2025/302

20.2.2025

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

(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 cuarto,

Considerando lo siguiente:

(1) A fin de garantizar que las entidades financieras notifiquen los incidentes graves a sus autoridades competentes de manera coherente y de que faciliten a dichas autoridades datos de buena calidad, debe especificarse qué campos de datos deben proporcionar las entidades financieras en las distintas fases de la elaboración de informes a que se refiere el artículo 19, apartado 4, del Reglamento (UE) 2022/2554. Es importante que esta información se presente de manera que permita tener una visión general única del incidente. Por lo tanto, es necesario establecer una plantilla única de notificación a tal efecto.

(2) Las entidades financieras deben cumplimentar los campos de datos de la plantilla de notificación que correspondan a los requisitos de información de la notificación o informe correspondiente. No obstante, las entidades financieras que ya dispongan de información que deban facilitar en una fase posterior, es decir, en los informes intermedio o final, deben poder anticipar la presentación de los datos.

(3) Dado que los incidentes múltiples o recurrentes pueden constituir un incidente grave, tal como se contempla en el artículo 8 del Reglamento Delegado (UE) 2024/1772 de la Comisión ([2]), el diseño de la plantilla de notificación y de los campos de datos debe permitir a las entidades financieras notificar dichos incidentes recurrentes.

(4) Para garantizar que la información sea exacta y esté actualizada, la plantilla de notificación debe permitir a las entidades financieras, al presentar los informes intermedio y final, actualizar cualquier información presentada previamente y, en caso necesario, reclasificar los incidentes graves como no graves.

(5) La identificación jurídica de las entidades debe ajustarse a los identificadores especificados en las normas técnicas de ejecución adoptadas de conformidad con el artículo 28, apartado 9, del Reglamento (UE) 2022/2554.

(6) Cuando las entidades financieras subcontraten las obligaciones de notificación de incidentes graves relacionados con las TIC a un tercero, las autoridades competentes deberán conocer la identidad del tercero que notifica la información en nombre de la entidad financiera antes de la presentación de la primera notificación, a fin de verificar la legitimidad de dicho tercero.

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

([2]) 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).

(7) Para determinar fácilmente las repercusiones de un incidente que se haya producido en un proveedor tercero o que haya sido causado por él, y que afecte a varias entidades financieras dentro de un único Estado miembro, y a fin de reducir el esfuerzo de notificación de las entidades financieras, la plantilla de notificación debe permitir la presentación de un informe agregado que abarque información agregada sobre las repercusiones del incidente en todas las entidades financieras afectadas que hayan clasificado el incidente como grave.

(8) La plantilla de notificación debe diseñarse de manera tecnológicamente neutra para permitir su implantación en diversas soluciones de notificación de incidentes que ya existan o que puedan desarrollarse para la aplicación de los requisitos del Reglamento (UE) 2022/2554.

(9) El diseño de la plantilla de notificación y de los campos de datos debe facilitar la notificación de incidentes graves relacionados con las TIC por parte de terceros a los que las entidades financieras hayan externalizado su obligación de notificación de conformidad con el artículo 19, apartado 5, del Reglamento (UE) 2022/2554.

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

(11) Las Autoridades Europeas de Supervisión han llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de ejecución en que se basa el presente Reglamento, han analizado los costes y beneficios potenciales conexos y han recabado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario, establecido 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.

(12) 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 establecidos en el Reglamento (UE) 2018/1725.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Plantilla para la notificación de incidentes graves relacionados con las TIC

1. Las entidades financieras utilizarán la plantilla establecida en el anexo I para presentar la notificación inicial, el informe intermedio y el informe final a que se refiere el artículo 19, apartado 4, del Reglamento (UE) 2022/2554, como sigue:

a) las entidades financieras que presenten una notificación inicial cumplimentarán los campos de datos de la plantilla que correspondan a la información que debe facilitarse de conformidad con el artículo 2 del Reglamento Delegado (UE) 2025/301 ([7]) y podrán cumplimentar, cuando ya dispongan de esa información, los campos de datos cuya cumplimentación no sea necesaria para la notificación inicial, pero sí para el informe intermedio o final;

([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).

([7]) 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. (DO L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) las entidades financieras que presenten un informe intermedio cumplimentarán los campos de datos de la plantilla que correspondan a la información que debe facilitarse de conformidad con el artículo 3 del Reglamento Delegado (UE) 2025/301 y podrán cumplimentar, cuando ya dispongan de la información pertinente, los campos de datos cuya cumplimentación no sea necesaria para el informe intermedio, pero sí para el informe final;

c) las entidades financieras que presenten un informe final cumplimentarán los campos de datos de la plantilla que correspondan a la información que debe facilitarse de conformidad con el artículo 4 del Reglamento Delegado (UE) 2025/301.

2. Las entidades financieras velarán por que la información contenida en la notificación inicial, así como en los informes intermedio y final, esté completa y sea exacta.

3. Las entidades financieras facilitarán valores estimados basados en otros datos e información disponibles, en la medida de lo posible, cuando no se disponga de datos exactos en el momento de presentar la notificación inicial o el informe intermedio.

4. Al presentar un informe intermedio o final, las entidades financieras utilizarán la plantilla que figura en el anexo I para presentar toda la información requerida y actualizar, en su caso, la información facilitada previamente en la notificación inicial o en el informe intermedio.

5. Las entidades financieras seguirán el glosario de datos y las instrucciones que figuran en el anexo II al cumplimentar la plantilla incluida en el anexo I.

Artículo 2

Presentación conjunta de la notificación inicial y los informes intermedio y final

Las entidades financieras podrán combinar la presentación de la notificación inicial, el informe intermedio y el informe final para facilitar al mismo tiempo dos de ellos o todos, cuando se hayan recuperado las actividades regulares o se haya finalizado el análisis de las causas subyacentes y siempre que se cumplan los plazos establecidos en el artículo 5 del Reglamento Delegado (UE) 2025/301.

Artículo 3

Incidentes relacionados con las TIC recurrentes

Las entidades financieras que faciliten información sobre incidentes no graves relacionados con las TIC recurrentes que cumplan acumulativamente las condiciones para un incidente grave relacionado con las TIC establecidas en el artículo 8, apartado 2, del Reglamento Delegado (UE) 2024/1772 facilitarán dicha información de forma agregada.

Artículo 4

Uso de canales electrónicos seguros

1. Las entidades financieras utilizarán los canales electrónicos seguros puestos a disposición por su autoridad competente para presentar la notificación inicial y los informes intermedio y final.

2. Las entidades financieras que no puedan utilizar los canales electrónicos seguros puestos a disposición por su autoridad competente informarán a esta sobre un incidente grave relacionado con las TIC por otros medios seguros, de acuerdo con la autoridad competente. Si así lo exige dicha autoridad, las entidades financieras volverán a presentar la notificación inicial, o el informe intermedio o final, a través del canal electrónico seguro puesto a disposición una vez que puedan hacerlo.

Artículo 5

Reclasificación de incidentes graves relacionados con las TIC

Cuando, tras una nueva evaluación, la entidad financiera concluya que el incidente relacionado con las TIC notificado previamente como grave no cumplía en ningún momento los criterios y umbrales de clasificación establecidos en el artículo 8 del Reglamento Delegado (UE) 2024/1772, notificará a la autoridad competente que ha reclasificado el incidente relacionado con las TIC de grave a no grave facilitando la información sobre dicha reclasificación en la plantilla que figura en el anexo II del presente Reglamento en relación con los campos «tipo de informe» y «otra información».

Artículo 6

Notificación de la externalización de las obligaciones de notificación

1. Las entidades financieras que hayan externalizado la obligación de notificar incidentes graves relacionados con las TIC de conformidad con el artículo 19, apartado 5, del Reglamento (UE) 2022/2554 informarán a su autoridad competente de dicho acuerdo de externalización tan pronto como se haya celebrado este y, a más tardar, antes de la primera notificación o informe.

2. Las entidades financieras facilitarán a la autoridad competente el nombre, los datos de contacto y el código de identificación del tercero que vaya a presentar las notificaciones de incidentes graves relacionados con las TIC o los informes correspondientes.

3. Las entidades financieras informarán a su autoridad competente tan pronto como dejen de externalizar sus obligaciones de notificación a que se refiere el artículo 19, apartado 5, del Reglamento (UE) 2022/2554.

Artículo 7

Notificación agregada

1. Un proveedor tercero de servicios al que se hayan externalizado las obligaciones de notificación a que se refiere el artículo 19, apartado 5, del Reglamento (UE) 2022/2554 podrá utilizar la plantilla que figura en el anexo I del presente Reglamento para proporcionar información agregada sobre un incidente grave relacionado con las TIC que afecte a varias entidades financieras en una única notificación o informe, y presentar dicha notificación o informe a la autoridad competente en nombre de todas las entidades financieras afectadas, siempre que se cumplan todas las condiciones siguientes:

a) que el incidente grave relacionado con las TIC que deba notificarse tenga su origen en un proveedor tercero de servicios de TIC o esté causado por este;

b) que el proveedor tercero de servicios preste el servicio de TIC pertinente a más de una entidad financiera o a un grupo;

c) que el incidente relacionado con las TIC esté clasificado como grave por todas las entidades financieras incluidas en la notificación o informe agregado;

d) que el incidente grave relacionado con las TIC afecte a entidades financieras de un único Estado miembro y el informe agregado se refiera a entidades financieras supervisadas por la misma autoridad competente;

e) que las autoridades competentes hayan permitido explícitamente a este tipo de entidades financieras agregar su notificación.

2. El apartado 1 no se aplicará a las entidades de crédito que se consideren de importancia significativa según el artículo 2, punto 16, del Reglamento (UE) n.º 468/2014 del Banco Central Europeo ([8]), a los gestores de centros de negociación ni a las entidades de contrapartida central, que solo utilizarán la plantilla del anexo I para presentar notificaciones o informes de incidentes graves relacionados con las TIC individualmente a su autoridad competente.

3. Cuando las autoridades competentes exijan información sobre las repercusiones específicas del incidente grave relacionado con las TIC en una única entidad financiera, a petición de la autoridad competente, la entidad financiera presentará una notificación o un informe individual sobre el incidente grave relacionado con las TIC.

([8]) Reglamento (UE) n.º 468/2014 del Banco Central Europeo, de 16 de abril de 2014, por el que se establece el marco de cooperación en el Mecanismo Único de Supervisión entre el Banco Central Europeo y las autoridades nacionales competentes y con las autoridades nacionales designadas (Reglamento Marco del MUS) (BCE/2014/17) (DO L 141 de 14.5.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Artículo 8

Notificación de ciberamenazas importantes

1. Las entidades financieras que notifiquen ciberamenazas importantes a las autoridades competentes de conformidad con el artículo 19, apartado 2, del Reglamento (UE) 2022/2554 utilizarán la plantilla que figura en el anexo III del presente Reglamento y seguirán el glosario de datos y las instrucciones que figuran en el anexo IV del presente Reglamento.

2. Las entidades financieras velarán por que la información contenida en la notificación de ciberamenazas importantes esté completa y sea exacta.

Artículo 9

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

ANEXO I

PLANTILLAS PARA LA NOTIFICACIÓN DE INCIDENTES GRAVES

Número de campo	Campo de datos	
Información general sobre la entidad financiera		
1.1	Tipo de presentación	
1.2	Nombre de la entidad que presenta el informe	
1.3	Código de identificación de la entidad que presenta el informe	
1.4	Tipo de entidad financiera afectada	
1.5	Nombre de la entidad financiera afectada	
1.6	Código LEI de la entidad financiera afectada	
1.7	Nombre de la persona de contacto principal	
1.8	Correo electrónico de la persona de contacto principal	
1.9	Teléfono de la persona de contacto principal	
1.10	Nombre de la segunda persona de contacto	
1.11	Correo electrónico de la segunda persona de contacto	
1.12	Teléfono de la segunda persona de contacto	
1.13	Razón social de la empresa matriz última	
1.14	Código LEI de la empresa matriz última	
1.15	Moneda de referencia	
Contenido de la notificación inicial		
2.1	Código de referencia del incidente asignado por la entidad financiera	
2.2	Fecha y hora de detección del incidente grave relacionado con las TIC	
2.3	Fecha y hora de la clasificación del incidente relacionado con las TIC como grave	
2.4	Descripción del incidente grave relacionado con las TIC	
2.5	Criterios de clasificación que activaron el informe de incidente	
2.6	Umbrales de importancia para el criterio de clasificación «Distribución geográfica»	
2.7	Descubrimiento del incidente grave relacionado con las TIC	

Número de campo	Campo de datos	
2.8	Indicación de si el incidente grave relacionado con las TIC tiene su origen en un proveedor tercero u otra entidad financiera	
2.9	Activación del plan de continuidad de la actividad, si se activa	
2.10	Otros datos de interés	
Contenido del informe intermedio		
3.1	Código de referencia del incidente facilitado por la autoridad competente	
3.2	Fecha y hora en que se produjo el incidente grave relacionado con las TIC	
3.3	Fecha y hora en que se han recuperado los servicios, actividades u operaciones	
3.4	Número de clientes afectados	
3.5	Porcentaje de clientes afectados	
3.6	Número de contrapartes financieras afectadas	
3.7	Porcentaje de contrapartes financieras afectadas	
3.8	Repercusión en los clientes o las contrapartes financieras pertinentes	
3.9	Número de transacciones afectadas	
3.10	Porcentaje de transacciones afectadas	
3.11	Valor de las transacciones afectadas	
3.12	Información sobre si las cifras son reales o estimadas, o si no se ha producido ninguna repercusión	
3.13	Repercusión en la reputación	
3.14	Información contextual sobre la repercusión en la reputación	
3.15	Duración del incidente grave relacionado con las TIC	
3.16	Duración de la interrupción del servicio	
3.17	Información sobre si las cifras correspondientes a la duración del incidente y a la duración de la interrupción del servicio son reales o estimadas.	
3.18	Tipos de repercusiones en los Estados miembros	
3.19	Descripción de la repercusión del incidente grave relacionado con las TIC en otros Estados miembros	
3.20	Umbrales de importancia para el criterio de clasificación «Pérdidas de datos»	
3.21	Descripción de las pérdidas de datos	

Número de campo	Campo de datos	
3.22	Criterio de clasificación «Servicios esenciales afectados»	
3.23	Tipo de incidente grave relacionado con las TIC	
3.24	Otros tipos de incidentes	
3.25	Amenazas y técnicas utilizadas por el agente de riesgo	
3.26	Otros tipos de técnicas	
3.27	Información sobre las áreas funcionales y los procesos empresariales afectados	
3.28	Componentes de la infraestructura afectados que apoyan los procesos empresariales	
3.29	Información sobre los componentes de la infraestructura afectados que apoyan los procesos empresariales	
3.30	Repercusiones en los intereses financieros de los clientes	
3.31	Notificación a otras autoridades	
3.32	Especificación de «otras» autoridades	
3.33	Acciones/medidas temporales adoptadas o previstas para recuperarse del incidente	
3.34	Descripción de las acciones y medidas temporales adoptadas o previstas para recuperarse del incidente	
3.35	Indicadores de compromiso	
Contenido del informe final		
4.1	Clasificación de alto nivel de las causas profundas del incidente	
4.2	Clasificación detallada de las causas profundas del incidente	
4.3	Clasificación adicional de las causas profundas del incidente	
4.4	Otros tipos de causas profundas	
4.5	Información sobre las causas profundas del incidente	
4.6	Resumen de la resolución del incidente	
4.7	Fecha y hora en que se abordó la causa profunda del incidente	
4.8	Fecha y hora en que se resolvió el incidente	
4.9	Información si la fecha de resolución permanente del incidente difiere de la fecha de aplicación inicialmente prevista	
4.10	Evaluación del riesgo para las funciones esenciales a efectos de resolución	
4.11	Información pertinente para las autoridades de resolución	

Número de campo	Campo de datos	
4.12	Umbral de importancia para el criterio de clasificación «Consecuencias económicas»	
4.13	Importe de los costes y pérdidas directos e indirectos brutos	
4.14	Importe de las recuperaciones financieras	
4.15	Información sobre si los incidentes no graves han sido recurrentes	
4.16	Fecha y hora en que se produjeron los incidentes recurrentes	

ANEXO II

GLOSARIO DE DATOS E INSTRUCCIONES PARA LA NOTIFICACIÓN DE INCIDENTES GRAVES

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
Información general sobre la entidad financiera						
1.1.	Tipo de presentación	Indíquese el tipo de notificación o informe de incidente que se presenta a la autoridad competente.	Sí	Sí	Sí	Opciones: — notificación inicial; — informe intermedio; — informe final; — incidente grave reclasificado como no grave.
1.2.	Nombre de la entidad que presenta el informe	Razón social completa de la entidad que presenta el informe.	Sí	Sí	Sí	Alfanumérico
1.3.	Código de identificación de la entidad que presenta el informe	Código de identificación de la entidad que presenta el informe. Cuando las entidades financieras presenten la notificación o el informe, el código de identificación será un identificador de entidad jurídica (LEI), que es un código único de veinte caracteres alfanuméricos, basado en la norma ISO 17442-1:2020. Cuando un proveedor tercero presente un informe en nombre de una entidad financiera, este podrá utilizar un código de identificación tal como se especifica en las normas técnicas de ejecución adoptadas de conformidad con el artículo 28, apartado 9, del Reglamento (UE) 2022/2554.	Sí	Sí	Sí	Alfanumérico
1.4.	Tipo de entidad financiera afectada	Tipo de entidad a que se refiere el artículo 2, apartado 1, letras a) a t), del Reglamento (UE) 2022/2554 para la que se presenta el informe. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, los diferentes tipos de entidades financieras incluidas en el informe agregado que se seleccionará.	Sí	Sí	Sí	Opciones (selección múltiple): — entidad de crédito; — entidad de pago; — entidad de pago exenta; — proveedor de servicios de información sobre cuentas; — entidad de dinero electrónico; — entidad de dinero electrónico exenta; — empresa de servicios de inversión; — proveedor de servicios de criptoactivos; — emisor de fichas referenciadas a activos; — depositario central de valores; — entidad de contrapartida central; — centro de negociación; — registro de operaciones;

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
					— gestor de fondos de inversión alternativos; — sociedad de gestión; — proveedor de servicios de suministro de datos; — empresas de seguros y de reaseguros; — intermediario de seguros, intermediario de reaseguros e intermediario de seguros complementarios; — fondo de pensiones de empleo; — agencia de calificación crediticia; — administrador de índices de referencia cruciales; — proveedor de servicios de financiación participativa; — registro de titulizaciones.
1.5. Nombre de la entidad financiera afectada	Razón social completa de la entidad financiera afectada por el incidente grave relacionado con las TIC y obligada a notificar el incidente grave a su autoridad competente con arreglo al artículo 19 del Reglamento (UE) 2022/2554. En caso de notificación agregada: a) lista de todos los nombres de las entidades financieras afectadas por el incidente grave relacionado con las TIC, separados por un punto y coma; b) el proveedor tercero que presente una notificación o un informe de incidente grave de forma agregada, tal como se contempla en el artículo 7 del presente Reglamento, debe enumerar los nombres de todas las entidades financieras afectadas por el incidente, separados por un punto y coma.	Sí, si la entidad financiera afectada por el incidente es diferente de la entidad que presenta el informe y en caso de notificación agregada.	Sí, si la entidad financiera afectada por el incidente es diferente de la entidad que presenta el informe y en caso de notificación agregada.	Sí, si la entidad financiera afectada por el incidente es diferente de la entidad que presenta el informe y en caso de notificación agregada	Alfanumérico
1.6. Código LEI de la entidad financiera afectada	Identificador de entidad jurídica (LEI) de la entidad financiera afectada por el incidente grave relacionado con las TIC, asignado de conformidad con la Organización Internacional de Normalización. En caso de notificación agregada: a) lista de todos los códigos LEI de las entidades financieras afectadas por el incidente grave relacionado con las TIC, separados por un punto y coma;	Sí, si la entidad financiera afectada por el incidente grave relacionado con las TIC es	Sí, si la entidad financiera afectada por el incidente grave relacionado con las TIC es diferente de la	Sí, si la entidad financiera afectada por el incidente grave relacionado con las TIC es	Código único de veinte caracteres alfanuméricos, basado en la norma ISO 17442-1:2020

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		b) el proveedor tercero que presente una notificación o un informe de incidente grave de forma agregada, tal como se contempla en el artículo 7 del presente Reglamento, debe enumerar los códigos LEI de todas las entidades financieras afectadas por el incidente, separadas por un punto y coma. El orden de aparición de los códigos LEI y los nombres de las entidades financieras será idéntico.	diferente de la entidad que presenta el informe y en caso de notificación agregada.	entidad que presenta el informe y en caso de notificación agregada.	diferente de la entidad que presenta el informe y en caso de notificación agregada.	
1.7.	Nombre de la persona de contacto principal	Nombre y apellidos de la persona de contacto principal de la entidad financiera. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el nombre de la persona de contacto principal de la entidad que presenta el informe agregado.	Sí	Sí	Sí	Alfanumérico
1.8.	Correo electrónico de la persona de contacto principal	Dirección de correo electrónico de la persona de contacto principal que puede utilizar la autoridad competente para la comunicación de seguimiento. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el correo electrónico de la persona de contacto principal de la entidad que presenta el informe agregado.	Sí	Sí	Sí	Alfanumérico
1.9.	Teléfono de la persona de contacto principal	Número de teléfono de la persona de contacto principal que puede utilizar la autoridad competente para la comunicación de seguimiento. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el número de teléfono de la persona de contacto principal de la entidad que presenta el informe agregado. Se indicará el número de teléfono con todos los prefijos internacionales (por ejemplo, +33 XXXXXXXXX).	Sí	Sí	Sí	Alfanumérico
1.10.	Nombre de la segunda persona de contacto	Nombre y apellidos de la segunda persona de contacto o nombre del equipo responsable de la entidad financiera o de una entidad que presente el informe en nombre de la entidad financiera.	Sí	Sí	Sí	Alfanumérico
1.11.	Correo electrónico de la segunda persona de contacto	Dirección de correo electrónico de la segunda persona de contacto o dirección de correo electrónico funcional del equipo que pueda utilizar la autoridad competente para la comunicación de seguimiento.	Sí	Sí	Sí	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
1.12. Teléfono de la segunda persona de contacto	Número de teléfono de la segunda persona de contacto, o de un equipo, que puede utilizar la autoridad competente para la comunicación de seguimiento. Se indicará el número de teléfono con todos los prefijos internacionales (por ejemplo, +33 XXXXXXXXX).	Sí	Sí	Sí	Alfanumérico
1.13. Razón social de la empresa matriz última	Razón social de la empresa matriz última del grupo al que pertenece la entidad financiera afectada, cuando proceda.	Sí, si la entidad financiera pertenece a un grupo.	Sí, si la entidad financiera pertenece a un grupo.	Sí, si la entidad financiera pertenece a un grupo.	Alfanumérico
1.14. Código LEI de la empresa matriz última	LEI de la empresa matriz última del grupo al que pertenece la entidad financiera afectada, cuando proceda. Asignado de conformidad con la Organización Internacional de Normalización.	Sí, si la entidad financiera pertenece a un grupo.	Sí, si la entidad financiera pertenece a un grupo.	Sí, si la entidad financiera pertenece a un grupo.	Código único de veinte caracteres alfanuméricos, basado en la norma ISO 17442-1:2020.
1.15. Moneda de referencia	Moneda utilizada para la notificación de incidentes	Sí	Sí	Sí	La opción que corresponda se indicará utilizando los códigos de moneda ISO 4217
Contenido de la notificación inicial					
2.1. Código de referencia del incidente asignado por la entidad financiera	Código de referencia único emitido por la entidad financiera que identifique inequívocamente el incidente grave relacionado con las TIC. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el código de referencia del incidente asignado por el proveedor tercero.	Sí	Sí	Sí	Alfanumérico
2.2. Fecha y hora de detección del incidente relacionado con las TIC	Fecha y hora en que la entidad financiera ha tenido conocimiento del incidente relacionado con las TIC. En el caso de incidentes recurrentes, fecha y hora en que se detectó el último incidente relacionado con las TIC.	Sí	Sí	Sí	UTC conforme a la norma ISO 8601 (AAAA-MM-DD hh: mm:ss)

	Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
2.3.	Fecha y hora de la clasificación del incidente como grave	Fecha y hora en que el incidente relacionado con las TIC se clasificó como grave con arreglo a los criterios de clasificación establecidos en el Reglamento Delegado (UE) 2024/1772.	Sí	Sí	Sí	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)
2.4.	Descripción del incidente relacionado con las TIC	Descripción de los aspectos más pertinentes del incidente grave relacionado con las TIC. Las entidades financieras proporcionarán un resumen general de la siguiente información, como posibles causas, repercusiones inmediatas, sistemas afectados y otros. Las entidades financieras incluirán, cuando se conozca o se prevea razonablemente, si el incidente afecta a proveedores terceros u otras entidades financieras, el tipo de proveedor o entidad financiera, su nombre, sus respectivos códigos de identificación y el tipo de código de identificación (por ejemplo, LEI o EUID). En informes posteriores, el contenido del campo puede evolucionar con el tiempo para reflejar lo que se vaya conociendo sobre el incidente relacionado con las TIC y describir cualquier otra información pertinente sobre este no recogida en los campos de datos, como la evaluación interna de la gravedad por parte de la entidad financiera (por ejemplo, muy baja, baja, media, alta o muy alta) y una indicación del nivel y el nombre de las estructuras de decisión de mayor rango que hayan participado en la respuesta al incidente relacionado con las TIC.	Sí	Sí	Sí	Alfanumérico
2.5.	Criterios de clasificación que activaron el informe de incidente	Criterios de clasificación con arreglo al Reglamento Delegado (UE) 2024/1772 que han dado lugar a la determinación del incidente relacionado con las TIC como grave y a su posterior notificación. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, los criterios de clasificación que hayan dado lugar a la determinación del incidente relacionado con las TIC como grave para al menos una de las entidades financieras.	Sí	Sí	Sí	Opciones (selección múltiple): — clientes, contrapartes financieras y transacciones afectados; — repercusión en la reputación; — duración del incidente y duración de la interrupción del servicio; — extensión geográfica; — pérdidas de datos; — servicios esenciales afectados; — consecuencias económicas.
2.6.	Umbrales de importancia para el criterio de clasificación «Distribución geográfica»	Estados miembros del EEE afectados por el incidente grave relacionado con las TIC. Al evaluar la repercusión del incidente grave relacionado con las TIC en otros Estados miembros, las entidades financieras tendrán en cuenta los artículos 4 y 12 del Reglamento Delegado (UE) 2024/1772.	Sí, si se alcanza el umbral de «Extensión geográfica».	Sí, si se alcanza el umbral de «Extensión geográfica».	Sí, si se alcanza el umbral de «Extensión geográfica».	La opción (selección múltiple) que corresponda se indicará utilizando los códigos conforme a la norma ISO 3166 alfa-2 de los países afectados.

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
2.7.	Descubrimiento del incidente grave relacionado con las TIC	Indicación de cómo se ha descubierto el incidente grave relacionado con las TIC.	Sí	Sí	Sí	Opciones: — seguridad informática; — personal; — auditoría interna; — auditoría externa; — clientes; — contrapartes financieras; — proveedor tercero; — atacante; — sistemas de control; — autoridad/agencia/autoridad policial; — otros.
2.8.	Indicación de si el incidente tiene su origen en un proveedor tercero u otra entidad financiera	Indicación de si el incidente grave relacionado con las TIC procede de un proveedor tercero u otra entidad financiera. Las entidades financieras indicarán si el incidente grave relacionado con las TIC tiene su origen en un proveedor tercero u otra entidad financiera (incluidas las entidades financieras pertenecientes al mismo grupo que la entidad informadora) y el nombre, el código de identificación del proveedor tercero o la entidad financiera y el tipo de código de identificación (por ejemplo, LEI o EUID).	Sí, si el incidente procede de un proveedor tercero u otra entidad financiera	Sí, si el incidente procede de un proveedor tercero u otra entidad financiera	Sí, si el incidente procede de un proveedor tercero u otra entidad financiera	Alfanumérico
2.9.	Activación del plan de continuidad de la actividad, si se activa	Indicación de si ha habido una activación formal de las medidas de respuesta de continuidad de la actividad de la entidad financiera.	Sí	Sí	Sí	Booleano (sí o no)
2.10.	Otros datos de interés	Cualquier otra información no incluida en la plantilla. Las entidades financieras que hayan reclasificado un incidente grave relacionado con las TIC como no grave describirán las razones por las que este no cumple ni se espera que cumpla los criterios para ser considerado un incidente grave relacionado con las TIC.	Sí, si hay otra información no incluida en la plantilla o si el incidente	Sí, si hay otra información no incluida en la plantilla o si el incidente grave	Sí, si hay otra información no incluida en la plantilla o si el	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		grave relacionado con las TIC se ha reclasificado como no grave.	relacionado con las TIC se ha reclasificado como no grave.	incidente grave relacionado con las TIC se ha reclasificado como no grave	
Contenido del informe intermedio					
3.1. Código de referencia del incidente facilitado por la autoridad competente	Código de referencia único asignado por la autoridad competente en el momento de la recepción de la notificación inicial para identificar inequívocamente el incidente grave relacionado con las TIC.	No	Sí, si procede.	Sí, si procede	Alfanumérico
3.2. Fecha y hora en que se produjo el incidente	Fecha y hora en que se produjo el incidente grave relacionado con las TIC, si es diferente del momento en que la entidad financiera tuvo conocimiento de este. En el caso de los incidentes graves relacionados con las TIC recurrentes, fecha y hora en que se produjera el último de ellos.	No	Sí	Sí	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)
3.3. Fecha y hora en que se han recuperado los servicios, actividades u operaciones	Información sobre la fecha y hora de recuperación de los servicios, actividades u operaciones afectados por el incidente grave relacionado con las TIC.	No	Sí, si se ha cumplimentado el campo de datos 3.16, «Duración de la interrupción del servicio».	Sí, si se ha cumplimentado el campo de datos 3.16, «Duración de la interrupción del servicio».	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)
3.4. Número de clientes afectados	Número de clientes afectados por el incidente grave relacionado con las TIC que utilizan el servicio prestado por la entidad financiera. Al evaluar el número de clientes afectados, las entidades financieras tendrán en cuenta el artículo 1, apartado 1, y el artículo 9, apartado 1, letra b), del Reglamento Delegado (UE) 2024/1772 en su evaluación. Las entidades financieras que no puedan determinar el número real de clientes afectados utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el número total de clientes afectados de todas las entidades financieras.	No	Sí	Sí	Número entero

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.5.	Porcentaje de clientes afectados	Porcentaje de clientes afectados por el incidente grave relacionado con las TIC respecto al número total de clientes que hacen uso del servicio prestado por la entidad financiera afectado. En caso de que haya más de un servicio afectado, los servicios se indicarán de forma agregada. Las entidades financieras tendrán en cuenta el artículo 1, apartado 1, y el artículo 9, apartado 1, letra a), del Reglamento Delegado (UE) 2024/1772 en su evaluación. Las entidades financieras que no puedan determinar el porcentaje real de clientes afectados utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, la entidad financiera dividirá la suma de todos los clientes afectados por el número total de clientes de todas las entidades financieras afectadas.	No	Sí	Sí	Expresado como porcentaje, cualquier valor de hasta cinco caracteres numéricos, incluido hasta un decimal (por ejemplo, 2,4 en lugar de 2,4 %). Si el valor tiene más de un dígito después del decimal, las contrapartes notificantes redondearán hacia arriba.
3.6.	Número de contrapartes financieras afectadas	Número de contrapartes financieras afectadas por el incidente grave relacionado con las TIC que han celebrado un contrato con la entidad financiera. Al evaluar el número de contrapartes financieras afectadas, las entidades financieras tendrán en cuenta el artículo 1, apartado 2, del Reglamento Delegado (UE) 2024/1772 en su evaluación. Las entidades financieras que no puedan determinar el número real de contrapartes financieras afectadas utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el número total de contrapartes financieras afectadas en todas las entidades financieras.	No	Sí	Sí	Número entero

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.7.	Porcentaje de contrapartes financieras afectadas	Porcentaje de contrapartes financieras afectadas por el incidente grave relacionado con las TIC respecto al número total de contrapartes financieras que han celebrado un contrato con la entidad financiera. Al evaluar el porcentaje de contrapartes financieras afectadas, las entidades financieras tendrán en cuenta el artículo 1, apartado 1, y el artículo 9, apartado 1, letra c), del Reglamento Delegado (UE) 2024/1772 en su evaluación. Las entidades financieras que no puedan determinar el porcentaje real de contrapartes financieras afectadas utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, indíquese la suma de todas las contrapartes financieras afectadas dividida por el número total de contrapartes financieras de todas las entidades financieras afectadas.	No	Sí	Sí	Expresado como porcentaje, cualquier valor de hasta cinco caracteres numéricos, incluido hasta un decimal (por ejemplo, 2,4 en lugar de 2,4 %). Si el valor tiene más de un dígito después del decimal, las contrapartes notificantes redondearán hacia arriba.
3.8.	Repercusión en los clientes o las contrapartes financieras pertinentes	Cualquier repercusión detectada en los clientes o las contrapartes financieras pertinentes a que se refieren el artículo 1, apartado 3, y el artículo 9, apartado 1, letra f), del Reglamento Delegado (UE) 2024/1772.	No	Sí, si se alcanza el umbral de «Pertinencia de los clientes y las contrapartes financieras»	Sí, si se alcanza el umbral de «Pertinencia de los clientes y las contrapartes financieras»	Booleano (sí o no)
3.9.	Número de transacciones afectadas	Número de transacciones afectadas por el incidente grave relacionado con las TIC. Al evaluar la repercusión en las transacciones, las entidades financieras tendrán en cuenta el artículo 1, apartado 4, del Reglamento Delegado (UE) 2024/1772, incluidas todas las transacciones nacionales y transfronterizas afectadas que contengan un importe monetario y que se hayan llevado a cabo al menos parcialmente en la Unión.	No	Sí, si alguna transacción se ha visto afectada por el incidente.	Sí, si alguna transacción se ha visto afectada por el incidente	Número entero

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		Las entidades financieras que no puedan determinar el número real de transacciones afectadas utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, indíquese el número total de transacciones afectadas en todas las entidades financieras.				
3.10.	Porcentaje de transacciones afectadas	Porcentaje de transacciones afectadas en relación con el número medio diario de transacciones nacionales y transfronterizas realizadas por la entidad financiera en relación con el servicio afectado. Las entidades financieras tendrán en cuenta el artículo 1, apartado 4, y el artículo 9, apartado 1, letra d), del Reglamento Delegado (UE) 2024/1772. Las entidades financieras que no puedan determinar el porcentaje real de transacciones afectadas utilizarán estimaciones. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, la entidad financiera sumará el número de todas las transacciones afectadas y lo dividirá por el número total de transacciones de todas las entidades financieras afectadas.	No	Sí, si alguna transacción se ha visto afectada por el incidente	Sí, si alguna transacción se ha visto afectada por el incidente	Expresado como porcentaje, cualquier valor de hasta cinco caracteres numéricos, incluido hasta un decimal (por ejemplo, 2,4 en lugar de 2,4 %). Si el valor tiene más de un dígito después del decimal, las contrapartes notificantes redondearán hacia arriba.
3.11.	Valor de las transacciones afectadas	El valor total de las transacciones afectadas por el incidente grave relacionado con las TIC se evaluará de conformidad con el artículo 1, apartado 4, y el artículo 9, apartado 1, letra e), del Reglamento Delegado (UE) 2024/1772. Las entidades financieras que no puedan determinar el valor real de transacciones afectadas utilizarán estimaciones basadas en los datos disponibles de períodos de referencia comparables. Las entidades financieras comunicarán el importe monetario como valor positivo. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, el valor total de las transacciones afectadas de todas las entidades financieras.	No	Sí, si alguna transacción se ha visto afectada por el incidente.	Sí, si alguna transacción se ha visto afectada por el incidente	Monetario Las entidades financieras comunicarán este dato en unidades utilizando una precisión mínima equivalente a miles de unidades (por ejemplo, 2,5 en lugar de 2 500 EUR).

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.12.	Información sobre si las cifras son reales o estimadas, o si no se ha producido ninguna repercusión	Información sobre si los valores comunicados en los campos de datos 3.4 a 3.11 son reales o estimados, o si no se ha producido ninguna repercusión.	No	Sí	Sí	Opciones (selección múltiple): — cifras reales de los clientes afectados; — cifras reales de las contrapartes financieras afectadas; — cifras reales de las transacciones afectadas; — estimaciones de los clientes afectados; — estimaciones de las contrapartes financieras afectadas; — estimaciones de las transacciones afectadas; — ninguna repercusión en los clientes; — ninguna repercusión en las contrapartes financieras; — ninguna repercusión en las transacciones.
3.13.	Repercusión en la reputación	Información sobre la repercusión en la reputación derivada del incidente grave relacionado con las TIC a que se refieren los artículos 2 y 10 del Reglamento Delegado (UE) 2024/1772. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las categorías de repercusión en la reputación que se aplican al menos a una entidad financiera.	No	Sí, si se cumple el criterio «Repercusión en la reputación».	Sí, si se cumple el criterio «Repercusión en la reputación»	Opciones (selección múltiple): — el incidente grave relacionado con las TIC se ha reflejado en los medios de comunicación; — el incidente grave relacionado con las TIC ha dado lugar a quejas reiteradas de distintos clientes o contrapartes financieras sobre servicios de cara al cliente o relaciones comerciales esenciales; — la entidad financiera no podrá cumplir los requisitos reglamentarios, o es probable que no pueda cumplirlos, como consecuencia del incidente grave relacionado con las TIC; — la entidad financiera perderá, o es probable que pierda, clientes o contrapartes financieras como consecuencia del incidente grave relacionado con las TIC, lo que acarreará consecuencias importantes para sus actividades.
3.14.	Información contextual sobre la repercusión en la reputación	Información que describa de qué manera el incidente grave relacionado con las TIC ha afectado o podría afectar a la reputación de la entidad financiera, en particular las infracciones de la legislación, los requisitos reglamentarios no cumplidos, el número de quejas de los clientes, etc.	No	Sí, si se cumple el criterio «Repercusión en la reputación».	Sí, si se cumple el criterio «Repercusión en la reputación».	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	La información contextual incluirá el tipo de medios de comunicación (por ejemplo, medios tradicionales y digitales, blogs, plataformas de emisión en continuo) y la cobertura mediática, incluido el alcance de los medios de comunicación (local, nacional, internacional). La cobertura mediática en este contexto no se referirá a unos cuantos comentarios negativos de seguidores o usuarios de redes sociales. Las entidades financieras indicarán también si la cobertura mediática ha puesto de relieve riesgos significativos para sus clientes en relación con el incidente grave relacionado con las TIC, incluido el riesgo de insolvencia de la entidad financiera o el riesgo de pérdida de fondos. Las entidades financieras también indicarán si han facilitado información a los medios de comunicación que haya servido para informar de manera fiable al público sobre el incidente grave relacionado con las TIC y sus consecuencias. Las entidades financieras también podrán indicar si se ha difundido información falsa en los medios de comunicación sobre el incidente relacionado con las TIC, en particular información basada en la difusión deliberada de información errónea por parte de agentes de riesgo, o información relativa a la degradación del sitio web de la entidad financiera o que refleje dicha degradación.				
3.15. Duración del incidente	Las entidades financieras medirán la duración del incidente grave relacionado con las TIC desde el momento en que se haya producido hasta el momento en que se haya resuelto. Las entidades financieras que no puedan determinar el momento en que se haya producido el incidente grave relacionado con las TIC medirán su duración o bien desde el momento en que lo hayan detectado, o bien desde el momento en que lo hayan reflejado en registros de redes o sistemas o en otras fuentes de datos, en caso de que esto se haya producido antes de su detección. Las entidades financieras que aún no sepan cuándo se va a resolver el incidente grave relacionado con las TIC realizarán estimaciones. El valor se expresará en días, horas y minutos. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las entidades financieras indicarán la duración más larga del incidente grave relacionado con las TIC en caso de haber diferencias entre las entidades financieras.	No	Sí	Sí	DD: HH: MM

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.16.	Duración de la interrupción del servicio	Duración de la interrupción del servicio medida desde el momento en que el servicio no esté total o parcialmente disponible 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 grave relacionado con las TIC. Cuando la interrupción del servicio provoque retrasos en la prestación del servicio después de que se hayan restablecido las actividades u operaciones regulares, las entidades financieras medirán su duración desde el inicio del incidente grave relacionado con las TIC hasta el momento en que se preste el servicio que haya sufrido un retraso. Las entidades financieras que no puedan determinar el momento en que se haya iniciado la interrupción del servicio medirán su duración desde el momento en que se haya detectado el incidente o desde el momento en que se haya registrado, en caso de que esto se haya producido antes de su detección. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las entidades financieras indicarán la duración más larga de la interrupción del servicio en caso de haber diferencias entre las entidades financieras.	No	Sí, si el incidente ha provocado una interrupción del servicio.	Sí, si el incidente ha provocado una interrupción del servicio	DD: HH: MM
3.17.	Información sobre si las cifras correspondientes a la duración del incidente y a la duración de la interrupción del servicio son reales o estimadas.	Información sobre si los valores comunicados en los campos de datos 3.15 y 3.16 son reales o estimados.	No	Sí, si se cumple el criterio «Duración del incidente y duración de la interrupción del servicio».	Sí, si se cumple el criterio de «Duración del incidente y a la duración de la interrupción del servicio»	Opciones: — cifras reales; — estimaciones; — cifras reales y estimaciones; — no hay información disponible.
3.18.	Tipos de repercusiones en los Estados miembros	Tipos de repercusiones en los respectivos Estados miembros del EEE. Indicación de si el incidente grave relacionado con las TIC ha tenido repercusiones en otros Estados miembros del EEE (distintos del Estado miembro de la autoridad competente a la que se haya notificado directamente el incidente), de conformidad con el artículo 4 del Reglamento Delegado (UE) 2024/1772, y en particular la importancia de dichas repercusiones en lo que respecta a: a) los clientes y las contrapartes financieras afectados de otros Estados miembros; o	No	Sí, si se alcanza el umbral de «Extensión geográfica».	Sí, si se alcanza el umbral de «Extensión geográfica»	Opciones (selección múltiple): — clientes; — contrapartes financieras; — sucursal de la entidad financiera; — entidades financieras del grupo que lleven a cabo actividades en el Estado miembro en cuestión; — infraestructuras de los mercados financieros — proveedores terceros que pueden ser comunes a otras entidades financieras.

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		b) las sucursales u otras entidades financieras del grupo que lleven a cabo actividades en otros Estados miembros; o c) las infraestructuras de los mercados financieros o los proveedores terceros que puedan afectar a entidades financieras de otros Estados miembros a las que prestan servicios.				
3.19.	Descripción de la repercusión del incidente en otros Estados miembros	Descripción de la repercusión y la gravedad del incidente grave relacionado con las TIC en cada Estado miembro afectado, incluida una evaluación de la repercusión y la gravedad en relación con: a) clientes; b) contrapartes financieras; c) sucursales de la entidad financiera; d) otras entidades financieras del grupo que lleven a cabo actividades en el respectivo Estado miembro; e) infraestructuras de los mercados financieros; f) proveedores terceros que puedan ser comunes a otras entidades financieras, según proceda en otros Estados miembros.	No	Sí, si se alcanza el umbral de «Extensión geográfica»	Sí, si se alcanza el umbral de «Extensión geográfica»	Alfanumérico
3.20.	Umbrales de importancia para el criterio de clasificación «Pérdidas de datos»	Tipos de pérdidas de datos que el incidente grave relacionado con las TIC acarree, en relación con la disponibilidad, la autenticidad, la integridad y la confidencialidad de los datos. Las entidades financieras tendrán en cuenta los artículos 5 y 13 del Reglamento Delegado (UE) 2024/1772 en su evaluación. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las pérdidas de datos que afecten al menos a una entidad financiera.	No	Sí, si se cumple el criterio «Pérdidas de datos».	Sí, si se cumple el criterio «Pérdidas de datos»	Opciones (selección múltiple): — disponibilidad; — autenticidad; — integridad; — confidencialidad.
3.21.	Descripción de las pérdidas de datos	Descripción de la repercusión del incidente grave relacionado con las TIC en la disponibilidad, autenticidad, integridad y confidencialidad de los datos esenciales, de conformidad con los artículos 5 y 13 del Reglamento Delegado (UE) 2024/1772. Información sobre la repercusión en la consecución de los objetivos empresariales de la entidad financiera o en el cumplimiento de los requisitos reglamentarios. Como parte de la información facilitada, las entidades financieras indicarán si los datos afectados son datos de clientes, datos de otras entidades (por ejemplo, contrapartes financieras) o datos de la propia entidad financiera.	No	Sí, si se cumple el criterio «Pérdidas de datos»	Sí, si se cumple el criterio «Pérdidas de datos»	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	La entidad financiera también puede indicar el tipo de datos afectados por el incidente, en particular, si los datos son confidenciales y de qué tipo de confidencialidad se trata (por ejemplo, secreto comercial, datos personales, secreto profesional: secreto bancario, secreto de los seguros, secreto de los servicios de pago, etc.). La información también puede incluir posibles riesgos asociados a las pérdidas de datos, por ejemplo, si los datos afectados por el incidente pueden utilizarse para identificar a personas concretas y si pueden ser utilizados por el agente de riesgo para obtener créditos o préstamos sin su consentimiento, para llevar a cabo ataques de *phishing* personalizado o para divulgar información públicamente. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, una descripción general de las repercusiones del incidente en las entidades financieras afectadas. Cuando existan diferencias entre las repercusiones, su descripción indicará claramente la repercusión específica en las distintas entidades financieras.				
3.22. Criterio de clasificación «Servicios esenciales afectados»	Información relacionada con el criterio «Servicios esenciales afectados». Las entidades financieras tendrán en cuenta el artículo 6 del Reglamento Delegado (UE) 2024/1772 en su evaluación, en particular la información sobre: — los servicios o actividades afectados que requieran una autorización o un registro o que sean supervisados por las autoridades competentes; o — los servicios de TIC o redes y sistemas de información que sustenten funciones esenciales o importantes de la entidad financiera; y — la naturaleza del acceso malintencionado y no autorizado a las redes y sistemas de información de la entidad financiera. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las repercusiones en los servicios esenciales de al menos a una entidad financiera.	No	Sí	Sí	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.23.	Tipo de incidente	Clasificación de los incidentes por tipo.	No	Sí	Sí	Opciones (selección múltiple): — Relacionado con la ciberseguridad — Fallo de proceso — Fallo del sistema — Acontecimiento externo — Relacionado con los pagos — Otros (especifíquense)
3.24.	Otros tipos de incidentes	Otros tipos de incidentes relacionados con las TIC: las entidades financieras que hayan seleccionado «otros» tipos de incidentes en el campo de datos 3.23 especificarán el tipo de incidente relacionado con las TIC.	No	Sí, si se selecciona «otros» tipos de incidentes en el campo de datos 3.23	Sí, si se selecciona «otros» tipos de incidentes en el campo de datos 3.23	Alfanumérico
3.25.	Amenazas y técnicas utilizadas por el agente de riesgo	Indicación de los tipos de amenazas y técnicas utilizadas por el agente de riesgo, como por ejemplo: a) ingeniería social, incluido el *phishing* (ataque por suplantación de identidad); b) ataque (distribuido) de denegación de servicio [(D)DoS]; c) usurpación de identidad; d) cifrado de datos para causar una incidencia, incluido el uso de programas de secuestro (*ransomware*); e) secuestro de recursos; f) exfiltración y manipulación de datos, excluida la usurpación de identidad; g) destrucción de datos; h) degradación; i) ataque a la cadena de suministro; j) otros (especifíquense).	No	Sí, si el tipo de incidente relacionado con las TIC está «relacionado con la ciberseguridad», según el campo 3.23.	Sí, si el tipo de incidente relacionado con las TIC está «relacionado con la ciberseguridad» en el campo 3.23	Opciones (selección múltiple): — ingeniería social (incluido el *phishing*), — (D)DoS, — usurpación de identidad — cifrado de datos para la repercusión, incluidos los programas de secuestro — secuestro de recursos, — exfiltración y manipulación de datos, incluida la usurpación de identidad, — destrucción de datos, — degradación, — ataque a la cadena de suministro, — otros (especifíquense).
3.26.	Otros tipos de técnicas	Otros tipos de técnicas Las entidades financieras que hayan seleccionado «otros» tipos de técnicas en el campo de datos 3.25 especificarán el tipo de técnica.	No	Sí, si se selecciona «otros» tipos de técnicas en el campo de datos 3.25	Sí, si se selecciona «otros» tipos de técnicas en el campo de datos 3.25	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.27. Información sobre las áreas funcionales y los procesos empresariales afectados	Indicación de las áreas funcionales y los procesos empresariales afectados por el incidente, incluidos los productos y servicios. Entre las áreas funcionales figurarán las siguientes: a) comercialización y desarrollo económico; b) servicio al cliente; c) gestión de productos; d) cumplimiento de la normativa; e) gestión de riesgos; f) finanzas y contabilidad; g) recursos humanos y servicios generales; h) tecnologías de la información; Entre los procesos empresariales figurarán los siguientes: — información sobre cuentas; — servicios actuariales; — adquisición de operaciones de pago; — autenticación/autorización; — autoridad — incorporación de clientes; — administración de prestaciones; — gestión del pago de prestaciones; — compra y venta de paquetes de pólizas de seguros entre seguros; — pagos con tarjeta; — gestión de efectivo; — colocación o retirada de efectivo; — gestión de créditos de seguros; — seguro de tramitación de siniestros; — compensación; — conglomerados de préstamos a empresas; — seguros colectivos; — operaciones de transferencia; — custodia de activos; — incorporación de clientes; — ingesta de datos; — tratamiento de datos; — adeudos domiciliados; — seguros de exportación; — finalización de operaciones/acuerdos; — colocación de instrumentos financieros; — contabilidad del fondo;	No	Sí	Sí	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	— dinero en divisas; — asesoramiento en materia de inversión; — gestión de inversiones; — emisión de instrumentos de pago; — gestión de préstamos; — proceso de pago de seguros de vida; — envío de dinero; — cálculo del activo neto; — órdenes; — iniciación de pagos; — suscripción de seguros; — gestión de cartera; — cobro de primas; — recepción/transmisión/ejecución; — reaseguros; — liquidación; — supervisión de las transacciones. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las áreas funcionales y los procesos empresariales afectados en al menos una entidad financiera.				
3.28. Componentes de la infraestructura afectados que apoyan los procesos empresariales	Información sobre si los componentes de la infraestructura (servidores, sistemas operativos, *software*, servidores de aplicación, *middleware*, componentes de red, otros) que apoyan los procesos empresariales se han visto afectados por el incidente grave relacionado con las TIC.	No	Sí	Sí	Opciones: — Sí — No — No se dispone de la información
3.29. Información sobre los componentes de la infraestructura afectados que apoyan los procesos empresariales	Descripción de las repercusiones del incidente grave relacionado con las TIC en los componentes de la infraestructura que apoyan los procesos empresariales, incluidos el *hardware* y el *software*. El *hardware* abarca servidores, ordenadores, centros de datos, conmutadores, encaminadores y concentradores. El *software* abarca sistemas operativos, aplicaciones, bases de datos, herramientas de seguridad, componentes de red y otros componentes (especifíquense). Las descripciones explicarán o nombrarán los componentes o sistemas de la infraestructura afectados e incluirán, cuando esté disponible: a) información sobre la versión; b) la infraestructura interna/parcialmente externalizada/totalmente externalizada (nombre del proveedor tercero);	No	Sí, si el incidente ha afectado a los componentes de la infraestructura que apoyan los procesos empresariales.	Sí, si el incidente ha afectado a los componentes de la infraestructura que apoyan los procesos empresariales	Alfanumérico

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		c) si la infraestructura se utiliza o comparte entre múltiples funciones empresariales; d) disposiciones pertinentes en materia de resiliencia/continuidad/recuperación/sustituibilidad en vigor.				
3.30.	Repercusiones en los intereses financieros de los clientes	Información sobre si el incidente grave relacionado con las TIC ha afectado a los intereses financieros de los clientes.	No	Sí	Sí	Opciones: — Sí — No — No se dispone de la información
3.31.	Notificación a otras autoridades	Especificación de qué autoridades han sido informadas sobre el incidente grave relacionado con las TIC. Teniendo en cuenta las diferencias que se derivan de la legislación nacional de los Estados miembros, las entidades financieras interpretarán el concepto de autoridades policiales en sentido amplio para incluir a las autoridades públicas facultadas para perseguir la ciberdelincuencia, entre ellas la Policía, las fuerzas y cuerpos de seguridad y los fiscales.	No	Sí	Sí	Opciones (selección múltiple): — Policía/Fuerzas o cuerpos de seguridad — Equipo de respuesta a incidentes de seguridad informática (CSIRT) — Autoridad de protección de datos personales — Agencia Nacional de Ciberseguridad — Ninguna — Otras (especifíquense)
3.32.	Especificación de «otras» autoridades	Especificación de los otros tipos de autoridades que fueron informadas sobre el incidente grave relacionado con las TIC. Si se selecciona en el campo de datos 3.31. En caso de seleccionarse «otras», la descripción incluirá información más detallada sobre la autoridad a la que la entidad financiera haya presentado información sobre el incidente grave relacionado con las TIC.	No	Sí, si la entidad financiera ha informado a otro tipo de autoridades sobre el incidente grave relacionado con las TIC.	Sí, si la entidad financiera ha informado a otro tipo de autoridades sobre el incidente grave relacionado con las TIC.	Alfanumérico
3.33.	Acciones/medidas temporales adoptadas o previstas para recuperarse del incidente	Indicación de si la entidad financiera ha aplicado (o tiene previsto aplicar) alguna medida temporal que se haya adoptado (o se prevea adoptar) para recuperarse del incidente grave relacionado con las TIC.	No	Sí	Sí	Booleano (sí o no)

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
3.34.	Descripción de las acciones y medidas temporales adoptadas o previstas para recuperarse del incidente	La información describirá las medidas inmediatas adoptadas, como el aislamiento del incidente a nivel de red, los procedimientos alternativos activados, los puertos USB bloqueados, el centro de recuperación en caso de catástrofe activado y cualquier otro control de seguridad adicional establecido temporalmente. Las entidades financieras indicarán la fecha y la hora de ejecución de las acciones temporales y la fecha prevista de retorno al centro primario. En el caso de las acciones temporales que aún no se hayan ejecutado, sino que estén previstas, indicación de la fecha en que se espera su ejecución. Si no se han emprendido medidas o acciones temporales, indíquese el motivo.	No	Sí, si se han adoptado acciones o medidas temporales o está previsto que se adopten (campo de datos 3.33)	Sí, si se han adoptado acciones o medidas temporales o está previsto que se adopten (campo de datos 3.33)	Alfanumérico
3.35.	Indicadores de compromiso	Información relativa al incidente grave relacionado con las TIC que pueda ayudar a detectar actividades malintencionadas dentro de una red o sistema de información (indicadores de compromiso), cuando proceda. Este campo se aplica únicamente a las entidades financieras que entran en el ámbito de aplicación de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([1]) y a las entidades financieras identificadas como entidades esenciales o importantes con arreglo a las normas nacionales de transposición del artículo 3 de la Directiva (UE) 2022/2555, cuando proceda. Los indicadores de compromiso proporcionados por la entidad financiera incluirán las siguientes categorías de datos: a) direcciones IP; b) direcciones URL; c) ámbitos; d) resúmenes criptográficos de archivos; e) datos de programas maliciosos (nombre de los programas maliciosos, nombres de archivos y su ubicación, claves de registro específicas asociadas a la actividad de programas maliciosos); f) datos de actividad de la red (puertos, protocolos, direcciones, *referrers*, agentes del usuario, encabezamientos, registros específicos o patrones distintivos en el tráfico de red); g) datos del mensaje de correo electrónico (remitente, destinatario, asunto, encabezamiento, contenido);	No	Sí, si se selecciona «relacionado con la ciberseguridad» como tipo de incidente en el campo de datos 3.23.	Sí, si se selecciona «relacionado con la ciberseguridad» como tipo de incidente en el campo de datos 3.23.	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	h) solicitudes de DNS y configuraciones de registro; i) actividades relacionadas con cuentas de usuarios (conexiones, actividad de cuenta de usuario privilegiada, escalada de privilegios); j) tráfico de la base de datos (lectura/escritura), solicitudes al mismo archivo. En la práctica, este tipo de información puede incluir datos relativos, entre otras cosas, a indicadores que describan patrones en el tráfico de la red correspondientes a ataques o comunicaciones de redes de ordenadores esclavos conocidos, direcciones IP de máquinas infectadas con programas maliciosos (*bots*), datos relativos a servidores de «mando y control» utilizados por programas maliciosos (normalmente dominios o direcciones IP) y URL relativas a sitios de *phishing* o sitios web en los que se haya observado el alojamiento de programas maliciosos o kits de programas intrusos.				
Contenido del informe final					
4.1. Clasificación de alto nivel de las causas profundas del incidente	Clasificación general de las causas subyacentes del incidente grave relacionado con las TIC según el tipo de incidente, de tal manera que figuren, entre otras, las siguientes categorías generales: a) acciones malintencionadas; b) fallo de proceso; c) fallo/mal funcionamiento del sistema; d) error humano; e) evento externo.	No	No	Sí	Opciones (selección múltiple): — acciones malintencionadas; — fallo de proceso; — fallo/mal funcionamiento del sistema; — error humano; — evento externo.
4.2. Clasificación detallada de las causas profundas del incidente	Clasificación detallada de las causas subyacentes del incidente grave relacionado con las TIC según el tipo de incidente, de tal manera que figuren, entre otras, las siguientes categorías detalladas vinculadas a las categorías generales que se hayan notificado en el campo de datos 4.1: 1. **Acciones malintencionadas** (si se selecciona, elegir una o varias de las opciones siguientes): a) acciones internas deliberadas; b) daños físicos, manipulación o robo deliberados; c) acciones fraudulentas. 2. **Fallo de proceso** (si se selecciona, elegir una o varias de las opciones siguientes): a) supervisión insuficiente o fallo de la supervisión y el control;	No	No	Sí	Opciones (selección múltiple): — acciones malintencionadas: acciones internas deliberadas; — acciones malintencionadas: daños físicos, manipulación o robo deliberados; — acciones malintencionadas: acciones fraudulentas; — fallo de proceso: supervisión insuficiente o fallo de la supervisión y el control; — fallo de proceso: funciones y responsabilidades insuficientes o poco claras; — fallo de proceso: fallo del proceso de gestión del riesgo relacionado con las TIC; — fallo de proceso: insuficiencia o fracaso de las operaciones de TIC y de las operaciones relativas a la seguridad de estas;

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	b) funciones y responsabilidades insuficientes o poco claras; c) fallo del proceso de gestión del riesgo relacionado con las TIC; d) insuficiencia o fracaso de las operaciones de TIC y de las operaciones relativas a la seguridad de estas; e) insuficiencia o fracaso de la gestión de proyectos relacionados con las TIC; f) políticas, procedimientos y documentación internos inadecuados; g) adquisición, desarrollo o mantenimiento inadecuados de los sistemas de TIC; h) otros (especifíquense). 3. **Fallo/mal funcionamiento del sistema** (si se selecciona, elegir una o varias de las opciones siguientes): a) capacidad y rendimiento del *hardware*: incidentes graves relacionados con las TIC causados por recursos del *hardware* que resulten inadecuados en términos de capacidad o rendimiento para cumplir los requisitos legislativos aplicables; b) mantenimiento del *hardware*: incidentes graves relacionados con las TIC derivados de un mantenimiento inadecuado o insuficiente de los componentes del *hardware*, distintos de la obsolescencia o la antigüedad de este; c) obsolescencia/antigüedad del *hardware*: este tipo de causa subyacente acarrea incidentes graves relacionados con las TIC derivados de componentes del *hardware* que estén obsoletos o hayan envejecido; d) compatibilidad/configuración del *software*: incidentes graves relacionados con las TIC causados por componentes del *software* incompatibles con otras configuraciones de *software* o sistemas, incluidos los incidentes graves relacionados con las TIC derivados de conflictos de *software*, ajustes incorrectos o parámetros mal configurados que afecten a la funcionalidad general del sistema; e) rendimiento del *software*: incidentes graves relacionados con las TIC derivados de componentes de *software* que presenten un rendimiento deficiente o ineficiencias por razones distintas de las especificadas en el apartado «Compatibilidad/configuración del *software*», incluidos los incidentes graves relacionados con las TIC causados por tiempos de respuesta lentos, un consumo excesivo de recursos o una ejecución ineficiente de las consultas que afecten al rendimiento del *software* o del sistema;				— fallo de proceso: insuficiencia o fracaso de la gestión de proyectos relacionados con las TIC; — fallo de proceso: políticas, procedimientos y documentación internos inadecuados; — fallo de proceso: adquisición, desarrollo y mantenimiento inadecuados de los sistemas de TIC; — fallo de proceso: otros (especifíquense); — fallo del sistema: capacidad y rendimiento del *hardware*; — fallo del sistema: mantenimiento del *hardware*; — fallo del sistema: obsolescencia/antigüedad del *hardware*; — fallo del sistema: compatibilidad/configuración del *software*; — fallo del sistema: rendimiento del *software*; — fallo del sistema: configuración de red; — fallo del sistema: daños físicos; — fallo del sistema: otros (especifíquense); — error humano: omisión; – — error humano: error; — error humano: capacidades y conocimientos; — error humano: recursos humanos inadecuados; — error humano: problemas de comunicación; — error humano: otros (especifíquense); — evento externo: catástrofes naturales/fuerza mayor; — evento externo: fallos de terceros; — evento externo: otros (especifíquense).

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	f) configuración de red: incidentes graves relacionados con las TIC derivados de ajustes o infraestructuras de la red incorrectos o mal configurados, incluidos los incidentes graves relacionados con las TIC causados por errores de configuración de la red, problemas de encaminamiento, configuraciones incorrectas de cortafuegos u otros problemas relacionados con la red que afecten a la conectividad o la comunicación; g) daños físicos: incidentes graves relacionados con las TIC causados por daños físicos a la infraestructura de TIC que den lugar a fallos del sistema; h) otros (especifíquense). 4. **Error humano** (si se selecciona, elegir una o varias de las opciones siguientes): a) omisión (involuntaria); b) error; c) capacidades y conocimientos: incidentes graves relacionados con las TIC derivados de una falta de conocimientos especializados o de competencias en la gestión de sistemas o procesos de TIC que puedan deberse a una formación inadecuada, a conocimientos insuficientes o a lagunas en las capacidades necesarias para llevar a cabo tareas específicas o hacer frente a retos técnicos; d) recursos humanos inadecuados: incidentes graves relacionados con las TIC causados por la falta de recursos necesarios, como *hardware*, *software*, infraestructura o personal, incluidas aquellas situaciones en las que la insuficiencia de recursos da lugar a ineficiencias operativas, fallos del sistema o incapacidad para satisfacer las demandas de las empresas; e) problemas de comunicación; f) otros (especifíquense). 5. **Hecho externo** (si se selecciona, elegir una o varias de las opciones siguientes): a) catástrofes naturales/fuerza mayor; b) fallos de terceros;				

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	c) otros (especifíquense). Las entidades financieras considerarán que, en el caso de los incidentes graves relacionados con las TIC recurrentes, se tiene en cuenta la aparente causa subyacente específica del incidente y no las categorías generales incluidas en este campo.				
4.3. Clasificación adicional de las causas profundas del incidente	Clasificación adicional de las causas subyacentes del incidente grave relacionado con las TIC según el tipo de incidente, de tal manera que figuren, entre otras, las siguientes categorías de clasificación adicionales vinculadas a las categorías detalladas que se notifican en el campo de datos 4.2. El campo es obligatorio para el informe final si en el campo de datos 4.2 se indican categorías específicas que requieren un mayor nivel de detalle. 2 **a) Insuficiencia o fallo de la supervisión y el control:** a) seguimiento del cumplimiento de las políticas; b) supervisión de proveedores terceros de servicios de TIC; c) seguimiento y verificación de la subsanación de las vulnerabilidades; d) gestión de la identidad y del acceso; e) cifrado y criptografía; f) registro. 2 **c) Fallo del proceso de gestión del riesgo relacionado con las TIC:** a) incumplimiento de la especificación de niveles exactos de tolerancia al riesgo; b) evaluaciones insuficientes de la vulnerabilidad y las amenazas; c) medidas inadecuadas de tratamiento del riesgo; d) gestión deficiente de los riesgos residuales relacionados con las TIC. 2 **d) Insuficiencia o fracaso de las operaciones de TIC y de las operaciones relativas a la seguridad de estas:** a) gestión de las vulnerabilidades y los parches; b) gestión de los cambios; c) gestión de la capacidad y el rendimiento; d) gestión de activos de TIC y clasificación de la información;	No	No	Sí	Opciones (selección múltiple): — seguimiento del cumplimiento de las políticas; — supervisión de proveedores terceros de servicios de TIC; — seguimiento y verificación de la subsanación de las vulnerabilidades; — gestión de la identidad y del acceso; — cifrado y criptografía; — registro; — incumplimiento de la especificación de niveles exactos de tolerancia al riesgo; — evaluaciones insuficientes de la vulnerabilidad y las amenazas; — medidas inadecuadas de tratamiento del riesgo; — gestión deficiente de los riesgos residuales relacionados con las TIC; — gestión de las vulnerabilidades y los parches; — gestión de los cambios; — gestión de la capacidad y el rendimiento; — gestión de activos de TIC y clasificación de la información; — copia de seguridad y restablecimiento; — gestión de errores; — adquisición, desarrollo y mantenimiento inadecuados de los sistemas de TIC; — pruebas insuficientes del *software* o fallo de estas.

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
		e) copia de seguridad y restablecimiento; f) gestión de errores. 2 **g) Adquisición, desarrollo y mantenimiento inadecuados de los sistemas de TIC:** a) adquisición, desarrollo y mantenimiento inadecuados de los sistemas de TIC; b) pruebas insuficientes del *software* o fallo de estas.				
4.4.	Otros tipos de causas profundas	Las entidades financieras que hayan seleccionado «otros» tipos de causas subyacentes en el campo de datos 4.2 especificarán los otros tipos de causas subyacentes.	No	No	Sí, si se selecciona «otros» tipos de causas subyacentes en el campo de datos 4.2.	Alfanumérico
4.5.	Información sobre las causas profundas del incidente	Descripción de la secuencia de hechos que han dado lugar al incidente grave relacionado con las TIC y descripción de cómo dicho incidente tiene aparentemente una causa subyacente similar si se clasifica como incidente recurrente, incluida una descripción concisa de todas las razones subyacentes y de los principales factores que han contribuido a que se produzca el incidente grave relacionado con las TIC. Cuando se hayan producido acciones malintencionadas, descripción del *modus operandi* de dichas acciones, incluidas las tácticas, técnicas y procedimientos utilizados, así como el vector de entrada del incidente grave relacionado con las TIC, incluida una descripción de las investigaciones y el análisis que hayan conducido a la determinación de las causas subyacentes, si procede.	No	No	Sí	Alfanumérico
4.6.	Resolución de incidentes	Información adicional sobre las acciones/medidas emprendidas o previstas para resolver de forma permanente el incidente grave relacionado con las TIC y evitar que este vuelva a producirse. Experiencia adquirida a partir del incidente grave relacionado con las TIC.	No	No	Sí	Alfanumérico

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	La descripción contendrá los siguientes puntos: 1. **Descripción de las acciones de resolución** a) acciones emprendidas para resolver de forma permanente el incidente grave relacionado con las TIC (sin incluir las medidas temporales); b) para cada acción adoptada, indíquese la posible participación de un proveedor tercero y de la entidad financiera; c) indíquese si los procedimientos se han adaptado a raíz del incidente grave relacionado con las TIC; d) indíquense los controles adicionales que se hayan puesto en marcha o que estén previstos con el correspondiente calendario de aplicación. Posibles problemas detectados en relación con la solidez de los sistemas informáticos afectados o en lo que se refiere a los procedimientos o controles existentes, si procede. Las entidades financieras indicarán claramente cómo las medidas de subsanación previstas van a abordar las causas subyacentes detectadas y cuándo se espera que el incidente grave relacionado con las TIC se resuelva de forma permanente. 2. **Experiencia adquirida** Las entidades financieras describirán las conclusiones de la revisión realizada tras el incidente.				
4.7. Fecha y hora en que se abordó la causa profunda del incidente	Fecha y hora en que se abordó la causa profunda del incidente.	No	No	Sí	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)
4.8. Fecha y hora en que se resolvió el incidente	Fecha y hora en que se resolvió el incidente.	No	No	Sí	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)

	Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
4.9.	Información si la fecha de resolución permanente de los incidentes difiere de la fecha de aplicación inicialmente prevista	Descripción de la razón por la que la fecha de resolución permanente de los incidentes graves relacionados con las TIC es diferente de la fecha de aplicación inicialmente prevista, cuando proceda.	No	No	Sí	Alfanumérico
4.10.	Evaluación del riesgo para las funciones esenciales a efectos de resolución	Evaluación de si el incidente grave relacionado con las TIC plantea un riesgo para las funciones esenciales en el sentido del artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE del Parlamento Europeo y del Consejo ([2]). Las entidades a que se refiere el artículo 1, apartado 1, de la Directiva 2014/59/UE indicarán si el incidente plantea un riesgo para las funciones esenciales en el sentido del artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE, y según lo notificado en la plantilla Z 07.01 del Reglamento de Ejecución (UE) 2018/1624 de la Comisión ([3]) y asignadas a la entidad correspondiente en la plantilla Z 07.02.	No	No	Sí, si el incidente plantea un riesgo para las funciones esenciales de las entidades financieras en el sentido del artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE.	Alfanumérico
4.11.	Información pertinente para las autoridades de resolución	Descripción de si el incidente grave relacionado con las TIC ha afectado a la resolubilidad de la entidad o del grupo y, en caso afirmativo, de qué manera. Las entidades a que se refiere el artículo 1, apartado 1, de la Directiva 2014/59/UE facilitarán información sobre si el incidente grave relacionado con las TIC ha afectado a la resolubilidad de la entidad o del grupo y, en caso afirmativo, de qué manera. Dichas entidades indicarán también si el incidente grave relacionado con las TIC afecta a la solvencia o liquidez de la entidad financiera y la posible cuantificación de las repercusiones. Dichas entidades también facilitarán información sobre las repercusiones en la continuidad operativa y en la resolubilidad de la entidad, así como cualquier otra repercusión en los costes y pérdidas derivados del incidente grave relacionado con las TIC, incluida la posición de capital de la entidad financiera, y si los acuerdos contractuales sobre el uso de servicios de TIC siguen siendo sólidos y plenamente ejecutables en caso de resolución de la entidad.	No	No	Sí, si el incidente ha afectado a la resolubilidad de la entidad o del grupo.	Alfanumérico

Campo de datos		Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
4.12.	Umbral de importancia para el criterio de clasificación «Consecuencias económicas»	Información detallada sobre los umbrales finalmente alcanzados por el incidente grave relacionado con las TIC en relación con el criterio «Consecuencias económicas» a que se refieren los artículos 7 y 14 del Reglamento Delegado (UE) 2024/1772.	No	No	Sí	Alfanumérico
4.13.	Importe de los costes y pérdidas directos e indirectos brutos	Importe total de los costes y pérdidas directos e indirectos brutos soportados por la entidad financiera como consecuencia del incidente grave relacionado con las TIC, entre ellos: a) el importe de los fondos o los activos financieros expropiados de los que es responsable la entidad financiera; b) el importe de los costes de sustitución o reubicación de *software*, *hardware* o infraestructuras; c) el importe de 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 del personal; d) el importe de los desembolsos por incumplimiento de las obligaciones contractuales; e) el importe de los costes de reparación y de indemnización a los clientes; f) el importe de las pérdidas por lucro cesante; g) el importe de los costes asociados a la comunicación interna y externa; h) el importe de los costes de asesoramiento, incluidos los relacionados con el asesoramiento jurídico, los servicios forenses y los servicios de reparación; i) el importe de otros costes y pérdidas, entre ellos: i) los gastos directos, incluidos los deterioros de valor y los gastos de liquidación, contabilizados en la cuenta de resultados y las depreciaciones debidas al incidente grave relacionado con las TIC; ii) provisiones o reservas contabilizadas en la cuenta de resultados frente a pérdidas probables relacionadas con el incidente grave relacionado con las TIC;	No	No	Sí	Monetario

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	iii) las pérdidas pendientes, en forma de pérdidas derivadas del incidente grave relacionado con las TIC, que se contabilicen de forma temporal en cuentas transitorias y que todavía no se reflejen en la cuenta de resultados, pero que se prevea incluir en un plazo acorde con el tamaño y la antigüedad del elemento pendiente; iv) los ingresos significativos no percibidos, relativos a obligaciones contractuales con terceros, incluida la decisión de compensar a un cliente tras el incidente grave relacionado con las TIC, no mediante reembolso o pago directo, sino a través de un ajuste de los ingresos con arreglo al cual no se cobren honorarios contractuales, o estos se reduzcan, durante un determinado período de tiempo en el futuro; v) las pérdidas por periodificación, cuando abarquen más de un ejercicio contable y generen un riesgo jurídico. Las entidades financieras tendrán en cuenta en su evaluación el artículo 7, apartados 1 y 2, del Reglamento Delegado (UE) 2024/1772. Las entidades financieras no incluirán en esta cifra las recuperaciones financieras de ningún tipo. Las entidades financieras comunicarán el importe monetario como valor positivo. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las entidades financieras tendrán en cuenta el importe total de los costes y pérdidas de todas las entidades financieras. Las entidades financieras comunicarán este dato en unidades utilizando una precisión mínima equivalente a miles de unidades.				
4.14. Importe de las recuperaciones financieras	Importe total de las recuperaciones financieras. Las recuperaciones financieras se referirán a la pérdida original causada por el incidente, independientemente del momento en que se reciban las recuperaciones financieras en forma de fondos o entradas de beneficios económicos.	No	No	Sí	Monetario Las entidades financieras comunicarán el punto de entrada de datos en unidades utilizando una precisión mínima equivalente a miles de unidades

Campo de datos	Descripción	Obligatorio para la notificación inicial	Obligatorio para el informe intermedio	Obligatorio para el informe final	Tipo de campo
	Las entidades financieras comunicarán el importe monetario como valor positivo. En el caso de la notificación agregada a que se refiere el artículo 7 del presente Reglamento, las entidades financieras tendrán en cuenta el importe total de las recuperaciones financieras de todas las entidades financieras.				
4.15. Información sobre si los incidentes no graves han sido recurrentes	Información sobre si más de un incidente no grave relacionado con las TIC ha sido recurrente y, en conjunto, se consideran un incidente grave a efectos del artículo 8, apartado 2, del Reglamento Delegado (UE) 2024/1772. Las entidades financieras indicarán si los incidentes no graves relacionados con las TIC han sido recurrentes y, en conjunto, se consideran un incidente grave relacionado con las TIC. Las entidades financieras indicarán también el número de estos incidentes no graves relacionados con las TIC.	No	No	Sí, si el incidente grave comprende más de un incidente no grave recurrente.	Alfanumérico
4.16. Fecha y hora en que se produjeron los incidentes recurrentes	Cuando las entidades financieras notifiquen incidentes relacionados con las TIC recurrentes, fecha y hora en que se produjera el primero de ellos.	No	No	Sí, en el caso de los incidentes recurrentes.	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)

([1]) 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).

([2]) Directiva 2014/59/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, por la que se establece un marco para la reestructuración y la resolución de entidades y empresas de servicios de inversión, y por la que se modifican la Directiva 82/891/CEE del Consejo y las Directivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE y 2013/36/UE, y los Reglamentos (UE) n.º 1093/2010 y n.º 648/2012 del Parlamento Europeo y del Consejo (DO L 173 de 12.6.2014, p. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Reglamento de Ejecución (UE) 2018/1624 de la Comisión, de 23 de octubre de 2018, por el que se establecen normas técnicas de ejecución en relación con los procedimientos, modelos de formularios y plantillas para la notificación de información a efectos de los planes de resolución para las entidades de crédito y las empresas de servicios de inversión, de conformidad con la Directiva 2014/59/UE del Parlamento Europeo y del Consejo, y por el que se deroga el Reglamento de Ejecución (UE) 2016/1066 de la Comisión (DO L 277 de 7.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ANEXO III

PLANTILLAS PARA LA NOTIFICACIÓN DE CIBERAMENAZAS IMPORTANTES

Número de campo	Campo de datos	
1	Nombre de la entidad que presenta la notificación	
2	Código de identificación de la entidad que presenta la notificación	
3	Tipo de entidad financiera que presenta la notificación	
4	Nombre de la entidad financiera	
5	Código LEI de la entidad financiera	
6	Nombre de la persona de contacto principal	
7	Correo electrónico de la persona de contacto principal	
8	Teléfono de la persona de contacto principal	
9	Nombre de la segunda persona de contacto	
10	Correo electrónico de la segunda persona de contacto	
11	Teléfono de la segunda persona de contacto	
12	Fecha y hora de detección de la ciberamenaza	
13	Descripción de la ciberamenaza importante	
14	Información sobre la posible repercusión	
15	Criterios de clasificación de posibles incidentes	
16	Situación de la ciberamenaza	
17	Medidas adoptadas para evitar la materialización	
18	Notificación a otras partes interesadas	
19	Indicadores de compromiso	
20	Otros datos de interés	

ANEXO IV

GLOSARIO DE DATOS E INSTRUCCIONES PARA LA NOTIFICACIÓN DE CIBERAMENAZAS IMPORTANTES

Campo de datos	Descripción	Campo obligatorio	Tipo de campo
1. Nombre de la entidad que presenta la notificación	Razón social completa de la entidad que presenta la notificación.	Sí	Alfanumérico
2. Código de identificación de la entidad que presenta la notificación	Código de identificación de la entidad que presenta la notificación. Cuando las entidades financieras presenten la notificación o el informe, el código de identificación será un identificador de entidad jurídica (LEI), que es un código único de veinte caracteres alfanuméricos, basado en la norma ISO 17442-1:2020. Cuando un proveedor tercero presente un informe en nombre de una entidad financiera, este podrá utilizar un código de identificación tal como se especifica en las normas técnicas de ejecución adoptadas de conformidad con el artículo 28, apartado 9, del Reglamento (UE) 2022/2554.	Sí	Alfanumérico
3. Tipo de entidad financiera que presenta el informe	Tipo de entidad a que se refiere el artículo 2, apartado 1, letras a) a t), del Reglamento (UE) 2022/2554 que presenta el informe.	Sí, si la entidad financiera afectada no presenta el informe directamente.	Opciones (selección múltiple): — entidad de crédito; — entidad de pago; — entidad de pago exenta; — proveedor de servicios de información sobre cuentas; — entidad de dinero electrónico; — entidad de dinero electrónico exenta; — empresa de servicios de inversión; — proveedor de servicios de criptoactivos; — emisor de fichas referenciadas a activos; — depositario central de valores; — entidad de contrapartida central; — centro de negociación; — registro de operaciones; — gestor de fondos de inversión alternativos; — sociedad de gestión; — proveedor de servicios de suministro de datos;

Campo de datos		Descripción	Campo obligatorio	Tipo de campo
				— empresas de seguros y de reaseguros; — intermediario de seguros, intermediario de reaseguros e intermediario de seguros complementarios; — fondo de pensiones de empleo; — agencia de calificación crediticia; — administrador de índices de referencia cruciales; — proveedor de servicios de financiación participativa; — registro de titulizaciones.
4.	Nombre de la entidad financiera	Razón social completa de la entidad financiera que notifica la ciberamenaza importante.	Sí, si la entidad financiera es diferente de la entidad que presenta la notificación.	Alfanumérico
5.	Código LEI de la entidad financiera	Identificador de entidad jurídica (LEI) de la entidad financiera que notifica la ciberamenaza importante, asignado de conformidad con la Organización Internacional de Normalización.	Sí, si la entidad financiera que notifica la ciberamenaza importante es diferente de la entidad que presenta el informe.	Código único de veinte caracteres alfanuméricos, basado en la norma ISO 17442-1:2020.
6.	Nombre de la persona de contacto principal	Nombre y apellidos de la persona de contacto principal de la entidad financiera.	Sí	Alfanumérico
7.	Correo electrónico de la persona de contacto principal	Dirección de correo electrónico de la persona de contacto principal que puede utilizar la autoridad competente para la comunicación de seguimiento.	Sí	Alfanumérico
8.	Teléfono de la persona de contacto principal	Número de teléfono de la persona de contacto principal que puede utilizar la autoridad competente para la comunicación de seguimiento. Se indicará el número de teléfono con todos los prefijos internacionales (por ejemplo, +33 XXXXXXXXX).	Sí	Alfanumérico
9.	Nombre de la segunda persona de contacto	Nombre y apellidos de la segunda persona de contacto de la entidad financiera o de una entidad que presente la notificación en nombre de la entidad financiera, cuando esté disponible.	Sí, si se dispone del nombre y los apellidos de la segunda persona de contacto de la entidad financiera o de una entidad que presente la notificación en nombre de la entidad financiera.	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de datos	Descripción	Campo obligatorio	Tipo de campo
10. Correo electrónico de la segunda persona de contacto	Dirección de correo electrónico de la segunda persona de contacto o dirección de correo electrónico funcional del equipo que pueda utilizar la autoridad competente para la comunicación de seguimiento, cuando esté disponible.	Sí, si se dispone de la dirección de correo electrónico de la segunda persona de contacto o de una dirección de correo electrónico funcional del equipo que pueda utilizar la autoridad competente para la comunicación de seguimiento.	Alfanumérico
11. Teléfono de la segunda persona de contacto	Número de teléfono de la segunda persona de contacto que puede utilizar la autoridad competente para la comunicación de seguimiento, cuando esté disponible. Se indicará el número de teléfono con todos los prefijos internacionales (por ejemplo, +33 XXXXXXXXX).	Sí, si se dispone del número de teléfono de la segunda persona de contacto que puede utilizar la autoridad competente para la comunicación de seguimiento.	Alfanumérico
12. Fecha y hora de detección de la ciberamenaza	Fecha y hora en que la entidad financiera ha tenido conocimiento de la ciberamenaza importante.	Sí	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)
13. Descripción de la ciberamenaza importante	Descripción de los aspectos más pertinentes de la ciberamenaza importante. Las entidades financieras facilitarán: a) un resumen general de los aspectos más pertinentes de la ciberamenaza importante; b) los riesgos derivados de ello, incluidas las posibles vulnerabilidades de los sistemas de la entidad financiera que puedan explotarse; c) información sobre la probabilidad de materialización de la ciberamenaza importante; y d) detalles sobre la fuente de información relativa a la ciberamenaza.	Sí	Alfanumérico
14. Información sobre la posible repercusión	Información sobre la posible repercusión de la ciberamenaza en la entidad financiera, sus clientes o sus contrapartes financieras si se ha materializado la ciberamenaza.	Sí	Alfanumérico
15. Criterios de clasificación de posibles incidentes	Los criterios de clasificación que podrían haber dado lugar a un informe de incidente grave si se hubiera materializado la ciberamenaza.	Sí	Opciones (selección múltiple): — clientes, contrapartes financieras y transacciones afectados; — repercusión en la reputación; — duración del incidente y duración de la interrupción del servicio; — extensión geográfica; — pérdidas de datos; — servicios esenciales afectados; — consecuencias económicas.

Campo de datos		Descripción	Campo obligatorio	Tipo de campo
16.	Situación de la ciberamenaza	Información sobre la situación de la ciberamenaza para la entidad financiera y si se han producido cambios en la actividad de la amenaza. Cuando la ciberamenaza haya dejado de comunicarse con los sistemas de información de la entidad financiera, la situación puede marcarse como inactiva. Si la entidad financiera dispone de información de que la amenaza sigue estando activa contra otras partes o contra el sistema financiero en su conjunto, la situación se marcará como activa.	Sí	Opciones: — activa — inactiva
17.	Medidas adoptadas para evitar la materialización	Información general sobre las medidas adoptadas por la entidad financiera para evitar la materialización de las ciberamenazas importantes, si procede.	Sí	Alfanumérico
18.	Notificación a otras partes interesadas	Información sobre la notificación de la ciberamenaza a otras entidades financieras o autoridades.	Sí, si otras entidades financieras o autoridades han sido informadas de la ciberamenaza.	Alfanumérico
19.	Indicadores de compromiso	Información relativa a la amenaza importante que pueda ayudar a detectar actividades malintencionadas dentro de una red o sistema de información (indicadores de compromiso), cuando proceda. Los indicadores de compromiso proporcionados por la entidad financiera pueden incluir, entre otras, las siguientes categorías de datos: a) direcciones IP; b) direcciones URL; c) ámbitos; d) resúmenes criptográficos de archivos; e) datos de programas maliciosos (nombre de los programas maliciosos, nombres de archivos y su ubicación, claves de registro específicas asociadas a la actividad de programas maliciosos); f) datos de actividad de la red (puertos, protocolos, direcciones, *referrers*, agentes del usuario, encabezamientos, registros específicos o patrones distintivos en el tráfico de red); g) datos del mensaje de correo electrónico (remitente, destinatario, tema, encabezamiento, contenido); h) Solicitudes de DNS y configuraciones de registro; i) actividades relacionadas con cuentas de usuario (conexiones, actividad de cuenta de usuario privilegiada, escalada de privilegios); j) tráfico de la base de datos (lectura/escritura), solicitudes al mismo archivo. Este tipo de información puede incluir datos relativos a indicadores que describan patrones en el tráfico de la red correspondientes a ataques o comunicaciones *botnet* conocidos, direcciones IP de máquinas infectadas con programas maliciosos (*bots*), datos relativos a servidores de «mando y control» utilizados por programas maliciosos (normalmente dominios o direcciones IP) y URL relativas a sitios de *phishing* o sitios web en los que se haya observado alojamiento de programas maliciosos o kits de programas intrusos.	Sí, si se dispone de información sobre los indicadores de compromiso relacionados con la ciberamenaza.	Alfanumérico
20.	Otros datos de interés	Cualquier otra información pertinente sobre la ciberamenaza importante.	Sí, si procede y si se dispone de más información que no se haya incluido en la plantilla.	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj