

Ficha informativa de la plataforma única de notificación del Reglamento de Ciberresiliencia

Cómo notificar incidentes y vulnerabilidades explotadas activamente a través de la plataforma única de notificación.

Objetivos

A partir del 11 de septiembre de 2026, el Reglamento de Ciberresiliencia exige a los fabricantes que notifiquen las vulnerabilidades explotadas activamente y los incidentes graves que repercutan en la seguridad de los productos con elementos digitales vendidos en el mercado de la UE.

El Reglamento de Ciberresiliencia también exige a los responsables de software de código abierto que informen de estos acontecimientos en la medida en que estén involucrados en el desarrollo de productos con elementos digitales.

Destinatarios



Fabricantes



Responsables de
Software de Código
Abierto

¿Cuáles son sus nuevas obligaciones de notificación?

La plataforma única de notificación del Reglamento de Ciberresiliencia (CRA SRP, por sus siglas en inglés) es una herramienta en línea para que los fabricantes y los responsables de software de código abierto cumplan la obligación de notificar las vulnerabilidades explotadas activamente y los incidentes graves. Diseñada para simplificar las obligaciones de información de la UE, la plataforma única de notificación del Reglamento de Ciberresiliencia es un sistema electrónico que

permite presentar un único informe para comunicarlo a todas las autoridades pertinentes. La plataforma incorpora medidas de seguridad para proteger la confidencialidad.

Cada notificación permite enviar información automáticamente a su CSIRT nacional, que recibe inicialmente la notificación, a los demás CSIRT nacionales donde el producto con elementos digitales está disponible, y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

¿Cómo averiguar a qué CSIRT nacional debe dirigir su notificación?

En general, el CSIRT nacional al que debe informar a través de la plataforma única de notificación está determinado fundamentalmente por su sede principal. El artículo 14, apartado 7, del Reglamento de Ciberresiliencia ofrece información detallada que le permite identificar el CSIRT nacional al que debe dirigir su notificación.

¿Qué eventos está obligado a notificar?

- **Vulnerabilidades activamente explotadas:** Vulnerabilidades en productos con elementos digitales de las que se tiene constancia que están siendo explotadas actualmente por un agente malintencionado, de conformidad con el artículo 3, punto 42, del Reglamento de Ciberresiliencia.
- **Incidentes graves:** Incidentes que tengan un impacto grave en la seguridad de un producto con elementos digitales (por ejemplo, que pongan en peligro la disponibilidad, la autenticidad, la integridad o la confidencialidad), de acuerdo con el artículo 3, punto 44; los criterios de severidad se definen en el artículo 14, apartado 5.

¿Cuándo tiene que notificar estos acontecimientos?

El proceso de notificación comienza en el momento en el que usted, como fabricante o responsable de software de código abierto, tiene conocimiento de la explotación activa de una vulnerabilidad o un incidente grave. Deben respetarse los siguientes plazos:

Alerta temprana



- En un plazo de **veinticuatro horas** desde que se tenga conocimiento de la vulnerabilidad o del incidente.

Notificación de vulnerabilidad activamente explotada/incidente grave



- En un plazo de **setenta y dos horas** desde que se tenga conocimiento del hecho, se facilitará información general y se realizará una evaluación inicial.

Informe final



- **Para las vulnerabilidades:** A más tardar catorce días después de que se disponga de una medida correctora (por ejemplo, un parche).
- **Para los incidentes graves:** En el plazo de un mes a partir de la presentación de la notificación de vulnerabilidad activamente explotada/incidente grave en un plazo de setenta y dos horas

■ ¿Qué ocurre una vez enviadas las notificaciones?

Una vez enviadas las notificaciones, el CSIRT que las reciba en primer lugar difundirá la información sin demora a otros CSIRT pertinentes de los Estados miembros de la UE en los que el producto también esté disponible. La notificación se pone simultáneamente a disposición de la ENISA.

Los CSIRT nacionales también compartirán cierta información con sus respectivas autoridades de vigilancia del mercado para que estas puedan cumplir sus obligaciones en materia de aplicación de la ley.

■ ¿Puede retrasarse la difusión de la información?

Sí, en circunstancias excepcionales, la difusión de la información puede retrasarse, de conformidad con el artículo 16, apartado 2, del Reglamento de Ciberresiliencia. El Reglamento Delegado (UE) 2026/881 de la Comisión especifica con mayor detalle las condiciones en las que puede retrasarse la difusión de las notificaciones.

■ ¿Cómo utilizaría la plataforma?



1 Iniciar sesión



2 Seleccionar CSIRT nacional



3 Rellenar los datos y enviar

■ Proceso de notificación sencillo

