# REGLAMENTO DELEGADO (UE) 2026/881 DE LA COMISIÓN

## de 11 de diciembre de 2025

## por el que se completa el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo mediante la especificación de las condiciones de aplicación de los motivos relacionados con la ciberseguridad en lo que respecta al aplazamiento de la difusión de notificaciones

**(Texto pertinente a efectos del EEE)**

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia) ([1]), y en particular su artículo 14, apartado 9,

Considerando lo siguiente:

(1) En circunstancias excepcionales, y en particular a petición del fabricante y a la luz del nivel de sensibilidad de la información notificada, y por motivos justificados relacionados con la ciberseguridad, el equipo de respuesta a incidentes de seguridad informática (CSIRT) designado como coordinador que reciba inicialmente la notificación de una vulnerabilidad aprovechada activamente o de un incidente grave con repercusiones en la seguridad de un producto con elementos digitales («el CSIRT que recibe inicialmente la notificación») podrá decidir aplazar, durante el período de tiempo estrictamente necesario, la difusión de la notificación a través de la plataforma única de notificación a los CSIRT designados como coordinadores en cuyo territorio el fabricante que presenta la notificación haya indicado que el producto con elementos digitales se ha puesto a disposición («los CSIRT pertinentes»). Por lo tanto, es necesario establecer las condiciones de aplicación de dichos motivos. Cuando se den tales motivos, el CSIRT que haya recibido inicialmente la notificación podrá aplazar la difusión a los CSIRT pertinentes durante el período de tiempo que sea estrictamente necesario, pero no estará obligado a hacerlo. De conformidad con el artículo 16, apartado 2, del Reglamento (UE) 2024/2847, cuando un CSIRT que haya recibido inicialmente la notificación decida invocar dichos motivos, debe informar inmediatamente a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) de su decisión de aplazar la notificación, así como de sus motivos, y de cuándo tiene intención de difundir la notificación.

(2) De conformidad con el artículo 16, apartado 2, párrafo segundo, del Reglamento (UE) 2024/2847, las condiciones de aplicación de los motivos relacionados con la ciberseguridad establecidas en el presente Reglamento no se aplicarán al acceso de la ENISA a la información notificada. El acceso de la ENISA a la información notificada solo podrá restringirse en circunstancias particularmente excepcionales: cuando el fabricante indique en su notificación que se cumple una de las tres condiciones a que se refiere el artículo 16, apartado 2, párrafo tercero, letras a), b) o c), del Reglamento (UE) 2024/2847, y solo en relación con la notificación de la vulnerabilidad en el plazo de setenta y dos horas a que se refiere el artículo 14, apartado 2, letra b), del Reglamento (UE) 2024/2847. En tales casos, la única información que debe ponerse simultáneamente a disposición de ENISA es la información de que un fabricante ha realizado una notificación; información general sobre el producto con elementos digitales; información sobre el carácter general de la vulnerabilidad; y la información de que se han invocado motivos relacionados con la seguridad.

(3) El acceso a la información notificada permite a los CSIRT tener una visión general del entorno de seguridad en su territorio y poner en marcha medidas paliativas, lo que eleva el nivel general de ciberseguridad en la Unión. Por consiguiente, solo deben ser posibles nuevas restricciones a la difusión de notificaciones a la luz de la naturaleza sensible de la información que se notifica en los casos en que los riesgos de ciberseguridad derivados de una mayor difusión superen los beneficios en materia de seguridad para la Unión, y dichos riesgos no puedan paliarse adecuadamente imponiendo restricciones a la gestión y a la difusión a terceros de la notificación a través de protocolos adecuados en uso en la red de CSIRT, como el Protocolo TLP (del inglés, «traffic light protocol» o «protocolo del semáforo») para el intercambio de información o el Protocolo de Acciones Admisibles. Este puede ser

([1]) DO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

el caso, por ejemplo, cuando un fabricante haya informado al CSIRT que recibió inicialmente la notificación de que espera ofrecer una medida paliativa (como un parche) en breve. También puede ser el caso, cuando el CSIRT que recibe inicialmente la notificación decide compartir solo partes de una notificación, y estas partes son, no obstante, suficientes para que los CSIRT pertinentes garanticen que pueden poner en marcha medidas adecuadas de reducción de riesgos. Además, y con el fin de fomentar la cooperación en materia de detección y divulgación de vulnerabilidades entre fabricantes, CSIRT e investigadores en materia de seguridad, este también puede ser el caso cuando el CSIRT actúe como intermediario de confianza para un procedimiento continuo de divulgación coordinada de vulnerabilidades, tal como se contempla en el artículo 12, apartado 1, de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([2]). En tal caso, cuando el CSIRT decida aplazar la difusión de una notificación, y de conformidad con el artículo 16, apartado 6, del Reglamento (UE) 2024/2847, dicho CSIRT deba aplazarla durante un período que no sea superior al estrictamente necesario y hasta que las partes implicadas en la divulgación coordinada de vulnerabilidades den su consentimiento a la divulgación.

(4) La información incluida en la notificación ayudará a los CSIRT a desempeñar sus tareas en el contexto de la reducción de riesgos y la gestión de incidentes. Sin embargo, en casos excepcionales, esta información podría ser suficiente para permitir la creación de una técnica para aprovechar esa vulnerabilidad sin necesidad de realizar ninguna investigación, incluso por parte de agentes con capacidades y recursos limitados. Si los agentes malintencionados accedieran a dicha información, la ciberseguridad de la Unión se vería gravemente afectada, dada la facilidad de aprovechar esa vulnerabilidad. Este podría ser el caso, por ejemplo, cuando la versión vulnerable de un programa informático difiera solo marginalmente de versiones anteriores no vulnerables. En tales casos, si el CSIRT que recibió inicialmente la notificación considera que los riesgos de ciberseguridad derivados de una mayor difusión no pueden paliarse adecuadamente imponiendo restricciones a la gestión y a la difusión a terceros, podrá decidir aplazar la difusión hasta que se disponga de una medida eficaz de reducción de riesgos, como una actualización de seguridad u orientaciones para los usuarios.

(5) Si un CSIRT pertinente no es capaz de proteger adecuadamente la información notificada, los agentes malintencionados podrían acceder a información sensible y aprovecharla en todo el mercado único. Por lo tanto, cuando existan serias dudas sobre la capacidad de un CSIRT pertinente para garantizar la confidencialidad de la información notificada, el CSIRT que reciba inicialmente la notificación podrá decidir aplazar la difusión de una notificación únicamente a dicho CSIRT pertinente hasta que se hayan abordado dichas dudas. Este puede ser el caso en situaciones en las que un CSIRT pertinente haya sufrido un incidente de ciberseguridad que afecte a su capacidad para operar de forma segura, o cuando existan pruebas o información de que se han detectado deficiencias significativas en las capacidades del CSIRT, como limitaciones graves de recursos que comprometan su capacidad para desempeñar sus funciones, o dependencia de programas informáticos obsoletos o vulnerables.

(6) Con el fin de evitar que los agentes malintencionados accedan a información sensible, cuando la plataforma única de notificación establecida en virtud del artículo 16 del Reglamento (UE) 2024/2847 se haya visto comprometida por un incidente de ciberseguridad, el CSIRT que reciba inicialmente la notificación debe aplazar la difusión a través de la plataforma única de notificación hasta que se haya restablecido la capacidad de la plataforma para garantizar la confidencialidad de la información notificada.

(7) De conformidad con el artículo 16, apartado 2, párrafo primero, del Reglamento (UE) 2024/2847, el CSIRT que reciba inicialmente la notificación no tendrá que difundir una notificación a ningún otro CSIRT pertinente si el fabricante indica que el producto con elementos digitales solo se comercializa en el mercado del Estado miembro del CSIRT que recibió inicialmente la notificación.

(8) La Comisión ha consultado y recabado la opinión de las partes interesadas pertinentes en la preparación del proyecto de acto delegado, y ha consultado al Grupo de Expertos sobre Ciberseguridad de los Productos con Elementos Digitales.

(9) De conformidad con el artículo 14, apartado 9, del Reglamento (UE) 2024/2847, la Comisión ha cooperado estrechamente con la red de CSIRT establecida en virtud del artículo 15 de la Directiva (UE) 2022/2555 y con la ENISA en la preparación del proyecto de acto delegado.

([2]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

HA ADOPTADO EL PRESENTE REGLAMENTO:

*Artículo 1*

**Objeto**

El presente Reglamento especifica las condiciones de aplicación de los motivos relacionados con la ciberseguridad a que se refiere el artículo 16, apartado 2, del Reglamento (UE) 2024/2847 que permiten al CSIRT designado como coordinador que recibe inicialmente una notificación de conformidad con el artículo 14, apartados 1 y 3, y el artículo 15, apartados 1 y 2, de dicho Reglamento aplazar la difusión de la notificación a los CSIRT designados como coordinadores en cuyo territorio el fabricante haya indicado que se ha comercializado el producto con elementos digitales.

*Artículo 2*

**Definiciones**

A los efectos del presente Reglamento, se entenderá por:

1) «CSIRT que recibe inicialmente la notificación»: el CSIRT designado como coordinador que recibe inicialmente la notificación de conformidad con el artículo 14, apartados 1 y 3, y el artículo 15, apartados 1 y 2, del Reglamento (UE) 2024/2847;

2) «CSIRT pertinente»: el CSIRT designado como coordinador en cuyo territorio el fabricante haya indicado que se ha comercializado el producto con elementos digitales.

*Artículo 3*

**Condiciones de aplicación de los motivos relacionados con la ciberseguridad derivados de la naturaleza de la información notificada**

El CSIRT que reciba inicialmente la notificación podrá decidir aplazar, durante un período de tiempo limitado al estrictamente necesario, la difusión de notificaciones o partes de ellas a los CSIRT pertinentes en los casos en que, a la luz de la sensibilidad de la información notificada, los riesgos de ciberseguridad planteados por la difusión superen sus beneficios en materia de seguridad y dichos riesgos no puedan paliarse imponiendo restricciones a la gestión y a la difusión a terceros de la notificación a través de protocolos adecuados, como el Protocolo TLP (del inglés, «traffic light protocol» o «protocolo del semáforo») para el intercambio de información o el Protocolo de Acciones Admisibles, y cuando se cumpla al menos una de las condiciones siguientes:

a) que el fabricante haya informado al CSIRT que recibió inicialmente la notificación de que se espera que se ponga a disposición en un plazo de setenta y dos horas una medida eficaz de reducción de riesgos, como una actualización de seguridad u orientaciones para los usuarios; si no se pone a disposición una medida eficaz de reducción de riesgos dentro de este plazo, el CSIRT que haya recibido inicialmente la notificación difundirá la notificación a los CSIRT pertinentes;

b) que la información incluida en la notificación se considere suficiente, a la luz de la naturaleza de la vulnerabilidad aprovechada activamente notificada, para crear una técnica para aprovechar esa vulnerabilidad, en particular cuando la vulnerabilidad pueda ser fácilmente detectada y aprovechada por agentes con capacidades y recursos limitados; una vez que se disponga de una medida eficaz de reducción de riesgos, como una actualización de seguridad u orientaciones para los usuarios, el CSIRT que haya recibido inicialmente la notificación difundirá la notificación a los CSIRT pertinentes;

c) que el CSIRT que haya recibido inicialmente la notificación pueda compartir con los CSIRT pertinentes información suficiente para garantizar que los CSIRT pertinentes puedan poner en marcha medidas adecuadas de reducción del riesgo; una vez que se disponga de una medida eficaz de reducción de riesgos, como una actualización de seguridad u orientaciones para los usuarios, el CSIRT que haya recibido inicialmente la notificación difundirá la notificación completa a los CSIRT pertinentes;

d) que el CSIRT que haya recibido inicialmente la notificación de la vulnerabilidad aprovechada activamente haya sido informado de ello como parte de una divulgación coordinada de vulnerabilidades para la que dicho CSIRT actúa como intermediario de confianza de conformidad con el artículo 12, apartado 1, de la Directiva (UE) 2022/2555; en tal caso, y de conformidad con el artículo 16, apartado 6, del Reglamento (UE) 2024/2847, el CSIRT que haya recibido inicialmente la notificación la difundirá a los CSIRT pertinentes cuando un aplazamiento ya no sea estrictamente necesario y las partes implicadas en la divulgación coordinada de vulnerabilidades den su consentimiento para la divulgación.

*Artículo 4*

**Condiciones de aplicación de los motivos relacionados con la ciberseguridad en relación con un CSIRT específico**

El CSIRT que reciba inicialmente la notificación podrá decidir aplazar durante el período de tiempo estrictamente necesario la difusión de notificaciones o partes de las mismas a un CSIRT pertinente específico en los casos en que:

a) el CSIRT pertinente se haya visto afectado por un incidente de ciberseguridad que ponga en duda su capacidad para garantizar la confidencialidad de la información notificada;

b) tenga motivos suficientes para creer que las capacidades del CSIRT pertinente son inadecuadas para garantizar la confidencialidad de la información notificada.

En los casos a que se refiere la letra a) del primer párrafo, el CSIRT que haya recibido inicialmente la notificación podrá aplazar la difusión hasta que el CSIRT pertinente haya informado a la red de CSIRT a que se refiere el artículo 15 de la Directiva 2022/2555 de que se ha restablecido su capacidad para garantizar la confidencialidad de las notificaciones.

En los casos a que se refiere la letra b) del primer párrafo, el CSIRT que haya recibido inicialmente la notificación podrá aplazar la difusión al CSIRT pertinente hasta que dicho CSIRT haya aportado pruebas de que ha subsanado las deficiencias detectadas.

*Artículo 5*

**Condiciones de aplicación de los motivos relacionados con la ciberseguridad en relación con la plataforma única de notificación**

El CSIRT que reciba inicialmente la notificación podrá decidir aplazar la difusión de notificaciones a través de la plataforma única de notificación establecida por el artículo 16 del Reglamento (UE) 2024/2847 cuando la ENISA haya informado a la red de CSIRT, de conformidad con el artículo 16, apartado 4, de dicho Reglamento, de que la plataforma única de notificación se ha visto afectada por un incidente de ciberseguridad que pone en duda su capacidad para garantizar la confidencialidad de la información notificada. En tales casos, el CSIRT que reciba inicialmente la notificación podrá aplazar la difusión a través de la plataforma única de notificación hasta que la ENISA haya informado a la red de CSIRT de que se ha restablecido la capacidad de la plataforma para garantizar la confidencialidad de las notificaciones.

*Artículo 6*

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 11 de diciembre de 2025.

*Por la Comisión*
*La Presidenta*
Ursula VON DER LEYEN