NOTA INFORMATIVA

Cyber Resilience Act: obligaciones de notificación de vulnerabilidades e incidentes desde septiembre de 2026

El 11 de septiembre de 2026 entran en aplicación las primeras obligaciones del Cyber Resilience Act. Los fabricantes de productos con elementos digitales deberán notificar vulnerabilidades activamente explotadas e incidentes graves de seguridad. El resto de obligaciones se aplicarán a partir de diciembre de 2027.

Puntos claves a destacar

- Desde el 11 de septiembre de 2026, los fabricantes deben notificar vulnerabilidades activamente explotadas e incidentes graves.
- Alerta temprana en 24 horas; notificación detallada en 72 horas; informe final en 14 días de vulnerabilidades o 1 mes en el caso de incidentes.
- Notificación simultánea al CSIRT coordinador del Estado miembro y a ENISA, a través de la Plataforma Única de Notificación.
- Las obligaciones aplican a todos los productos en el mercado, con independencia de su fecha de comercialización, y continúan tras expirar el periodo de soporte.

1. Antecedentes

El Reglamento (UE) 2024/2847 (Cyber Resilience Act, en adelante "CRA"), en vigor desde el 10 de diciembre de 2024, establece requisitos horizontales de ciberseguridad aplicables a los productos con elementos digitales comercializados en el mercado interior.

Estos "productos con elementos digitales" pueden referirse a software autónomo (como por ejemplo aplicaciones móviles o programas descargables), hardware con software integrado (como dispositivos conectados - IoT, portátiles, etc), hardware autónomo, y combinaciones de hardware y software destinadas a funcionar conjuntamente.

Sin embargo, los servicios SaaS (Software-as-a-Service) y otras soluciones cloud autónomas que se ejecuten de forma remota y a las que el usuario simplemente acceda —sin que el software se descargue ni instale en su sistema de manera local— quedan fuera del ámbito de aplicación del CRA, salvo que cumplan la definición de "tratamiento de datos a distancia", es decir, que hayan sido diseñados y desarrollados por el fabricante (o bajo su responsabilidad) y resulten necesarios para que el producto con elementos digitales pueda cumplir sus funciones.

Su aplicación íntegra se producirá el 11 de diciembre de 2027. No obstante, las obligaciones de notificación previstas en el artículo 14 son exigibles desde el 11 de septiembre de 2026. Estas obligaciones se aplican a todos los productos con elementos digitales que se encuentren en el ámbito del CRA, con independencia de su fecha de comercialización.

El 27 de julio de 2026, la Comisión publicó la primera guía interpretativa no vinculante en sentido estricto, pero recomendable a la hora de implementar CRA en las organizaciones (C(2026) 5252) (en adelante, "la Guía"), que aborda, entre otras cuestiones, el alcance práctico de las obligaciones de notificación y la gestión de vulnerabilidades.

2. Obligaciones de notificación desde el 11 de septiembre de 2026

El artículo 14 del CRA obliga a los fabricantes a notificar simultáneamente cualquier vulnerabilidad aprovechada activamente y cualquier incidente grave al CSIRT designado como coordinador y a la ENISA, a través de la Plataforma Única de Notificación, de conformidad con el artículo 16 del CRA.

La notificación se presenta mediante el "nodo final" de notificación electrónica del CSIRT correspondiente, es decir, el punto de entrada a la red a través del cual dicho CSIRT reciba las notificaciones remitidas por los fabricantes, de modo que la información queda simultáneamente accesible para ENISA.

2.1 Vulnerabilidades aprovechadas activamente

Una vulnerabilidad se considera "aprovechada activamente" cuando un atacante la utiliza de forma efectiva contra el producto. No basta con que la vulnerabilidad exista, sino que se debe haber tenido constancia de que dicha vulnerabilidad ha sido explotada de manera activa.

El artículo 14, apartado 2, del CRA establece los siguientes plazos en caso de producirse una vulnerabilidad:

- Alerta temprana: 24 horas desde la toma de conocimiento.
- Notificación detallada: 72 horas desde la toma de conocimiento.
- Informe final: 14 días desde la disponibilidad de una medida correctiva.

El sistema de notificación previsto en el artículo 14 del CRA se basa en una lógica progresiva. El fabricante debe remitir la información disponible en cada momento, sin necesidad de esperar a disponer de todos los detalles técnicos sobre la vulnerabilidad o el incidente. A medida que avance la investigación y se disponga de nuevos datos, la información inicialmente comunicada deberá completarse mediante las notificaciones posteriores previstas por el Reglamento. Así, el contenido de cada comunicación evoluciona desde una primera alerta temprana hasta un informe final más detallado.

En el caso de una vulnerabilidad explotada activamente, la notificación inicial de 24 horas tiene por objeto alertar sobre su existencia. Posteriormente, la notificación de 72 horas debe incluir, en la medida en que la información esté disponible, datos generales sobre el producto afectado, la naturaleza de la vulnerabilidad y su explotación, las medidas correctoras o de mitigación adoptadas por el fabricante, así como las actuaciones que puedan llevar a cabo los usuarios para reducir el riesgo. También podrá indicarse el grado de sensibilidad de la información comunicada. Finalmente, una vez exista una medida correctora o de mitigación, deberá remitirse un informe final que incorpore una descripción de la vulnerabilidad, su gravedad e impacto, información disponible sobre los actores maliciosos implicados y detalles de las medidas adoptadas para subsanarla.

2.2 Incidentes graves

Según el CRA, se entiende por incidente grave aquel que tiene un impacto significativo que repercuta en la seguridad del producto con elementos digitales cuando:

> (a) afecte o pueda afectar negativamente a la capacidad del producto para proteger la disponibilidad, autenticidad, integridad o confidencialidad de datos o funciones sensibles o importantes; o
>
> (b) haya llevado o pueda llevar a la introducción o ejecución de código malicioso en el producto o en la red y los sistemas de información de un usuario. La definición comprende, por tanto, tanto los incidentes que ya han producido una afectación como aquellos que presentan un riesgo suficiente de producirla.

En el caso de los incidentes graves, se mantienen los plazos de la alerta temprana y de la notificación detallada. En cambio, **el informe final debe presentarse en el plazo de un mes desde la notificación de 72 horas.**

De forma análoga, las notificaciones relativas a incidentes graves pueden completarse y actualizarse a medida que avance el análisis técnico de los hechos. El CRA parte expresamente de la premisa de que la información disponible durante las primeras horas de gestión de un incidente suele ser limitada, por lo que exige una comunicación escalonada que permita a las autoridades competentes recibir información temprana sin perjuicio de su posterior ampliación o corrección.

2.3 ¿Cómo se realiza la notificación?

Las obligaciones de notificación previstas en los artículos 14 y 15 del CRA se cumplirán a través de la Plataforma Única de Notificación (en adelante "SRP" por sus siglas en inglés "Single Reporting Platform"). La plataforma estará disponible a partir del 11 de septiembre de 2026 y constituye una herramienta desarrollada y gestionada por ENISA, con el objetivo de centralizar la comunicación de vulnerabilidades explotadas activamente e incidentes graves relacionados con productos con elementos digitales.

La notificación debe ser realizada por un representante principal, encargado de registrar a la organización en la plataforma, que deberá autenticarse mediante el sistema EU Login para acceder a la plataforma y gestionar las comunicaciones correspondientes. Asimismo, podrá disponer de uno o varios representantes secundarios o de respaldo, que podrán actuar en nombre del mismo fabricante y garantizar la continuidad de las obligaciones de reporte.

La validación por parte del CSIRT de la representación del usuario no constituye un requisito previo para presentar una notificación. Dicha validación podrá realizarse de forma paralela al proceso de reporte y no impedirá el cumplimiento de los plazos establecidos por el CRA. Asimismo, ENISA recomienda que fabricantes y *open-source software stewards* se registren únicamente cuando necesiten presentar una notificación concreta, evitando la creación anticipada de cuentas que todavía no vayan a utilizarse.

La plataforma permitirá gestionar todas las fases de notificación previstas en el CRA mediante formularios estructurados que podrán actualizarse progresivamente a medida que el fabricante disponga de nueva información. A medida que la organización disponga de nueva información sobre la vulnerabilidad o el incidente, podrá completar y actualizar los datos previamente comunicados a través de la plataforma. Este enfoque permite cumplir con los plazos exigidos por el CRA sin necesidad de esperar a disponer de toda la información técnica o forense desde el inicio, garantizando al mismo tiempo que las autoridades competentes reciban una visión cada vez más completa de la situación.

La información que debe facilitarse en cada fase dependerá del tipo de notificación y del grado de conocimiento existente en ese momento. No obstante, con carácter general, las organizaciones deberán proporcionar los datos necesarios para identificar el producto afectado, describir la vulnerabilidad o el incidente, valorar su impacto y comunicar las medidas de mitigación o corrección adoptadas o previstas. Las actualizaciones posteriores permitirán complementar o rectificar la información inicialmente remitida cuando se disponga de nuevos elementos de análisis.

Por último, la ENISA ya ha publicado materiales preparatorios que anticipan el funcionamiento de la plataforma y detallan, entre otros aspectos, los campos que deberán cumplimentarse en cada notificación y los pasos para acreditar la representación de la entidad notificante.

3. Principales aclaraciones de la Guía

3.1 Concepto de "toma de conocimiento"

El fabricante se considera conocedor cuando, tras una evaluación inicial e inmediata, alcanza un grado razonable de certeza de que:

(i) una vulnerabilidad contenida en su producto está siendo aprovechada activamente, o
(ii) se ha producido un incidente grave que ha comprometido la seguridad del producto.

El momento en que se alcanza ese grado de certeza depende de las circunstancias concretas del caso: puede ser claro desde el inicio o requerir un periodo de investigación para confirmar que el producto está afectado y que existe un aprovechamiento malintencionado. La Guía vincula este criterio con el Reglamento de Ejecución (UE) 2024/2690 y con las Directrices 9/2022 del EDPB, que exigen actuar con prontitud en la evaluación inicial.

3.2 No retroactividad

No existe obligación de notificar una vulnerabilidad cuyo aprovechamiento activo ya era conocido por el fabricante antes del 11 de septiembre de 2026, porque la obligación de notificación no tiene carácter retroactivo.

Distinto es el caso en que el fabricante ya conociera la vulnerabilidad, pero no el aprovechamiento activo, antes de esa fecha: si el aprovechamiento se produce o llega a su conocimiento después del 11 de septiembre de 2026, nace la obligación de notificar conforme al artículo 14 del CRA. La Guía exige, por tanto, separar la fecha en que se conoció el defecto de la fecha en que se conoció su aprovechamiento.

3.3 Vulnerabilidades en componentes de terceros

Cuando un componente de terceros integrado en un producto contenga una vulnerabilidad aprovechada activamente en dicho producto, el fabricante deberá notificarla a través de los canales indicados anteriormente.

Como se ha indicado, la notificación no es obligatoria si la vulnerabilidad no ha sido explotada activamente, sin embargo, el artículo 15 del CRA abre la puerta a una comunicación voluntaria. Adicionalmente, el fabricante del producto deberá informar de la vulnerabilidad al fabricante o a la entidad responsable de fabricar o mantener el componente de terceros afectado, así como abordarla y subsanarla (artículo 13, apartado 6, del CRA).

3.4 Información a usuarios

Cuando una vulnerabilidad explotada activamente o un incidente grave pueda afectar a la seguridad del producto o a los intereses de sus usuarios, el fabricante deberá informarles sin demora indebida y de forma clara sobre los riesgos identificados, las medidas de mitigación disponibles y las actuaciones que pueden adoptar para protegerse.

La información facilitada deberá ser proporcionada al riesgo existente. Por ello, no será necesario divulgar todos los detalles técnicos de la vulnerabilidad o del incidente cuando ello pueda comprometer la seguridad del producto o favorecer nuevas explotaciones.

3.5 Difusión diferida

El CRA permite retrasar la difusión de determinada información cuando una divulgación inmediata pueda facilitar nuevos ataques, comprometer la adopción de medidas correctoras o interferir con procesos de divulgación coordinada de vulnerabilidades. En estos supuestos, el CSIRT coordinador podrá aplazar temporalmente la difusión de la información durante el tiempo estrictamente necesario para proteger los intereses de ciberseguridad afectados.

4. Alcance subjetivo: ¿quién debe notificar?

Aunque el artículo 14 atribuye principalmente las obligaciones de notificación a los fabricantes, el CRA contempla determinados supuestos en los que otros actores de la cadena de suministro o del ecosistema de software de código abierto pueden quedar sujetos a obligaciones de notificación específicas.

- Fabricantes de productos con elementos digitales: Los fabricantes constituyen el principal sujeto obligado por las obligaciones de notificación establecidas en el artículo 14 del CRA. En consecuencia, cuando tengan conocimiento de una vulnerabilidad explotada activamente o de un incidente grave que afecte a la seguridad de un producto con elementos digitales incluido en el ámbito de aplicación del Reglamento, deberán realizar las notificaciones correspondientes a través de la plataforma única gestionada por ENISA y cumplir los restantes deberes de información previstos por la normativa. La obligación se aplica con carácter general a todos los fabricantes sujetos al CRA, con independencia de la categoría específica del producto.
- Importadores y distribuidores que adquieren la condición de fabricante: Los importadores o distribuidores no están sujetos, por regla general, a las obligaciones de notificación del artículo 14. No obstante, asumirán las obligaciones correspondientes al fabricante cuando comercialicen un producto con elementos digitales bajo su propio nombre o marca, o cuando realicen una modificación sustancial del producto ya comercializado. En tales casos, pasarán a ser considerados fabricantes respecto del producto o de la parte afectada por la modificación y deberán cumplir las obligaciones que el CRA atribuye a dicha figura, incluidas las relacionadas con la notificación de vulnerabilidades e incidentes cuando resulten aplicables.
- Open-source software stewards: están sujetos a un régimen específico previsto en el artículo 24 del CRA. Esta figura comprende a determinadas entidades que proporcionan apoyo continuado al desarrollo de productos con elementos digitales que califican como software libre y de código abierto destinado a actividades comerciales, contribuyendo a su mantenimiento y viabilidad sin ostentar la condición de fabricante. El artículo 24.3 únicamente les hace aplicable la obligación de notificar vulnerabilidades explotadas activamente prevista en el artículo 14.1 en la medida en que participen en el desarrollo del producto con elementos digitales de que se trate. Asimismo, les resultan aplicables determinadas obligaciones vinculadas a los incidentes graves cuando éstos afecten a los sistemas de red e información que el propio *open-source software steward* proporciona para el desarrollo de dichos productos.

Régimen sancionador:

El CRA prevé un régimen de multas administrativas graduado en función de la naturaleza del incumplimiento, sin perjuicio de otras medidas correctoras o restrictivas que puedan adoptar las autoridades de vigilancia del mercado. Las cuantías máximas aplicables son las siguientes:

- Hasta 15 M€ / 2,5% facturación mundial — Incumplimiento de requisitos esenciales de ciberseguridad.
- Hasta 10 M€ / 2% facturación mundial — Incumplimiento de otras obligaciones del CRA.
- Hasta 5 M€ / 1% facturación mundial — Información incorrecta, incompleta o engañosa.

En todos los casos se aplica el importe más elevado. No obstante, los fabricantes que tengan la consideración de microempresa o pequeña empresa no podrán ser sancionados por el incumplimiento del plazo de 24 horas para la presentación de la alerta temprana.

Esta excepción no les exime de las demás obligaciones previstas en el CRA, por lo que deberán seguir notificando las vulnerabilidades explotadas activamente y los incidentes graves, así como cumplir el resto de los requisitos que les resulten aplicables.

Además de las sanciones económicas previstas por el CRA, las autoridades de vigilancia del mercado podrán ordenar la retirada del producto afectado. Asimismo, el CRA establece que el mero hecho de realizar una notificación de vulnerabilidad o incidente no genera responsabilidad adicional para quien la presenta.

5. Resumen ejecutivo

El 11 de septiembre de 2026 marca el primer hito relevante en la aplicación efectiva del CRA, ya que, desde esa fecha, serán exigibles las obligaciones de notificación previstas en su artículo 14 respecto de todos los productos con elementos digitales incluidos en su ámbito de aplicación, con independencia de la fecha en que hayan sido comercializados.

En consecuencia, las organizaciones que fabriquen, importen o distribuyan estos productos deben anticiparse y adaptar sus procedimientos internos para identificar los productos afectados, definir responsabilidades, establecer mecanismos de escalado e implantar procesos que permitan cumplir los plazos de notificación aplicables, que oscilan entre las 24 horas, las 72 horas y los 14 días o un mes, según el tipo de incidente o vulnerabilidad de que se trate.

No obstante, la aplicación plena del CRA no tendrá lugar hasta el 11 de diciembre de 2027. A partir de esa fecha, las organizaciones deberán cumplir de forma íntegra los requisitos esenciales de ciberseguridad y el resto de las obligaciones previstas en el Reglamento, sin perjuicio de que las obligaciones de notificación resulten exigibles con anterioridad.

Área de Privacidad y Ciberseguridad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60