Directrices conjuntas sobre la estimación de los costes y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC en virtud del Reglamento (UE) 2022/2554

(JC/2024/34)

Estas Directrices conjuntas de las Autoridades Europeas de Supervisión (AES) van dirigidas a las autoridades competentes, tal como se definen en el artículo 46 del Reglamento 2022/2554 (Reglamento DORA[1]), y a las entidades financieras, tal como se definen en el artículo 4, apartado 1, del Reglamento n.º 1093/2010 (UE), el artículo 4, apartado 1, del Reglamento (UE) n.º 1094/2010 y el artículo 4, apartado 1, del Reglamento (UE) n.º 1095/2010.

Las AES publican estas Directrices a efectos de cumplir con el mandato otorgado en virtud del artículo 11, apartado 11, del Reglamento DORA, de elaborar directrices comunes sobre la estimación de los costes y pérdidas anuales agregados de los incidentes graves relacionados con las TIC a que se refiere el artículo 11, apartado 10, del citado Reglamento. Las Directrices detallan disposiciones sobre la estimación de los costes y pérdidas anuales agregados de los incidentes graves relacionados con las TIC, y especifican una plantilla común para la presentación de los costes y pérdidas anuales agregados.

Las AES publicaron la versión en inglés de estas Directrices, así como su traducción al español, el 19 de marzo de 2025. Se aplicarán a partir del 19 de mayo de 2025.

La Comisión Ejecutiva del Banco de España, en su calidad de autoridad competente de la supervisión directa de las entidades de crédito menos significativas, entidades de pago, entidades prestadoras del servicio de información sobre cuentas y entidades de dinero electrónico, adoptó estas Directrices como propias el 5 de mayo de 2025.

En la medida en que el Reglamento DORA no aplica a los establecimientos financieros de crédito, de acuerdo con su artículo 2, estas Directrices tampoco les son de aplicación.

[1] 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.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5 de junio de 2024

Directrices conjuntas

sobre la estimación de los costes y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC en virtud del Reglamento (UE) 2022/2554

Las presentes Directrices contienen referencias a reglamentos delegados y de ejecución de la Comisión Europea que aún no se han publicado en el Diario Oficial de la UE. Una vez que estos reglamentos de próxima publicación se hayan publicado en el Diario Oficial, las presentes Directrices se finalizarán incluyendo dichas referencias. Las referencias se insertarán en las secciones resaltadas en amarillo.

La fecha de aplicación de las presentes Directrices solo podrá determinarse una vez finalizadas. La fecha prevista de aplicación de las presentes Directrices es el 17 de enero de 2025. En caso de que se produzca un retraso en la finalización de las presentes Directrices, su fecha de aplicación será, a más tardar, dos meses después de la fecha de publicación de las traducciones de las presentes Directrices en todas las lenguas oficiales de la UE.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Directrices conjuntas sobre la estimación de los costes y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC

Rango jurídico de las presentes directrices

El presente documento contiene las Directrices conjuntas emitidas de conformidad con el artículo 16 del Reglamento (UE) n.º 1093/2010[1]; el artículo 16 del Reglamento (UE) n.º 1094/2010[2]; y el artículo 16 del Reglamento (UE) n.º 1095/2010[3]: «los Reglamentos de las AES». De conformidad con el artículo 16, apartado 3, de los Reglamentos de las AES respectivas, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a las Directrices.

Las Directrices conjuntas exponen el punto de vista de las AES sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. Las autoridades competentes a las que sean de aplicación las Directrices conjuntas deberían cumplirlas incorporándolas a sus prácticas de supervisión de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las Directrices conjuntas vayan dirigidas principalmente a las entidades.

Requisitos de notificación

De conformidad con el artículo 16, apartado 3, de los Reglamentos de las AES, las autoridades competentes deberán notificar a la AES respectiva, a más tardar el 19.05.2025 (dos meses después de su emisión), si cumplen o se proponen cumplir las presentes Directrices o Recomendaciones conjuntas indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho plazo, la AES respectiva considerará que las autoridades competentes no las cumplen. Las notificaciones se enviarán a compliance@eba.europa.eu, compliance@eiopa.europa.eu y DORA@esma.europa.eu con la referencia «JC/GL/2024/34». En los sitios web de las AES se encuentra disponible un modelo para estas notificaciones. Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes.

[1] 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).

[2] 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.° 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión (*DO L 331 de 15.12.2010, pp. 48-83*).

[3] 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, pp. 84–119).

Las notificaciones se publicarán en los sitios web de las AES, tal como contempla el artículo 16, apartado 3.

Título I. Objeto, ámbito de aplicación, destinatarios y definiciones

Objeto y ámbito de aplicación

1. Las presentes directrices tienen por objeto cumplir el mandato otorgado a las AES en virtud del artículo 11, apartado 11, del Reglamento (UE) 2022/2554[4], de elaborar directrices comunes sobre la estimación de los costes y pérdidas anuales agregados de los incidentes graves relacionados con las TIC a que se refiere el artículo 11, apartado 10, de dicho Reglamento. Las presentes directrices también especifican una plantilla común para la presentación de los costes y pérdidas anuales agregados.

Destinatarios

2. Las presentes directrices están dirigidas a las autoridades competentes, tal como se definen en el artículo 46 del Reglamento 2022/2554, y a las entidades financieras, tal como se definen en el artículo 4, apartado 1, del Reglamento n.º 1093/2010 (UE), el artículo 4, apartado 1, del Reglamento (UE) n.º 1094/2010 y el artículo 4, apartado 1, del Reglamento (UE) n.º 1095/2010.

Definiciones

3. Los términos utilizados y definidos en el Reglamento (UE) 2022/2554 tienen el mismo significado en las presentes directrices.

Título II - Aplicación

Fecha de aplicación

4. Las presentes Directrices se aplicarán a partir del 19.05.2025.

[4] 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 *(DO L 333 de 27.12.2022, pp. 1–79).*

Título III - Disposiciones sobre la estimación de los costes y pérdidas anuales agregados de los incidentes graves relacionados con las TIC

5. Las entidades financieras estimarán los costes y pérdidas anuales agregados de los incidentes graves relacionados con las TIC agregando los costes y pérdidas de los incidentes graves relacionados con las TIC que se produzcan en el año de referencia para el que la autoridad competente haya solicitado la estimación. La entidad financiera podrá elegir si el año de referencia corresponde, bien al año natural completo, o bien al ejercicio contable completo de la entidad financiera para el que la entidad financiera haya finalizado sus estados financieros. Una vez que la entidad financiera haya decidido si proporcionará la estimación basada en el año natural o en su ejercicio contable, dicha decisión se aplicará a las futuras estimaciones de costes y pérdidas anuales agregados. La entidad financiera podrá modificar dicha decisión notificándola a la autoridad competente y siempre que la autoridad competente no se oponga en el plazo de dos meses a partir de la recepción de la notificación. Las entidades financieras no incluirán los costes y pérdidas relacionados con los incidentes que se produzcan antes o después de ese año de referencia.

6. Las entidades financieras incluirán en la estimación todos los incidentes relacionados con las TIC que, independientemente de la razón, hayan sido clasificados como graves de conformidad con el Reglamento Delegado [OJ L, 2024/1772, 25.6.2024][5] de la Comisión sobre la clasificación de incidentes y

   (a) para los que la entidad financiera haya presentado un informe final de conformidad con el artículo 19, apartado 4, letra c), del Reglamento (UE) 2022/2554 en el año de referencia pertinente, o

   (b) para los que la entidad financiera haya presentado en años de referencia anteriores un informe final de conformidad con el artículo 19, apartado 4, letra c), del Reglamento (UE) 2022/2554 que haya tenido un impacto financiero cuantificable en la entidad financiera en el año de referencia pertinente.

7. Las entidades financieras estimarán los costes y pérdidas anuales agregados siguiendo los siguientes pasos de forma secuencial:

   (a) estimarán individualmente los costes y pérdidas de cada incidente grave relacionado con las TIC a que se refiere el apartado 6. Dichas estimaciones darán como resultado los costes y pérdidas brutos teniendo en cuenta los tipos de costes y pérdidas establecidos en el artículo 7, apartados 1 y 2, del Reglamento Delegado [OJ L, 2024/1772, 25.6.2024] de la Comisión;

[5] 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. [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) para cada incidente grave relacionado con las TIC, las entidades financieras también estimarán las recuperaciones financieras según lo especificado en el anexo II del Reglamento de Ejecución [*OJ L, 2025/302, 20.2.2025*][6] de la Comisión;

(c) las entidades financieras agregarán los costes y pérdidas brutos y las recuperaciones financieras de los incidentes graves relacionados con las TIC.

8. Como base para las estimaciones, las entidades financieras se referirán a los costes, pérdidas y recuperaciones financieras que se reflejan en sus estados financieros, como la cuenta de pérdidas y ganancias, o, en su caso, en sus informes de supervisión, del año de referencia pertinente. En su estimación, las entidades financieras también incluirán las provisiones contables que se reflejan en sus estados financieros, como la cuenta de pérdidas y ganancias, del año de referencia pertinente. Cuando no se disponga de datos precisos, las entidades financieras basarán su estimación en otros datos e información disponibles en la medida de lo posible.

9. Las entidades financieras incluirán los ajustes sobre los costes y pérdidas de una estimación que presentó para un año anterior en la estimación del año de referencia pertinente en el que se realizan los ajustes.

10. Las entidades financieras incluirán en el informe de su estimación de los costes y pérdidas anuales agregados también el desglose de los costes y pérdidas brutos y de las recuperaciones financieras para cada incidente grave relacionado con las TIC que se hayan incluido en la agregación.

11. Las entidades financieras utilizarán la plantilla que figura en el anexo para presentar a la autoridad competente la estimación de sus costes y pérdidas anuales agregados para el año de referencia. Para cada elemento de los apartados 6 y 9 que se incluya en la estimación del año de referencia, las entidades financieras utilizarán los mismos códigos de referencia de incidentes facilitados por la entidad financiera que los utilizados en el informe final de conformidad con el artículo 19, apartado 4, letra c), del Reglamento (UE) 2022/2554.

[6] Reglamento de Ejecución (UE) 2025/302 de la Comisión, de 23 de octubre de 2024, por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a los formularios, las plantillas y los procedimientos normalizados que deberán aplicar las entidades financieras para informar de un incidente grave relacionado con las TIC y para notificar una ciberamenaza importante. [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

Anexo: Plantilla de notificación de los costes y pérdidas brutos y las recuperaciones financieras en un año de referencia

Nombre de la entidad financiera	
Identificador de entidad jurídica	
Fecha de inicio y fin del año de referencia de la entidad financiera	
Moneda	

Número del incidente	Fecha de presentación del informe final del incidente	Número de referencia del incidente	Costes y pérdidas brutos del incidente en el año de referencia (miles de unidades)	Recuperaciones del incidente en el año de referencia (miles de unidades)
1				
2				
…				
Total para el año de referencia	----------	----------		