ADC21
COL·LEGI D'ACTUARIS DE CATALUNYA | Nº9 PRIMER SEMESTRE 2022.

Alberto Igartua Medina
Senior Manager Consulting FS KPMG

Berta Muñoz Diez
Senior Manager Consulting FS KPMG

El Reglamento de Resiliencia Operativa Digital (DORA) y su impacto en el sector asegurador

1.- ¿En qué contexto surge DORA?

El sector asegurador se encuentra actualmente inmerso en un proceso de transformación digital integral, que está provocando un incremento de su complejidad operativa, así como de la exposición a nuevas tipologías de riesgos y, por ende, de las vulnerabilidades a las que se enfrentan, derivadas de determinadas disrupciones operativas. Estas amenazas no solo afectan a las entidades desde la óptica financiera, sino que también influyen en su estabilidad operativa debido a la multitud y heterogeneidad de los potenciales eventos, y de un factor importante, su impredecibilidad.

Ante esta situación, los reguladores, supervisores y otros organismos internacionales están evolucionando su foco tradicional - centrado fundamentalmente en la resiliencia financiera de las entidades, principalmente en el ámbito de la gestión del capital y la liquidez - hacia la necesidad de asegurar también la resiliencia de estas en términos operacionales.

En los últimos meses, distintos organismos han publicado numerosos documentos relacionados con la resiliencia operativa. Si bien, a nivel europeo, cobra especial relevancia el borrador de Reglamento publicado por la Comisión Europea el 24 de septiembre de 2020 (conocido comúnmente con el nombre de DORA), el cual tiene por objetivo regular la resiliencia operativa digital.

En este sentido, las distintas Autoridades Europeas de Supervisión (AES), la Autoridad Bancaria Europea (EBA), la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) y la Autoridad Europea de Valores y Mercados (ESMA), han alineado sus posturas con el objetivo de crear este marco único de gestión y supervisión para todo el sector financiero.

Este reglamento comunitario pretende establecer un marco de medición, gestión, monitorización y supervisión de los riesgos de las tecnologías de la información y las comunicaciones (TIC), dirigido no solo a las entidades financieras tradicionales, sino que lo hace extensivo a los grandes proveedores de servicios tecnológicos, así como a nuevos participantes del sector financiero, como es el caso de determinadas fintechs e insurtechs.

Una de las grandes reivindicaciones del sector asegurador ha sido excluir a intermediarios de seguros, reaseguros y seguros complementarios de menor tamaño y, así lo ha reconocido la nueva versión de la norma en la que se recoge expresamente que los intermediarios que sean micro, pequeñas o medianas empresas estarán excluidos de la aplicación de la norma, salvo en el supuesto de que sean exclusivamente sistemas de venta automatizados.

El documento definitivo está siendo debatido actualmente en el Parlamento Europeo y su aprobación definitiva se espera que tenga lugar en los próximos meses. No obstante, si bien es cierto que se están terminando de perfilar determinados aspectos, no cabe duda de que su publicación tendrá un gran impacto sobre la gestión actual de los riesgos tecnológicos y de la ciberseguridad de las entidades aseguradoras.

2.- Controversias del sector asegurador

Fruto del gran impacto sobre la gestión actual de los riesgos tecnológicos y de la ciberseguridad de las entidades aseguradoras, se ha generado un debate abierto sobre algunos aspectos considerados más controvertidos.

Un gran reto ya identificado por las aseguradoras y, que va a ser una realidad con la publicación del Reglamento DORA, es la necesidad de alinearlo con lo dispuesto en las Directrices TIC de EIOPA, las obligaciones ya derivadas de la normativa Solvencia II, y otras disposiciones como el Reglamento General de Protección de Datos.

Otra de las controversias de las entidades aseguradoras, ha girado en torno a la aplicación del criterio de "proporcionalidad" con respecto a su ámbito de aplicación. Una parte del sector consideraba que DORA debe circunscribirse a las funciones

críticas, y parece que el nuevo borrador efectivamente delimita su alcance a los activos y funciones de negocio más críticas de las aseguradoras.

Además, desde el sector remarcan la necesidad de que los plazos o periodos para efectuar las actividades de supervisión se adapten en función del perfil de riesgo de las entidades.

Por último, el plazo de implementación del reglamento también ha generado divergencia de opiniones, solicitando que se ampliase de uno a tres años, a estos efectos, parece que el regulador ha atendido en parte las demandas del sector, habiéndose ampliado el plazo en la versión sobre la que se está trabajando actualmente de uno a dos años, a excepción de las pruebas de penetración que continúan siendo 3 años.

3.- ¿Cuáles son los principales objetivos de DORA?

Inspirado en estándares, directrices, recomendaciones y enfoques de gestión del riesgo, el objetivo fundamental de esta norma es promover un conjunto de funciones e instrumentos que permitan establecer los mimbres para una gestión global del riesgo TIC en las entidades financieras, asegurando que las entidades dispongan de las capacidades necesarias asociadas al ciclo completo de la gestión de riesgos (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución y comunicación) de tal manera que se asegure una mayor agilidad y eficiencia en la respuesta de las entidades ante la materialización de una disrupción. En este contexto, los principales objetivos que busca el reglamento DORA son los siguientes:

- Unificar y mejorar la gestión de riesgos TIC a nivel europeo, armonizando las normas y requerimientos para la gestión de riesgos de las TIC en todos los participantes del sector financiero, sobre la base de las directrices existentes actualmente. En el caso del sector asegurador, supondrá en determinados aspectos una evolución de las actuales directrices de EIOPA para la gestión y gobernanza de los riesgos ICT.
- Establecer pruebas exhaustivas recurrentes en los sistemas de TIC, así como de los riesgos derivados de la dependencia de proveedores de servicios TIC por parte del sector asegurador.
- Reforzar la exigencia de los supervisores sobre los riesgos digitales y los incidentes relacionados con las TIC.
- Armonizar la clasificación y notificación de incidentes de TIC, y abrir la puerta para el establecimiento de un único centro a nivel de la Unión Europea para la notificación de incidentes importantes relacionados con las TIC por parte de las instituciones financieras.

- Incluir a los proveedores externos de servicios TIC críticos del perímetro regulatorio, incluyendo los proveedores de servicios cloud.

4.- ¿Qué aspectos trata DORA y cómo afecta ésta a las entidades aseguradoras?

La resiliencia operativa debe entenderse y ser gestionada como la consecuencia o el resultado de una correcta gestión de los riesgos de la entidad, diseñando un modelo operativo que aúne e integre los elementos contenidos en los diferentes marcos que tienen relación (TIC, proveedores, etc.) en uno solo, permitiendo gestionar de manera eficiente y ágil la resiliencia operativa digital.

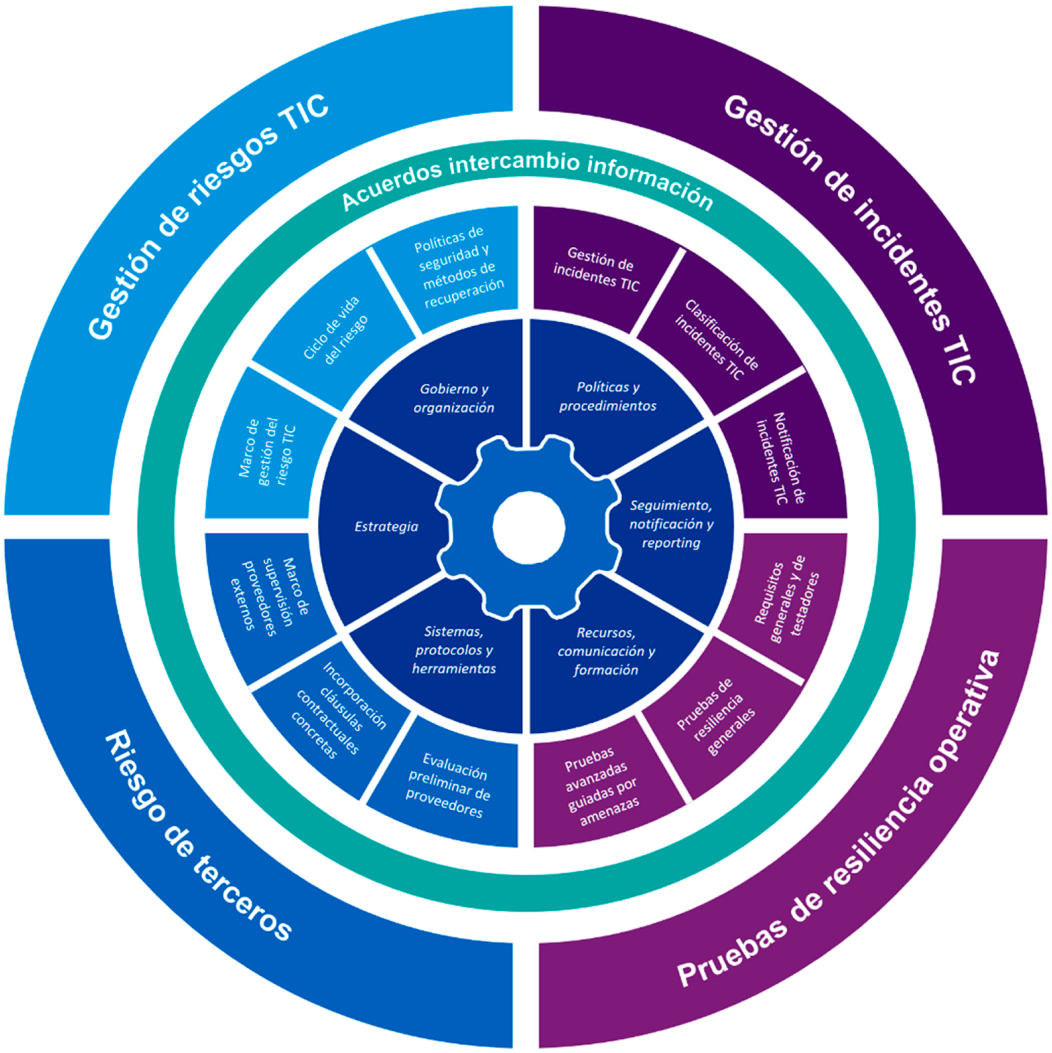
En este contexto, DORA requiere que se cubran, como mínimo, los siguientes aspectos:

- Gobernanza y organización: disponer de marcos internos de gobernanza y control que cubran las funciones específicas de gestión de los riesgos de TIC (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución, y comunicación, entre otras) y que garanticen una gestión eficaz y prudente de todos los riesgos de TIC. Adicionalmente, asegurar la implicación de la Alta Dirección, identificar las funciones / áreas esenciales de la Entidad e imponer una revisión anual del carácter de esencialidad o importancia de dichas funciones / áreas.
- Gestión de riesgos TIC: contar con un proceso de gestión del riesgo de TIC sólido y completo focalizado en las funciones / áreas de carácter esencial o importante que permita el tratamiento y gestión de incidentes de TIC considerados como graves, y garantizar un alto nivel de resiliencia operativa digital que se ajuste a las necesidades, tamaño y complejidad de las Entidades.
- Notificación de incidentes: controlar, registrar y clasificar los incidentes relacionados con las TIC, así como notificar a las autoridades los incidentes TIC graves y presentar informes iniciales, intermedios y finales. Asimismo, realizar un *reporting* de todos los costes financieros estimados y pérdidas causados por perturbaciones considerables de las TIC e incidentes TIC graves.
- Pruebas de resiliencia: disponer de un enfoque basado en el riesgo, a medida que se desarrolla el programa de pruebas de resiliencia operativa digital, teniendo en cuenta el panorama cambiante de los riesgos de TIC.
- Riesgo de terceros: evaluar el riesgo de concentración de TIC respecto a los proveedores externos e incluir ciertas cláusulas contractuales con sus proveedores, incrementando la seguridad a la hora de que las Entidades contraten la prestación de servicios digitales. Además, obliga a analizar y evaluar los riesgos asociados a las cadenas de subcontratación de

proveedores (*fourth parties*) así como extender los actuales análisis de proveedores a los proveedores intragrupo.

- Intercambio de información: posibilidad de establecer acuerdos entre las distintas entidades para el intercambio de información e inteligencia relativa a ciberamenazas, con el fin de crear conciencia sobre el riesgo de TIC, minimizar su propagación, apoyar las capacidades defensivas de las entidades y las técnicas de detección de amenazas.

A continuación, se ilustran los elementos que componen el alcance y contenido de la regulación DORA:



5.- ¿Cómo están afrontado DORA las principales aseguradoras?

Como se ha comentado previamente, el impulso que se ha producido en todo el sector financiero en torno a la digitalización de los negocios y de las nuevas formas de trabajo, así como los cambios en las preferencias y hábitos de los consumidores, ha tenido su claro reflejo por supuesto también al sector asegurador, lo que ha provocado la injerencia de nuevos riesgos emergentes que deben ser identificados, evaluados y monitorizados.

En este contexto, el informe *"Global Insurance CEO Outlook 2021"* llevado a cabo por KPMG, en el que han participado más de 129 CEOs de entidades aseguradoras en más de 11 países, se ha concluido que los riesgos ligados a tecnologías emergentes y la ciberseguridad están en el top 5 de los mayores riesgos que preocupan a las entidades actualmente.

Respecto al foco de riesgo vinculado a las tecnologías emergentes, el estudio revela que las entidades aseguradoras están buscando crear una resiliencia digital alineada con su estrategia y totalmente vinculada al crecimiento potencial de las entidades.

La encuesta pone de manifiesto que el 68% de las entidades aseguradoras consideran que para seguir creciendo resulta necesario incrementar las inversiones en instrumentos de detección de disrupciones, así como en procesos de innovación y digitalización. Asimismo, más del 50% considera necesario crear alianzas y consorcios como canalizador de inversiones que permitan el desarrollo de tecnologías innovadoras, que eviten o reduzcan el posible estancamiento del sector.

En este contexto, los CEOs del sector asegurador reconocen que el primer paso hacia la digitalización de sus negocios reside en la capacidad que tienen las organizaciones para detectar y evitar una posible disrupción de sus servicios, así como en la capacidad de mantenerse innovadoras y de crear nuevas fuentes de valor. Para lograr dicho objetivo, el 75% de los CEOs pone de manifiesto que necesitan ser más ágiles y rápidos a la hora de evolucionar y cambiar sus inversiones, y desinvertir en aquellos negocios que se enfrentan de forma más directa a la obsolescencia digital.

Un dato relevante que marcará la tendencia en la evolución del sector asegurador es que el 65% de los entrevistados siente que los *partnerships* con empresas digitales y de soluciones tecnológicas innovadoras serán fundamentales para continuar con el actual ritmo de transformación digital de las aseguradoras.

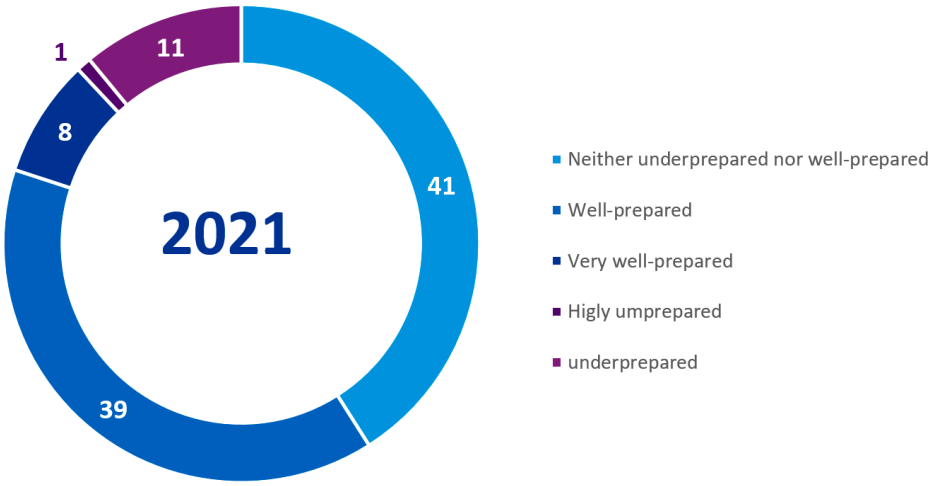
Fuente: KPMG Internacional, 2021.

Por otro lado, en relación con la importancia de la gestión de los riesgos relacionados con la ciberseguridad, de la encuesta realizada por KPMG se extrae también que las amenazas a la seguridad cibernética limitan el crecimiento y crean barreras para el desarrollo y la inclusión digital de las aseguradoras.

En este sentido, el 88% de los CEOs de las entidades aseguradoras afirman que han acometido inversiones, y están bien preparadas ante un potencial ataque cibernético bien están adaptando actualmente sus organizaciones, e implementando medias para protegerlas de futuros ataques.

De este modo, la necesidad de establecer unos niveles adecuados y prácticas sostenibles de ciberseguridad se considera un elemento crucial dentro de las aseguradoras. La madurez de las iniciativas y recursos destinados al efecto ayudará a que los ecosistemas digitales prosperen, los plazos de recuperación se reduzcan en caso de ataque, y se traslade al exterior un mensaje de confianza en la estructura de gobierno de las entidades aseguradoras.

Preparación de la organización para la seguridad cibernética:



Fuente: KPMG Internacional, 2021.

6.- ¿Cuáles son los próximos pasos?

Una vez se publique la versión definitiva del reglamento, las entidades aseguradoras deberán llevar a cabo un diagnóstico de la situación actual de las aseguradoras en relación con los requerimientos de DORA con el fin de entender el punto de partida en cuanto a las necesidades y desarrollos a realizar. Este diagnóstico permitirá identificar las diferencias existentes a nivel de políticas y procedimientos, marcos de gestión de riesgos TIC, clasificación de funciones y activos esenciales, circuitos de *reporting*, etc.

Tras finalizar el diagnóstico, las aseguradoras deberán diseñar un modelo operativo que les permita identificar los diferentes elementos que forman parte de su estrategia de resiliencia digital. Dicho modelo permitirá articular la adaptación / construcción de un marco de gestión de riesgos de TIC a la realidad de la aseguradora en función de los requerimientos de DORA, entre otros:

- Diseño de indicadores de tecnología y la definición de umbrales alineados con el apetito al riesgo definido por la entidad,
- Identificación de las funciones esenciales dentro de la organización, mapeo de los recursos existentes e identificación de los procesos llevados a cabo.
- Establecimiento de un modelo de relación con terceros / proveedores externos,
- Desarrollo de un inventario de medidas de contingencia y pasos preparatorios relacionados, etc.)

Por último, las entidades aseguradoras deberán definir un plan estratégico de trabajo que permita cumplir con los requerimientos de la normativa, los cuales precisan de ser aplicados en un plazo de 24 meses de acuerdo con lo establecido en la norma con carácter general. No obstante, dicho plazo se amplía a 36 meses en el caso de las pruebas avanzadas de penetración guiadas por amenazas.

De este modo, las entidades aseguradoras, en función de su grado de madurez en la gestión de los riesgos TIC y la ciberseguridad, se van a ver obligadas a emprender procesos transformacionales de gran calado en sus modelos actuales de gestión de la tecnología y riesgos, sobre los que KPMG tiene una gran experiencia en el acompañamiento y asesoramiento a las principales entidades financieras a nivel nacional e internacional.