che in pratica corrono come un unico flusso di lavoro.

Il CRA enuncia tre requisiti separati per il modo in cui comunica intorno alle vulnerabilità: un modo per ricevere segnalazioni, una politica di divulgazione coordinata e un advisory quando spedisce una correzione. Ecco cosa chiede ciascun dovere.

Intake

Offra ai segnalanti una via di accesso chiara e a basso attrito. Pubblichi un metodo di contatto visibile per la segnalazione delle vulnerabilità (indirizzo e-mail dedicato o modulo web). Supporti comunicazioni sicure, per esempio pubblicando una chiave PGP. Il dovere copre le segnalazioni sul suo prodotto e sui componenti di terzi che contiene.

Triage

Confermi ogni segnalazione, la registri in un sistema di tracciamento, la assegni per esame e la risolva entro tempi definiti. Invii conferme e aggiornamenti di stato al segnalante. Quando il problema sta in un componente di terzi, lo indirizzi al manutentore upstream in parallelo alla sua remediation.

Politica di divulgazione coordinata delle vulnerabilità

Pubblichi una politica CVD che fissi le aspettative per segnalanti e partner: metodo di contatto, tempi di risposta attesi, impegni che assume, cosa chiede loro. Coordini la divulgazione per proteggere gli utenti riconoscendo il contributo del segnalante.

Advisory alla correzione

Una volta disponibile la correzione, pubblichi un advisory per il problema risolto. Includa l'identificativo CVE, le versioni del prodotto interessate, un punteggio di gravità standardizzato (per esempio CVSS) e informazioni chiare e accessibili su cosa devono fare gli utenti. Scriva in una lingua accessibile sia agli amministratori tecnici sia agli utenti non tecnici.

Divulgazione pubblica posticipata

Può ritardare la divulgazione pubblica solo se ha una ragione debitamente giustificata che i rischi di cibersicurezza di una divulgazione immediata superano i benefici, e solo finché gli utenti abbiano avuto la possibilità di applicare la correzione. Documenti il ragionamento.

5. Meccanismi sicuri di distribuzione degli aggiornamenti

Il meccanismo di aggiornamento deve essere affidabile e resistente alle alterazioni. Quando gli aggiornamenti automatici sono tecnicamente possibili, riducono il tempo in cui gli utenti restano esposti.

Per soddisfare questo requisito:

- Trasmetta gli aggiornamenti tramite canali sicuri e li verifichi con firme digitali
- Applichi gli aggiornamenti in modo da evitare installazioni incomplete o corrotte
- Usi aggiornamenti differenziali o modulari per ridurre l'impatto operativo e consegnare più rapidamente le correzioni ai sistemi
- Conservi log di aggiornamento così che utenti o amministratori possano verificare lo stato degli aggiornamenti

6. Aggiornamenti di sicurezza gratuiti con messaggi di avviso

Distribuisca gli aggiornamenti di sicurezza rapidamente e senza costi aggiuntivi, salvo quando esiste un accordo distinto per prodotti professionali su misura. Ogni aggiornamento ha bisogno di un messaggio di avviso chiaro che dica agli utenti cosa è cambiato e cosa fare.

Per soddisfare questo requisito:

- Mantenga un sistema di distribuzione capace di notificare direttamente gli utenti o applicare gli aggiornamenti in automatico, secondo il contesto del prodotto
- Scriva i messaggi di avviso in una lingua comprensibile per utenti tecnici e non tecnici
- Includa le informazioni di gravità nei messaggi di avviso quando pertinente
- Dica agli utenti quale azione intraprendere, come applicare l'aggiornamento, modificare una configurazione o vigilare sui sintomi di compromissione
- Diffonda gli aggiornamenti di sicurezza senza ritardo una volta disponibili, così che gli utenti non restino esposti mentre la correzione esiste già
- Pubblichi gli advisory tramite un canale controllato dal fabbricante e li colleghi dalla pagina di supporto del prodotto

I doveri di gratuità e tempestività corrono per la durata del periodo di supporto dichiarato. La deroga su misura cambia solo la base commerciale; i messaggi di avviso si applicano comunque.

Contenuto della documentazione tecnica

Documentazione tecnica

La documentazione tecnica è la prova centrale della conformità CRA. Deve coprire le misure di progettazione, tecniche e procedurali usate per soddisfare i requisiti essenziali di cibersicurezza. Deve esistere **prima dell'immissione sul mercato** e restare aggiornata per tutto il **periodo di supporto**.

Prove della documentazione tecnica nel flusso engineering

Passo 1	**Definire ambito e classe**	Finalità del prodotto, uso previsto, decisione di immissione sul mercato, classe del prodotto, percorso normativo.
Passo 2	**Architettura e rischio**	Architettura, connessioni dati, condizioni d'uso, valutazione dei rischi, mitigazioni.
Passo 3	**Componenti e SBOM**	SBOM leggibile da macchina, componenti di terzi, input dei fornitori, tracciamento delle vulnerabilità.
Passo 4	**Build, test, aggiornamento**	Configurazioni sicure di default, hardening, rapporti di prova, meccanismo sicuro di aggiornamento, avvisi.
Passo 5	**Rilascio e supporto**	Istruzioni per gli utenti, dichiarazione UE, prove CE, motivazione del supporto, registrazioni degli aggiornamenti.

La documentazione tecnica ha otto componenti richiesti. Insieme spiegano **che cos'è il prodotto**, **come è stato costruito e testato**, **quali rischi sono stati considerati**, **quali norme sono state applicate** e **come sarà supportato** una volta sul mercato. Non serve copiare le intestazioni legali, ma ogni argomento deve essere coperto.

N.	Componente	Contenuto richiesto
1	Descrizione generale del prodotto	Finalità prevista e funzioni, versioni software pertinenti, foto o illustrazioni per l'hardware, informazioni e istruzioni per gli utenti
2	Dettagli di progettazione, sviluppo e produzione	Descrizione dell'architettura, componenti e interazioni, distinta base del software (SBOM), processi di trattamento delle vulnerabilità, politica CVD, punto di contatto, meccanismi sicuri di aggiornamento, processi di produzione e monitoraggio, inclusa la validazione
3	Valutazione dei rischi di cibersicurezza	Analisi documentata dei rischi del prodotto, spiegazione di come ciascun requisito essenziale di cibersicurezza si applica al prodotto, mitigazione dei rischi individuati
4	Determinazione del periodo di supporto	Documentazione dei fattori usati per fissare il periodo di supporto, come aspettative degli utenti, prodotti comparabili e orientamenti giuridici
5	Norme armonizzate e specifiche applicate	Elenco delle norme armonizzate, specifiche comuni o schemi di certificazione dell'UE applicati; indicazione dell'applicazione totale o parziale; soluzioni alternative quando le norme non sono applicate
6	Rapporti di prova	Prove di conformità per il prodotto e per i processi di trattamento delle vulnerabilità
7	Dichiarazione UE di conformità	Copia della dichiarazione che collega la documentazione tecnica agli obblighi di marcatura CE
8	SBOM completa (su richiesta)	Le autorità di vigilanza del mercato possono richiedere la SBOM completa per verificare la conformità

Una documentazione tecnica consolidata può coprire il CRA e altre normative UE applicabili, per esempio la direttiva sulle apparecchiature radio o l'ESPR, purché includa tutti gli obblighi applicabili.

Dichiarazione UE di conformità

La dichiarazione UE di conformità è la dichiarazione formale del fabbricante secondo cui il prodotto soddisfa i requisiti di cibersicurezza CRA applicabili. Ogni dichiarazione deve includere:

- Nome, tipo e identificativi unici del prodotto
- Nome e indirizzo del fabbricante, o del mandatario
- Dichiarazione di responsabilità esclusiva del fabbricante
- Descrizione del prodotto che ne assicuri la tracciabilità, eventualmente con immagine
- Dichiarazione esplicita di conformità alla pertinente normativa dell'Unione
- Riferimenti a norme armonizzate, specifiche o certificazioni utilizzate
- Dettagli di qualsiasi organismo notificato coinvolto, con nome, numero, procedura e numero di certificato
- Blocco firma: luogo, data, nome, funzione e firma del firmatario

Una volta firmata, la dichiarazione è giuridicamente vincolante e conferma la piena responsabilità del fabbricante per la conformità in materia di cibersicurezza.

Una dichiarazione semplificata è consentita su imballaggi o manuali nella forma: «Con la presente, [fabbricante] dichiara che il prodotto [tipo/designazione] è conforme al Regolamento (UE) 2024/2847. Il testo completo della dichiarazione UE di conformità è disponibile al seguente indirizzo Internet: [indirizzo Internet].» Questa forma semplificata mantiene la trasparenza e riduce la documentazione. È particolarmente utile per piccoli fabbricanti o portafogli con molti prodotti.

Informazioni e istruzioni per gli utenti

Le informazioni e istruzioni per gli utenti sono una condizione per l'immissione lecita sul mercato. I fabbricanti devono tenere disponibili le istruzioni per **almeno 10 anni** o per l'**intero periodo di supporto**. Importatori e distributori devono verificare che le istruzioni esistano, siano aggiornate e siano fornite nella lingua UE corretta prima di immettere o fornire il prodotto.

Le istruzioni per gli utenti devono contenere:

- Identità e dati di contatto del fabbricante
- Punto di contatto unico per la segnalazione delle vulnerabilità
- Identificazione del prodotto, finalità prevista e contesto d'uso sicuro
- Rischi informatici noti o ragionevolmente prevedibili
- Link alla dichiarazione UE di conformità
- Condizioni di supporto e data chiara di fine supporto
- Istruzioni di sicurezza passo per passo per configurazione, aggiornamenti, uso sicuro, dismissione e, se applicabile, integrazione e accesso alla SBOM

Scelta del percorso di valutazione della conformità

Modulo A: autovalutazione

Il modulo A, controllo interno, consente al fabbricante di autocertificare che il prodotto rispetta i requisiti essenziali di cibersicurezza, assumendosi piena responsabilità per progettazione e produzione. Questo percorso è disponibile per i fabbricanti di prodotti predefiniti, cioè non classificati. È disponibile anche per i prodotti importanti di classe I solo quando le norme armonizzate, le specifiche comuni o gli schemi europei di certificazione della cibersicurezza pertinenti sono disponibili e applicati come richiesto dalle regole di percorso del CRA.

Con il modulo A, occorre:

- Preparare una documentazione tecnica completa
- Descrivere progettazione del prodotto, processi di produzione, meccanismi di cibersicurezza e procedure di trattamento delle vulnerabilità
- Mantenere una responsabilità continua per la conformità durante tutto il ciclo di vita del prodotto
- Predisporre un piano per gli aggiornamenti di sicurezza e la gestione delle vulnerabilità durante la vita operativa del prodotto
- Tenere disponibili le registrazioni per almeno 10 anni

Moduli B e C: valutazione centrata sul prodotto

I moduli B e C si applicano quando è richiesta una verifica di terza parte per uno specifico tipo di prodotto. Si applicano ai prodotti importanti di classe I quando il fabbricante non ha applicato, ha applicato solo in parte o non può applicare norme armonizzate, specifiche comuni o schemi di certificazione pertinenti. Per i prodotti importanti di classe II, il fabbricante deve usare il modulo B+C, il modulo H o uno schema europeo di certificazione della cibersicurezza applicabile almeno al livello di affidabilità «sostanziale».

Modulo B, esame UE del tipo: un organismo notificato esamina un campione rappresentativo del prodotto e la documentazione tecnica correlata. Verifica la conformità a tutti i requisiti essenziali di cibersicurezza e rilascia un certificato di esame UE del tipo quando la progettazione del prodotto risponde ai criteri del CRA.

Modulo C, conformità al tipo e controllo della produzione: il fabbricante garantisce che tutte le unità prodotte siano conformi al tipo approvato nel modulo B. Appone la marcatura CE, redige la dichiarazione UE di conformità e conserva le registrazioni per almeno 10 anni. Insieme, i moduli B e C dimostrano che uno specifico modello di prodotto è tecnicamente conforme e che ogni lotto di produzione resta coerente con il progetto approvato.

Modulo H: valutazione centrata sul processo, garanzia qualità totale

Il modulo H, garanzia qualità totale, riguarda l'intero sistema qualità interno del fabbricante, non i test su un singolo prodotto. È disponibile per i prodotti importanti di classe I e di classe II. I prodotti critici seguono il percorso di certificazione quando le condizioni pertinenti sono soddisfatte; quando tali condizioni non sono soddisfatte, seguono gli stessi percorsi disponibili per i prodotti importanti di classe II.

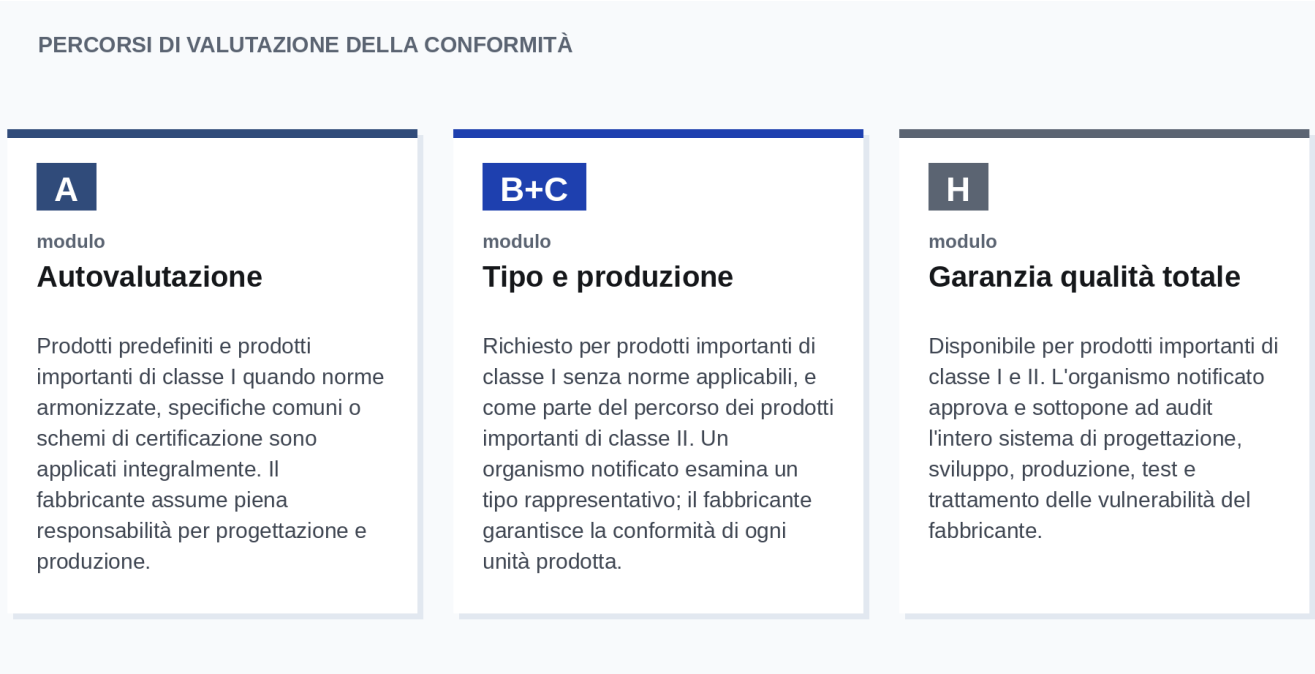
Con il modulo H, occorre:

- Stabilire e mantenere un sistema qualità che copra progettazione, sviluppo, produzione, test e trattamento delle vulnerabilità per l'intera categoria di prodotti
- Sottoporre il sistema qualità a un organismo notificato per valutazione e approvazione
- Accettare la sorveglianza continua dell'organismo notificato, con audit, ispezioni e revisioni di processo, per verificare la conformità nel tempo

Una volta approvato, il fabbricante può emettere dichiarazioni di conformità per tutti i prodotti fabbricati sotto quel sistema qualità, senza ripetere l'esame dell'organismo notificato per ogni singolo tipo di prodotto.

La distinzione chiave tra i percorsi:

- Moduli B+C: l'attenzione è sul prodotto. Un tipo di prodotto rappresentativo viene testato e certificato.
- Modulo H: l'attenzione è sul processo. L'intero sistema di progettazione e produzione del fabbricante è certificato e monitorato.



Flusso di immissione sul mercato

Il CRA nel quadro normativo UE

Il CRA non opera da solo. La domanda pratica per un fabbricante è: dove il mio lavoro CRA fa risparmiare sforzo sotto un altro regime UE, e dove restano obblighi separati da gestire in parallelo?

Dove il suo lavoro CRA può essere riutilizzato

- **Sistemi di IA ad alto rischio (regolamento sull'IA, Regolamento (UE) 2024/1689).** Se il prodotto è un sistema di IA ad alto rischio nell'ambito del CRA, soddisfare i requisiti essenziali di cibersicurezza del CRA si considera soddisfacente per i requisiti di cibersicurezza del regolamento sull'IA nella misura coperta dalla dichiarazione UE di conformità. La procedura di valutazione della conformità si snoda di regola attraverso il regime del regolamento sull'IA, con una deroga per i prodotti CRA importanti e critici. La valutazione dei rischi di cibersicurezza del CRA deve tenere conto dei rischi specifici dell'IA come l'avvelenamento dei dati e gli attacchi avversari.
- **Valutazione del rischio consolidata con altra normativa dell'Unione.** Il CRA consente espressamente che la valutazione dei rischi di cibersicurezza faccia parte di una valutazione più ampia richiesta da un altro atto giuridico dell'Unione, quando il prodotto rientra in entrambi i regimi. Un solo artefatto di valutazione, due usi normativi.
- **Una sola documentazione tecnica per più regimi.** Come già detto nella sezione sulla documentazione tecnica, una documentazione tecnica consolidata può coprire il CRA insieme ad altre normative UE applicabili, a condizione che siano affrontati gli obblighi di ciascun regime. Utile quando lo stesso prodotto necessita già di documentazione sotto la direttiva sulle apparecchiature radio, il regolamento sulla progettazione ecocompatibile dei prodotti sostenibili o altra normativa di prodotto.
- **Definizioni condivise di ricondizionamento, manutenzione e riparazione.** Il CRA importa queste definizioni dal regolamento sulla progettazione ecocompatibile dei prodotti sostenibili. Quando analizza se un intervento di servizio conta come modifica sostanziale, il riferimento sono le definizioni Ecodesign, non un termine specifico del CRA.

Dove restano obblighi separati

- **Tutto il resto del regolamento sull'IA.** La cibersicurezza è solo una fetta del regolamento sull'IA. Classificazione del rischio, trasparenza, governance dei dataset, supervisione umana, monitoraggio post-mercato del comportamento dell'IA e il resto sono doveri del regolamento sull'IA che il CRA non affronta. La cibersicurezza conforme al CRA non è una presunzione di conformità complessiva al regolamento sull'IA.
- **Contenuto Ecodesign e del passaporto digitale di prodotto.** I requisiti Ecodesign su efficienza energetica, durabilità, punteggio di riparabilità e i contenuti di sostenibilità del passaporto digitale di prodotto non rientrano nell'ambito CRA. La catena di prove CRA può stare accanto al lavoro Ecodesign ma non lo sostituisce.
- **Diritti di accesso ai dati IoT del Data Act.** Il Data Act dà agli utenti diritti contrattuali di accesso, condivisione e trasferimento dei dati che i loro prodotti connessi generano. Il CRA copre la sicurezza di quei dati; non fissa il regime dei diritti di accesso. Obbligo diverso, prove diverse.
- **Responsabilità per prodotti difettosi.** La direttiva 2024/2853 mantiene la responsabilità oggettiva del fabbricante. Aggiornamenti di sicurezza post-mercato mancanti possono attivarla. Contratti, assicurazioni e playbook di incidente devono coprire il rischio oltre alla conformità CRA.

Come aiuta CRA Evidence

CRA Evidence trasforma gli obblighi del Cyber Resilience Act dell'UE in prove di prodotto verificabili, combinando una piattaforma di conformità con consulenza tecnica.

Piattaforma

Un unico luogo per gestire le prove alla base della preparazione CRA:

- **Inventario SBOM e componenti:** registri CycloneDX, SPDX e HBOM per versioni e release di prodotto
- **Automazione prove CI/CD:** flussi CLI e API per scansioni, caricamenti SBOM, release gate e registri di audit
- **SBOM firmata e provenienza:** prove versionate, attestazioni dei fornitori e registri di diligenza
- **Operazioni sulle vulnerabilità:** CISA KEV, EPSS, VEX, monitoraggio, triage e flussi di segnalazione
- **Documentazione tecnica e prove CE:** registri della dichiarazione UE, storico di conservazione e passaporti di conformità collegati tramite QR

Consulenza tecnica

Supporto mirato per tradurre gli obblighi CRA in decisioni ingegneristiche su prodotto, architettura, release e fornitori.

- **Sprint di preparazione tecnica:** revisione dei gap sui requisiti essenziali, raccomandazioni architetturali e piano d'azione prioritizzato
- **Responsabile del programma CRA:** modello di responsabilità, tracciamento degli obblighi, milestone delle prove e manutenzione della documentazione tecnica
- **Piano di risposta ad autorità e incidenti:** flussi di segnalazione, playbook per richieste, comunicazioni agli utenti e preparazione dei pacchetti di prove
- **Allineamento normativo:** collegare le prove CRA con Data Act, ESPR, AI Act, RED e requisiti settoriali
- **Workshop tecnici:** sessioni remote o in presenza con prodotto, ingegneria, sicurezza, conformità e fornitori

Indipendente dagli strumenti: CRA Evidence si integra con CycloneDX, SPDX, Grype, Trivy, pipeline CI/CD e issue tracker.

Un primo passo pratico

Scelga una famiglia di prodotti. Mappi il responsabile, la decisione di ambito, la SBOM, il flusso delle vulnerabilità, i gap della documentazione tecnica e le prove di release. Il team ottiene così una base CRA concreta senza trasformare la conformità in un progetto separato.

Scopra cosa copre CRA Evidence per il prodotto su craevidence.com/it. Prezzi e opzioni di piano sono disponibili su craevidence.com/it/prezzi.