Continúan los preparativos para DORA



Publicado el 13 de febrero de 2023 por [**Editor**](https://www.xbrl.org/news/preparations-for-dora-continue/)

Esta semana, las Autoridades Europeas de Supervisión (ESA) celebraron un debate técnico sobre la próxima Ley de resiliencia operativa digital (DORA). DORA tiene como objetivo armonizar los requisitos de resiliencia operativa digital en toda la UE y entrará en vigor el 16 de enero de 2023, aplicable a partir del 17 de enero de 2025.

DORA tiene como objetivo aumentar la resiliencia del sector financiero con la nueva regulación que requiere que las empresas tengan una seguridad cibernética fuerte. Los mandatos de política discutidos esta semana incluyen la gestión de riesgos de TIC, la notificación de incidentes, el registro de información y los criterios de criticidad.

DORA es una pieza importante de la legislación que tendrá un impacto en las partes interesadas en múltiples sectores que suministran servicios financieros a los actores. Se espera que una consulta abierta contribuya al desarrollo de los mandatos de políticas (el RTS aún no se ha publicado). Observe este espacio para ver los desarrollos.

Lea más y acceda a las presentaciones del evento [aquí](https://www.eba.europa.eu/european-supervisory-authorities-meet-stakeholders-across-financial-sector-amid-preparations-digital).

[CIBERSEGURIDAD](https://www.xbrl.org/tag/cybersecurity/) [DORA](https://www.xbrl.org/tag/dora/) [UE](https://www.xbrl.org/tag/eu/) [EUROPA](https://www.xbrl.org/tag/europe/)



(1) En la era digital, las tecnologías de la información y la comunicación (TIC) soportan sistemas complejos que se utilizan para las actividades sociales cotidianas. Mantiene nuestras economías en funcionamiento en sectores clave, incluidas las finanzas, y mejora el funcionamiento del mercado único. El aumento de la digitalización y la interconexión también amplifica los riesgos de las TIC, lo que hace que la sociedad en su conjunto, y el sistema financiero en particular, sea más vulnerable a las amenazas cibernéticas o las interrupciones de las TIC. Si bien el uso ubicuo de los sistemas de TIC y la alta digitalización y conectividad son hoy en día características centrales de todas las actividades de las entidades financieras de la Unión, la resiliencia digital aún no está suficientemente integrada en sus marcos operativos.

(2) El uso de las TIC ha ganado en las últimas décadas un papel central en las finanzas, asumiendo hoy una relevancia crítica en la operación de las funciones diarias típicas de todas las entidades financieras. La digitalización cubre, por ejemplo, los pagos, que se han desplazado cada vez más de los métodos en efectivo y en papel al uso de soluciones digitales, así como la compensación y liquidación de valores, el comercio electrónico y algorítmico, las operaciones de préstamo y financiación, la financiación entre pares, calificación crediticia, suscripción de seguros, gestión de siniestros y operaciones administrativas. Las finanzas no solo se han vuelto en gran medida digitales en todo el sector, sino que la digitalización también ha profundizado las interconexiones y dependencias dentro del sector financiero y con proveedores de servicios e infraestructura de terceros.

(3) La Junta Europea de Riesgo Sistémico (JERS) ha reafirmado en un informe de 2020 que aborda el riesgo cibernético sistémico [27](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote28) ​​cómo el alto nivel existente de interconexión entre las entidades financieras, los mercados financieros y las infraestructuras de los mercados financieros, y en particular las interdependencias de sus sistemas de TIC, puede constituir potencialmente un vulnerabilidad sistémica, ya que los ciber incidentes localizados podrían propagarse rápidamente desde cualquiera de las aproximadamente 22 000 entidades financieras de la Unión [28](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote29) a todo el sistema financiero, sin obstáculos geográficos. Las infracciones graves en materia de TIC que se producen en las finanzas no afectan únicamente a las entidades financieras de forma aislada. También allanan el camino para la propagación de vulnerabilidades localizadas a través de los canales de transmisión financiera y pueden desencadenar consecuencias adversas para la estabilidad del sistema financiero de la Unión, generando corridas de liquidez y una pérdida general de confianza en los mercados financieros.

(4) En los últimos años, los riesgos de las TIC han atraído la atención de los responsables políticos, reguladores y organismos normativos nacionales, europeos e internacionales en un intento por mejorar la resiliencia, establecer estándares y coordinar el trabajo de regulación o supervisión. A nivel internacional, el Comité de Supervisión Bancaria de Basilea, el Comité de Pagos e Infraestructuras de Mercados, el Consejo de Estabilidad Financiera, el Instituto de Estabilidad Financiera, así como los grupos de países G7 y G20 tienen como objetivo proporcionar autoridades competentes y operadores de mercado en diferentes jurisdicciones con herramientas para reforzar la resiliencia de sus sistemas financieros.

(5) A pesar de las iniciativas políticas y legislativas específicas nacionales y europeas, los riesgos de las TIC siguen planteando un desafío para la resiliencia operativa, el rendimiento y la estabilidad del sistema financiero de la Unión. La reforma que siguió a la crisis financiera de 2008 reforzó principalmente la resiliencia financiera del sector financiero de la Unión y tenía como objetivo salvaguardar la competitividad y la estabilidad de la Unión desde las perspectivas de conducta económica, prudencial y de mercado. Aunque la seguridad de las TIC y la resiliencia digital son parte del riesgo operativo, han estado menos en el centro de la agenda regulatoria posterior a la crisis, y solo se han desarrollado en algunas áreas del panorama normativo y normativo de los servicios financieros de la Unión, o solo en unos pocos miembros. estados

(6) El plan de acción Fintech de la Comisión de 2018 [29](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote30) destacó la importancia primordial de hacer que el sector financiero de la Unión sea más resistente también desde una perspectiva operativa para garantizar su seguridad tecnológica y su buen funcionamiento, su rápida recuperación de las infracciones e incidentes de las TIC y, en última instancia, permitir que los servicios financieros sean eficaces y efectivos. entregados sin problemas en toda la Unión, incluso en situaciones de estrés, preservando al mismo tiempo la confianza de los consumidores y del mercado.

(7) En abril de 2019, la Autoridad Bancaria Europea (EBA), la Autoridad Europea de Valores y Mercados (ESMA) y la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) (conjuntamente denominadas “Autoridades Europeas de Supervisión” o “ESA”) emitieron conjuntamente dos piezas de asesoramiento técnico que pide un enfoque coherente del riesgo de las TIC en las finanzas y recomienda reforzar, de forma proporcionada, la resiliencia operativa digital del sector de los servicios financieros a través de una iniciativa sectorial específica de la Unión.

(8) El sector financiero de la Unión está regulado por un código normativo único armonizado y se rige por un sistema europeo de supervisión financiera. No obstante, las disposiciones que abordan la resiliencia operativa digital y la seguridad de las TIC aún no están armonizadas total o uniformemente, a pesar de que la resiliencia operativa digital es vital para garantizar la estabilidad financiera y la integridad del mercado en la era digital, y no menos importante que, por ejemplo, las normas comunes de conducta prudencial o de mercado. Por lo tanto, el Reglamento Único y el sistema de supervisión deben desarrollarse para cubrir también este componente, ampliando los mandatos de los supervisores financieros encargados de monitorear y proteger la estabilidad financiera y la integridad del mercado.

(9) Las disparidades legislativas y los enfoques reguladores o supervisores nacionales desiguales sobre el riesgo de las TIC crean obstáculos al mercado único de servicios financieros, lo que impide el ejercicio fluido de la libertad de establecimiento y la prestación de servicios para las entidades financieras con presencia transfronteriza. La competencia entre el mismo tipo de entidades financieras que operan en diferentes Estados miembros puede verse igualmente distorsionada. En particular, en áreas en las que la armonización de la Unión ha sido muy limitada -como las pruebas de resiliencia operativa digital- o inexistente -como la supervisión del riesgo de terceros de las TIC-, las disparidades derivadas de los desarrollos previstos a nivel nacional podrían generar nuevos obstáculos para el funcionamiento del mercado único en detrimento de los participantes en el mercado y de la estabilidad financiera.

(10) La forma parcial en que las disposiciones relacionadas con los riesgos de las TIC se han abordado hasta ahora a nivel de la Unión muestra lagunas o superposiciones en áreas importantes, como la notificación de incidentes relacionados con las TIC y las pruebas de resiliencia operativa digital, y crea incoherencias debido a la aparición de normas nacionales divergentes o aplicación rentable de reglas superpuestas. Esto es especialmente perjudicial para un usuario intensivo en TIC como las finanzas, ya que los riesgos tecnológicos no tienen fronteras y el sector financiero despliega sus servicios de forma transfronteriza dentro y fuera de la Unión.

Entidades financieras individuales que operan de forma transfronteriza o que poseen varias autorizaciones (por ejemplo, una entidad financiera puede tener una licencia bancaria, de empresa de inversión y de entidad de pago, cada una de ellas emitida por una autoridad competente diferente en uno o varios Estados miembros) enfrentan desafíos operativos para abordar los riesgos de TIC y mitigar los impactos adversos de los incidentes de TIC por sí mismos y de una manera coherente y rentable.

(11) Dado que el Reglamento Único no ha ido acompañado de un marco integral de riesgo operativo o de TIC, se requiere una mayor armonización de los requisitos clave de resiliencia operativa digital para todas las entidades financieras. Las capacidades y la resiliencia general que desarrollarían las entidades financieras, sobre la base de tales requisitos clave, con el fin de soportar interrupciones operativas, ayudarían a preservar la estabilidad y la integridad de los mercados financieros de la Unión y contribuirían así a garantizar un alto nivel de protección de los inversores y consumidores de la Unión. Dado que el presente Reglamento tiene por objeto contribuir al buen funcionamiento del mercado único, debe basarse en las disposiciones del artículo 114 del TFUE interpretadas de conformidad con la jurisprudencia reiterada del Tribunal de Justicia de la Unión Europea.

(12) Este Reglamento tiene como objetivo, en primer lugar, consolidar y mejorar los requisitos de riesgo de las TIC abordados hasta ahora por separado en los diferentes Reglamentos y Directivas. Mientras que esos, los actos jurídicos de la Unión cubrían las principales categorías de riesgo financiero (por ejemplo, riesgo de crédito, riesgo de mercado, riesgo de crédito y de liquidez de la contraparte, riesgo de conducta del mercado), pero no podían abordar de forma exhaustiva, en el momento de su adopción, todos los componentes de la resiliencia operativa. Los requisitos de riesgo operativo, cuando se desarrollaron más en estos actos jurídicos de la Unión, a menudo favorecieron un enfoque cuantitativo tradicional para abordar el riesgo (es decir, establecer un requisito de capital para cubrir los riesgos de TIC) en lugar de consagrar requisitos cualitativos específicos para impulsar las capacidades a través de requisitos destinados a la protección, capacidades de detección, contención, recuperación y reparación frente a incidentes relacionados con las TIC o mediante el establecimiento de capacidades de informes y pruebas digitales.

A través de este ejercicio, que consolida y actualiza las normas sobre el riesgo de las TIC, todas las disposiciones que abordan el riesgo digital en las finanzas se reunirían por primera vez de manera coherente en un único acto legislativo. Por lo tanto, esta iniciativa debería llenar los vacíos o subsanar las incoherencias en algunos de esos actos jurídicos, incluso en relación con la terminología utilizada en ellos, y debería hacer referencia explícita al riesgo de TIC a través de normas específicas sobre capacidades de gestión de riesgos de TIC, informes y pruebas y riesgo de terceros. supervisión.

(13) Las entidades financieras deben seguir el mismo enfoque y las mismas reglas basadas en principios al abordar el riesgo de TIC. La consistencia contribuye a aumentar la confianza en el sistema financiero y preservar su estabilidad, especialmente en tiempos de uso excesivo de los sistemas, plataformas e infraestructuras TIC, lo que conlleva un mayor riesgo digital.

El respeto de una higiene cibernética básica también debería evitar imponer altos costos a la economía al minimizar el impacto y los costos de las interrupciones de las TIC.

(14) El uso de una regulación ayuda a reducir la complejidad regulatoria, fomenta la convergencia de la supervisión, aumenta la seguridad jurídica, al mismo tiempo que contribuye a limitar los costos de cumplimiento, especialmente para las entidades financieras que operan en el extranjero, y a reducir las distorsiones competitivas. La elección de un Reglamento para el establecimiento de un marco común para la resiliencia operativa digital de las entidades financieras parece, por tanto, la forma más adecuada de garantizar una aplicación homogénea y coherente de todos los componentes de la gestión de riesgos de las TIC por parte de los sectores financieros de la Unión.

(15) Además de la legislación sobre servicios financieros, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo [30](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote31) es el actual marco general de ciberseguridad a nivel de la Unión. Entre los siete sectores críticos, esa Directiva también se aplica a tres tipos de entidades financieras, a saber, entidades de crédito, centros de negociación y entidades de contrapartida central. Sin embargo, dado que la Directiva (UE) 2016/1148 establece un mecanismo de identificación a nivel nacional de los operadores de servicios esenciales, en la práctica solo se incluyen en su ámbito de aplicación determinadas entidades de crédito, centros de negociación y entidades de contrapartida central identificadas por los Estados miembros, por lo que se les exige para cumplir con los requisitos de seguridad TIC y notificación de incidentes establecidos en el mismo.

(16) Dado que el presente Reglamento eleva el nivel de armonización de los componentes de resiliencia digital, al introducir requisitos sobre la gestión de riesgos de las TIC y la notificación de incidentes relacionados con las TIC que son más estrictos con respecto a los establecidos en la actual legislación de la Unión sobre servicios financieros, esto constituye también una mayor armonización en comparación con los requisitos establecidos en la Directiva (UE) 2016/1148. En consecuencia, el presente Reglamento constituye los especialistas de la Directiva (UE) 2016/1148.

Es crucial mantener una fuerte relación entre el sector financiero y el marco de ciberseguridad horizontal de la Unión que garantizaría la coherencia con las estrategias de ciberseguridad ya adoptadas por los Estados miembros y permitiría que los supervisores financieros estuvieran al tanto de los ciber incidentes que afectan a otros sectores cubiertos por la Directiva (UE) 2016/1148.

(17) Para permitir un proceso de aprendizaje intersectorial y aprovechar de manera efectiva las experiencias de otros sectores para hacer frente a las ciber amenazas, las entidades financieras a las que se hace referencia en la Directiva (UE) 2016/1148 deben seguir formando parte del «ecosistema» de dicha Directiva (por ejemplo, el Grupo de Cooperación NIS y CSIRT).

Las AES y las autoridades nacionales competentes, respectivamente, deben poder participar en los debates de política estratégica y los trabajos técnicos del Grupo de Cooperación NIS, respectivamente, intercambiar información y seguir cooperando con los puntos de contacto únicos designados en virtud de la Directiva (UE) 2016/1148. Las autoridades competentes en virtud del presente Reglamento también deben consultar y cooperar con los CSIRT nacionales designados de conformidad con el artículo 9 de la Directiva (UE) 2016/1148.

(18) También es importante garantizar la coherencia con la Directiva Europea de Infraestructura Crítica (ECI), que actualmente se está revisando para mejorar la protección y la resiliencia de las infraestructuras críticas contra amenazas no relacionadas con la cibernética, con posibles implicaciones para el sector financiero. [31](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote32)

(19) Los proveedores de servicios de computación en la nube son una categoría de proveedores de servicios digitales cubiertos por la Directiva (UE) 2016/1148. Como tales, están sujetos a la supervisión ex post que llevan a cabo las autoridades nacionales designadas de conformidad con dicha Directiva, que se limita a los requisitos sobre seguridad de las TIC y notificación de incidentes establecidos en dicha ley. Dado que el marco de supervisión establecido por el presente Reglamento se aplica a todos los proveedores de servicios críticos de terceros de TIC, incluidos los proveedores de servicios de computación en la nube, cuando prestan servicios de TIC a entidades financieras, debe considerarse complementario a la supervisión que se lleva a cabo en virtud de la Directiva (UE) 2016/1148. Además,

(20) Para mantener el control total de los riesgos de TIC, las entidades financieras deben contar con capacidades integrales que permitan una gestión de riesgos de TIC sólida y eficaz, junto con mecanismos y políticas específicos para la notificación de incidentes relacionados con las TIC, pruebas de sistemas, controles y procesos de TIC, así como como para la gestión del riesgo de terceros TIC. Debe elevarse el listón de la resiliencia operativa digital del sistema financiero, al tiempo que se permite una aplicación proporcionada de los requisitos para las entidades financieras que son microempresas tal como se definen en la Recomendación 2003/361/CE de la Comisión [32](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote33) .

(21) Los umbrales y las taxonomías de notificación de incidentes relacionados con las TIC varían significativamente a nivel nacional. Si bien se puede lograr un terreno común a través del trabajo relevante realizado por la Agencia de Ciberseguridad de la Unión Europea (ENISA) [33](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote34) y el Grupo de Cooperación NIS para las entidades financieras bajo la Directiva (UE) 2016/1148, aún existen o pueden surgir enfoques divergentes sobre umbrales y taxonomías para el resto de las entidades financieras. Esto implica múltiples requisitos que las entidades financieras deben cumplir, especialmente cuando operan en varias jurisdicciones de la Unión y cuando forman parte de un grupo financiero. Además, estas divergencias pueden dificultar la creación de más mecanismos uniformes o centralizados de la Unión que aceleren el proceso de notificación y respalden un intercambio de información rápido y fluido entre las autoridades competentes, lo cual es crucial para abordar los riesgos de las TIC en caso de ataques a gran escala con consecuencias potencialmente sistémicas.

(22) Para permitir que las autoridades competentes cumplan con sus funciones de supervisión mediante la obtención de una visión completa de la naturaleza, frecuencia, importancia e impacto de los incidentes relacionados con las TIC y para mejorar el intercambio de información entre las autoridades públicas pertinentes, incluidas las autoridades encargadas de hacer cumplir la ley y las autoridades de resolución, es necesario establecer reglas para completar el régimen de notificación de incidentes relacionados con las TIC con los requisitos que actualmente faltan en la legislación del subsector financiero y eliminar las superposiciones y duplicidades existentes para aliviar los costos. Por lo tanto, es fundamental armonizar el régimen de notificación de incidentes relacionados con las TIC exigiendo que todas las entidades financieras informen únicamente a sus autoridades competentes. Además, las ESA deben estar facultadas para especificar aún más los elementos de notificación de incidentes relacionados con las TIC, como la taxonomía,

(23) Los requisitos de prueba de resiliencia operativa digital se han desarrollado en algunos subsectores financieros dentro de varios marcos nacionales no coordinados que abordan los mismos problemas de una manera diferente. Esto conduce a la duplicación de costos para las entidades financieras transfronterizas y dificulta el reconocimiento mutuo de los resultados. Por lo tanto, las pruebas no coordinadas pueden segmentar el mercado único.

(24) Además, cuando no se requieren pruebas, las vulnerabilidades permanecen sin detectar, lo que pone a la entidad financiera y, en última instancia, a la estabilidad e integridad del sector financiero en mayor riesgo. Sin la intervención de la Unión, las pruebas de resiliencia operativa digital seguirían siendo irregulares y no habría reconocimiento mutuo de los resultados de las pruebas en diferentes jurisdicciones. Además, dado que es poco probable que otros subsectores financieros adopten tales esquemas en una escala significativa, se perderían los beneficios potenciales, como revelar vulnerabilidades y riesgos, probar las capacidades de defensa y la continuidad del negocio, y aumentar la confianza de los clientes, proveedores y Compañeros de negocio. Para remediar tales superposiciones, divergencias y lagunas, es necesario establecer normas destinadas a realizar pruebas coordinadas por parte de las entidades financieras y las autoridades competentes,

(25) La dependencia de las entidades financieras en los servicios de TIC se debe en parte a su necesidad de adaptarse a una economía global digital competitiva emergente, para impulsar su eficiencia comercial y satisfacer la demanda de los consumidores. La naturaleza y el alcance de dicha dependencia ha evolucionado continuamente en los últimos años, impulsando la reducción de costos en la intermediación financiera, permitiendo la expansión comercial y la escalabilidad en el despliegue de actividades financieras al tiempo que ofrece una amplia gama de herramientas TIC para administrar procesos internos complejos.

(26) Este uso extensivo de los servicios de TIC se evidencia en arreglos contractuales complejos, en los que las entidades financieras a menudo encuentran dificultades para negociar términos contractuales que se ajusten a las normas prudenciales u otros requisitos reglamentarios a los que están sujetas, o para hacer valer derechos específicos, como el acceso o derechos de auditoría, cuando éstos estén consagrados en los convenios. Además, muchos de estos contratos no prevén garantías suficientes que permitan un seguimiento completo de los procesos de subcontratación, lo que priva a la entidad financiera de su capacidad para evaluar estos riesgos asociados. Además, dado que los proveedores de servicios de TIC de terceros a menudo brindan servicios estandarizados a diferentes tipos de clientes, es posible que dichos contratos no siempre satisfagan adecuadamente las necesidades individuales o específicas de los actores de la industria financiera.

(27) A pesar de algunas normas generales sobre externalización en algunos actos legislativos de servicios financieros de la Unión, el control de la dimensión contractual no está plenamente arraigado en la legislación de la Unión. A falta de normas de la Unión claras y personalizadas que se apliquen a los acuerdos contractuales celebrados con terceros proveedores de servicios de TIC, la fuente externa de riesgo de TIC no se aborda de forma exhaustiva. En consecuencia, es necesario establecer ciertos principios clave que guíen la gestión del riesgo de terceros TIC por parte de las entidades financieras, acompañados de un conjunto de derechos contractuales básicos en relación con varios elementos en la ejecución y terminación de los contratos con el fin de consagrar ciertos salvaguardias mínimas que sustentan la capacidad de las entidades financieras para monitorear de manera efectiva todos los riesgos que surgen a nivel de terceros de TIC.

(28) Existe una falta de homogeneidad y convergencia sobre el riesgo de terceros de TIC y las dependencias de terceros de TIC. A pesar de algunos esfuerzos para abordar el área específica de la subcontratación, como las recomendaciones de 2017 sobre la subcontratación a proveedores de servicios en la nube, [34](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote35) el problema del riesgo sistémico que puede ser desencadenado por la exposición del sector financiero a un número limitado de proveedores de servicios externos de TIC críticos es apenas se aborda en la legislación de la Unión. Esta carencia a nivel de la Unión se ve agravada por la ausencia de mandatos y herramientas específicos que permitan a los supervisores nacionales adquirir una buena comprensión de las dependencias de terceros de TIC y controlar adecuadamente los riesgos derivados de la concentración de dichas dependencias de terceros de TIC.

(29) Teniendo en cuenta los posibles riesgos sistémicos que implican el aumento de las prácticas de subcontratación y la concentración de terceros de TIC, y conscientes de la insuficiencia de los mecanismos nacionales que permiten a los superiores financieros cuantificar, calificar y corregir las consecuencias de los riesgos de TIC que se producen en terceros críticos de TIC, terceros proveedores de servicios, es necesario establecer un marco de supervisión de la Unión adecuado que permita un seguimiento continuo de las actividades de los terceros proveedores de servicios de TIC que son proveedores críticos para las entidades financieras.

(30) Con las amenazas de las TIC cada vez más complejas y sofisticadas, las buenas medidas de detección y prevención dependen en gran medida del intercambio regular de inteligencia sobre amenazas y vulnerabilidades entre las entidades financieras. El intercambio de información contribuye a una mayor conciencia sobre las amenazas cibernéticas, lo que, a su vez, mejora la capacidad de las entidades financieras para evitar que las amenazas se materialicen en incidentes reales y les permite contener mejor los efectos de los incidentes relacionados con las TIC y recuperarse de manera más eficiente. A falta de orientación a nivel de la Unión, varios factores parecen haber inhibido dicho intercambio de inteligencia, en particular la incertidumbre sobre la compatibilidad con las normas de protección de datos, antimonopolio y responsabilidad.

(31) Además, las dudas sobre el tipo de información que se puede compartir con otros participantes del mercado, o con autoridades no supervisoras (como ENISA, para datos analíticos, o Europol, con fines policiales) conducen a la retención de información útil. El alcance y la calidad del intercambio de información siguen siendo limitados, fragmentados, y los intercambios pertinentes se realizan principalmente a nivel local (a través de iniciativas nacionales) y sin acuerdos coherentes de intercambio de información a nivel de la Unión adaptados a las necesidades de un sector financiero integrado.

(32) Por lo tanto, se debe alentar a las entidades financieras a aprovechar colectivamente su conocimiento individual y experiencia práctica a nivel estratégico, táctico y operativo con el fin de mejorar sus capacidades para evaluar, monitorear, defenderse y responder adecuadamente a las amenazas cibernéticas. Por lo tanto, es necesario permitir el surgimiento a nivel de la Unión de mecanismos para acuerdos voluntarios de intercambio de información que, cuando se llevan a cabo en entornos confiables, ayudarían a la comunidad financiera a prevenir y responder colectivamente a las amenazas al limitar rápidamente la propagación de los riesgos de las TIC e impedir el contagio potencial. a través de los canales financieros. Esos mecanismos deben llevarse a cabo en pleno cumplimiento de las normas aplicables del derecho de la competencia de la Unión [35](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote36) así como de forma que garantice el pleno respeto de las normas de protección de datos de la Unión, principalmente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 36 en particular en el [contexto](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote37) del tratamiento de datos personales que sea necesario para los fines del interés legítimo perseguido por el responsable del tratamiento o por un tercero, a que se refiere el artículo 6, apartado 1, letra f), de dicho Reglamento.

(33) Sin perjuicio de la amplia cobertura prevista por el presente Reglamento, la aplicación de las normas de resiliencia operativa digital debe tener en cuenta las diferencias significativas entre entidades financieras en términos de tamaño, perfiles de negocio o exposición al riesgo digital. Como principio general, al dirigir recursos y capacidades a la implementación del marco de gestión de riesgos de las TIC, las entidades financieras deben equilibrar debidamente sus necesidades relacionadas con las TIC con su tamaño y perfil comercial, mientras que las autoridades competentes deben continuar evaluando y revisando el enfoque de tal distribución.

(34) Dado que las entidades financieras más grandes pueden disfrutar de mayores recursos y podrían desplegar fondos rápidamente para desarrollar estructuras de gobernanza y establecer diversas estrategias corporativas, solo las entidades financieras que no sean microempresas en el sentido del presente Reglamento deben estar obligadas a establecer mecanismos de gobernanza más complejos. Estas entidades están mejor equipadas, en particular, para establecer funciones de gestión dedicadas a la supervisión de acuerdos con terceros proveedores de servicios de TIC o para hacer frente a la gestión de crisis, para organizar su gestión de riesgos de TIC de acuerdo con el modelo de las tres líneas de defensa, o para adoptar un enfoque humano. documento de recursos que explica exhaustivamente las políticas de derechos de acceso.

Del mismo modo, solo dichas entidades financieras deben ser llamadas a realizar evaluaciones profundas después de cambios importantes en las infraestructuras y procesos de la red y del sistema de información, para realizar periódicamente análisis de riesgo en los sistemas de TIC heredados, o ampliar las pruebas de continuidad y respuesta del negocio. y planes de recuperación para capturar escenarios de cambios entre la infraestructura primaria de TIC y las instalaciones redundantes.

(35) Además, dado que solo las entidades financieras identificadas como significativas a los efectos de las pruebas avanzadas de resiliencia digital deberían estar obligadas a realizar pruebas de penetración dirigidas por amenazas, los procesos administrativos y los costos financieros que implica la realización de tales pruebas deben devolverse a un pequeño porcentaje de entidades financieras. Finalmente, con miras a aliviar las cargas regulatorias, solo se debe solicitar a las entidades financieras que no sean microempresas que informen regularmente a las autoridades competentes sobre todos los costos y pérdidas causados ​​por las interrupciones de las TIC y los resultados de las revisiones posteriores al incidente luego de interrupciones significativas de las TIC.

(36) Para garantizar la plena alineación y la coherencia general entre las estrategias comerciales de las entidades financieras, por un lado, y la conducción de la gestión de riesgos de TIC, por otro lado, debe exigirse al órgano de administración que mantenga un papel fundamental y activo en la dirección y adaptación de la Marco de gestión de riesgos de TIC y la estrategia general de resiliencia digital. El enfoque que debe adoptar el órgano de administración no solo debe centrarse en los medios para garantizar la resiliencia de los sistemas de TIC, sino que también debe cubrir a las personas y los procesos a través de un conjunto de políticas que cultiven, en cada nivel corporativo y para todo el personal, un fuerte sentido de conciencia sobre los riesgos cibernéticos y un compromiso de respetar una estricta higiene cibernética en todos los niveles.

La responsabilidad final del órgano de administración en la gestión de los riesgos de TIC de una entidad financiera debe ser un principio general de ese enfoque integral, traducido además en la participación continua del órgano de administración en el control del seguimiento de la gestión de riesgos de TIC.

(37) Además, la plena rendición de cuentas del órgano de administración va de la mano con la garantía de un nivel de inversiones en TIC y un presupuesto general para que la entidad financiera pueda alcanzar su línea de base de resiliencia operativa digital.

(38) Inspirándose en las normas, directrices, recomendaciones o enfoques internacionales, nacionales y establecidos por la industria pertinentes para la gestión del riesgo cibernético, 37 [este](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote38) Reglamento promueve un conjunto de funciones que facilitan la estructuración general de la gestión del riesgo de las TIC. Mientras las principales capacidades que las entidades financieras pongan en marcha respondan a las necesidades de los objetivos previstos por las funciones (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución y comunicación) establecidas en este Reglamento, las entidades financieras seguirán siendo Modelos de gestión de riesgos de TIC de libre uso que se enmarcan o clasifican de manera diferente.

(39) Para seguir el ritmo de un panorama de amenazas cibernéticas en evolución, las entidades financieras deben mantener sistemas de TIC actualizados que sean confiables y dotados de la capacidad suficiente no solo para garantizar el procesamiento de datos según sea necesario para el desempeño de sus servicios, sino también para asegurar la resiliencia tecnológica. permitiendo a las entidades financieras atender adecuadamente las necesidades de procesamiento adicionales que puedan generar condiciones de estrés en el mercado u otras situaciones adversas. Si bien este Reglamento no implica ningún anormalización de sistemas, herramientas o tecnologías TIC específicos, se basa en el uso adecuado por parte de las entidades financieras de las normas técnicas europeas e internacionalmente reconocidas (por ejemplo, ISO) o las mejores prácticas de la industria, en la medida en que dicho uso cumpla plenamente con las instrucciones de supervisión específicas sobre el uso y incorporación de estándares internacionales.

(40) Se requieren planes eficientes de recuperación y continuidad del negocio que permitan a las entidades financieras resolver de forma rápida y oportuna los incidentes relacionados con las TIC, en particular los ciberataques, limitando los daños y dando prioridad a la reanudación de actividades y acciones de recuperación. Sin embargo, si bien los sistemas de respaldo deben comenzar a procesarse sin demoras indebidas, dicho inicio no debe poner en peligro de ninguna manera la integridad y seguridad de la red y los sistemas de información o la confidencialidad de los datos.

(41) Si bien este Reglamento permite a las entidades financieras determinar los objetivos de tiempo de recuperación de manera flexible y, por lo tanto, establecer tales objetivos teniendo plenamente en cuenta la naturaleza y la criticidad de la función relevante y cualquier necesidad comercial específica, una evaluación del impacto general potencial en la eficiencia del mercado también debería exigirse al determinar dichos objetivos.

(42) Las consecuencias significativas de los ataques cibernéticos se amplifican cuando ocurren en el sector financiero, un área que corre mucho más riesgo de ser el objetivo de propagadores maliciosos que buscan ganancias financieras directamente en la fuente. Para mitigar tales riesgos y evitar que los sistemas de TIC pierdan integridad o dejen de estar disponibles, que se vulneren datos confidenciales o que la infraestructura física de TIC sufra daños, la notificación de los principales incidentes relacionados con las TIC por parte de las entidades financieras debe mejorarse significativamente.

La notificación de incidentes relacionados con las TIC debe armonizarse para todas las entidades financieras exigiéndoles que informen únicamente a sus autoridades competentes. Si bien todas las entidades financieras estarían sujetas a este informe, no todas deberían verse afectadas de la misma manera, ya que los umbrales de materialidad y los plazos pertinentes deben calibrarse para capturar solo los principales incidentes relacionados con las TIC. La notificación directa permitiría el acceso de los supervisores financieros a la información sobre incidentes relacionados con las TIC. No obstante, los supervisores financieros deben transmitir esta información a las autoridades públicas no financieras (autoridades competentes NIS, autoridades nacionales de protección de datos y autoridades policiales para incidentes de naturaleza delictiva). La información de incidentes relacionados con las TIC debe canalizarse mutuamente:

(43) Debería preverse una mayor reflexión sobre la posible centralización de los informes de incidentes relacionados con las TIC, por medio de un único Centro de la UE central que reciba directamente los informes pertinentes y notifique automáticamente a las autoridades nacionales competentes, o que simplemente centralice los informes enviados por las autoridades nacionales competentes y cumpla una función de coordinación. Las ESA deberían estar obligadas a preparar, en consulta con el BCE y ENISA, antes de una fecha determinada, un informe conjunto que explore la viabilidad de establecer un Centro de la UE central de este tipo.

(44) Con el fin de lograr una resiliencia operativa digital robusta, y en línea con los estándares internacionales (p. ej., los Elementos fundamentales G7 para las pruebas de penetración dirigidas por amenazas), las entidades financieras deben probar periódicamente sus sistemas y personal de TIC con respecto a la efectividad de sus sistemas preventivos, de detección y de respuesta. y capacidades de recuperación, para descubrir y abordar las posibles vulnerabilidades de las TIC Para responder a las diferencias entre y dentro de los subsectores financieros con respecto a la preparación de las entidades financieras en materia de seguridad cibernética, las pruebas deben incluir una amplia variedad de herramientas y acciones, que van desde una evaluación de los requisitos básicos (por ejemplo, evaluaciones y escaneos de vulnerabilidades, análisis de fuente abierta, evaluaciones de seguridad de red, análisis de brechas, revisiones de seguridad física, cuestionarios y soluciones de software de escaneo, revisiones de código fuente cuando sea factible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento o pruebas de extremo a extremo) hasta pruebas más avanzadas (por ejemplo, TLPT para aquellas entidades financieras lo suficientemente maduras desde una perspectiva de TIC para ser capaces de llevar a cabo dichas pruebas). Por lo tanto, las pruebas de resiliencia operativa digital deberían ser más exigentes para las entidades financieras importantes (como las grandes instituciones de crédito, las bolsas de valores, los depósitos centrales de valores, las contrapartes centrales, etc.). Al mismo tiempo, las pruebas de resiliencia operativa digital también deberían ser más relevantes para algunos subsectores que desempeñan un papel sistémico central (por ejemplo, pagos, banca, compensación y liquidación), y menos relevante para otros subsectores (por ejemplo, gestores de activos, agencias de calificación crediticia, etc.). Las entidades financieras transfronterizas que ejerzan su libertad de establecimiento o prestación de servicios dentro de la Unión deben cumplir un conjunto único de requisitos de prueba avanzada (por ejemplo, TLPT) en su Estado miembro de origen, y esa prueba debe incluir las infraestructuras de TIC en todas las jurisdicciones donde grupo transfronterizo opera dentro de la Unión, lo que permite a los grupos transfronterizos incurrir en costos de prueba en una sola jurisdicción.

(45) Para garantizar un seguimiento sólido del riesgo de terceros de TIC, es necesario establecer un conjunto de reglas basadas en principios para guiar el seguimiento de los riesgos que surgen en el contexto de las funciones subcontratadas a proveedores de servicios de terceros de TIC por parte de las entidades financieras y, más generalmente, en el contexto de las dependencias de terceros de las TIC.

(46) Una entidad financiera debe seguir siendo en todo momento plenamente responsable del cumplimiento de las obligaciones en virtud del presente Reglamento. Debería organizarse un seguimiento proporcionado de los riesgos que surjan a nivel del proveedor de servicios de TIC de terceros, teniendo debidamente en cuenta la escala, la complejidad y la importancia de las dependencias relacionadas con las TIC, la criticidad o la importancia de los servicios, procesos o funciones sujetos al contrato. y, en última instancia, sobre la base de una evaluación cuidadosa de cualquier impacto potencial en la continuidad y calidad de los servicios financieros a nivel individual y de grupo, según corresponda.

(47) La realización de dicho seguimiento debe seguir un enfoque estratégico del riesgo de terceros de TIC formalizado a través de la adopción por parte del órgano de administración de la entidad financiera de una estrategia específica, arraigada en una evaluación continua de todas esas dependencias de terceros de TIC. Para mejorar la conciencia de los supervisores sobre las dependencias de terceros de las TIC, y con el fin de seguir apoyando el Marco de Supervisión establecido por el presente Reglamento, los supervisores financieros deben recibir regularmente información esencial de los Registros y deben poder solicitar extractos de la misma de forma ad hoc.

(48) Un análisis exhaustivo previo a la contratación debe respaldar y preceder a la conclusión formal de los acuerdos contractuales, mientras que la rescisión de los contratos debe ser provocada por al menos un conjunto de circunstancias que muestren deficiencias en el proveedor de servicios de TIC externo.

(49) Para hacer frente al impacto sistémico del riesgo de concentración de terceros de TIC, se debe promover una solución equilibrada a través de un enfoque flexible y gradual, ya que los topes rígidos o las limitaciones estrictas pueden obstaculizar la conducta empresarial y la libertad contractual. Las entidades financieras deben evaluar exhaustivamente los acuerdos contractuales para identificar la probabilidad de que surja dicho riesgo, incluso mediante análisis en profundidad de los acuerdos de subcontratación, especialmente cuando se celebren con terceros proveedores de servicios de TIC establecidos en un tercer país. En esta etapa, y con el fin de lograr un justo equilibrio entre el imperativo de preservar la libertad contractual y el de garantizar estabilidad financiera, no se considera apropiado prever topes y límites estrictos a las exposiciones de terceros de TIC. La ESA designada para llevar a cabo la supervisión de cada proveedor externo crítico de TIC ("el supervisor principal") debe, en el ejercicio de las tareas de supervisión, prestar especial atención para comprender completamente la magnitud de las interdependencias y descubrir instancias específicas donde existe un alto grado de concentración de Es probable que los terceros proveedores de servicios de TIC críticos en la Unión ejerzan presión sobre la estabilidad e integridad del sistema financiero de la Unión y, en su lugar, deben prever un diálogo con los terceros proveedores de servicios de TIC críticos cuando se identifique ese riesgo.[38](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote39)

(50) Para poder evaluar y monitorear periódicamente la capacidad del tercero proveedor de servicios de TIC para prestar servicios de manera segura a la entidad financiera sin efectos adversos en la resiliencia de esta última, debe haber una armonización de los elementos contractuales clave a lo largo de la ejecución de contratos con terceros proveedores de TIC. Esos elementos solo cubren aspectos contractuales mínimos considerados cruciales para permitir el monitoreo completo por parte de la entidad financiera desde la perspectiva de garantizar su resiliencia digital basada en la estabilidad y seguridad del servicio TIC.

(51) Los arreglos contractuales deben prever, en particular, una especificación de descripciones completas de funciones y servicios, de los lugares donde se prestan dichas funciones y donde se procesan los datos, así como una indicación de las descripciones completas del nivel de servicio acompañadas de objetivos de rendimiento cuantitativos y cualitativos dentro del servicio acordado. niveles que permitan un efectivo seguimiento por parte de la entidad financiera. En el mismo sentido, las disposiciones sobre accesibilidad, disponibilidad, integridad, seguridad y protección de los datos de carácter personal, así como las garantías de acceso, recuperación y devolución en caso de concurso, resolución o interrupción de la actividad empresarial del servicio TIC de terceros. proveedor también deben ser considerados elementos esenciales para que una entidad financiera pueda asegurar el seguimiento del riesgo de terceros.

(52) Para garantizar que las entidades financieras mantengan el control total de todos los desarrollos que puedan menoscabar su seguridad de TIC, se deben establecer períodos de aviso y obligaciones de información del proveedor de servicios de terceros de TIC en caso de desarrollos con un impacto material potencial en el proveedor de servicios de terceros de TIC. la capacidad del proveedor de servicios para llevar a cabo con eficacia funciones críticas o importantes, incluida la prestación de asistencia por parte de este último en caso de un incidente relacionado con las TIC sin costo adicional o a un costo determinado ex ante.

(53) Los derechos de acceso, inspección y auditoría por parte de la entidad financiera o de un tercero designado son instrumentos cruciales en el monitoreo continuo por parte de las entidades financieras del desempeño del proveedor de servicios de TIC de terceros, junto con la plena cooperación de este último durante las inspecciones. En la misma línea, la autoridad competente de la entidad financiera debe tener esos derechos, basados ​​en notificaciones, para inspeccionar y auditar al tercero proveedor de servicios TIC, sujeto a confidencialidad.

(54) Los acuerdos contractuales deben prever derechos de rescisión claros y avisos mínimos relacionados, así como estrategias de salida dedicadas que permitan, en particular, períodos de transición obligatorios durante los cuales los terceros proveedores de servicios de TIC deben continuar brindando las funciones relevantes con el fin de reducir el riesgo de interrupciones. a nivel de la entidad financiera o permitir a esta última cambiar efectivamente a otros proveedores de servicios TIC de terceros, o alternativamente recurrir al uso de soluciones on-premise, consistentes con la complejidad del servicio prestado.

(55) Además, el uso voluntario de cláusulas contractuales estándar desarrolladas por la Comisión para los servicios de computación en la nube puede brindar mayor comodidad a las entidades financieras y a sus proveedores externos de TIC, al mejorar el nivel de seguridad jurídica sobre el uso de los servicios de computación en la nube por parte de las entidades financieras. sector, en plena alineación con los requisitos y expectativas establecidos por la regulación de servicios financieros. Este trabajo se basa en las medidas ya previstas en el Plan de Acción Fintech de 2018, que anunció la intención de la Comisión de fomentar y facilitar el desarrollo de cláusulas contractuales estándar para el uso de la subcontratación de servicios de computación en la nube por parte de las entidades financieras, aprovechando los esfuerzos intersectoriales de las partes interesadas en los servicios de computación en la nube. que la Comisión ha facilitado con la ayuda de la participación del sector financiero.

(56) Con miras a promover la convergencia y la eficiencia en relación con los enfoques de supervisión del riesgo de terceros de TIC para el sector financiero, fortalecer la resiliencia operativa digital de las entidades financieras que dependen de proveedores de servicios de terceros críticos de TIC para el desempeño de funciones operativas, y por lo tanto, para contribuir a preservar la estabilidad del sistema financiero de la Unión, la integridad del mercado único de servicios financieros, los terceros proveedores de servicios de TIC críticos deben estar sujetos a un marco de supervisión de la Unión.

(57) Dado que solo los proveedores de servicios externos críticos merecen un trato especial, debe establecerse un mecanismo de designación a efectos de aplicar el Marco de Supervisión de la Unión para tener en cuenta la dimensión y la naturaleza de la dependencia del sector financiero de dicho servicio de terceros de TIC. proveedores, lo que se traduce en un conjunto de criterios cuantitativos y cualitativos que establecerían los parámetros de criticidad como base para su inclusión en la Vigilancia. Los proveedores de servicios críticos de TIC de terceros que no se designen automáticamente en virtud de la aplicación de los criterios mencionados anteriormente deben tener la posibilidad de participar voluntariamente en el marco de supervisión.

(58) El requisito de constitución legal en la Unión de terceros proveedores de servicios de TIC que hayan sido designados como críticos no equivale a la localización de datos, ya que el presente Reglamento no implica ningún requisito adicional sobre el almacenamiento o el procesamiento de datos que deban realizarse en la Unión.

(59) Este marco debe entenderse sin perjuicio de la competencia de los Estados miembros para llevar a cabo sus propias misiones de supervisión con respecto a los terceros proveedores de servicios de TIC que no son fundamentales en virtud del presente Reglamento pero que podrían considerarse importantes a nivel nacional.

(60) Para aprovechar la actual arquitectura institucional de múltiples niveles en el área de los servicios financieros, el Comité Conjunto de las ESA debe continuar asegurando la coordinación intersectorial general en relación con todos los asuntos relacionados con el riesgo de las TIC, de acuerdo con sus tareas sobre ciberseguridad, respaldado por un nuevo Subcomité (el Foro de Supervisión) que lleva a cabo el trabajo preparatorio tanto para las decisiones individuales dirigidas a los proveedores de servicios externos de TIC críticos como para las recomendaciones colectivas, en particular sobre la evaluación comparativa de los programas de supervisión de los proveedores de servicios externos de TIC críticos, y la identificación de las mejores prácticas para abordar los problemas de riesgo de concentración de TIC.

(61) Para garantizar que los terceros proveedores de servicios de TIC que desempeñan un papel fundamental para el funcionamiento del sector financiero sean supervisados ​​de forma adecuada a escala de la Unión, debe designarse a una de las AES como supervisor principal para cada tercero proveedor de servicios de TIC fundamental.

(62) Los supervisores principales deben tener las facultades necesarias para realizar investigaciones, inspecciones in situ y externas en proveedores de servicios de TIC críticos, acceder a todas las instalaciones y ubicaciones pertinentes y obtener información completa y actualizada que les permita adquirir una visión real del tipo, la dimensión y el impacto. del riesgo de terceros TIC que suponen para las entidades financieras y, en última instancia, para el sistema financiero de la Unión.

Confiar a las ESA la supervisión principal es un requisito previo para comprender y abordar la dimensión sistémica del riesgo de las TIC en las finanzas. La huella en la Unión de los proveedores de servicios de TIC críticos de terceros y los posibles problemas de riesgo de concentración de TIC que conlleva exigen que se adopte un enfoque colectivo ejercido a nivel de la Unión. El ejercicio de múltiples auditorías y derechos de acceso, realizado por numerosas autoridades competentes por separado con poca o ninguna coordinación, no conduciría a una visión completa del riesgo de terceros de TIC y crearía redundancia, carga y complejidad innecesaria a nivel de terceros críticos de TIC. proveedores de fiestas que se enfrentan a solicitudes tan numerosas.

(63) Además, los supervisores principales deben poder presentar recomendaciones sobre asuntos de riesgo de TIC y remedios adecuados, incluida la oposición a ciertos arreglos contractuales que en última instancia afectan la estabilidad de la entidad financiera o el sistema financiero. Las autoridades nacionales competentes deben tener debidamente en cuenta el cumplimiento de las recomendaciones sustantivas establecidas por los Supervisores Principales como parte de su función relacionada con la supervisión prudencial de las entidades financieras.

(64) El Marco de Supervisión no sustituirá, ni en modo alguno ni en parte sustituirá la gestión por parte de las entidades financieras del riesgo que implica el uso de terceros proveedores de servicios TIC, incluyendo la obligación de seguimiento continuo de sus acuerdos contractuales celebrados con críticos TIC. terceros proveedores de servicios, y no afectará la plena responsabilidad de las entidades financieras en el cumplimiento y cumplimiento de todos los requisitos establecidos en este Reglamento y la legislación de servicios financieros pertinente. Para evitar duplicaciones y superposiciones, las autoridades competentes deben abstenerse de tomar individualmente cualquier medida destinada a monitorear los riesgos críticos del proveedor de servicios de TIC de terceros. Tales medidas deben coordinarse y acordarse previamente en el contexto del Marco de Supervisión.

(65) Para promover la convergencia a nivel internacional sobre las mejores prácticas que se utilizarán en la revisión de la gestión de riesgos digitales de los proveedores de servicios de terceros de TIC, se debe alentar a las AES a celebrar acuerdos de cooperación con las autoridades competentes de supervisión y regulación de terceros países para facilitar el desarrollo de mejores prácticas que aborden el riesgo de terceros de las TIC.

(66) Para aprovechar la experiencia técnica de los expertos de las autoridades competentes en la gestión de riesgos operativos y de TIC, los supervisores principales deben aprovechar la experiencia de supervisión nacional y establecer equipos de examen dedicados para cada proveedor de servicios de TIC crítico individual, reuniendo equipos multidisciplinarios para apoyar la preparación y la ejecución real de las actividades de supervisión, incluidas las inspecciones in situ de los proveedores de servicios externos de TIC críticos, así como el seguimiento necesario de los mismos.

(67) Las autoridades competentes deben poseer todos los poderes de supervisión, investigación y sanción necesarios para garantizar la aplicación del presente Reglamento. Las sanciones administrativas deberían, en principio, ser publicadas. Dado que las entidades financieras y los terceros proveedores de servicios de TIC pueden estar establecidos en diferentes Estados miembros y ser supervisados ​​por diferentes autoridades sectoriales competentes, la estrecha cooperación entre las autoridades competentes pertinentes, incluido el BCE, con respecto a las tareas específicas que le atribuye el Reglamento (UE) n.º 1024/2013 [39](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote40) , y la consulta con las AES debe garantizarse mediante el intercambio mutuo de información y la prestación de asistencia en el contexto de las actividades de supervisión.

(68) Con el fin de cuantificar y cualificar en mayor medida los criterios de designación de los proveedores de servicios externos de TIC críticos y armonizar las tasas de supervisión, deben delegarse en la Comisión los poderes para adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea. con respecto a: especificar más el impacto sistémico que la falla de un proveedor externo de TIC podría tener en las entidades financieras a las que sirve, el número de instituciones de importancia sistémica mundial (G-SII) u otras instituciones de importancia sistémica (O-SII) que dependen del respectivo proveedor de servicios de terceros de TIC, el número de proveedores de servicios de terceros de TIC activos en un mercado específico, los costos de migrar a otro proveedor de servicios de terceros de TIC, el número de Estados miembros en los que el tercero proveedor de servicios de TIC pertinente presta servicios y en los que operan las entidades financieras que utilizan el tercero proveedor de servicios de TIC pertinente, así como el importe de las tasas de supervisión y la forma en que se pagan a pagar.

Es de especial importancia que la Comisión lleve a cabo las consultas adecuadas durante su trabajo preparatorio, incluso a nivel de expertos, y que dichas consultas se lleven a cabo de conformidad con los principios establecidos en el Acuerdo Interinstitucional de 13 de abril de 2016 sobre Legislar mejor. [40](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote41) En particular, para garantizar la igualdad de participación en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben todos los documentos al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso de forma sistemática a las reuniones de los grupos de expertos de la Comisión que se ocupan de la preparación de actos delegados.

(69) Dado que este Reglamento, junto con la Directiva (UE) 20xx/xx del Parlamento Europeo y del Consejo, [41](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595#footnote42) implica una consolidación de las disposiciones de gestión de riesgos de las TIC que abarcan múltiples reglamentos y directivas del acervo de servicios financieros de la Unión, incluidos los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012 (UE) n.º 600/2014 y (UE) n.º 909/2014, a fin de garantizar la plena coherencia, dichos Reglamentos deben modificarse para aclarar que las disposiciones pertinentes relacionadas con los riesgos de las TIC se establecen en el presente Reglamento.

Las normas técnicas deben garantizar la armonización coherente de los requisitos establecidos en el presente Reglamento. Como organismos con experiencia altamente especializada, las ESA deben tener el mandato de desarrollar proyectos de normas técnicas de regulación que no impliquen decisiones políticas, para presentarlas a la Comisión. Se deben desarrollar estándares técnicos regulatorios en las áreas de gestión de riesgos de TIC, informes, pruebas y requisitos clave para un control sólido del riesgo de terceros de TIC.

(70) Es de particular importancia que la Comisión lleve a cabo las consultas adecuadas durante su trabajo preparatorio, incluso a nivel de expertos. La Comisión y las AES deben garantizar que todas las entidades financieras puedan aplicar dichas normas y requisitos de forma proporcionada a la naturaleza, escala y complejidad de dichas entidades y sus actividades.

(71) Para facilitar la comparabilidad de los principales informes de incidentes relacionados con las TIC y garantizar la transparencia en los arreglos contractuales para el uso de los servicios de TIC proporcionados por terceros proveedores de servicios de TIC, las ESA deben tener el mandato de desarrollar proyectos de normas técnicas de implementación que establezcan plantillas, formularios y formularios estandarizados. procedimientos para que las entidades financieras reporten un incidente mayor relacionado con las TIC, así como plantillas estandarizadas para el registro de información. Al desarrollar esos estándares, las ESA deben tener en cuenta el tamaño y la complejidad de las entidades financieras, así como la naturaleza y el nivel de riesgo de sus actividades. La Comisión debe estar facultada para adoptar dichas normas técnicas de ejecución mediante actos de ejecución de conformidad con el artículo 291 del TFUE y de conformidad con el artículo 15 de los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095 /2010, respectivamente. Dado que ya se han especificado requisitos adicionales mediante actos delegados y de ejecución basados ​​en normas técnicas de regulación y de ejecución en los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014, respectivamente, procede encomendar a las AES, ya sea de forma individual o conjunta a través de la Comisión Mixta,

(72) Este ejercicio supondrá la posterior modificación de los actos delegados y de ejecución existentes adoptados en diferentes ámbitos de la legislación de servicios financieros. Debe modificarse el ámbito de aplicación de los artículos sobre riesgo operativo en virtud de los cuales las habilitaciones en esos actos habían ordenado la adopción de actos delegados y de ejecución con el fin de trasladar al presente Reglamento todas las disposiciones relativas a la resiliencia operativa digital que actualmente forman parte de dicho Reglamento.

(73) Dado que los objetivos del presente Reglamento, a saber, lograr un alto nivel de resiliencia operativa digital aplicable a todas las entidades financieras, no pueden ser alcanzados de manera suficiente por los Estados miembros porque requieren la armonización de una multitud de normas diferentes, actualmente existentes en algunos actos de la Unión , bien en los ordenamientos jurídicos de los distintos Estados miembros, sino que, debido a su escala y sus efectos, puede lograrse mejor a nivel de la Unión, la Unión podrá adoptar medidas de conformidad con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.