Texto del acuerdo provisional del Parlamento Europeo y el Consejo sobre el proyecto de Reglamento relativo a la resiliencia operativa digital del sector financiero. Boletín Internacional de noviembre de 2022.

El acuerdo provisional acerca del Reglamento relativo a la resiliencia operativa digital del sector financiero *(Digital Operational Resilience Act*, DORA por sus siglas en inglés), entre el Parlamento Europeo y el Consejo, tuvo lugar el 11 de mayo. Este Reglamento es parte del conjunto de medidas sobre finanzas digitales que la Comisión Europea (CE) publicó el 24 de septiembre de 2020, integrado también por las iniciativas siguientes: a) una nueva estrategia de finanzas digitales para avanzar hacia un espacio europeo de datos financieros, promover nuevas formas de canalizar la financiación de las PYMES y mejores productos financieros para los consumidores; b) una estrategia de pagos minoristas para ofrecer servicios de pago seguros, rápidos, fiables y eficaces en términos de costes; c) un Reglamento relativo a los mercados de criptoactivos que quedan fuera de la legislación de servicios financieros vigente en la Unión Europea (UE) para regular su emisión y los servicios relacionados ellos, cuya publicación se espera en breve en el Diario Oficial de la Unión Europea (DOUE); y d) un Reglamento con un régimen piloto que permite excepciones temporales para las infraestructuras de mercado que deseen negociar y liquidar operaciones de instrumentos financieros en forma de criptoactivos basadas en la tecnología de registro descentralizado, publicado en el DOUE el 2 de junio de 2022.

El acuerdo provisional se publicó el 23 de junio en la página web del Consejo y se votó en el Comité de Asuntos Económicos y Monetarios del Parlamento el 13 de julio. A continuación, se procederá a la adopción formal de la propuesta de Reglamento por el Parlamento y el Consejo, que cada Estado Miembro incorporará posteriormente a su legislación. Las respectivas autoridades nacionales competentes (ANC) supervisarán el cumplimiento y la aplicación del Reglamento, sin perjuicio de la supervisión de los proveedores terceros esenciales de servicios de tecnologías de la información y la comunicación (TIC), que recaerá en las Autoridades Europeas de Supervisión (*European Supervisory Authorities*, ESAs por sus siglas en inglés), en la forma que se describe a continuación.

La propuesta de Reglamento relativo a la resiliencia operativa digital tiene como objetivo garantizar que el sector financiero en Europa pueda seguir funcionando de forma resiliente en caso de grave perturbación operativa, de forma que todas las empresas deben asegurarse de que pueden resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse de ella. Para ello, establece requisitos uniformes para la seguridad de las redes y sistemas de información de las entidades financieras, así como de proveedores terceros esenciales de servicios de TIC (proveedores de servicios de computación en la nube o servicios de análisis de datos), que impulsarán la seguridad informática del sector financiero. Los principales aspectos del texto del acuerdo son los siguientes:

Capítulo I Disposiciones generales

El texto establece una lista muy amplia que abarca casi todas las entidades del sector financiero, que bajo la denominación de **"entidades financieras"**, constituyen el ámbito de aplicación subjetivo del Reglamento DORA incluyendo, a modo de ejemplo, las entidades de crédito, empresas de servicios de inversión, sociedades gestoras, aseguradoras y proveedores de servicios de criptoactivos, de financiación participativa o de suministro de datos. Los auditores legales y sociedades de auditoría se incluirán en una futura revisión del Reglamento.

Además, el acuerdo recoge, a diferencia de la propuesta de la CE, un conjunto de supuestos de no aplicación, tales como las personas físicas o jurídicas exentas de la aplicación de MiFID o aquellos intermediarios financieros o de seguros que sean microempresas o pequeñas y medianas empresas.

El acuerdo añade a la propuesta de la CE un artículo general sobre el **principio de proporcionalidad** con el fin

de que las entidades financieras implementen las normas sobre la gestión del riesgo TIC, incidentes, pruebas y la gestión del riesgo de terceros relacionados con las TIC conforme a este principio teniendo en cuenta su tamaño, naturaleza, escala y complejidad de los servicios, actividades y operaciones y su perfil de riesgo general.

Para las entidades financieras identificadas como operadoras de servicios esenciales, este Reglamento tiene la consideración de norma sectorial específica. La interacción con la Directiva sobre Ciberseguridad (SRI) se aborda desde la aplicación del principio de *lex specialis*, siendo la Directiva sobre Ciberseguridad (SRI) aplicable en lo no previsto en este Reglamento.

Capítulo II Gestión de riesgos de TIC

Las entidades financieras dispondrán de requisitos internos de gobernanza y control que garanticen una gestión eficaz y prudente de todos los riesgos TIC para alcanzar un alto nivel de resiliencia operativa, asignando la responsabilidad a una **función de control** (no obligatoria para microempresas) que tenga un adecuado nivel de independencia para evitar conflictos de interés, separada de la función de control general y de la de auditoría interna.

El órgano de dirección de la entidad financiera definirá, aprobará, supervisará y será responsable de la aplicación del **marco de gestión del riesgo de TIC**, que formará parte de su sistema general de gestión de riesgos. En concreto, las entidades financieras dispondrán de: a) mecanismos, sujetos a pruebas periódicas, para detectar rápidamente las actividades anómalas, incluidos los problemas de rendimiento de la red de TIC y los incidentes relacionados para identificar los posibles puntos concretos de fallos significativos y b) una política de continuidad de las actividades de TIC exhaustiva que formará parte del plan general de continuidad de las actividades. El acuerdo, de nuevo a diferencia de la propuesta de la CE y en aplicación del principio de proporcionalidad, incorpora la posibilidad de un **marco simplificado de gestión del riesgo de TIC** para una serie de entidades financieras de pequeño tamaño no interconectadas.

Las ESAs, a través del Comité Mixto, elaborarán: 1) directrices sobre la estimación de los costes anuales agregados y las pérdidas causadas por incidentes graves relacionados con las TIC; 2) proyectos de normas técnicas de regulación (*Regulatory Technical Standards*, RTS por sus siglas en inglés), en consulta con la Agencia Europea para la Ciberseguridad (*European Union Agency on Cybersecurity*, ENISA por sus siglas en inglés) sobre un conjunto de elementos regulatorios y técnicos bastante extenso para lograr una mayor armonización de las herramientas, métodos, procesos y políticas de gestión del riesgo de TIC.

C**apítulo III Incidentes relacionados con las TIC: gestión, clasificación e información**

Las entidades financieras establecerán un **proceso de gestión** de incidentes relacionados con las TIC que permita una respuesta adecuada y la identificación de las causas subyacentes para prevenir nuevos incidentes a la vez que llevarán un registro de incidentes y de amenazas cibernéticas significativas. La propuesta de la CE no contemplaba referencias a las amenazas cibernéticas.

La **clasificación** de los incidentes se realiza en función de un conjunto de criterios: número de afectados y la repercusión en su reputación, duración del incidente y de la interrupción del servicio, extensión geográfica, pérdida de datos, carácter esencial de los servicios afectados y repercusión económica. Las amenazas cibernéticas se considerarán significativas en función del carácter crítico de los servicios en riesgo, el número y/o la relevancia de los posibles afectados y la distribución geográfica de las áreas afectadas. Las ESAs, a través del Comité Mixto y en consulta con el Banco Central Europeo (BCE) y ENISA, desarrollarán proyectos de RTS para especificar: a) los umbrales de importancia relativa para considerar grave un incidente relacionado con las TIC; b) los criterios que deben aplicar las ANC para valorar la importancia de un incidente grave para la ANC de otro Estado Miembro y 3) los umbrales de materialidad, para determinar cuándo una amenaza cibernética es significativa.

La **notificación** de los incidentes graves relacionados con las TIC a las ANC se realizará mediante una notificación inicial, un informe intermedio con información actualizada y un informe final cuando se conozca la causa del incidente que, independientemente de que hayan adoptado o no medidas de mitigación, incluya un análisis de impacto con cifras reales. La ANC determinará la importancia del incidente, evaluará los posibles impactos transfronterizos y adoptará (en coordinación con las ESAs y el BCE) todas las medidas necesarias para proteger la estabilidad inmediata del sistema financiero.

Las ciber amenazas significativas se pueden notificar, de forma voluntaria, cuando sea relevante para el sistema financiero, sus usuarios o clientes. En el caso de entidades de crédito clasificadas como significativas, la ANC informará de los incidentes graves y las ciber amenazas significativas al BCE. Los incidentes graves que tengan un

impacto en los intereses financieros de los clientes deberán ser, sin demora indebida, comunicados a los clientes junto con las medidas adoptadas para mitigar los efectos adversos del incidente.

Las ESAs, a través del Comité Mixto y en consulta con ENISA y el BCE, elaborarán: a) proyectos de RTS para armonizar el contenido y las plantillas de los informes teniendo en cuenta el principio de proporcionalidad, especialmente para garantizar que los diferentes plazos de presentación de información puedan reflejar, según corresponda, las especificidades de los sectores financieros y b) un informe en el que se evalúe la viabilidad del establecimiento de un centro único de la UE para la notificación de incidentes graves. El informe explorará la forma de reducir los costes asociados y mejorar la convergencia supervisora.

Capítulo IV Pruebas de resiliencia operativa digital

Las entidades financieras -distintas de las microempresas- deberán establecer, mantener y revisar un **programa de pruebas de resiliencia operativa digital** sólido y completo con un enfoque basado en el riesgo que forme parte del marco de gestión de riesgo TIC para evaluar el estado de preparación ante incidentes y detectar deficiencias en la resiliencia operativa digital. Las pruebas serán realizadas por partes independientes, externas o internas, si bien en este último caso se deberán dedicar suficientes recursos y garantizar que se eviten los conflictos de interés durante las fases de diseño y ejecución de la prueba. Las pruebas podrán consistir, por ejemplo, evaluaciones y exploraciones de vulnerabilidad, análisis del código abierto, evaluaciones de seguridad de la red, análisis de brechas, exámenes de la seguridad física, cuestionarios y soluciones de software de detección, revisiones de código fuente cuando sea factible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo o pruebas de penetración. Los DCV y las ECC realizarán evaluaciones de vulnerabilidad antes de implantar o reimplantar servicios nuevos o existentes que sustenten funciones, aplicaciones e infraestructuras esenciales. Las microempresas realizarán las pruebas combinando un enfoque basado en el riesgo con una planificación estratégica y equilibrando los recursos y tiempo empleados con y la urgencia, tipo de riesgos, importancia de los activos/servicios u otros factores relevantes.

Las entidades financieras -distintas de microempresas y de aquellas sujetas a un marco simplificado de gestión del riesgo TIC- llevarán a cabo, al menos cada tres años, **pruebas de penetración guiadas por amenazas**. La ANC podrá solicitar a la entidad financiera que reduzca o amplíe esta frecuencia e identificar las entidades que deben realizar las pruebas previa evaluación de la criticalidad de los servicios, impacto en la estabilidad financiera y perfil de riesgo ICT. La prueba cubrirá funciones y servicios esenciales y se realizarán sobre los sistemas de producción que las sustenten; el alcance concreto será determinado por la entidad y validado por la ANC.

En el caso de servicios externalizados, se adoptarán medidas para asegurar la participación de los terceros proveedores. Cuando se empleen testadores internos, deberán contratar un probador externo cada tres pruebas, si bien las entidades de crédito significativas sólo utilizarán testadores externos. Los Estados Miembros podrán designar una sola autoridad del sector financiero como responsable de los asuntos relacionados con las pruebas de penetración.

Las ESAs, previa consulta al BCE y conforme al marco TIBER-EU, elaborarán proyectos de RTS para especificar: a) el criterio de estabilidad financiera y el carácter sistémico de la entidad como determinantes de la realización de las pruebas de penetración y los requisitos de los testadores internos; b) los requisitos del alcance de las pruebas, de la metodología de cada fase y de los resultados y adopción de medidas correctoras; y c) el tipo de supervisión y otra cooperación relevante entre ANC para la implementación y el reconocimiento mutuo de dichas pruebas.

Capítulo V Gestión del riesgo de terceros relacionado con las TIC

El riesgo de terceros relacionado con las TIC es uno de los elementos integrantes del marco de gestión de los riesgos de TIC, sujeto a los principios de responsabilidad de las entidades financieras y proporcionalidad. Las entidades financieras: a) adoptarán una **estrategia** teniendo en cuenta la prestación de servicios esenciales por terceros o los múltiples proveedores (excepto microempresas o con un marco de gestión simplificado); b) mantendrán y actualizarán un **registro de información** con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros, los cuales distinguirán claramente si comprenden servicios esenciales o no y 3) informarán a la ANC de los acuerdos, en particular si están relacionados con funciones esenciales, y pondrán a su disposición el registro.

La propuesta recoge un conjunto de requisitos ex ante para los acuerdos contractuales con proveedores terceros como, por ejemplo, evaluar si se cumplen las condiciones para la supervisión o analizar el posible reforzamiento del riesgo de concentración de TIC así como determinadas causas que ponen fin al mismo -entre las que destaca que la ANC haya dejado de poder supervisar eficazmente a la entidad financiera como resultado del acuerdo-.

Las entidades financieras contarán con **estrategias de salida** de los proveedores terceros que tengan en cuenta los riesgos que puedan surgir-como fallos, deterioro de la calidad del servicio o cualquier perturbación de la actividad por falta o inadecuada prestación del servicio-.

Las ESAs, a través del Comité Mixto, elaborarán proyectos de RTS en relación con el registro de información y sobre la política a seguir en los acuerdos contractuales relativos al uso de terceros proveedores para la prestación de servicios esenciales relacionados con las TIC.

En cuanto a la **subcontratación**, cuando el acuerdo contractual incluya la posibilidad de que el proveedor tercero subcontrate, a su vez, una función esencial a otros terceros, se ponderarán los beneficios y riesgos, en particular cuando se trate de un subcontratista de TIC establecido en un tercer país. En este último caso, se tendrán en cuenta las normas sobre insolvencia, el respecto a las normas de protección de datos y las garantías de cumplimiento efectivo de la legislación en el tercer país. Las ESAs, a través del Comité Mixto, especificarán los elementos que se deberán tener en cuenta para valorar la subcontratación de funciones esenciales.

L**as ESAs, a través del Comité Mixto y por recomendación del Foro de Supervisión, designarán a: a) los proveedores terceros esenciales de servicios de TIC para las entidades financieras, conforme a los criterios establecidos en el Reglamento (carácter sistémico, interdependencia, grado de sustituibilidad, etc.); b) un supervisor principal -que será ESMA, EBA o EIOPA- para cada proveedor tercero esencial de servicios de TIC,** en función de si el valor total de los activos de las entidades financieras del mismo sector que utilizan sus servicios representan más de la mitad del valor de los activos total de todas las entidades financieras que utilizan los servicios del proveedor tercero según balance y c) notificarán al proveedor tercero la fecha a partir de la cual estarán sujetos a actividades de supervisión.

La supervisión (evaluación de normas y procedimientos para gestionar los riesgos de TIC) se centrará en los proveedores terceros que realicen funciones o servicios esenciales para las entidades financieras y, cuando sea necesario, se extenderá a otras funciones no esenciales. Sobre la base de esta evaluación y tras la coordinación de la Red Conjunta de Supervisión, el Supervisor Principal adoptará un **plan de supervisión individual** claro, detallado y razonado que describa los objetivos anuales de supervisión y las principales acciones de supervisión previstas para cada tercero proveedor esencial de servicios de TIC. En particular, el Supervisor Principal preparará una serie de recomendaciones (y, entre ellas, la prohibición de celebrar un acuerdo adicional de subcontratación en determinadas circunstancias) para los terceros proveedores e informará a la ANC y a las entidades financieras de los riesgos identificados y de las medidas adoptadas por los terceros.

El Comité Mixto establecerá el **Foro de Supervisión** como subcomité permanente con el fin de apoyar el trabajo del comité conjunto y del supervisor principal formado por: i) los presidentes de las ESAs, ii) un representante de alto nivel de la AC de cada Estado Miembro, iii) directores ejecutivos de las ESAs, un representante de la CE, de la JERS (Junta Europea de Riesgo Sistémico), del BCE y de ENISA como observadores, iv) otro representante adicional de la AC de cada Estado Miembro como observador, v) un representante de las ANC designado para la identificación de operadores de servicios esenciales conforme a la Directiva 2016/1148. Además, para avanzar hacia una mayor **convergencia supervisora**: a) el Supervisor Principal puede, después de consultar al Foro de Supervisión, emitir **opiniones no vinculantes** y no públicas a las ANC para promover medidas de seguimiento supervisoras consistentes y convergentes y b) las tres ESAs establecerán una **red conjunta de supervisión** para coordinarse en las etapas preparatorias y en la realización de actividades de supervisión, con el objetivo de adoptar estrategias generales de supervisión coordinadas. Las ESAs, a través del Comité Mixto, elaborarán proyectos de RTS para especificar un conjunto de condiciones (información a facilitar por el proveedor tercero esencial, detalle de las evaluaciones de las ANC, etc.) que permitan una mayor armonización de la supervisión.

Capítulo VI Acuerdos de intercambio de información

El texto contempla que las entidades financieras celebren acuerdos de intercambio de información en relación con información sobre ciber amenazas para mejorar la resiliencia operativa digital, especialmente mediante la sensibilización, la limitación de la capacidad de propagación, el apoyo a capacidades defensivas, las técnicas de detección, las estrategias de mitigación o las fases de respuesta y recuperación.

Capítulo VII Autoridades Competentes

Sin perjuicio de lo previsto en el marco de supervisión para terceros proveedores esenciales de servicios de TIC, las AC son las autoridades designadas en los distintos actos jurídicos del sector financiero europeo para cada tipo de entidad financiera comprendido en el ámbito subjetivo de este Reglamento.

Enlace de interés:

Texto del acuerdo provisional de la Secretaría General del Consejo al COREPER sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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 y (UE) n.º 909/2014