SECURE
Cyber Resilience for SMEs

CRA101: Comprensión de las obligaciones en materia de CRA

31/03/2026

Funded by the European Union

Declaración de financiación de la UE: Financiado por la Unión Europea en el marco del número de subvención 101190325. Las opiniones y puntos de vista expresados son, no obstante, exclusivamente las de los autores y no reflejan necesariamente las de la Unión Europea ni las Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad. Ni la Unión Europea ni la autoridad concedente pueden ser consideradas responsables de las mismas.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Descargo de responsabilidad del ECCC: El proyecto cuenta con el apoyo del Centro Europeo de Competencia en Ciberseguridad y sus miembros.

EXENCIÓN DE RESPONSABILIDAD

Este documento forma parte del entregable D4.1 «Directrices y materiales para el cumplimiento de la CRA por parte de las pymes» del proyecto SECURE

Este documento ha sido traducido al español utilizando como apoyo un sistema de traducción automática, por lo que podría contener inexactitudes o errores.

Autor principal: *Centro de Ciberseguridad de Bélgica (CCB)*

Segundo autor: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Funded by the European Union

Índice

Lista de tablas y figuras

Abreviaturas

CE: Conformité Européenne, o Conformidad Europea

CRA: Ley de Resiliencia Cibernética

CSIRT: Equipo de respuesta a incidentes de seguridad informática

CVD: Divulgación coordinada de vulnerabilidades

ENISA: Agencia de la Unión Europea para la Ciberseguridad

OC – Organismo de certificación

PDE – Producto con elementos digitales

PYME – Pequeña y mediana empresa

SBOM – Lista de materiales de software

SPOC – Punto único de contacto

UE – Unión Europea

UE DoC – Declaración de conformidad de la UE

Introducción

La Ley de Ciberresiliencia de la Unión Europea (UE) (CRA), Reglamento (UE) 2024/2847, se adoptó con el objetivo de mejorar la preparación y la resiliencia en materia de ciberseguridad del mercado digital de la UE ante los crecientes retos en este ámbito. Mediante la introducción de normas armonizadas y requisitos mínimos claros de ciberseguridad, la CRA pretende reducir las vulnerabilidades y proteger tanto a los consumidores como a las empresas. Aunque este reglamento histórico entró en vigor en diciembre de 2024, se ha optado por una aplicación gradual, lo que permite un período de transición y adaptación desde 2024 a 2027. Concretamente, la CRA enumera las obligaciones de los fabricantes, importadores y distribuidores de productos con elementos digitales (PDE). El **artículo 13 y el anexo I** de la CRA enumeran los requisitos esenciales de ciberseguridad que deben cumplir los fabricantes, tanto al introducir sus PDE en el mercado de la UE como a lo largo de todo el ciclo de vida del PDE. La parte I de los requisitos del anexo I se centra en las propiedades de los PDE, mientras que la parte II se centra en la gestión de vulnerabilidades. Sin embargo, más allá del anexo I y del artículo 13 de la CRA, se imponen otros requisitos, como por ejemplo, sobre la información y las instrucciones de uso (anexo II), las obligaciones de notificación (artículos 14-17) y la conformidad (artículos 27-32). En un esfuerzo preliminar por traducir las obligaciones legales clave en orientaciones tangibles, **esta guía ofrece una visión general simplificada[1] de las obligaciones**, divididas en **cinco secciones**, que deben tenerse **en** cuenta **como mínimo**. El objetivo es mejorar la accesibilidad del reglamento y aumentar la concienciación y la comprensión a un nivel básico, en particular de las pequeñas y medianas empresas (pymes), en consonancia con los objetivos del proyecto SECURE[2] . Para obtener orientación técnica y herramientas sobre la aplicación de estas disposiciones en la práctica, se publican continuamente nuevos materiales en el **repositorio abierto de SECURE**.

[1] Esta es una lista no exhaustiva destinada a simplificar las obligaciones de la CRA y no incluye las excepciones contempladas en dicho reglamento. Solo se incluyen las obligaciones principales para ofrecer una visión general. Se han seleccionado tras una lectura detallada del texto legislativo del CRA.

[2] El proyecto «Fortalecimiento de la ciberresiliencia de las pymes de la UE» (SECURE) ofrece apoyo financiero y orientación a las pymes para que cumplan con el CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Calendario de la CRA:

- Entrada en vigor: 10 de diciembre de 2024
- Entrada en vigor de las obligaciones de notificación: 11 de septiembre de 2026
- Aplicación plena de los requisitos de la CRA: 11 de diciembre de 2027

Comprender las obligaciones de la CRA - CRA 101

1. Evaluación de riesgos de ciberseguridad

Para cumplir con la obligación de garantizar que su PDE «haya sido diseñado, desarrollado y fabricado de conformidad con los requisitos esenciales de ciberseguridad establecidos en la parte I del anexo I»[3] —es decir, garantizando «un nivel adecuado de ciberseguridad basado en los riesgos»[4] —, es necesario llevar a cabo una evaluación de riesgos de ciberseguridad. Esta evaluación debe **documentarse**[5] y **actualizarse periódicamente** a lo largo del denominado «período de soporte»[6] .

En concreto, la evaluación de riesgos debe incluir, como mínimo,[7] :

1) Un **análisis de los riesgos de ciberseguridad** teniendo en cuenta:
   - La finalidad prevista y el uso previsible del PDE;
   - Las condiciones de uso (por ejemplo, el entorno operativo, los activos que deben protegerse).

2) Una **aclaración, explicación y/o justificación** de
   - La aplicación de la ciberseguridad desde el diseño[8] , es decir, ¿cómo se aplica?
   - La aplicabilidad (o no aplicabilidad) de los requisitos del anexo I, parte I, al PDE; es decir, ¿son aplicables los requisitos de seguridad y de qué manera?

[3] Art. 13, apartado 1, CRA.
[4] Anexo I, parte I, apartado 1, CRA.
[5] Documentación técnica: aclarada en el punto 5.
[6] Período de apoyo: aclarado en el punto 2.
[7] Art. 13, apartado 3, CRA.
[8] Anexo I, parte I, apartado 1, CRA.

- La aplicación y la implementación de los requisitos de gestión de vulnerabilidades[9] , es decir, ¿cómo se aplican los requisitos de gestión de vulnerabilidades?

Cuando un PDE contiene componentes procedentes de terceros, la CRA espera que usted actúe con **la diligencia debida** para salvaguardar la ciberseguridad del producto final. Esto puede significar, por ejemplo, notificar una vulnerabilidad que haya identificado al fabricante de dicho componente y, además, abordarla. Para ello, se debe mantener una lista de materiales de software (SBOM)[10] y una política de divulgación coordinada de vulnerabilidades (CVD) para los proveedores, y ponerlas a disposición de las autoridades de vigilancia del mercado cuando estas lo soliciten.

2. Gestión de vulnerabilidades y actualizaciones de seguridad

Tal y como se establece en el artículo 13, apartado 8, los fabricantes deben garantizar que las vulnerabilidades del PDE y de sus componentes se «gestionen de manera eficaz y de conformidad con los requisitos esenciales establecidos en la parte II del anexo I»[11] durante todo el período de asistencia.

Esto significa, entre otras cosas[12] :

1) **Identificar y documentar las vulnerabilidades**, es decir, elaborar la SBOM (al menos para las dependencias de nivel superior) y mantenerla disponible para facilitarla a las autoridades de vigilancia del mercado cuando así lo soliciten[13] ;
2) Abordar y subsanar las vulnerabilidades sin demora, es decir, **proporcionar actualizaciones de seguridad** sin demoras indebidas y de forma gratuita (con mensajes de aviso para los usuarios):
    - Cada actualización de seguridad publicada durante el periodo de soporte debe permanecer disponible durante al menos 10 años tras su publicación, o durante el resto del periodo de soporte, si este plazo fuera más largo[14] .

[9] Anexo I, Parte II, CRA.
[10] Un registro formal de los detalles y las relaciones de la cadena de suministro de los componentes incluidos en los elementos de software de los PDE (art. 3, apartado 39, CRA).
[11] Art. 13(8), CRA.
[12] Anexo I, Parte II, CRA.
[13] Compartirlo con los usuarios es opcional.
[14] Art. 13(9), CRA.

3) **Revisar y testear** periódicamente la seguridad del producto;

4) **Compartir información** sobre las vulnerabilidades corregidas (y potenciales), su repercusión y gravedad, instrucciones para los usuarios sobre cómo subsanarlas, direcciones de contacto para notificar vulnerabilidades, así como establecer y hacer cumplir una política de CVD.

El «período de soporte» mencionado anteriormente «refleja el tiempo durante el cual se espera que vaya a utilizarse el producto»[15] y debe tener en cuenta de manera proporcional las expectativas de los usuarios, la naturaleza (finalidad) del PDE y la legislación pertinente de la Unión.

Concretamente, al definir su período de soporte, este debe ser:

- De al menos cinco años (a menos que la vida útil del producto sea inferior a cinco años, en cuyo caso el período de soporte será igual a la vida útil del producto);
- Estar claramente especificado (fecha de finalización: mes y año) en el momento de la compra, en el embalaje o en formato digital (una vez alcanzado, lo ideal es notificarlo a los usuarios)[16] .

La determinación y definición del período de soporte debe incluirse en la documentación técnica[17] .

3. Información para el usuario, instrucciones y punto único de contacto

De conformidad con el artículo 13, apartados 14 a 18, y el anexo II, los fabricantes *deben*, como mínimo, **informar claramente a los usuarios** incluyendo en papel o en formato digital:

- Datos del fabricante (nombre, razón social o marca comercial, dirección postal, dirección de correo electrónico o contacto digital, sitio web);
- Datos del PDE (nombre, tipo, finalidad prevista, entorno de seguridad y propiedades de seguridad, funcionalidades esenciales, posibles riesgos de ciberseguridad, asistencia técnica de seguridad prestada, fecha de finalización del período de asistencia);
- Instrucciones detalladas o enlace a las mismas (relativas a las medidas para un uso seguro, posibles efectos en la seguridad de los datos debidos a cambios en el producto, instalación de actualizaciones de seguridad, retirada del servicio segura y

[15] Art. 13(8), CRA.

[16] Art. 13, apartado 19, CRA.

[17] Documentación técnica: aclarada en el punto 5.

eliminación de los datos de usuario, configuración predeterminada de instalación de actualizaciones de seguridad);

- Se debe designar un punto único de contacto (SPOC) para que los usuarios puedan:
    - Comunicarse de forma directa y rápida con el fabricante a través de sus medios de comunicación preferidos (sin limitarse a las herramientas automatizadas);
    - Notificar vulnerabilidades;
    - Localizar la política de CVD.
- Enlaces (si procede) a la política de CVD, la declaración de conformidad de la UE (EU DoC)[18] y la SBOM (si está disponible para los usuarios).

Las instrucciones de uso deben estar disponibles en un lenguaje fácilmente comprensible, en línea o en papel, durante al menos diez años o el periodo de asistencia técnica (el que sea más largo).

4. Obligaciones de notificación: notificación de vulnerabilidades e incidentes

En cuanto a la notificación[19] , la tabla siguiente ofrece una visión general de sus obligaciones. A continuación se proporcionan más aclaraciones.

Tabla 1 :
Notificación de vulnerabilidades e incidentes

Notificación	Vulnerabilidades	Incidentes
QUÉ	*Obligatorio:* «vulnerabilidades explotadas activamente» *Opcional:* vulnerabilidades (no explotadas activamente); amenazas cibernéticas	*Obligatorio*: «incidentes graves» *Opcional*: incidentes (no graves); cuasi accidentes

[18] Declaración de conformidad de la UE: aclarado en el punto 5.
[19] Art. 14-17, CRA.

A QUIÉN	CSIRT[20] Plataforma única de notificación (ENISA) Usuarios afectados	
CÓMO	1) Notificación de alerta temprana (24 h) 2) Notificación de vulnerabilidad (72 h) 3) Informe final (14 días)	1) Notificación de alerta temprana (24 h) 2) Notificación de incidente (72 h) 3) Informe final (1 mes)

4.1. ¿Qué hay que notificar?

Según las definiciones establecidas en el artículo 3 de la CRA,

- Una «vulnerabilidad explotada activamente» requiere pruebas fiables de que un actor malintencionado la ha explotado en un sistema sin el permiso del propietario[21];
- Un incidente se considera «grave» cuando[22] :
    - Afecta o puede afectar negativamente a la capacidad del PDE para proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos o funciones; o
    - Ha dado lugar o puede dar lugar a la introducción o ejecución de código malicioso en el producto o en la red y los sistemas de información de un usuario.

4.2. ¿A quién hay que notificar?

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) al que debe informarse es el del Estado miembro en el que el fabricante[23] :

[20] Art. 3, apartado 51, CRA: «CSIRT designado como coordinador» significa un CSIRT designado como coordinador de conformidad con el artículo 12, apartado 1, de la Directiva (UE) 2022/2555.

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

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

[23] El CSIRT suele ser el CERT nacional: Equipo de Respuesta a Emergencias Informáticas.

- Tiene su establecimiento principal; o, si no se puede determinar,
- Tenga el establecimiento con mayor número de empleados.

Si se encuentra fuera de la UE, se puede seguir una cadena alternativa que tenga en cuenta el establecimiento del representante autorizado del fabricante → importador → distribuidor → donde se encuentre el mayor número de PDEs o usuarios.

Salvo varias excepciones, todas las notificaciones se tramitarán a través de la plataforma única de notificación, que aún debe establecer y que mantendrá la Agencia de la Unión Europea para la Ciberseguridad (ENISA), y se difundirán a otros CSIRT y autoridades de vigilancia del mercado a través de un punto final de notificación electrónico.

Los usuarios afectados (y, cuando proceda, todos los usuarios) también deben ser notificados sobre las vulnerabilidades o incidentes y las medidas que deban tomar, preferiblemente en formato legible por máquina. Los CSIRT pueden informar a los usuarios si el fabricante no lo hace[24] .

4.3. ¿Cómo hay que notificar?

Existen varias diferencias en la notificación de vulnerabilidades e incidentes.

Vulnerabilidades

1) **Notificación de alerta temprana**: debe enviarse a más tardar en un plazo de 24 horas desde que se tenga conocimiento y debe indicar, si procede, los Estados Miembros en los que está disponible el PDE.
2) **Notificación de vulnerabilidad**: debe presentarse a más tardar en un plazo de 72 horas desde que se tenga conocimiento de la misma y debe incluir:
    - Información general sobre el PDE;
    - Características generales de la vulnerabilidad;
    - Medidas correctivas o paliativas adoptadas o que pueden adoptar los usuarios;
    - Sensibilidad de la información notificada.

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

3) **Informe final**: deberá presentarse a más tardar **14 días** después de la aplicación de las medidas correctivas o mitigadoras y deberá incluir:
    - Descripción: gravedad e impacto;
    - Información sobre el autor malintencionado, si procede;
    - Detalles sobre la actualización de seguridad u otras medidas correctivas disponibles.

Incidentes

1) **Notificación de alerta temprana**: deberá presentarse a más tardar en un plazo de 24 horas desde que se tenga conocimiento del incidente y deberá indicar:
    - Si procede, los Estados miembros en los que está disponible el PDE;
    - Si se sospecha que ha sido causado por actos ilícitos o maliciosos.
2) **Notificación de incidentes**: deberá presentarse a más tardar en un plazo de 72 horas desde que se tenga conocimiento del mismo y deberá incluir:
    - Información general sobre la naturaleza del incidente;
    - Evaluación inicial del incidente;
    - Las medidas correctivas o mitigadoras adoptadas o que puedan adoptar los usuarios;
    - Sensibilidad de la información notificada.
3) **Informe final**: debe presentarse en el plazo de un mes tras la notificación del incidente y debe incluir:
    - Descripción: gravedad e impacto;
    - Tipo de amenaza o causa raíz que probablemente haya provocado el incidente;
    - Medidas de mitigación aplicadas y en curso.

5. Evaluación de la conformidad

Antes de que un PDE se comercialice, el fabricante debe demostrar que cumple los requisitos esenciales de ciberseguridad establecidos en el anexo I del CRA. Esto se lleva a cabo mediante el **procedimiento de evaluación de la conformidad** aplicable a la categoría de producto pertinente.

5.1. Procedimientos de evaluación de la conformidad

El CRA prevé, entre otras cosas:

- Control interno (Módulo A);
- Procedimiento de Examen tipo UE seguido de la conformidad con el tipo (Módulos B + C);
- Garantía de calidad total (Módulo H);
- Evaluación en el marco de un sistema europeo de certificación de ciberseguridad, cuando proceda.

Las normas armonizadas y las especificaciones comunes no son procedimientos de conformidad. Sin embargo, pueden servir de apoyo para demostrar la conformidad.

5.2. Presunción de conformidad

Un producto que cumple con:

- las normas armonizadas cuyas referencias se hayan publicado en el Diario Oficial, o
- las especificaciones comunes adoptadas por la Comisión Europea

se **presume que cumple**[25] con los requisitos esenciales cubiertos por dichas normas o especificaciones.

Cuando dichas normas o especificaciones no se apliquen (íntegramente), el fabricante deberá demostrar directamente el cumplimiento de los requisitos del anexo I mediante el procedimiento de evaluación de la conformidad aplicable. Cuando proceda, también podrá utilizarse un certificado europeo de ciberseguridad para demostrar la conformidad, dentro de los límites establecidos por la CRA.

[25] Art. 27, CRA.

5.3. Categorías de productos

El procedimiento de evaluación de la conformidad que debe aplicarse depende de la clasificación del PDE según el CRA, tal y como se especifica en los anexos III y IV de la CRA[26] . LA CRA distingue entre productos por defecto, importantes (clases I y II) y críticos.

Dependiendo de la categoría:

- El control interno puede ser suficiente;
- Puede ser necesaria la intervención de un organismo notificado (ON); o
- La evaluación en el marco de un sistema de certificación europeo puede ser obligatoria o permitida.

Por lo tanto, la **clasificación correcta** es decisiva para determinar el procedimiento aplicable.

En la tabla 2 de la página siguiente se ofrece una visión general de los procedimientos que pueden aplicarse según la clase de producto.

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

Tabla 2 :
Procedimientos de evaluación de la conformidad

	Control interno (módulo A)	Examen CE de tipo seguido de la conformidad con el tipo (módulos B + C)	Garantía de calidad total (módulo H)	Sistema europeo de certificación de ciberseguridad	Normas armonizadas/ Especificaciones comunes[27]
Productos por defecto	**X**	**X**	**X**	**X**	**X** Puede proporcionar apoyo en materia de conformidad para los requisitos cubiertos
Productos importantes de Clase I	**X**[28]	**X**	**X**	**X** Nivel: sustancial[29]	**X** Puede proporcionar apoyo en materia de conformidad para los requisitos cubiertos
Productos importantes de Clase II		**X**	**X**	**X** Nivel: sustancial[30]	**X** Puede proporcionar soporte de conformidad para los requisitos cubiertos
Productos críticos				**X** Nivel: sustancial	**X** Puede proporcionar apoyo en materia de conformidad para los requisitos cubiertos

[27] Las normas armonizadas y las especificaciones comunes no son procedimientos, pero pueden servir de apoyo para la demostración de la conformidad.

[28] El control interno (módulo A) solo podrá utilizarse cuando se apliquen normas armonizadas, especificaciones comunes o, en su caso, un sistema de certificación pertinente. Cuando no sea así, las vías aplicables son el examen de tipo de la UE seguido de la conformidad con el tipo (módulos B+C) o el aseguramiento de la calidad total (módulo H).

[29] Si, en virtud del art. 8, apartado 1, del CRA, se adopta un acto delegado, podrá utilizarse el sistema de certificación cibernética de la UE. En caso contrario, se recurrirá a las normas aplicables a los productos importantes de clase II.

[30] Se aplica la nota a pie de página 29.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.4. Declaración de conformidad de la UE (EU DoC)

Tras una evaluación de conformidad satisfactoria, el fabricante elabora una **Declaración de Conformidad de la UE** (EU DoC)[31] .

En esta declaración, se confirma que el PDE cumple con los requisitos esenciales aplicables e incluye los elementos requeridos según lo previsto en la CRA. La estructura del modelo se encuentra en el anexo V de la CRA. La UE DoC simplificada se encuentra en el anexo VI. Debe estar disponible en las lenguas exigidas por el Estado Miembro en el que se comercializa el PDE y debe permanecer disponible durante el período legalmente prescrito.

5.5. Marcado CE

Para que los consumidores puedan identificar los productos de consumo (PDE) que cumplen los requisitos de la (CRA) y tomar decisiones informadas a la hora de adquirir y utilizar dichos productos, el **marcado CE**[32] debe «colocarse de forma visible, legible e indeleble»[33] antes de que el producto de consumo se comercialice. Esto debe hacerse directamente sobre el propio producto. Cuando esto no sea posible debido a la naturaleza del producto, deberá colocarse en el embalaje e incluirse en la declaración de conformidad de la UE adjunta[34] [35] . El marcado CE indica que el producto cumple con toda la legislación de la Unión aplicable que exige el marcado CE, incluida la CRA.

5.6. Demostración de la conformidad mediante la documentación técnica

Un componente clave para evaluar la conformidad es la **documentación técnica.** Exigida por el artículo 31 de la CRA y el anexo VII, la documentación técnica es relevante para todos los puntos anteriormente mencionados, ya que debe elaborarse antes de que el PDE se comercialice y actualizarse continuamente durante todo el período de soporte[36] . Al reunir la mayoría de las obligaciones de la CRA, la documentación técnica debe incluir, por lo tanto,[37] :

[31] Artículo 28 del CRA; anexos V y VI del CRA.
[32] Marcado de Conformité Européenne (Conformidad Europea).
[33] Artículo 30, apartado 1, del CRA.
[34] Artículos 29 y 30 de la CRA.
[35] Se aplican normas adicionales si un organismo notificado participa en la evaluación de la conformidad.
[36] Art. 31(2), CRA.
[37] Anexo VII, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Descripción general del PDE (finalidad prevista, versiones de software que afectan al cumplimiento, pruebas de características externas, marcado y diseño interno para productos de hardware, información e instrucciones para el usuario);
- Descripción de los procesos de diseño, desarrollo y producción del PDE, así como de gestión de vulnerabilidades (por ejemplo, descripción de la arquitectura del sistema, SBOM, política de CVD, procesos de monitorización, etc.);
- Evaluación de riesgos de ciberseguridad;
- Definición y aclaración del periodo de soporte;
- Normas armonizadas aplicadas (o partes de las mismas);
- Informes de ensayos de conformidad e informes de gestión de vulnerabilidades;
- Copia de la declaración de conformidad de la UE.

La Comisión Europea elaborará un formulario **simplificado de documentación técnica** para microempresas y pequeñas empresas[38] . Además, el artículo 33 estipula que tanto los Estados Miembros como la Comisión Europea deben prestar **apoyo a las pymes**, entre otras cosas, en forma de orientación[39] y oportunidades de apoyo financiero.

El **proyecto SECURE ofrece apoyo financiero a las pymes que deben cumplir con la CRA y proporciona directrices y materiales de forma continua con el fin de ayudar a las pymes en la implementación de la CRA**, como esta guía CRA101.

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

[39] Art. 26, CRA.

Conclusión

Con el fin de ofrecer una **visión general accesible de las obligaciones clave establecidas en la CRA**, esta guía se centra en **cinco componentes** de la CRA que deben tenerse en cuenta como mínimo: (1) Evaluación de riesgos de ciberseguridad; (2) Gestión de vulnerabilidades y actualizaciones de seguridad; (3) Información al usuario, instrucciones y punto único de contacto; (4) Obligaciones de notificación: notificación de vulnerabilidades e incidentes; (5) Evaluación de la conformidad. Aclara elementos como el período de soporte, la declaración de conformidad de la UE y el marcado CE, así como la documentación técnica. Con el objetivo de **ayudar a las pymes a orientarse en el complejo marco jurídico**, esta guía ofrece un resumen de las principales obligaciones legales que deben entenderse antes de su aplicación. Para obtener orientación práctica sobre cómo abordar e implementar estas disposiciones legales, así como sobre elementos concretos de la CRA (por ejemplo, SBOM, gestión de vulnerabilidades, etc.), se irán publicando de forma continua directrices técnicas y herramientas adicionales en el repositorio central SECURE, a medida que avance la implementación de la CRA. Como próximos pasos para las pymes, se recomienda consultar las demás directrices del repositorio SECURE, como los **Requisitos esenciales de ciberseguridad de la CRA: Anexo I, Parte I** para obtener sugerencias y recomendaciones prácticas sobre cada una de las disposiciones del Anexo I, así como el **Marco metodológico de evaluación del cumplimiento de la CRA** para disponer de un conjunto de herramientas paso a paso y una lista de verificación sobre el cumplimiento de la CRA más allá del Anexo I.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE