2024/1773

25.6.2024

REGLAMENTO DELEGADO (UE) 2024/1773 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 el contenido detallado de la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC

(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 28, apartado 10, párrafo tercero,

Considerando lo siguiente:

(1) El marco sobre resiliencia operativa digital para el sector financiero establecido por el Reglamento (UE) 2022/2554 exige que las entidades financieras establezcan determinados principios clave para gestionar el riesgo relacionado con las TIC derivado de terceros, que revisten especial importancia cuando las entidades financieras colaboran con proveedores terceros de servicios de TIC para sustentar sus funciones esenciales o importantes.

(2) Las entidades financieras, como parte de su marco de gestión del riesgo relacionado con las TIC, deben adoptar una estrategia sobre el riesgo de terceros relacionado con las TIC y revisarla periódicamente. De conformidad con el artículo 28, apartado 2, del Reglamento (UE) 2022/2554, dicha estrategia debe incluir una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC, y se debe aplicar a título particular y, cuando proceda, de forma subconsolidada y consolidada.

(3) Las entidades financieras varían considerablemente en cuanto al tamaño, la estructura y la organización interna, así como en cuanto a la naturaleza y complejidad de sus actividades y operaciones. A la hora de desarrollar la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de TIC (en lo sucesivo, «política»), es necesario tener en cuenta esta diversidad, pero imponer al mismo tiempo determinados requisitos reglamentarios fundamentales que sean adecuados para todas las entidades financieras, garantizando que dichos requisitos se apliquen de manera proporcionada.

(4) Cuando las entidades financieras pertenezcan a un grupo, la sociedad matriz responsable de presentar los estados financieros consolidados o subconsolidados del grupo debe, por tanto, garantizar que la política se aplique de manera uniforme y coherente dentro del grupo.

(5) Al aplicar la política, los proveedores intragrupo de servicios de TIC, incluidos los que sean propiedad plena o colectiva de entidades financieras dentro del mismo sistema institucional de protección, deben considerarse proveedores terceros de servicios de TIC. Los riesgos que plantean los proveedores intragrupo de servicios de TIC pueden ser diferentes, pero los requisitos que les resultan aplicables en virtud del Reglamento (UE) 2022/2554 son los mismos. De manera similar, la política debe ser aplicable a los subcontratistas que presten servicios de TIC que sustenten funciones esenciales o importantes, o partes sustanciales de ellas, a proveedores terceros de servicios de TIC, cuando exista una cadena de proveedores terceros de servicios de TIC.

(6) La responsabilidad última del órgano de dirección en la gestión del riesgo relacionado con las TIC de una entidad financiera es un principio fundamental que también es aplicable cuando se recurre a proveedores terceros de servicios de TIC. Esta responsabilidad debe traducirse además en la implicación continua del órgano de dirección en el control y el seguimiento de la gestión del riesgo relacionado con las TIC, incluida la adopción y revisión, al menos una vez al año, de la política.

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

(7) Para garantizar una información adecuada al órgano de dirección, la política debe especificar y determinar claramente las responsabilidades internas relativas a la aprobación, la gestión, el control y la documentación de los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC (en lo sucesivo, «acuerdos contractuales»), incluidos los servicios de TIC prestados en virtud de los acuerdos contractuales a que se refiere el artículo 28, apartado 1, letra a), del Reglamento (UE) 2022/2554.

(8) A fin de tener en cuenta todos los posibles riesgos que puedan surgir al contratar servicios de TIC que sustenten funciones esenciales o importantes, la estructura de la política debe seguir todas las etapas de cada una de las fases principales del ciclo de vida de los acuerdos contractuales con proveedores terceros.

(9) Para mitigar los riesgos detectados, la política debe especificar la planificación de los acuerdos contractuales, en particular la evaluación de riesgos, la diligencia debida y el proceso de aprobación de cambios nuevos o significativos en dichos acuerdos contractuales. A fin de gestionar los riesgos que puedan surgir antes de celebrar un acuerdo contractual con un proveedor tercero de servicios de TIC, la política debe especificar un proceso adecuado y proporcionado para seleccionar y evaluar la idoneidad de los posibles proveedores terceros de servicios de TIC y exigir que la entidad financiera tenga en cuenta una lista no exhaustiva de los elementos de que deben disponer los proveedores terceros de servicios de TIC. La lista debe incluir aspectos relacionados con la reputación empresarial de los proveedores de servicios, sus recursos financieros, humanos y técnicos, su seguridad de la información, su estructura organizativa, incluida la gestión de riesgos, y sus controles internos.

(10) Para garantizar una gestión del riesgo sólida en la prestación de servicios de TIC que sustenten funciones esenciales o importantes por parte de proveedores terceros de servicios de TIC, la política debe contener información sobre la aplicación, el seguimiento y la gestión de los acuerdos contractuales, también a nivel consolidado y subconsolidado, cuando proceda. Esto implica, entre otras cosas, establecer requisitos para las cláusulas contractuales sobre las obligaciones mutuas de las entidades financieras y los proveedores terceros de servicios de TIC, lo que debe hacerse por escrito. Con el fin de garantizar una supervisión eficiente y fomentar la resiliencia en caso de que el modelo de negocio o el entorno empresarial cambien, la política debe garantizar los derechos de las entidades financieras o de terceros designados y de las autoridades competentes a las inspecciones y al acceso a la información, así como especificar en mayor medida las estrategias de salida y los procesos de extinción.

(11) En la medida en la que los proveedores terceros de servicios de TIC traten datos personales, esta política y cualquier acuerdo contractual se entienden sin perjuicio de las obligaciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]) y deben complementarlas, como el requisito de disponer de un contrato escrito en el que se describa el tratamiento de datos personales, el requisito de garantizar la seguridad del tratamiento de datos personales y establecer todos los demás elementos exigidos en virtud de dicho Reglamento.

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

(12) El Comité Mixto de las Autoridades Europeas de Supervisión a que se refieren el artículo 54 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([3]), el artículo 54 del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([4]) y el artículo 54 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([5]) ha llevado a cabo consultas públicas abiertas sobre el proyecto de normas técnicas de regulación en que se basa el presente Reglamento, ha analizado los posibles costes y beneficios de las normas propuestas y ha solicitado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1093/2010, el Grupo de Partes Interesadas del Sector de Seguros y Reaseguros y el Grupo de Partes Interesadas del Sector de Pensiones de Jubilación creados de conformidad con el artículo 37 del Reglamento (UE) n.º 1094/2010, y el Grupo de partes interesadas del sector de los valores y mercados creado de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010.

(13) 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 el 24 de enero de 2024,

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Perfil de riesgo general y complejidad

La política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC (en lo sucesivo, «política») tendrá en cuenta el tamaño y el perfil de riesgo general de la entidad financiera, así como la naturaleza, la escala y los elementos que suponen un aumento o una disminución de la complejidad de sus servicios, actividades y operaciones, en particular los elementos relacionados con:

a) el tipo de servicios de TIC incluidos en el acuerdo contractual sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC (en lo sucesivo, «acuerdo contractual») entre la entidad financiera y el proveedor tercero de servicios de TIC;

b) la ubicación del proveedor tercero de servicios de TIC o la ubicación de su empresa matriz;

c) si los servicios de TIC que sustenten funciones esenciales o importantes son prestados por un proveedor tercero de servicios de TIC ubicado en un Estado miembro o en un tercer país, teniendo también en cuenta la ubicación desde la que se prestan los servicios de TIC y la ubicación en la que se tratan y almacenan los datos;

d) la naturaleza de los datos compartidos con el proveedor tercero de servicios de TIC;

e) si el proveedor tercero de servicios de TIC forma parte del mismo grupo que la entidad financiera a la que se prestan los servicios;

([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).

f) el recurso a proveedores terceros de servicios de TIC que estén autorizados, registrados o sujetos a vigilancia o supervisión por una autoridad competente de un Estado miembro o sujetos al marco de supervisión con arreglo al capítulo V, sección II, del Reglamento (UE) 2022/2554, y el recurso a proveedores terceros de servicios de TIC que no lo estén;

g) el recurso a proveedores terceros de servicios de TIC que estén autorizados, registrados o sujetos a vigilancia o supervisión por una autoridad de supervisión de un tercer país, y el recurso a proveedores terceros de servicios de TIC que no lo estén;

h) si la prestación de servicios de TIC que sustenten funciones esenciales o importantes se concentra en un único proveedor tercero de servicios de TIC o en un pequeño número de dichos proveedores de servicios;

i) la transferibilidad de los servicios de TIC que sustenten funciones esenciales o importantes a otro proveedor tercero de servicios de TIC, también como resultado de especificidades tecnológicas;

j) la repercusión que pueden tener las perturbaciones en la prestación de los servicios de TIC que sustenten funciones esenciales o importantes en la continuidad de las actividades de la entidad financiera y en la disponibilidad de sus servicios.

Artículo 2

Aplicación a nivel de grupo

Cuando el presente Reglamento se aplique de forma subconsolidada o consolidada, la sociedad matriz responsable de proporcionar los estados financieros consolidados o subconsolidados del grupo velará por que la política se aplique de manera consistente en todas las entidades financieras que formen parte del grupo y sea adecuada para la aplicación efectiva del presente Reglamento a todos los niveles pertinentes del grupo.

Artículo 3

Mecanismos de gobernanza

1. El órgano de dirección revisará la política al menos una vez al año y la actualizará cuando sea necesario. Los cambios introducidos en la política se aplicarán oportunamente y tan pronto como sea posible en el marco de los acuerdos contractuales pertinentes. La entidad financiera documentará el calendario previsto para la aplicación.

2. La política establecerá una metodología para determinar qué servicios de TIC sustentan funciones esenciales o importantes, o hará referencia a ella. La política también especificará cuándo debe llevarse a cabo y revisarse esta evaluación.

3. La política asignará claramente las responsabilidades internas relativas a la aprobación, la gestión, el control y la documentación de los acuerdos contractuales pertinentes y garantizará que se mantengan en la entidad financiera las capacidades, la experiencia y los conocimientos adecuados para supervisar de forma efectiva los acuerdos contractuales pertinentes, incluidos los servicios de TIC prestados en virtud de dichos acuerdos.

4. Sin perjuicio de la responsabilidad final de la entidad financiera de supervisar de forma efectiva los acuerdos contractuales pertinentes, la política exigirá que se evalúe si el proveedor tercero de servicios de TIC dispone de recursos suficientes para garantizar que la entidad financiera cumpla todos sus requisitos legales y reglamentarios en relación con los servicios de TIC que sustenten funciones esenciales o importantes que se prestan.

5. La política determinará claramente el cargo o el miembro de la alta dirección responsable de supervisar los acuerdos contractuales pertinentes. La política especificará el modo en que dicho cargo o miembro de la alta dirección cooperará con las funciones de control, a menos que forme parte de estas, y establecerá los canales para informar al órgano de dirección, así como la naturaleza de la información que debe comunicarse y los documentos que deben facilitarse. También establecerá la frecuencia de dicha información.

6. La política garantizará que los acuerdos contractuales sean compatibles con lo siguiente:

a) el marco de gestión del riesgo relacionado con las TIC a que se refiere el artículo 6 del Reglamento (UE) 2022/2554;

b) la política de seguridad de la información a que se refiere el artículo 9, apartado 4, del Reglamento (UE) 2022/2554;

c) la política de continuidad de la actividad en materia de TIC a que se refiere el artículo 11 del Reglamento (UE) 2022/2554;

d) los requisitos en materia de notificación de incidentes establecidos en el artículo 19 del Reglamento (UE) 2022/2554.

7. La política exigirá que los servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC sean objeto de una revisión independiente y se incluyan en el plan de auditoría.

8. La política especificará explícitamente que los acuerdos contractuales:

a) no eximen a la entidad financiera ni a su órgano de dirección de sus obligaciones reglamentarias ni de sus responsabilidades frente a sus clientes;

b) no deben impedir la supervisión efectiva de una entidad financiera y no deben contravenir ninguna restricción sobre servicios y actividades impuesta por el supervisor;

c) deben exigir que los proveedores terceros de servicios de TIC cooperen con las autoridades competentes;

d) deben exigir que la entidad financiera, sus auditores y las autoridades competentes tengan acceso efectivo a los datos y locales relacionados con el uso de servicios de TIC que sustenten funciones esenciales o importantes.

Artículo 4

Principales fases del ciclo de vida para la adopción y la aplicación de los acuerdos contractuales

La política especificará los requisitos, incluidas las normas, las responsabilidades y los procesos, para cada una de las fases principales del ciclo de vida del acuerdo contractual, que abarcarán, como mínimo, lo siguiente:

a) las responsabilidades del órgano de dirección, incluida su participación, según proceda, en el proceso de toma de decisiones sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC;

b) la planificación de los acuerdos contractuales, incluida la evaluación de riesgos y la diligencia debida establecidas en los artículos 5 y 6, así como el proceso de aprobación de cambios nuevos o significativos en los acuerdos contractuales establecido en el artículo 8, apartado 4;

c) la participación de unidades operativas, controles internos y otras unidades pertinentes en relación con los acuerdos contractuales;

d) la aplicación, el seguimiento y la gestión de los acuerdos contractuales a que se refieren los artículos 7, 8 y 9, también a nivel consolidado y subconsolidado, cuando proceda;

e) la documentación y la conservación de registros, teniendo en cuenta los requisitos relativos al registro de información establecidos en el artículo 28, apartado 3, del Reglamento (UE) 2022/2554;

f) las estrategias de salida y los procesos de extinción establecidos en el artículo 10.

Artículo 5

***Evaluación de riesgos* ex ante**

1. La política exigirá que se definan las necesidades empresariales de la entidad financiera antes de la celebración de un acuerdo contractual.

2. La política exigirá que se lleve a cabo una evaluación de riesgos a nivel de la entidad financiera y, cuando proceda, a nivel consolidado y subconsolidado antes de la celebración de un acuerdo contractual.

La evaluación de riesgos tendrá en cuenta todos los requisitos pertinentes establecidos en el Reglamento (UE) 2022/2554 y en la legislación sectorial de la Unión aplicable. Tendrá en cuenta, en particular, los efectos para la entidad financiera derivados de la prestación de servicios de TIC que sustenten funciones esenciales o importantes por parte de proveedores terceros de servicios de TIC, así como todos los riesgos que plantee la prestación de dichos servicios de TIC que sustenten funciones esenciales o importantes por parte de proveedores terceros de servicios de TIC, en particular los siguientes:

a) los riesgos operativos;

b) los riesgos jurídicos;

c) los riesgos relacionados con las TIC;

d) los riesgos de reputación;

e) los riesgos relacionados con la protección de datos confidenciales o personales;

f) los riesgos relacionados con la disponibilidad de datos;

g) los riesgos relacionados con la ubicación en la que se tratan y almacenan los datos;

h) los riesgos relacionados con la ubicación del proveedor tercero de servicios de TIC;

i) los riesgos de concentración de TIC a nivel de la entidad.

Artículo 6

Diligencia debida

1. La política establecerá un proceso adecuado y proporcionado para la selección y evaluación de los posibles proveedores terceros de servicios de TIC, teniendo en cuenta si estos son o no proveedores intragrupo de servicios de TIC, y exigirá que la entidad financiera evalúe, antes de celebrar un acuerdo contractual, si el proveedor tercero de servicios de TIC:

a) cuenta con la reputación empresarial, las capacidades y los conocimientos especializados suficientes y los recursos financieros, humanos y técnicos adecuados, los estándares en materia de seguridad de la información, la estructura organizativa adecuada, la gestión del riesgo y los controles internos y, cuando proceda, las autorizaciones o registros necesarios para prestar los servicios de TIC que sustenten funciones esenciales o importantes de manera fiable y profesional;

b) tiene capacidad para seguir los avances tecnológicos pertinentes y determinar las prácticas punteras en materia de seguridad de las TIC y aplicarlas cuando proceda con el fin de disponer de un marco de resiliencia operativa digital efectivo y sólido;

c) recurre o tiene la intención de recurrir a subcontratistas de TIC para prestar los servicios de TIC que sustenten funciones esenciales o importantes o partes sustanciales de dichos servicios;

d) está ubicado o procesa o almacena los datos en un tercer país y, en tal caso, si ello afecta a la magnitud de riesgos operativos o de reputación o al riesgo de verse afectado por medidas restrictivas, como embargos y sanciones, que puedan afectar a su capacidad para prestar los servicios de TIC o a la capacidad de la entidad financiera para recibir dichos servicios de TIC;

e) acepta los acuerdos contractuales que garanticen la posibilidad de que la propia entidad financiera, terceros designados y las autoridades competentes puedan llevar a cabo auditorías de dicho proveedor tercero de servicios de TIC, también *in situ*;

f) actúa de manera ética y socialmente responsable, respeta los derechos humanos y los derechos de la infancia, incluida la prohibición del trabajo infantil, respeta los principios aplicables en materia de protección del medio ambiente y garantiza unas condiciones de trabajo adecuadas.

2. La política especificará el nivel de garantía requerido respecto a la eficacia del marco de gestión del riesgo de los proveedores terceros de servicios de TIC para los servicios de TIC que sustenten funciones esenciales o importantes que haya de prestar un proveedor tercero de servicios de TIC. La política exigirá que en el proceso de diligencia debida se contemple una evaluación de la existencia de medidas de reducción del riesgo y de continuidad de las actividades, así como de la manera en que se garantiza su funcionamiento con respecto al proveedor tercero de servicios de TIC.

3. La política determinará el proceso de diligencia debida con vistas a la selección y evaluación de los posibles proveedores terceros de servicios de TIC e indicará cuáles de los siguientes elementos deben utilizarse para alcanzar el nivel de garantía requerido respecto del desempeño del proveedor tercero de servicios de TIC:

a) auditorías o evaluaciones independientes realizadas por la propia entidad financiera o en su nombre;

b) informes de auditoría independientes elaborados a petición del proveedor tercero de servicios de TIC;

c) informes de auditoría elaborados por la función de auditoría interna del proveedor tercero de servicios de TIC;

d) certificaciones adecuadas de terceros;

e) otras informaciones pertinentes de que disponga la entidad financiera o facilitadas por el proveedor tercero de servicios de TIC.

4. Las entidades financieras garantizarán un nivel de garantía adecuado respecto del desempeño del proveedor tercero de servicios de TIC, teniendo en cuenta los elementos enumerados en el apartado 3, letras a) a e). Cuando proceda, se utilizará más de un elemento de los enumerados en dichas letra s).

Artículo 7

Conflictos de intereses

1. La política especificará las medidas adecuadas para detectar, prevenir y gestionar los conflictos de intereses reales o potenciales que se deriven del recurso a proveedores terceros de servicios de TIC que deban adoptarse antes de celebrar los acuerdos contractuales pertinentes y establecerá un seguimiento continuo de dichos conflictos de intereses.

2. Cuando los proveedores intragrupo de servicios de TIC presten servicios de TIC que sustenten funciones esenciales o importantes, la política especificará que las decisiones sobre las condiciones de los servicios de TIC, incluidas las condiciones financieras, deben adoptarse de manera objetiva.

Artículo 8

Cláusulas contractuales

1. La política especificará que el acuerdo contractual pertinente debe presentarse por escrito e incluir todos los elementos mencionados en el artículo 30, apartados 2 y 3, del Reglamento (UE) 2022/2554. La política también incluirá elementos relativos a los requisitos a que se refiere el artículo 1, apartado 1, letra a), del Reglamento (UE) 2022/2554, así como otras normas de carácter legislativo pertinentes del Derecho de la Unión y nacional, según proceda.

2. La política especificará que los acuerdos contractuales pertinentes deben incluir el derecho de la entidad financiera a acceder a la información, a llevar a cabo inspecciones y auditorías y a realizar pruebas de TIC. A tal efecto, la política exigirá que la entidad financiera utilice los siguientes métodos, sin perjuicio de su responsabilidad final:

a) su propia auditoría interna o una auditoría realizada por un tercero designado;

b) cuando proceda, auditorías conjuntas y pruebas conjuntas de TIC, incluidas pruebas de penetración guiadas por amenazas, organizadas conjuntamente con otras entidades financieras o empresas adjudicadoras que utilicen servicios de TIC del mismo proveedor tercero de servicios de TIC y que sean realizadas por dichas entidades financieras o empresas adjudicadoras o por un tercero designado por ellas;

c) cuando proceda, certificaciones de terceros;

d) cuando proceda, informes de auditoría interna o externa facilitados por el proveedor tercero de servicios de TIC.

3. La entidad financiera no se basará de manera indefinida únicamente en las certificaciones a que se refiere el apartado 2, letra c), ni en los informes de auditoría a que se refiere la letra d) de dicho apartado. La política solo permitirá el uso de los métodos a que se refiere el apartado 2, letras c) y d), cuando la entidad financiera:

a) considere satisfactorio el plan de auditoría del proveedor tercero de servicios de TIC para los acuerdos contractuales pertinentes;

b) garantice que las certificaciones o los informes de auditoría cubran los sistemas y controles clave determinados por la entidad financiera y garantice el cumplimiento de los requisitos reglamentarios pertinentes;

c) evalúe exhaustivamente el contenido de las certificaciones o de los informes de auditoría de forma continua y verifica que los informes o certificaciones no estén obsoletos;

d) garantice que las futuras versiones de la certificación o del informe de auditoría abarquen los sistemas y controles clave;

e) esté convencida de la aptitud de la parte certificadora o auditora;

f) tenga la convicción de que las certificaciones se han expedido y de que las auditorías se llevan a cabo con arreglo a normas profesionales pertinentes ampliamente reconocidas e incluyen una prueba de la eficacia operativa de los controles clave establecidos;

g) tenga el derecho contractual a solicitar, con una frecuencia razonable y legítima desde el punto de vista de la gestión del riesgo, modificaciones del alcance de las certificaciones o informes de auditoría ampliándolo a otros sistemas y controles pertinentes;

h) tenga el derecho contractual a realizar auditorías individuales y conjuntas discrecionales en relación con los acuerdos contractuales y a ejecutar dichos derechos de acuerdo con la frecuencia acordada.

4. La política garantizará que los cambios significativos en el acuerdo contractual se formalicen en un documento escrito fechado y firmado por todas las partes y especificará el proceso de reconducción de los acuerdos contractuales.

Artículo 9

Seguimiento de los acuerdos contractuales

1. La política exigirá que los acuerdos contractuales especifiquen las medidas e indicadores clave que deben permitir supervisar, de forma continua, el desempeño de los proveedores terceros de servicios de TIC, incluidas las medidas de supervisión del cumplimiento de los requisitos relativos a la confidencialidad, disponibilidad, integridad y autenticidad de los datos y la información, y el cumplimiento por parte de los proveedores terceros de servicios de TIC de las políticas y procedimientos pertinentes de la entidad financiera. La política también especificará las medidas aplicables cuando no se cumplan los acuerdos de nivel de servicio, incluidas, en su caso, las sanciones contractuales.

2. La política especificará el modo en que la entidad financiera debe evaluar si los proveedores terceros de servicios de TIC a los que se recurre para los servicios de TIC que sustenten funciones esenciales o importantes cumplen normas de desempeño y calidad adecuadas en consonancia con el acuerdo contractual y las políticas propias de la entidad financiera. La política garantizará, en particular, lo siguiente:

a) que los proveedores terceros de servicios de TIC faciliten informes adecuados sobre sus actividades y servicios a la entidad financiera, incluidos informes periódicos, informes de incidentes, informes sobre la prestación de servicios, sobre la seguridad de las TIC y sobre las medidas y las pruebas relacionadas con la continuidad de las actividades;

b) que el desempeño de los proveedores terceros de servicios de TIC se evalúe con indicadores clave de desempeño, indicadores clave de control, auditorías, autocertificaciones y revisiones independientes en consonancia con el marco de gestión del riesgo relacionado con las TIC de la entidad financiera;

c) que la entidad financiera reciba otras informaciones pertinentes facilitadas por los proveedores terceros de servicios de TIC;

d) que se notifique a la entidad financiera, cuando proceda, los incidentes relacionados con las TIC y los incidentes operativos o de seguridad relacionados con los pagos;

e) que se lleven a cabo una revisión y auditorías independientes que verifiquen el cumplimiento de los requisitos y las políticas legales y reglamentarios.

3. La política especificará que debe documentarse la evaluación a que se refiere el apartado 2 y que deben utilizarse sus resultados para actualizar la evaluación de riesgos de la entidad financiera a que se refiere el artículo 6.

4. La política establecerá las medidas adecuadas que debe adoptar la entidad financiera si detecta deficiencias en los proveedores terceros de servicios de TIC, incluidos los incidentes relacionados con las TIC y los incidentes operativos o de seguridad relacionados con los pagos, en la prestación de los servicios de TIC que sustenten funciones esenciales o importantes o en el cumplimiento de acuerdos contractuales o requisitos legales. También especificará el modo en que debe supervisarse la aplicación de dichas medidas a fin de garantizar su cumplimiento efectivo en un plazo definido, teniendo en cuenta la importancia de las deficiencias.

Artículo 10

Abandono y extinción de los acuerdos contractuales

La política establecerá la exigencia de documentar el plan de salida de cada acuerdo contractual y de revisar y probar periódicamente dicho plan de salida documentado. Al establecer el plan de salida, se tendrán en cuenta los siguientes elementos:

a) las interrupciones imprevistas y persistentes del servicio;

b) la prestación inadecuada de servicios o la falta de prestación de servicios;

c) la extinción imprevista del acuerdo contractual.

El plan de salida será realista y viable, se basará en escenarios verosímiles y en hipótesis razonables, y tendrá un calendario de ejecución planificado compatible con las condiciones de salida y extinción establecidas en los acuerdos contractuales.

Artículo 11

Entrada en vigor

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

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

Hecho en Bruselas, el 13 de marzo de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN