2024/1772

25.6.2024

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

(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 18, apartado 4, párrafo tercero,

Considerando lo siguiente:

(1) El Reglamento (UE) 2022/2554 tiene por objeto armonizar y racionalizar los requisitos de notificación para los incidentes relacionados con las TIC y los incidentes operativos o de seguridad relacionados con los pagos que afecten a entidades de crédito, entidades de pago, proveedores de servicios de información sobre cuentas y entidades de dinero electrónico (en lo sucesivo, «incidentes»). Teniendo en cuenta que las exigencias de notificación son aplicables a veinte tipos diferentes de entidades financieras, los criterios de clasificación y los umbrales de importancia relativa para determinar los incidentes graves y las ciberamenazas importantes deben especificarse de manera sencilla, armonizada y coherente y que tenga en cuenta las especificidades de los servicios y actividades de todas las entidades financieras pertinentes.

(2) A fin de garantizar la proporcionalidad, los criterios de clasificación y los umbrales de importancia relativa deben corresponderse con el tamaño y el perfil de riesgo general, así como con la naturaleza, escala y complejidad de los servicios de todas las entidades financieras. Además, los criterios y los umbrales de importancia relativa deben diseñarse de manera que se apliquen de manera coherente a todas las entidades financieras, independientemente de su tamaño y perfil de riesgo, y no supongan una carga de notificación desproporcionada para las entidades financieras más pequeñas. No obstante, para hacer frente a situaciones en las que un número significativo de clientes se vea afectado por un incidente que, como tal, no supere el umbral aplicable, debe establecerse un umbral absoluto dirigido principalmente a las entidades financieras de mayor tamaño.

(3) Debe garantizarse a las entidades financieras una continuidad en relación con los marcos de notificación de incidentes que existían antes de la entrada en vigor del Reglamento (UE) 2022/2554. Por consiguiente, los criterios de clasificación y los umbrales de importancia relativa deben apoyarse e inspirarse en las Directrices de la ABE en materia de notificación de incidentes graves con arreglo a la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo ([2]), las Directrices sobre la información y notificación periódica de cambios significativos que deben presentar a la AEVM los registros de operaciones, así como en el marco de notificación de ciberincidentes del BCE/MUS y en otras orientaciones pertinentes. Los criterios de clasificación y los umbrales también deben ser adecuados para las entidades financieras no sujetas a requisitos de notificación de incidentes antes de la entrada en vigor del Reglamento (UE) 2022/2554.

(4) Por lo que se refiere al criterio de clasificación «cantidad y número de transacciones afectadas», el concepto de transacciones es amplio y abarca diferentes actividades y servicios en todos los actos sectoriales aplicables a las entidades financieras. A efectos de dicho criterio de clasificación, deben estar cubiertas las operaciones de pago y todas las formas de intercambio de instrumentos financieros, criptoactivos, materias primas o cualquier otro activo, también en forma de margen, garantía o prenda, tanto contra efectivo como contra cualquier otro activo. Todas las transacciones que impliquen activos cuyo valor pueda expresarse en importes monetarios deben tenerse en cuenta a efectos de clasificación.

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

([2]) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Los criterios de clasificación deben garantizar que se reflejen todos los tipos pertinentes de incidentes graves. Es posible que muchos criterios de clasificación no reflejen necesariamente los ciberataques relacionados con la intrusión en redes o sistemas de información. Sin embargo, estos son importantes porque las intrusiones en las redes y los sistemas de información pueden perjudicar a la entidad financiera. En consecuencia, los criterios de clasificación «servicios esenciales afectados» y «pérdidas de datos» deben especificarse de manera que se reflejen estos tipos de incidentes graves, en particular las intrusiones no autorizadas que, aunque no se conozcan inmediatamente sus repercusiones, pueden dar lugar a graves consecuencias, en particular violaciones de la seguridad de los datos y fugas de datos.

(6) Dado que las entidades de crédito están sujetas tanto al marco de clasificación de incidentes de conformidad con el artículo 18 del Reglamento (UE) 2022/2554 como al marco del riesgo operativo de conformidad con el Reglamento Delegado (UE) 2018/959 de la Comisión ([3]), el enfoque adoptado para evaluar las consecuencias económicas de un incidente basado en el cálculo de costes y pérdidas debe ser, en la mayor medida posible, coherente con ambos marcos con el fin de evitar que se introduzcan requisitos incompatibles o contradictorios.

(7) El criterio relativo a la extensión geográfica de un incidente establecido en el artículo 18, apartado 1, letra c), del Reglamento (UE) 2022/2554 debe centrarse en sus efectos transfronterizos, ya que los efectos de un incidente en las actividades de una entidad financiera dentro de un único país o territorio se reflejará en los demás criterios establecidos en dicho artículo.

(8) Dado que los criterios de clasificación son interdependientes y están vinculados entre sí, el enfoque para detectar los incidentes graves que deben notificarse de conformidad con el artículo 19, apartado 1, del Reglamento (UE) 2022/2554 debe basarse en una combinación de criterios que otorgaría más importancia en la clasificación de incidentes graves a algunos criterios estrechamente relacionados con las definiciones de «incidente relacionado con las TIC» y de «incidente grave relacionado con las TIC» establecidas en el artículo 3, puntos 8 y 10, del Reglamento (UE) 2022/2554.

(9) Con el fin de garantizar que las notificaciones y los informes relacionados con incidentes graves recibidos por las autoridades competentes con arreglo al artículo 19, apartado 1, del Reglamento (UE) 2022/2554 sean útiles tanto a efectos de supervisión como para la prevención de contagios en el conjunto del sector financiero, los umbrales de importancia relativa deben permitir reflejar los incidentes graves, centrándose, entre otras cosas, en los efectos en los servicios esenciales específicos de la entidad, los umbrales absolutos y relativos específicos de clientes o contrapartes financieras, las transacciones que indiquen consecuencias importantes para la entidad financiera y la importancia de los efectos en otros Estados miembros.

(10) Los incidentes que afecten a servicios de TIC o a redes y sistemas de información que sustenten funciones esenciales o importantes, o a servicios financieros que requieran autorización o al acceso malintencionado no autorizado a redes y sistemas de información que sustenten funciones esenciales o importantes, deben considerarse incidentes que afectan a los servicios esenciales de las entidades financieras. El acceso malintencionado no autorizado a las redes y sistemas de información que sustentan funciones esenciales o importantes de las entidades financieras plantea graves riesgos para la entidad financiera y, dado que pueden afectar a otras entidades financieras, siempre debe considerarse un incidente grave que debe notificarse.

(11) Los incidentes recurrentes vinculados por una causa subyacente aparente similar, que individualmente no constituyen incidentes graves, pueden indicar deficiencias y puntos débiles significativos en los procedimientos de gestión de incidentes y riesgos de la entidad financiera. Por consiguiente, los incidentes recurrentes deben considerarse graves colectivamente cuando se produzcan repetidamente durante un determinado período de tiempo.

(12) Teniendo en cuenta que las ciberamenazas pueden tener efectos negativos en la entidad financiera y en el sector financiero, las notificaciones de ciberamenazas importantes que presenten las entidades financieras deben indicar la probabilidad de que se materialicen y la gravedad de los posibles efectos. En consecuencia, para garantizar una evaluación clara y coherente de la importancia de las ciberamenazas, la clasificación de una ciberamenaza como importante debe depender del tipo de ciberamenaza, de la información de que disponga la entidad financiera y de la probabilidad de que, si la ciberamenaza se materializase, el incidente cumpliera los criterios para ser clasificado como grave y alcanzara los umbrales correspondientes.

([3]) Reglamento Delegado (UE) 2018/959 de la Comisión, de 14 de marzo de 2018, por el que se completa el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación para la especificación del método de evaluación con arreglo al cual las autoridades competentes autorizan a las entidades a utilizar métodos avanzados de cálculo para el riesgo operativo (DO L 169 de 6.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Teniendo en cuenta que se debe notificar a las autoridades competentes de otros Estados miembros los incidentes que afecten a entidades financieras y clientes de su país o territorio, la evaluación de los efectos en otro territorio de conformidad con el artículo 19, apartado 7, del Reglamento (UE) 2022/2554 debe basarse en la causa subyacente del incidente, en el posible contagio a través de proveedores terceros y en las infraestructuras de los mercados financieros, así como en los efectos del incidente en grupos significativos de clientes o contrapartes financieras.

(14) Los procesos de notificación y de presentación de información a que se refiere el artículo 19, apartados 6 y 7, del Reglamento (UE) 2022/2554 deben permitir a los destinatarios respectivos evaluar los efectos de los incidentes. Por lo tanto, la información transmitida debe abarcar todos los datos incluidos en los informes de incidentes presentados por la entidad financiera a la autoridad competente.

(15) Cuando un incidente constituya una violación de la seguridad de los datos personales de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([4]) y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([5]), el presente Reglamento no debe afectar a las obligaciones de registro y notificación de las violaciones de la seguridad de los datos personales establecidas en dichas normas de la Unión. Las autoridades competentes deben cooperar e intercambiar información sobre todas las cuestiones pertinentes con las autoridades a que se refieren el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE.

(16) El presente Reglamento se basa en los proyectos de normas técnicas de regulación presentados a la Comisión por las Autoridades Europeas de Supervisión, en consulta con la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Banco Central Europeo (BCE).

(17) El Comité Mixto de las Autoridades Europeas de Supervisión a que se refieren el artículo 54 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([6]), el artículo 54 del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([7]) y el artículo 54 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([8]) ha llevado a cabo consultas públicas abiertas sobre el proyecto de normas técnicas de regulación en que se basa el presente Reglamento, ha analizado los posibles costes y beneficios de las normas propuestas y ha solicitado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1093/2010, del Grupo de Partes Interesadas del Sector de Seguros y Reaseguros y del Grupo de Partes Interesadas del Sector de Pensiones de Jubilación creados de conformidad con el artículo 37 del Reglamento (UE) n.º 1094/2010, y del Grupo de partes interesadas del sector de los valores y mercados creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010.

([4]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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).

([7]) 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).

([8]) 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).

(18) 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 ([9]), emitió su dictamen el 24 de enero de 2024.

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

CRITERIOS DE CLASIFICACIÓN

Artículo 1

Clientes, contrapartes financieras y transacciones

1. El número de clientes afectados por el incidente a que se refiere el artículo 18, apartado 1, letra a), del Reglamento (UE) 2022/2554 reflejará el número de todos los clientes afectados, ya sean personas físicas o jurídicas, que no puedan, o no hayan podido, utilizar el servicio prestado por la entidad financiera durante el incidente o que se hayan visto afectados negativamente por el incidente. Dicho número incluirá también a terceros que estén expresamente cubiertos por el acuerdo contractual entre la entidad financiera y el cliente como beneficiarios del servicio afectado.

2. El número de contrapartes financieras afectadas por el incidente a que se refiere el artículo 18, apartado 1, letra a), del Reglamento (UE) 2022/2554 reflejará el número de todas las contrapartes financieras afectadas que hayan celebrado un acuerdo contractual con la entidad financiera.

3. En relación con la pertinencia de los clientes y las contrapartes financieras afectados por el incidente a que se refiere el artículo 18, apartado 1, letra a), del Reglamento (UE) 2022/2554, la entidad financiera tendrá en cuenta la medida en que los efectos para un cliente o contraparte financiera incidirán en la consecución de los objetivos empresariales de la entidad financiera, así como el posible efecto del incidente en la eficiencia del mercado.

4. En relación con la cantidad o el número de transacciones afectadas por el incidente a que se refiere el artículo 18, apartado 1, letra a), del Reglamento (UE) 2022/2554, la entidad financiera tendrá en cuenta todas las transacciones afectadas que impliquen un importe monetario cuando al menos una parte de la transacción se lleve a cabo en la Unión.

5. Cuando no pueda determinarse el número real de clientes o contrapartes financieras afectados o el número o la cantidad reales de las transacciones afectadas, la entidad financiera estimará dicho número o dicha cantidad sobre la base de los datos disponibles de períodos de referencia comparables.

Artículo 2

Repercusión en la reputación

1. A efectos de determinar la repercusión en la reputación del incidente a que se refiere el artículo 18, apartado 1, letra a), del Reglamento (UE) 2022/2554, las entidades financieras considerarán que el incidente ha repercutido en la reputación cuando se cumpla al menos uno de los criterios siguientes:

a) el incidente se ha reflejado en los medios de comunicación;

b) el incidente ha dado lugar a quejas reiteradas de distintos clientes o contrapartes financieras sobre servicios de cara al cliente o relaciones comerciales esenciales;

c) la entidad financiera no podrá cumplir los requisitos reglamentarios, o es probable que no pueda cumplirlos, como consecuencia del incidente;

d) la entidad financiera perderá, o es probable que pierda, clientes o contrapartes financieras como consecuencia del incidente, lo que acarreará consecuencias importantes para sus actividades.

([9]) 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).

2. Al evaluar la repercusión en la reputación del incidente, las entidades financieras tendrán en cuenta el nivel de visibilidad que el incidente haya alcanzado o pueda alcanzar en relación con cada uno de los criterios enumerados en el apartado 1.

Artículo 3

Duración del incidente y duración de la interrupción del servicio

1. Las entidades financieras medirán la duración del incidente a que se refiere el artículo 18, apartado 1, letra b), del Reglamento (UE) 2022/2554, desde el momento en que se produzca el incidente hasta el momento en que se resuelva.

Cuando las entidades financieras no puedan determinar el momento en que se haya producido el incidente, medirán la duración del incidente desde el momento en que se detectase. Cuando las entidades financieras tengan conocimiento de que el incidente se ha producido antes de su detección, medirán la duración desde el momento en que se registre el incidente en registros de redes o sistemas o en otras fuentes de datos.

Cuando las entidades financieras aún no sepan cuándo se resolverá el incidente o no puedan verificar los datos en los registros o en otras fuentes de datos, realizarán estimaciones.

2. Las entidades financieras medirán la duración de la interrupción del servicio derivada de los incidentes a que se refiere el artículo 18, apartado 1, letra b), del Reglamento (UE) 2022/2554, desde el momento en que el servicio no esté disponible total o parcialmente para los clientes, las contrapartes financieras u otros usuarios internos o externos hasta el momento en que se restablezcan las actividades u operaciones regulares al nivel de servicio que se prestaba antes del incidente. Cuando la interrupción del servicio provoque retrasos en la prestación del servicio después de que se hayan restablecido las actividades u operaciones regulares, la duración de la interrupción del servicio se medirá desde el inicio del incidente hasta el momento en que el servicio que haya sufrido un retraso se preste en su totalidad.

Cuando las entidades financieras no puedan determinar el momento en que se haya iniciado la interrupción del servicio, medirán la duración de la interrupción del servicio desde el momento en que se detecte.

Artículo 4

Extensión geográfica

A efectos de determinar la extensión geográfica con respecto a las zonas afectadas por el incidente a que se refiere el artículo 18, apartado 1, letra c), del Reglamento (UE) 2022/2554, las entidades financieras evaluarán si el incidente tiene o ha tenido consecuencias en otros Estados miembros y, en particular, la importancia de dichas consecuencias en lo que respecta a:

a) los clientes y las contrapartes financieras de otros Estados miembros;

b) las sucursales u otras entidades financieras del grupo que lleven a cabo actividades en otros Estados miembros;

c) las infraestructuras de los mercados financieros o los proveedores terceros que puedan afectar a entidades financieras en otros Estados miembros a las que presten servicios, en la medida en que se disponga de tal información.

Artículo 5

Pérdidas de datos

A efectos de determinar las pérdidas de datos que acarrea el incidente a que se refiere el artículo 18, apartado 1, letra d), del Reglamento (UE) 2022/2554, las entidades financieras tendrán en cuenta lo siguiente:

a) en relación con la disponibilidad de los datos, si el incidente ha hecho que los datos solicitados por la entidad financiera, sus clientes o sus contrapartes sean inaccesibles o inutilizables de forma temporal o permanente;

b) en relación con la autenticidad de los datos, si el incidente ha puesto en peligro la fiabilidad de la fuente de los datos;

c) en relación con la integridad de los datos, si el incidente ha dado lugar a una modificación no autorizada de datos que haya hecho que dichos datos sean inexactos o incompletos;

d) en relación con la confidencialidad de los datos, si el incidente ha dado lugar a que una parte o un sistema no autorizado haya tenido acceso a los datos o los haya divulgado.

Artículo 6

Carácter esencial de los servicios afectados

A efectos de determinar el carácter esencial de los servicios afectados a que se refiere el artículo 18, apartado 1, letra e), del Reglamento (UE) 2022/2554, las entidades financieras evaluarán si el incidente:

a) afecta o ha afectado a servicios de TIC o redes y sistemas de información que sustenten funciones esenciales o importantes de la entidad financiera;

b) afecta o ha afectado a servicios financieros prestados por ellas que requieran una autorización o un registro o que sean supervisados por las autoridades competentes;

c) constituye o ha constituido un acceso efectivo, malintencionado y no autorizado a las redes y sistemas de información de la entidad financiera.

Artículo 7

Consecuencias económicas

1. A efectos de determinar las consecuencias económicas del incidente a que se refiere el artículo 18, apartado 1, letra f), del Reglamento (UE) 2022/2554, las entidades financieras tendrán en cuenta, sin contabilizar las recuperaciones financieras, los siguientes tipos de costes y pérdidas directos e indirectos que hayan sufrido como consecuencia del incidente:

a) los fondos o los activos financieros expropiados de los que sean responsables, incluidos los activos perdidos como consecuencia de un robo;

b) los costes de sustitución o reubicación de *software*, *hardware* o infraestructuras;

c) los gastos de personal, incluidos los costes relacionados con la sustitución o la reubicación de personal, la contratación de personal suplementario, la remuneración de las horas extraordinarias y la recuperación de las competencias perdidas o mermadas;

d) los desembolsos por incumplimiento de las obligaciones contractuales;

e) los costes de reparación y de indemnización a los clientes;

f) las pérdidas por lucro cesante;

g) los costes asociados a la comunicación interna y externa;

h) los costes de asesoramiento, incluidos los relacionados con el asesoramiento jurídico, los servicios forenses y los servicios de reparación.

2. Los costes y pérdidas a que se refiere el apartado 1 no incluirán los costes necesarios para el funcionamiento diario de la empresa, en particular:

a) los costes de mantenimiento general de las infraestructuras, los equipos, el *hardware* y el *software*, así como los costes de actualización de las competencias del personal;

b) los costes internos o externos dedicados a mejorar la actividad después del incidente, incluidas las actualizaciones, las mejoras y las iniciativas relacionadas con la evaluación de riesgos;

c) las primas de seguros.

3. Las entidades financieras calcularán los importes de los costes y las pérdidas sobre la base de los datos disponibles en el momento de la notificación. Cuando no puedan determinarse los importes reales de los costes y las pérdidas, las entidades financieras los estimarán.

4. Al evaluar las consecuencias económicas del incidente, las entidades financieras sumarán los costes y las pérdidas a que se refiere el apartado 1.

CAPÍTULO II

INCIDENTES GRAVES Y UMBRALES DE IMPORTANCIA RELATIVA

Artículo 8

Incidentes graves

1. Un incidente se considerará un incidente grave a efectos del artículo 19, apartado 1, del Reglamento (UE) 2022/2554 cuando haya afectado a los servicios esenciales a que se refiere el artículo 6 y se cumpla alguna de las condiciones siguientes:

a) si se alcanza el umbral de importancia relativa a que se refiere el artículo 9, apartado 5, letra b);

b) si se cumplen dos o más de los demás umbrales de importancia relativa a que se refiere el artículo 9, apartados 1 a 6.

2. Los incidentes recurrentes que no se consideren individualmente un incidente grave en el sentido del apartado 1 se considerarán un incidente grave cuando cumplan todas las condiciones siguientes:

a) si se han producido al menos dos veces en un plazo de seis meses;

b) si tienen la misma causa subyacente aparente, tal como se contempla en el artículo 20, párrafo primero, letra b), del Reglamento (UE) 2022/2554;

c) si se cumplen colectivamente los criterios para ser considerados un incidente grave enumerados en el apartado 1.

Las entidades financieras evaluarán mensualmente la existencia de incidentes recurrentes.

El presente apartado no se aplicará a las microempresas ni a las entidades financieras enumeradas en el artículo 16, apartado 1, del Reglamento (UE) 2022/2554.

Artículo 9

Umbrales de importancia relativa para determinar los incidentes graves

1. Se alcanzará el umbral de importancia relativa para el criterio «clientes, contrapartes financieras y transacciones» cuando se cumpla cualquiera de las condiciones siguientes:

a) cuando el número de clientes afectados sea superior al 10 % del conjunto de los clientes que utilizan el servicio afectado;

b) el número de clientes afectados que utilizan el servicio afectado sea superior a 100 000;

c) el número de contrapartes financieras afectadas sea superior al 30 % del conjunto de las contrapartes financieras que llevan a cabo actividades relacionadas con la prestación del servicio afectado;

d) el número de transacciones afectadas sea superior al 10 % del número medio diario de las transacciones realizadas por la entidad financiera relacionadas con el servicio afectado;

e) la cantidad de transacciones afectadas sea superior al 10 % del valor medio diario de las transacciones realizadas por la entidad financiera relacionadas con el servicio afectado;

f) se hayan visto afectados los clientes o las contrapartes financieras que se hayan considerado pertinentes con arreglo a lo establecidos en el artículo 1, apartado 3.

Cuando no pueda determinarse el número real de clientes o contrapartes financieras afectados o el número o la cantidad reales de las transacciones afectadas, la entidad financiera estimará dicho número o dicha cantidad sobre la base de los datos disponibles de períodos de referencia comparables.

2. Se alcanzará el umbral de importancia relativa para el criterio «repercusión en la reputación» cuando se cumpla cualquiera de las condiciones establecidas en el artículo 2, letras a) a d).

3. Se alcanzará el umbral de importancia relativa para el criterio «duración del incidente y duración de la interrupción del servicio» cuando se cumpla cualquiera de las condiciones siguientes:

a) cuando la duración del incidente sea superior a 24 horas;

b) cuando la duración de la interrupción del servicio sea superior a dos horas en el caso de los servicios de TIC que sustenten funciones esenciales o importantes.

4. Se alcanzará el umbral de importancia relativa para el criterio de «extensión geográfica» cuando el incidente tenga consecuencias en dos o más Estados miembros de conformidad con lo establecido en el artículo 4.

5. Se alcanzará el umbral de importancia relativa para el criterio «pérdidas de datos» cuando se cumpla cualquiera de las condiciones siguientes:

a) cuando la incidencia sobre la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos a que se refiere el artículo 5 tenga o vaya a tener efectos negativos en la consecución de los objetivos empresariales de la entidad financiera o en su capacidad para cumplir los requisitos reglamentarios;

b) cuando las redes y los sistemas de información sean objeto de un acceso efectivo, malintencionado y no autorizado no contemplado en la letra a), cuando dicho acceso pueda dar lugar a pérdidas de datos.

6. Se alcanzará el umbral de importancia relativa para el criterio «consecuencias económicas» cuando los costes y las pérdidas sufridas por la entidad financiera debido al incidente hayan superado o probablemente puedan superar los 100 000 EUR.

CAPÍTULO III

CIBERAMENAZAS IMPORTANTES

Artículo 10

Umbrales de importancia relativa elevada para determinar las ciberamenazas importantes

A efectos del artículo 18, apartado 2, del Reglamento (UE) 2022/2554, una ciberamenaza se considerará importante cuando se cumplan todas las condiciones siguientes:

a) cuando la ciberamenaza, si se materializa, pueda afectar o podría haber afectado a funciones esenciales o importantes de la entidad financiera, o pueda afectar a otras entidades financieras, proveedores terceros, clientes o contrapartes financieras, según la información de que disponga la entidad financiera;

b) cuando la ciberamenaza tenga una alta probabilidad de materializarse en la entidad financiera o en otras entidades financieras, teniendo en cuenta al menos los siguientes elementos:

   i) los riesgos aplicables relacionados con la ciberamenaza a que se refiere la letra a), incluidas las posibles vulnerabilidades de los sistemas de la entidad financiera que puedan explotarse,

   ii) las capacidades y la intención de los agentes de amenazas en la medida en que las conozca la entidad financiera,

   iii) la persistencia de la amenaza y cualquier conocimiento adquirido sobre incidentes que hayan afectado a la entidad financiera o a su proveedor tercero, clientes o contrapartes financieras;

c) cuando la ciberamenaza, si se materializa, pueda cumplir o alcanzar uno de los siguientes criterios o umbrales:

   i) el criterio relativo al carácter esencial de los servicios establecido en el artículo 18, apartado 1, letra e), del Reglamento (UE) 2022/2554, tal como se especifica en el artículo 6 del presente Reglamento,

   ii) el umbral de importancia relativa establecido en el artículo 9, apartado 1,

   iii) el umbral de importancia relativa establecido en el artículo 9, apartado 4.

Cuando, en función del tipo de ciberamenaza y de la información disponible, la entidad financiera concluya que podrían alcanzarse los umbrales de importancia relativa establecidos en el artículo 9, apartados 2, 3, 5 y 6, podrán tenerse en cuenta también dichos umbrales.

CAPÍTULO IV

RELEVANCIA DE LOS INCIDENTES GRAVES PARA LAS AUTORIDADES COMPETENTES DE OTROS ESTADOS MIEMBROS Y DATOS DE LAS NOTIFICACIONES QUE DEBEN COMPARTIRSE CON OTRAS AUTORIDADES COMPETENTES

Artículo 11

Relevancia de los incidentes graves para las autoridades competentes de otros Estados miembros

La evaluación de si el incidente grave es pertinente para las autoridades competentes de otros Estados miembros, de conformidad con el artículo 19, apartado 7, del Reglamento (UE) 2022/2554, se basará en si el incidente tiene una causa subyacente que tiene su origen en otro Estado miembro o si el incidente tiene o ha tenido una repercusión significativa en otro Estado miembro en relación con:

a) clientes o contrapartes financieras;

b) una sucursal de la entidad financiera u otra entidad financiera del grupo;

c) una infraestructura de los mercados financieros o un proveedor tercero que pueda afectar a entidades financieras a las que prestan servicios.

Artículo 12

Datos de los incidentes graves que deben compartirse con otras autoridades competentes

Los datos de los incidentes graves que deben presentar las autoridades competentes a otras autoridades competentes de conformidad con el artículo 19, apartado 6, del Reglamento (UE) 2022/2554 y las notificaciones que deben presentar la ABE, la AEVM o la AESPJ y el BCE a las autoridades competentes pertinentes de otros Estados miembros de conformidad con el artículo 19, apartado 7, de dicho Reglamento contendrán la misma cantidad de información, sin anonimización alguna, que las notificaciones e informes de incidentes graves recibidos de las entidades financieras de conformidad con el artículo 19, apartado 4, del Reglamento (UE) 2022/2554.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 13

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 13 de marzo de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN