# REGLAMENTO DELEGADO (UE) 2025/295 DE LA COMISIÓN

## de 24 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 relativas a la armonización de las condiciones que permiten llevar a cabo las actividades de supervisión

**(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 41, apartado 2, párrafo segundo,

Considerando lo siguiente:

(1) El marco sobre la resiliencia operativa digital del sector financiero establecido por el Reglamento (UE) 2022/2554 introduce un marco de supervisión de la Unión para los proveedores terceros de servicios de tecnologías de la información y la comunicación (TIC) al sector financiero designados como esenciales de conformidad con el artículo 31 de dicho Reglamento.

(2) Un proveedor tercero de servicios de TIC que decida presentar una solicitud de inclusión voluntaria para ser designado como esencial debe proporcionar a la Autoridad Europea de Supervisión (AES) receptora toda la información necesaria para demostrar su carácter esencial con arreglo a los principios y criterios establecidos en el Reglamento (UE) 2022/2554. Por este motivo, la información que debe incluirse en la solicitud de inclusión voluntaria debe ser lo suficientemente detallada y exhaustiva como para permitir una evaluación clara y completa del carácter esencial con arreglo al artículo 31, apartado 11, del citado Reglamento. La AES pertinente debe rechazar cualquier solicitud incompleta y pedir la información que falte.

(3) La identificación jurídica de los proveedores terceros de servicios de TIC incluidos dentro del ámbito de aplicación de la presente norma técnica de regulación debe armonizarse con el código de identificación establecido en el Reglamento de Ejecución de la Comisión adoptado de conformidad con el artículo 28, apartado 9, del Reglamento (UE) 2022/2554.

(4) Como seguimiento de las recomendaciones formuladas por el supervisor principal a los proveedores terceros esenciales de servicios de TIC, el supervisor principal debe vigilar el cumplimiento de las recomendaciones por parte de los proveedores terceros esenciales de servicios de TIC. Con el fin de garantizar un seguimiento eficiente y eficaz de las medidas adoptadas o de las medidas correctoras aplicadas por los proveedores terceros esenciales de servicios de TIC en relación con estas recomendaciones, el supervisor principal debe poder exigir los informes a que se refiere el artículo 35, apartado 1, letra c), del Reglamento (UE) 2022/2554, que deben considerarse informes intermedios de situación e informes finales.

(5) A efectos de la valoración especificada en el artículo 42, apartado 1, del Reglamento (UE) 2022/2554, según el cual el supervisor principal está obligado a evaluar si la explicación proporcionada por el proveedor tercero esencial de servicios de TIC es suficiente, la notificación al supervisor principal por parte del proveedor tercero esencial de servicios de TIC de su intención de seguir las recomendaciones recibidas debe complementarse con una descripción de las acciones y medidas adoptadas para mitigar los riesgos expuestos en las recomendaciones, junto con sus respectivos plazos. La mencionada explicación debe adoptar la forma de un plan corrector.

(6) Dado que está previsto que el supervisor principal evalúe los acuerdos de subcontratación del proveedor tercero esencial de servicios de TIC, debe elaborarse una plantilla para facilitar información sobre dichos acuerdos. La plantilla debe tener en cuenta el hecho de que los proveedores terceros esenciales de servicios de TIC tienen estructuras diferentes a las de las entidades financieras.

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

(7) Una vez que el supervisor principal formule las recomendaciones a un proveedor tercero esencial de servicios de TIC y que las autoridades competentes hayan informado a las entidades financieras pertinentes de los riesgos señalados en dichas recomendaciones, el supervisor principal debe evaluar la ejecución de las acciones y medidas correctoras por parte del proveedor tercero esencial de servicios de TIC para cumplir las recomendaciones y llevar a cabo un seguimiento de ella. Las autoridades competentes deberán supervisar y evaluar en qué medida las entidades financieras están expuestas a los riesgos señalados en dichas recomendaciones. Con el fin de mantener la igualdad de condiciones en el desempeño de sus funciones respectivas, en particular cuando los riesgos señalados en las recomendaciones sean graves y se compartan entre un gran número de entidades financieras de varios Estados miembros, tanto las autoridades competentes como el supervisor principal deben compartir entre sí todas las conclusiones pertinentes que sean necesarias para llevar a cabo sus respectivas tareas. El objetivo del intercambio de información es garantizar que las observaciones del supervisor principal al proveedor tercero esencial de servicios de TIC en relación con las medidas y soluciones que este último esté aplicando tengan en cuenta la incidencia en los riesgos de las entidades financieras, y que las actividades de supervisión llevadas a cabo por las autoridades competentes se basen en la evaluación realizada por el supervisor principal.

(8) Para permitir un intercambio de información eficaz y eficiente, las autoridades competentes deben evaluar, como parte de sus actividades de supervisión, en qué medida las entidades financieras supervisadas por ellas están expuestas a los riesgos señalados en las recomendaciones. Esta evaluación debe llevarse a cabo de manera proporcionada y basada en el riesgo. El supervisor principal debe solicitar a las autoridades competentes que informen sobre los resultados de esta evaluación en aquellos casos específicos en que los riesgos asociados a las recomendaciones sean graves y se compartan entre un gran número de entidades financieras de varios Estados miembros. Para hacer el mejor uso posible de los recursos de las autoridades competentes, al solicitar los resultados de esta evaluación, el supervisor principal debe tener siempre en cuenta que el objetivo de estas solicitudes es evaluar la ejecución de las acciones y medidas correctoras por parte de los proveedores terceros esenciales de servicios de TIC.

(9) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([2]), emitió su dictamen el 22 de julio de 2024.

(10) El presente Reglamento se basa en los proyectos de normas técnicas de regulación presentados por las AES a la Comisión.

(11) El Comité Mixto de las AES ha llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de regulación en que se basa el presente Reglamento, ha analizado los costes y beneficios posibles correspondientes y ha recabado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario establecido de conformidad con el artículo 37 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([3]), del Grupo de Partes Interesadas del Sector de Seguros y de Reaseguros y el Grupo de Partes Interesadas del Sector de Pensiones de Jubilación establecidos de conformidad con el artículo 37 del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([4]), y del Grupo de Partes Interesadas del Sector de Valores y Mercados establecido de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([5]).

([2]) 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).

([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).

HA ADOPTADO EL PRESENTE REGLAMENTO:

*Artículo 1*

**Información que debe facilitar el proveedor tercero de servicios de TIC en la solicitud para ser designado como esencial**

1. El proveedor tercero de servicios de tecnologías de la información y la comunicación (TIC) presentará la información siguiente en la solicitud motivada de inclusión voluntaria en virtud del artículo 31, apartado 11, del Reglamento (UE) 2022/2554 para ser designado como esencial con arreglo al artículo 31, apartado 1, letra a), del Reglamento (UE) 2022/2554:

a) nombre de la entidad jurídica;

b) código de identificación de la entidad jurídica;

c) nombre de la persona de contacto y datos de contacto del proveedor tercero esencial de servicios de TIC;

d) país en el que la entidad jurídica tiene su domicilio social;

e) una descripción de la estructura corporativa que incluya, como mínimo, información sobre su sociedad matriz y otras empresas vinculadas que presten servicios de TIC a entidades financieras de la Unión. Dicha información incluirá, cuando proceda:

   i) nombre de las entidades jurídicas,

   ii) código de identificación de la entidad jurídica,

   iii) país en el que la entidad jurídica tiene su domicilio social;

f) una estimación de la cuota de mercado del proveedor tercero de servicios de TIC en el sector financiero de la Unión y una estimación de la cuota de mercado por tipo de entidad financiera a que se refiere el artículo 2, apartado 1, del Reglamento (UE) 2022/2554 a partir del año de presentación de la solicitud para ser designado como esencial y del año anterior a dicha solicitud;

g) una descripción de cada servicio de TIC prestado a entidades financieras de la Unión, que incluya:

   i) una descripción de la naturaleza de la actividad empresarial y del tipo de servicios de TIC prestados a entidades financieras,

   ii) una lista de las funciones de las entidades financieras sustentadas por los servicios de TIC prestados, cuando estén disponibles,

   iii) información sobre si los servicios de TIC prestados a las entidades financieras sustentan funciones esenciales o importantes, cuando esté disponible;

h) una lista de las entidades financieras que hacen uso de los servicios de TIC prestados por el proveedor tercero de servicios de TIC, que incluya la información siguiente sobre cada una de las entidades financieras a las que se presta el servicio, cuando esté disponible:

   i) nombre,

   ii) código de identificación de la entidad jurídica, cuando el proveedor tercero de servicios de TIC lo conozca,

   iii) tipo de entidad financiera, según lo especificado el artículo 2, punto 1, del Reglamento (UE) n.º 2022/2554,

   iv) ubicación geográfica desde la que se prestan los servicios de TIC a esa entidad jurídica específica;

i) una lista de los proveedores terceros esenciales de servicios de TIC incluidos en la última lista disponible de dichos proveedores publicada por las AES de conformidad con el artículo 31, apartado 9, del Reglamento (UE) 2022/2554 que dependan de los servicios prestados por el solicitante cuando se disponga de ella;

j) una autoevaluación en relación con lo siguiente:

   i) el grado de sustituibilidad de cada servicio de TIC prestado por el solicitante, teniendo en cuenta lo siguiente:

      — la cuota de mercado del proveedor tercero de servicios de TIC en el sector financiero de la Unión,

— el número de competidores pertinentes conocidos por tipo de servicios de TIC o grupo de servicios de TIC,

— una descripción de las especificidades relacionadas con los servicios de TIC ofrecidos, en concreto en relación con cualquier tecnología protegida por derechos, o las características específicas de la organización o actividad del proveedor tercero de servicios de TIC,

ii) el conocimiento de la disponibilidad de proveedores terceros de servicios de TIC alternativos que presten los mismos servicios de TIC que el proveedor tercero de servicios de TIC que presenta la solicitud;

k) información sobre la futura estrategia empresarial en relación con la prestación de servicios e infraestructuras de TIC a entidades financieras de la Unión, incluidos los cambios previstos en el grupo o la estructura de gestión y la entrada en nuevos mercados o actividades;

l) la identificación de los subcontratistas del proveedor tercero de servicios de TIC que hayan sido designados como proveedores terceros esenciales de servicios de TIC;

m) cualquier otro motivo pertinente en relación con la solicitud del proveedor tercero de servicios de TIC para ser designado como esencial.

2. Cuando el proveedor tercero de servicios de TIC pertenezca a un grupo, la información a que se refiere el apartado 1 se facilitará en relación con los servicios de TIC prestados por el grupo en su conjunto.

*Artículo 2*

**Contenido, estructura y formato de la información que deben presentar, divulgar o notificar los proveedores terceros esenciales de servicios de TIC**

1. Los proveedores terceros esenciales de servicios de TIC facilitarán al supervisor principal, a petición de este, cualquier información que necesite el supervisor principal para cumplir sus responsabilidades de supervisión de conformidad con los requisitos establecidos en el Reglamento (UE) 2022/2554.

2. La información a que se refiere el apartado 1 incluye, entre otros elementos, los siguientes:

a) información sobre los acuerdos —y copias de los documentos contractuales— entre:

i) el proveedor tercero esencial de servicios de TIC y las entidades financieras a que se refiere el artículo 2, apartado 1, del Reglamento (UE) 2022/2554,

ii) el proveedor tercero esencial de servicios de TIC y sus subcontratistas, con vistas a conocer la cadena de valor tecnológica de los servicios de TIC prestados a las entidades financieras de la Unión;

b) información sobre la estructura organizativa y de grupo del proveedor tercero esencial de servicios de TIC, incluida la identificación de todas las entidades pertenecientes al mismo grupo que presten servicios de TIC de forma directa o indirecta a entidades financieras de la Unión;

c) información sobre los principales accionistas, incluida su estructura y su distribución geográfica, de cualquiera de las entidades siguientes:

i) entidades que posean, de manera exclusiva o conjuntamente con sus entidades vinculadas, el 25 % o más del capital o los derechos de voto del proveedor tercero esencial de servicios de TIC,

ii) entidades que tengan derecho a designar o destituir a la mayoría de los miembros del órgano de administración, dirección o supervisión del proveedor tercero esencial de servicios de TIC,

iii) entidades que controlen, en virtud de un acuerdo, la mayoría de los derechos de voto de los accionistas o miembros del proveedor tercero esencial de servicios de TIC;

d) información sobre la cuota de mercado del proveedor tercero esencial de servicios de TIC, por tipo de servicios, en los mercados pertinentes en los que opera;

e) información sobre los mecanismos de gobernanza internos del proveedor tercero esencial de servicios de TIC, incluida la estructura con líneas de responsabilidad en materia de gobernanza y normas de rendición de cuentas;

f) las actas de las reuniones del órgano de dirección del proveedor tercero esencial de servicios de TIC y de cualquier otro comité interno pertinente que se refieran de algún modo a actividades y riesgos relacionados con servicios de TIC prestados por terceros que apoyen funciones de entidades financieras dentro de la Unión;

g) información sobre la seguridad de las TIC del proveedor tercero esencial de servicios de TIC, incluidas las estrategias, los objetivos, las políticas, los procedimientos, los protocolos, los procesos y las medidas de control pertinentes para proteger los datos confidenciales, los controles de acceso, las prácticas de cifrado, los planes de respuesta a incidentes e información sobre el cumplimiento de todas las regulaciones y normas nacionales e internacionales pertinentes, cuando proceda;

h) información sobre medidas técnicas y organizativas para garantizar la protección y la confidencialidad de los datos, incluidos los datos personales y no personales, las medidas de control aplicadas para proteger los datos confidenciales, los controles de acceso, las prácticas de cifrado y el plan de respuesta a las violaciones de la seguridad de los datos; cuando, en lo que respecta al tratamiento de los datos personales, el proveedor tercero de servicios de TIC esté sujeto a la legislación de terceros países, incluida la solicitud de acceso por parte de Gobiernos de terceros países, la lista de los países y la legislación aplicable;

i) información sobre los mecanismos que ofrece el proveedor tercero esencial de servicios de TIC a las entidades financieras de la Unión para la portabilidad de los datos y la portabilidad e interoperabilidad de las aplicaciones;

j) información sobre la ubicación de los centros de datos y los centros de producción de TIC utilizados para prestar servicios a las entidades financieras, incluida una lista de todos los locales e instalaciones pertinentes del proveedor tercero esencial de servicios de TIC, también los situados fuera de la Unión;

k) información sobre la prestación de servicios por parte del proveedor tercero esencial de servicios de TIC desde terceros países, incluyendo información sobre las disposiciones jurídicas pertinentes aplicables a los datos personales y no personales tratados por el proveedor tercero de servicios de TIC;

l) información sobre las medidas adoptadas para hacer frente a los riesgos derivados de la prestación de servicios de TIC por parte del proveedor tercero esencial de servicios de TIC y sus subcontratistas desde terceros países;

m) información sobre el marco de gestión de riesgos y el marco de gestión de incidentes, incluidas las políticas, los procedimientos, las herramientas, los mecanismos y los mecanismos de gobernanza del proveedor tercero esencial de servicios de TIC y de sus subcontratistas, en particular la lista y la descripción de los incidentes graves con repercusión directa o indirecta en las entidades financieras de la Unión, así como los detalles pertinentes para determinar la importancia del incidente para las entidades financieras y evaluar las posibles consecuencias transfronterizas;

n) información sobre el marco de gestión de los cambios, incluidas las políticas, los procedimientos y los controles del proveedor tercero esencial de servicios de TIC y sus subcontratistas;

o) información sobre el marco general de respuesta y recuperación del proveedor tercero esencial de servicios de TIC, incluidos los planes de continuidad de la actividad y los mecanismos y procedimientos conexos, la política de desarrollo de *software*, los planes de respuesta y recuperación y los mecanismos y procedimientos conexos, así como los mecanismos y procedimientos de las políticas de respaldo;

p) información sobre el seguimiento del rendimiento, la supervisión de la seguridad y el seguimiento de incidentes, así como información sobre los mecanismos de notificación relacionados con el rendimiento de los servicios, los incidentes y el cumplimiento de los acuerdos de nivel de servicio consensuados y de los objetivos de nivel de servicio o acuerdos similares entre proveedores terceros esenciales de servicios de TIC y entidades financieras de la Unión;

q) información sobre el marco de gestión de proveedores terceros de servicios de TIC del proveedor tercero esencial de servicios de TIC, incluidas las estrategias, las políticas, los procedimientos, los procesos y los controles, con detalles sobre la diligencia debida con la que haya actuado el proveedor tercero esencial de servicios de TIC con respecto a sus subcontratistas y sobre la evaluación de riesgos a la que los haya sometido antes de celebrar un acuerdo con ellos, y para llevar a cabo un seguimiento de la relación contemplando todos los riesgos de TIC y de contraparte pertinentes;

r) extracciones de los sistemas de seguimiento y detección del proveedor tercero esencial de servicios de TIC y de sus subcontratistas, que abarquen, entre otras cosas, el seguimiento de la red, de los servidores, de las aplicaciones y de la seguridad, la exploración de vulnerabilidades, la gestión de registros, el seguimiento del rendimiento, la gestión de incidentes y las mediciones relacionadas con los objetivos de fiabilidad, como los de nivel de servicio;

s) extracciones de cualquier sistema o aplicación de producción, preproducción y prueba utilizado por el proveedor tercero esencial de servicios de TIC y sus subcontratistas para prestar servicios a entidades financieras de la Unión de manera directa o indirecta;

t) informes de conformidad y de auditoría disponibles, junto con cualquier conclusión de auditoría pertinente, también de las auditorías realizadas por autoridades nacionales de la Unión y fuera de la Unión cuando los acuerdos de cooperación con las autoridades competentes prevean dicho intercambio de información, o las certificaciones obtenidas por el proveedor tercero esencial de servicios de TIC o sus subcontratistas, incluidos los informes de auditores internos y externos, las certificaciones o las evaluaciones de la conformidad con las normas específicas del sector; esto incluye información sobre cualquier tipo de prueba independiente disponible de la resiliencia de los sistemas de TIC del proveedor tercero esencial de servicios de TIC, en particular cualquier tipo de prueba de penetración basada en amenazas realizada por el proveedor tercero de servicios de TIC;

u) información sobre cualquier evaluación realizada por el proveedor tercero esencial de servicios de TIC a petición de este o en su nombre en la que se evalúe la idoneidad e integridad de las personas que ocupen puestos clave en el proveedor tercero esencial de servicios de TIC;

v) información sobre cualquier plan corrector para abordar las recomendaciones formuladas con arreglo al artículo 3, así como información pertinente para confirmar que se han aplicado las medidas correctoras;

w) información sobre los programas de formación y de sensibilización en materia de seguridad disponibles para los empleados, incluida, cuando proceda, información sobre las inversiones, los recursos y los métodos del proveedor tercero esencial de servicios de TIC en la formación de su personal para tratar datos financieros sensibles y mantener unos altos niveles de seguridad;

x) información sobre las actividades y los estados financieros del proveedor tercero esencial de servicios de TIC, en particular información sobre el presupuesto y los recursos relacionados con las TIC y la seguridad.

*Artículo 3*

**Información de los proveedores terceros esenciales de servicios de TIC tras la formulación de recomendaciones**

1. El proveedor tercero esencial de servicios de TIC presentará al supervisor principal un informe que contendrá un plan corrector en relación con las recomendaciones y las medidas correctoras que el proveedor tercero esencial de servicios de TIC tenga previsto aplicar para mitigar los riesgos señalados en las recomendaciones a que se refiere el artículo 35, apartado 1, letra d), del Reglamento (UE) 2022/2254. El informe será coherente con el calendario establecido por el supervisor principal para cada recomendación.

2. Para posibilitar el seguimiento de la aplicación de las medidas adoptadas o de las medidas correctoras aplicadas por el proveedor tercero esencial de servicios de TIC en relación con las recomendaciones recibidas, el proveedor tercero esencial de servicios de TIC compartirá con el supervisor principal, cuando este se lo solicite:

a) informes intermedios de situación y documentos justificativos conexos en los que se especifiquen los avances en la ejecución de las acciones y medidas establecidas en el informe facilitado por el proveedor tercero esencial de servicios de TIC al supervisor principal dentro del plazo definido por este último;

b) informes finales y documentos justificativos conexos en los que se especifiquen las medidas adoptadas o las medidas correctoras aplicadas por el proveedor tercero esencial de servicios de TIC para mitigar los riesgos señalados en las recomendaciones recibidas.

*Artículo 4*

**Estructura y formato de la información facilitada por los proveedores terceros esenciales de servicios de TIC**

1. El proveedor tercero esencial de servicios de TIC facilitará la información solicitada al supervisor principal a través de los canales electrónicos seguros específicos indicados por el supervisor principal en su solicitud y en la forma establecida por este último.

2. Cuando faciliten información al supervisor principal, los proveedores terceros esenciales de servicios de TIC:

a) seguirán la estructura indicada por el supervisor principal en su solicitud de información;

b) indicarán con claridad dónde se encuentra la información pertinente en la documentación presentada.

3. La información presentada, divulgada o notificada al supervisor principal por el proveedor tercero esencial de servicios de TIC se redactará en una lengua de uso común en el ámbito de las finanzas internacionales.

*Artículo 5*

**Plantilla para facilitar información sobre los acuerdos de subcontratación**

Todo proveedor tercero esencial de servicios de TIC que esté obligado a compartir información sobre los acuerdos de subcontratación facilitará la información al supervisor principal con arreglo a la plantilla que figura en el anexo.

*Artículo 6*

**Evaluación por parte de las autoridades competentes de los riesgos abordados en las recomendaciones del supervisor principal**

1. En el marco de su labor de supervisión de las entidades financieras, la autoridad competente evaluará las repercusiones en las entidades financieras de las medidas adoptadas por el proveedor tercero esencial de servicios de TIC sobre la base de las recomendaciones del supervisor principal, de conformidad con el principio de proporcionalidad.

2. Al llevar a cabo la evaluación a que se refiere el apartado 1, la autoridad competente tendrá en cuenta todos los aspectos siguientes:

a) la adecuación y coherencia de las medidas correctoras y reparadoras aplicadas por las entidades financieras para mitigar los riesgos señalados en las recomendaciones;

b) la evaluación realizada por el supervisor principal del cumplimiento por parte del proveedor tercero esencial de servicios de TIC de las medidas y acciones incluidas en el informe, cuando tenga repercusiones en la exposición de las entidades financieras bajo su competencia a los riesgos señalados en las recomendaciones;

c) la opinión de cualquier otra autoridad competente a la que se haya consultado de conformidad con el artículo 42, apartado 5, del Reglamento (UE) 2022/2554;

d) si el supervisor principal ha considerado que las acciones y medidas correctoras ejecutadas por el proveedor tercero esencial de servicios de TIC son adecuadas para mitigar la exposición de las entidades financieras bajo su competencia a los riesgos señalados en las recomendaciones.

3. A petición del supervisor principal, la autoridad competente facilitará en un plazo razonable los resultados de la evaluación a que se refiere el apartado 1. Al solicitar los resultados de esta evaluación, el supervisor principal tendrá en cuenta el principio de proporcionalidad y la magnitud de los riesgos asociados a las recomendaciones, incluidas las repercusiones transfronterizas de estos riesgos cuando afecten a entidades financieras que operen en más de un Estado miembro.

4. Cuando proceda, la autoridad competente solicitará a las entidades financieras que faciliten toda la información necesaria para llevar a cabo la evaluación a que se refiere el apartado 1.

*Artículo 7*

**Entrada en vigor**

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 24 de octubre de 2024.

*Por la Comisión*
*La Presidenta*
Ursula VON DER LEYEN

*ANEXO*

**PLANTILLA PARA COMPARTIR INFORMACIÓN SOBRE LOS ACUERDOS DE SUBCONTRATACIÓN**

| Categoría de información | Elementos clave de información |
|---|---|
| Información general | — Nombre del proveedor tercero esencial de servicios de TIC.<br>— Código de identificación del proveedor tercero esencial de servicios de TIC.<br>— Nombre de la persona de contacto y datos de contacto del proveedor tercero esencial de servicios de TIC.<br>— Fecha de presentación de la plantilla. |
| Resumen de los acuerdos de subcontratación | — Inventario de acuerdos de subcontratación, incluida una breve descripción de la finalidad y el alcance de las relaciones de subcontratación (que deberá contener, entre otros elementos, una indicación del carácter esencial o el nivel de importancia de los acuerdos de subcontratación para el proveedor tercero esencial de servicios de TIC).<br>— Especificación y descripción de los tipos de servicios de TIC subcontratados y su importancia para los servicios de TIC prestados a entidades financieras, en consonancia con las normas técnicas de ejecución adoptadas con arreglo al artículo 28, apartado 9, del Reglamento (UE) 2022/2554.<br>— Al especificar los tipos de servicios de TIC, consúltese la lista que figura en el anexo IV de las normas técnicas de ejecución adoptadas con arreglo al artículo 28, apartado 9, del Reglamento (UE) 2022/2554. |
| Información sobre los subcontratistas | — Nombre y datos de la entidad jurídica (incluido el código de identificación) de cada subcontratista.<br>— Información de contacto de los miembros del personal responsables de cada una de las relaciones de subcontratación en la estructura de gestión del proveedor tercero esencial de servicios de TIC.<br>— Resumen de los conocimientos especializados, la experiencia y las cualificaciones de cada subcontratista en relación con los servicios de TIC contratados. |
| Descripción de los servicios prestados por los subcontratistas | — Descripción detallada de los servicios de TIC específicos prestados por cada subcontratista.<br>— Desglose de las responsabilidades y tareas asignadas a los subcontratistas, detallando las diferentes funciones en las distintas fases de los procesos de TIC.<br>— Información sobre el nivel de acceso de los subcontratistas a datos o sistemas personales o confidenciales en relación con los servicios de TIC prestados a las entidades financieras.<br>— Información sobre los emplazamientos desde los que prestan sus servicios los subcontratistas y sobre las medidas adoptadas para hacer frente a los riesgos derivados de los servicios prestados fuera de la Unión. |
| Gobernanza y supervisión de la subcontratación | — Descripción del marco contractual y de gobernanza existente para gestionar las relaciones de subcontratación, incluidas las cláusulas que restringen el uso de datos confidenciales.<br>— Explicación de los procesos de selección, contratación y seguimiento de los subcontratistas.<br>— Descripción general de los parámetros de rendimiento, los objetivos y acuerdos de nivel de servicio y los indicadores clave de rendimiento utilizados para evaluar el rendimiento y el seguimiento de la fiabilidad de los subcontratistas. |
| Gestión de riesgos y conformidad | — Evaluación de los perfiles de riesgo de los subcontratistas y de la posible repercusión en los servicios de TIC prestados a las entidades financieras.<br>— Explicación de las medidas de mitigación del riesgo aplicadas para hacer frente a los riesgos relacionados con la subcontratación.<br>— Información detallada sobre el cumplimiento de la normativa pertinente por parte del subcontratista, en particular en lo referente a la protección de datos y a las normas del sector. |

| Categoría de información | Elementos clave de información |
|---|---|
| Planificación de la continuidad de la actividad y de contingencias | — Resumen de los planes del subcontratista en materia de continuidad de la actividad y de respuesta y recuperación.<br>— Descripción de las medidas adoptadas para garantizar la continuidad del servicio en caso de perturbaciones o resolución por parte del subcontratista.<br>— Frecuencia de las pruebas de los planes de continuidad de la actividad y de los planes de respuesta y recuperación por parte de los subcontratistas, fechas de las últimas pruebas realizadas en los tres últimos años y especificación de si el proveedor tercero esencial de servicios de TIC participó en dichas pruebas. |
| Elaboración de informes | — Descripción de los mecanismos de elaboración de informes y de la frecuencia de comunicación de información entre el proveedor tercero esencial de servicios de TIC y sus subcontratistas. |
| Reparación y gestión de incidentes | — Descripción de los procedimientos utilizados para abordar los incidentes, las infracciones o los incumplimientos relacionados con los subcontratistas. |
| Certificaciones y auditorías | — Información sobre las certificaciones, auditorías independientes o evaluaciones a las que se ha sometido a los subcontratistas para validar sus controles de seguridad, sus normas de calidad o el cumplimiento de la normativa por su parte.<br>— Fecha y frecuencia de las auditorías de los subcontratistas realizadas por el proveedor tercero esencial de servicios de TIC. |