2024/3143

19.12.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/3143 DE LA COMISIÓN

de 18 de diciembre de 2024

por el que se establecen las circunstancias, los formatos y los procedimientos de notificación con arreglo al artículo 61, apartado 5, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») ([1]), y en particular su artículo 61, apartado 5,

Considerando lo siguiente:

(1) De conformidad con el artículo 61, apartado 1, del Reglamento (UE) 2019/881 (Reglamento sobre la seguridad), las autoridades nacionales de certificación de la ciberseguridad deben notificar a la Comisión los organismos de evaluación de la conformidad que hayan sido acreditados y, en su caso, autorizados para expedir certificados europeos de ciberseguridad de los niveles de garantía especificados, y deben mantener dicha notificación actualizada. Además, de acuerdo con el artículo 61, apartado 2, del Reglamento (UE) 2019/881, la Comisión debe publicar en el *Diario Oficial de la Unión Europea* una lista de los organismos de evaluación de la conformidad notificados en virtud de un esquema europeo de certificación de la ciberseguridad un año después de la entrada en vigor de este último. A fin de ofrecer un enfoque armonizado con relación a las notificaciones y de facilitar el proceso de notificación a las autoridades nacionales de certificación de la ciberseguridad, el presente Reglamento debe pormenorizar las circunstancias, los formatos y los procedimientos de dichas notificaciones. Es importante aclarar estos aspectos con vistas a la puesta en marcha del primer esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (en lo sucesivo, «EUCC») establecido por el Reglamento de Ejecución (UE) 2024/482 de la Comisión ([2]).

(2) El presente Reglamento reconoce las sinergias entre el Reglamento (UE) 2019/881 y la legislación de armonización pertinente, incluido el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo (Reglamento de Ciberresiliencia) ([3]). Por consiguiente, se propone que las autoridades nacionales de certificación de la ciberseguridad realicen las notificaciones a la Comisión a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión, contemplado en la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo ([4]). Sin perjuicio de la obligación de la Comisión de publicar en el *Diario Oficial de la Unión Europea* la lista de los organismos de evaluación de la conformidad notificados, dicha lista también debe publicarse en el sistema de notificación electrónica desarrollado y gestionado por la Comisión.

([1]) DO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

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

([4]) Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82, ELI: http://data.europa.eu/eli/dec/2008/768(1)/oj).

(3) La notificación de los organismos de evaluación de la conformidad acreditados y, en su caso, autorizados implica que puede confiarse a dichos organismos la realización de las actividades de evaluación y certificación de conformidad con el Reglamento (UE) 2019/881, contribuyendo así a la reputación global de los esquemas europeos de certificación de la ciberseguridad. Por consiguiente, resulta esencial garantizar que los organismos de evaluación de la conformidad que hayan sido notificados cumplan los requisitos y obligaciones conforme avanza el tiempo. La lista de organismos de evaluación de la conformidad publicada debe ser precisa y estar actualizada, reflejando así la conformidad con los requisitos establecidos en el Reglamento (UE) 2019/881 y, cuando proceda, otros requisitos específicos o adicionales en virtud de un esquema europeo de certificación de la ciberseguridad. A tal efecto, es necesario que las autoridades nacionales de certificación de la ciberseguridad informen a la Comisión, sin demora indebida, de cualquier cambio en la notificación, de conformidad con el artículo 61, apartado 1, del Reglamento (UE) 2019/881.

(4) Las autoridades nacionales de certificación de la ciberseguridad deben velar por que los organismos de evaluación de la conformidad respeten el Reglamento (UE) 2019/881 y los esquemas europeos de certificación de la ciberseguridad y por que, en este contexto, las notificaciones sean precisas. Estas actividades están sujetas a una revisión *inter pares*, cuyo resultado debe ayudar a determinar los cambios necesarios para mejorar su eficacia. Las autoridades nacionales de certificación de la ciberseguridad podrán verificar si un organismo de evaluación de la conformidad ha dejado de cumplir los requisitos pertinentes cuando, en distintas circunstancias, se les haya informado de algún problema. Cuando proceda, las conclusiones de los mecanismos de evaluación *inter pares* deben ayudar a las autoridades nacionales de certificación de la ciberseguridad a supervisar la competencia continua de los organismos de evaluación de la conformidad notificados. Además, otras autoridades nacionales de certificación de la ciberseguridad, la Comisión y demás partes interesadas pueden manifestar su preocupación junto con la autoridad nacional de certificación de la ciberseguridad notificante en lo que respecta a la competencia continua de un organismo de evaluación de la conformidad notificado.

(5) Cuando decida suspender, restringir o retirar la notificación de un organismo de evaluación de la conformidad, la autoridad nacional de certificación de la ciberseguridad deberá cooperar con el organismo nacional de acreditación designado con arreglo al Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([5]). Así se desprende del Reglamento (UE) 2019/881, según el cual las autoridades nacionales de certificación de la ciberseguridad deben asistir y apoyar activamente a los organismos nacionales de acreditación, así como cooperar con ellos, en el control y la supervisión de las actividades. La restricción de la notificación debe referirse a aquellos casos en que el alcance de la acreditación o, cuando proceda, el alcance de la autorización, y por consiguiente el alcance de la notificación, sea reducido.

(6) De conformidad con el artículo 54, apartado 1, letra n), del Reglamento (UE) 2019/881, cada esquema europeo de certificación de la ciberseguridad deberá incluir, en su caso, normas relativas a la conservación de los registros por parte de los organismos de evaluación de la conformidad. Por consiguiente, resulta necesario que, en caso de restricción, suspensión o retirada de la notificación, o cuando el organismo de evaluación de la conformidad notificado haya cesado su actividad, la autoridad nacional de certificación de la ciberseguridad encargada de la notificación vele por que los registros de dicho organismo se almacenen de manera segura y se conserven durante el período necesario, de acuerdo con lo establecido en el esquema europeo de certificación.

(7) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité creado en virtud del artículo 66 del Reglamento (UE) 2019/881.

([5]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto

El presente Reglamento establece las circunstancias, los formatos y los procedimientos de las notificaciones de los organismos de evaluación de la conformidad por parte de las autoridades nacionales de certificación de la ciberseguridad, de conformidad con el artículo 61, apartado 1, del Reglamento (UE) 2019/881.

Artículo 2

Procedimiento de notificación

1. De conformidad con el artículo 61, apartado 1, del Reglamento (UE) 2019/881, las autoridades nacionales de certificación de la ciberseguridad notificarán a la Comisión aquellos organismos de evaluación de la conformidad que hayan cumplido los requisitos establecidos en el Reglamento (UE) 2019/881 y, cuando proceda, otros requisitos específicos o adicionales en virtud de un esquema europeo de certificación de la ciberseguridad.

2. Las autoridades nacionales de certificación de la ciberseguridad enviarán las notificaciones a la Comisión a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión, contemplado en la Decisión n.º 768/2008/CE.

3. La notificación incluirá la información estipulada en el anexo.

Artículo 3

Números de identificación y lista de organismos de evaluación de la conformidad

1. La Comisión asignará un número de identificación a cada organismo de evaluación de la conformidad notificado. Asignará un solo número de identificación incluso cuando el organismo se notifique en virtud de varios esquemas europeos de certificación de la ciberseguridad o actos de la Unión.

2. Cuando publique la lista de organismos de evaluación de la conformidad notificados en el sistema de notificación electrónica desarrollado y gestionado por la Comisión, la Comisión incluirá los números de identificación que se hayan asignado a los organismos de evaluación de la conformidad notificados y las actividades con relación a las cuales hayan sido notificados.

3. La ENISA publicará la información relativa a los organismos de evaluación de la conformidad notificados en el sitio web de los esquemas europeos de certificación de la ciberseguridad contemplado en el artículo 50, apartado 1, del Reglamento (UE) 2019/881.

Artículo 4

Cambios en las notificaciones

1. Las autoridades nacionales de certificación de la ciberseguridad notificarán a la Comisión, sin demora indebida, todo cambio posterior en la notificación a que se refiere el artículo 2 a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión, de conformidad con el artículo 61, apartado 1, del Reglamento (UE) 2019/881.

2. Cuando una autoridad nacional de certificación de la ciberseguridad haya confirmado, en colaboración con el organismo de acreditación nacional, tal como prevé el Reglamento (UE) 2019/881, que un organismo de evaluación de la conformidad notificado ya no cumple los requisitos u obligaciones que le corresponden, la autoridad nacional de certificación de la ciberseguridad restringirá, suspenderá o retirará la notificación según proceda, dependiendo de la gravedad del incumplimiento de dichos requisitos u obligaciones. Dicha autoridad informará a la Comisión en consecuencia y sin demora indebida mediante el sistema de notificación electrónica desarrollado y gestionado por la Comisión.

3. En caso de restricción, suspensión o retirada de la notificación, o cuando el organismo de evaluación de la conformidad notificado haya cesado su actividad, la autoridad nacional de certificación de la ciberseguridad notificante tomará las medidas oportunas para que los registros de dicho organismo de evaluación de la conformidad se almacenen de manera segura y se conserven durante el período necesario, de acuerdo con lo establecido en el esquema europeo de certificación.

Artículo 5

Entrada en vigor

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 18 de diciembre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Información que debe incluirse en la notificación de un organismo de evaluación de la conformidad en virtud de un esquema europeo de certificación de la ciberseguridad con arreglo al artículo 61, apartado 1, del Reglamento (UE) 2019/881, tal como se contempla en el artículo 2, apartado 3, del presente Reglamento

1. Información general:
   1) Nombre del esquema de certificación de la ciberseguridad
   2) Nivel(es) de seguridad, cuando proceda, y procedimientos de evaluación de la conformidad asociados (por ejemplo, básico, importante, elevado)
   3) Ámbito (por ejemplo, ámbito de acreditación, categorías o tipos de productos, servicios, procesos)

2. Información sobre la autoridad nacional de certificación de la ciberseguridad notificante:
   1) Nombre
   2) País
   3) Dirección postal
   4) Dirección de correo electrónico
   5) Número de teléfono
   6) Sitio web

3. Información sobre el organismo de evaluación de la conformidad notificado:
   1) Nombre
   2) País
   3) Dirección postal
   4) Dirección de correo electrónico
   5) Número de teléfono
   6) Sitio web

4. Información sobre la acreditación:
   1) Acreditación:
      a) Fecha de la acreditación
      b) Número de referencia de la acreditación
      c) Alcance de la acreditación
      d) Duración de la validez de la acreditación
   2) Organismo nacional de acreditación:
      a) Nombre
      b) País
      c) Dirección postal
      d) Dirección de correo electrónico
      e) Número de teléfono
      f) Sitio web

5. Información sobre la autorización (según proceda):
   1) Autorización:
      a) Fecha de la autorización
      b) Número de referencia de la autorización
      c) Alcance de la autorización

d) Duración de la validez de la autorización

2) Autoridad nacional de autorización en materia de ciberseguridad (cuando sea diferente de la autoridad nacional de certificación de la ciberseguridad notificante):

a) Nombre

b) País

c) Dirección postal

d) Dirección de correo electrónico

e) Número de teléfono

f) Sitio web

6. Información complementaria:

1) Toda información complementaria requerida en un esquema europeo de certificación de la ciberseguridad específico

2) Todos los documentos justificativos