2025/301

20.2.2025

REGLAMENTO DELEGADO (UE) 2025/301 DE LA COMISIÓN

de 23 de octubre de 2024

por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación que especifican el contenido y los plazos para la notificación inicial y los informes intermedio y final sobre incidentes graves relacionados con las TIC, así como el contenido de la notificación voluntaria de ciberamenazas importantes

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 ([1]), y en particular su artículo 20, párrafo tercero,

Considerando lo siguiente:

(1) A fin de garantizar la armonización y la simplificación de los requisitos de notificación de incidentes graves relacionados con las TIC a que se refiere el artículo 19, apartado 4, del Reglamento (UE) 2022/2554, los plazos para notificar dichos incidentes deben seguir un enfoque coherente para todos los tipos de entidades financieras. Por estas razones, los plazos también deben seguir, en la mayor medida posible, un enfoque coherente con los requisitos establecidos en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([2]) y, como mínimo, ser equivalentes a ellos.

(2) Para evitar imponer una carga de notificación indebida a las entidades financieras en el momento en que estén gestionando el incidente relacionado con las TIC, el contenido de la notificación inicial debe limitarse a la información más significativa. Para poder adoptar las medidas de supervisión adecuadas, las autoridades competentes deben recibir información sobre los incidentes graves relacionados con las TIC lo antes posible, una vez que la entidad financiera haya clasificado un incidente relacionado con las TIC como grave. Por consiguiente, el plazo para presentar la notificación inicial a que se refiere el artículo 19, apartado 4, letra a), del Reglamento (UE) 2022/2554 debe ser lo más breve posible después de que un incidente relacionado con las TIC haya sido clasificado como grave, permitiendo al mismo tiempo cierta flexibilidad, especialmente en el caso de los modelos de negocio de servicios en los que, en particular, el tiempo no sea un factor primordial, siempre que las entidades financieras necesiten más tiempo para gestionar el incidente relacionado con las TIC tras haber tenido conocimiento de este.

(3) Tras recibir la notificación inicial, las autoridades competentes deben recibir información más detallada sobre el incidente relacionado con las TIC en el informe intermedio y toda la información pertinente en el informe final. La información contenida en dichos informes debe permitir a las autoridades competentes evaluar en mayor medida el incidente relacionado con las TIC, así como estudiar las medidas de supervisión que deseen adoptar.

(4) Los plazos de notificación a que se refiere el artículo 20, párrafo primero, letra a), inciso ii), del Reglamento (UE) 2022/2554 deben, por tanto, equilibrar la necesidad de que las autoridades competentes reciban la información rápidamente y la necesidad de proporcionar a las entidades financieras tiempo suficiente para obtener información completa y exacta.

(5) Teniendo en cuenta los criterios establecidos en el artículo 20, párrafo primero, letra a), del Reglamento (UE) 2022/2554, los plazos de notificación no deben suponer una carga desproporcionada para las microempresas y otras entidades financieras que no sean significativas. Además, para evitar una carga desproporcionada para las entidades financieras, los plazos de notificación deben tener en cuenta los fines de semana y los días festivos.

([1]) DO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([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).

(6) Dado que las ciberamenazas importantes deben notificarse de forma voluntaria, el contenido de dichas notificaciones no debe suponer una carga para las entidades financieras y debe ser más limitado que la información solicitada con respecto a incidentes graves relacionados con las TIC.

(7) El presente Reglamento se basa en los proyectos de normas técnicas de regulación presentados por las Autoridades Europeas de Supervisión a la Comisión.

(8) La Autoridades Europeas de Supervisión han llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de regulación en que se basa el presente Reglamento, han analizado los costes y beneficios potenciales conexos y han recabado el asesoramiento de los Grupo de Partes Interesadas, establecidos de conformidad con el artículo 37 de los Reglamentos (UE) n.º 1093/2010 ([3]), (UE) n.º 1094/2010 ([4]) y (UE) n.º 1095/2010 ([5]) del Parlamento Europeo y del Consejo.

(9) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]), emitió su dictamen positivo el 22 de julio de 2024. Todo tratamiento de datos personales en el ámbito de aplicación del presente Reglamento debe llevarse a cabo de conformidad con los principios y disposiciones aplicables en materia de protección de datos del Reglamento (UE) 2018/1725.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Información general que debe facilitarse en las notificaciones iniciales y en los informes intermedio y final sobre incidentes graves relacionados con las TIC

Las entidades financieras incluirán en la notificación inicial, el informe intermedio y el informe final a que se refiere el artículo 19, apartado 4, del Reglamento (UE) 2022/2554 la siguiente información general:

a) el tipo de presentación (notificación inicial, informe intermedio o informe final);

b) el nombre de la entidad financiera, su código LEI y el tipo de entidad financiera a que se refiere el artículo 2, apartado 1, del Reglamento (UE) 2022/2554;

c) el nombre y el código de identificación de la entidad que presenta la notificación inicial, o el informe intermedio o final, en nombre de la entidad financiera;

d) cuando proceda, los nombres y códigos LEI de todas las entidades financieras cubiertas por la notificación inicial agregada o el informe intermedio o final agregado;

e) los datos de contacto de las personas responsables de comunicarse con la autoridad competente sobre el incidente grave relacionado con las TIC;

f) cuando proceda, la identificación de la empresa matriz del grupo al que pertenece la entidad financiera;

g) cuando se produzcan repercusiones monetarias, la moneda en la que se basan los importes.

([3]) Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión (DO L 331 de 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión (DO L 331 de 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artículo 2

Información específica que debe facilitarse en las notificaciones iniciales

Las notificaciones iniciales a que se refiere el artículo 19, apartado 4, letra a), del Reglamento (UE) 2022/2554 contendrán al menos toda la información específica siguiente:

a) el código de referencia del incidente asignado por la entidad financiera;

b) la fecha y la hora de detección del incidente y su clasificación con arreglo al artículo 8 del Reglamento Delegado de la Comisión (UE) 2024/1772 ([7]);

c) una descripción del incidente relacionado con las TIC;

d) los criterios, establecidos en los artículos 1 a 8 del Reglamento Delegado (UE) 2024/1772, sobre cuya base la entidad financiera clasificó el incidente relacionado con las TIC como grave;

e) los Estados miembros afectados por el incidente relacionado con las TIC;

f) información sobre cómo se descubrió el incidente relacionado con las TIC;

g) cuando se disponga de ella, información sobre el origen del incidente relacionado con las TIC;

h) información sobre si la entidad financiera ha activado un plan de continuidad de la actividad;

i) cuando proceda, información sobre la reclasificación del incidente relacionado con las TIC de grave a no grave;

j) cuando se disponga de ella, cualquier otra información pertinente.

Artículo 3

Información específica que debe facilitarse en los informes intermedios

Los informes intermedios a que se refiere el artículo 19, apartado 4, letra b), del Reglamento (UE) 2022/2554 contendrán al menos toda la información específica siguiente:

a) cuando proceda, el código de referencia del incidente facilitado por la autoridad competente;

b) la fecha y la hora en que se produjo el incidente relacionado con las TIC;

c) cuando proceda, la fecha y la hora en que la entidad financiera haya recuperado sus actividades regulares;

d) información sobre cómo se han cumplido los criterios establecidos en los artículos 1 a 8 del Reglamento Delegado (UE) 2024/1772, sobre cuya base la entidad financiera clasificó el incidente relacionado con las TIC como grave;

e) el tipo de incidente relacionado con las TIC;

f) cuando proceda, las amenazas y las técnicas utilizadas por el agente de riesgo;

g) las áreas funcionales y los procesos empresariales afectados;

h) los componentes de la infraestructura afectados que apoyan los procesos empresariales;

i) las repercusiones en los intereses financieros de los clientes;

j) información sobre la notificación del incidente relacionado con las TIC a otras autoridades;

k) las acciones o medidas temporales emprendidas o previstas por parte de la entidad financiera para recuperarse del incidente relacionado con las TIC;

l) cuando proceda, información sobre los indicadores de compromiso.

([7]) Reglamento Delegado (UE) 2024/1772 de la Comisión, de 13 de marzo de 2024, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo mediante normas técnicas de regulación que especifican los criterios para la clasificación de los incidentes relacionados con las TIC y las ciberamenazas, establecen umbrales de importancia relativa y especifican la información detallada de las notificaciones de incidentes graves (DO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artículo 4

Información específica que debe facilitarse en los informes finales

Los informes finales a que se refiere el artículo 19, apartado 4, letra c), del Reglamento (UE) 2022/2554 contendrán toda la información específica siguiente:

a) información sobre las causas subyacentes del incidente relacionado con las TIC;

b) las fechas y las horas en que se resolvió el incidente relacionado con las TIC y se abordaron las causas subyacentes;

c) información sobre la resolución del incidente relacionado con las TIC;

d) cuando proceda, información pertinente para las autoridades de resolución;

e) información sobre los costes y pérdidas directos e indirectos derivados del incidente relacionado con las TIC e información sobre las recuperaciones financieras;

f) cuando proceda, información sobre incidentes recurrentes relacionados con las TIC.

Artículo 5

Plazos para la notificación inicial y para los informes intermedio y final

1. Las entidades financieras presentarán la notificación inicial y los informes intermedio y final a que se refiere el artículo 19, apartado 4, letras a), b) y c), del Reglamento (UE) 2022/2554 dentro de los plazos siguientes:

a) en el caso del informe inicial: lo antes posible, pero en cualquier caso, en un plazo de cuatro horas a partir de la clasificación del incidente relacionado con las TIC como grave y a más tardar veinticuatro horas después del momento en que la entidad financiera haya tenido conocimiento de dicho incidente;

b) en el caso del informe intermedio: a más tardar en un plazo de setenta y dos horas a partir de la presentación de la notificación inicial, incluso cuando la situación o la gestión del incidente no hayan cambiado con arreglo al artículo 19, apartado 4, letra b), del Reglamento (UE) 2022/2554; las entidades financieras presentarán un informe intermedio actualizado sin demora indebida y, en cualquier caso, cuando se hayan recuperado las actividades regulares;

c) en el caso del informe final: a más tardar un mes después de la presentación del informe intermedio o, cuando proceda, del último informe intermedio actualizado.

2. Cuando la entidad financiera no haya clasificado un incidente relacionado con las TIC como grave en un plazo de veinticuatro horas a partir del momento en que haya tenido conocimiento de este, pero lo clasifique como grave en una fase posterior, la entidad financiera presentará la notificación inicial en un plazo de cuatro horas a partir de la clasificación del incidente relacionado con las TIC como incidente grave.

3. Las entidades financieras que no puedan presentar la notificación inicial, el informe intermedio o el informe final en los plazos establecidos en el apartado 1 informarán de ello a la autoridad competente sin demora indebida, pero a más tardar en los plazos respectivos para la presentación de la notificación o el informe, y explicarán los motivos del retraso.

4. Cuando el plazo para la presentación de una notificación inicial, un informe intermedio o un informe final coincida con un fin de semana o un día festivo en el Estado miembro de la entidad financiera notificante, esta podrá presentarlos antes del mediodía del siguiente día hábil.

5. El apartado 4 no se aplicará a la presentación de una notificación inicial o un informe intermedio por parte de entidades de crédito, entidades de contrapartida central, gestores de centros de negociación y otras entidades financieras identificadas como esenciales o importantes de conformidad con el artículo 3 de la Directiva (UE) 2022/2555.

6. Las autoridades competentes podrán decidir que el apartado 4 no se aplique a la presentación de una notificación inicial o de un informe intermedio por parte de entidades financieras distintas de las contempladas en el apartado 5 que sean significativas o tengan un carácter sistémico para el sector financiero a escala nacional o de la Unión. Las autoridades competentes notificarán su decisión a las entidades financieras identificadas. La decisión de la autoridad competente solo se aplicará a los incidentes notificados después de la fecha de notificación de la decisión por la autoridad competente a las entidades financieras identificadas.

Artículo 6

Contenido de la notificación voluntaria de ciberamenazas importantes

El contenido de la notificación voluntaria en relación con las ciberamenazas importantes a que se refiere el artículo 19, apartado 2, del Reglamento (UE) 2022/2554 abarcará todo lo siguiente:

a) información general sobre la entidad financiera notificante, tal como se establece en el artículo 1;

b) la fecha y la hora de detección de la ciberamenaza importante y cualquier otro sello de tiempo pertinente relacionado con esta;

c) una descripción de la ciberamenaza importante;

d) información sobre la posible repercusión de la ciberamenaza importante en la entidad financiera, sus clientes o sus contrapartes financieras;

e) los criterios de clasificación que habrían dado lugar a un informe de incidente grave establecidos en los artículos 1 a 8 del Reglamento Delegado (UE) 2024/1772 si se hubiera materializado la ciberamenaza;

f) información sobre la situación de la ciberamenaza importante y cualquier cambio en la actividad de la amenaza;

g) cuando proceda, una descripción de las medidas adoptadas por la entidad financiera para evitar la materialización de las ciberamenazas importantes;

h) información sobre cualquier notificación de la ciberamenaza importante a otras entidades o autoridades financieras;

i) cuando proceda, información sobre los indicadores de compromiso;

j) cuando se disponga de ella, cualquier otra información pertinente.

Artículo 7

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 23 de octubre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN