KPMG

Digital Operational Resilience Act (DORA)

kpmg.es

—

Octubre 2023

DORA, como culminación del esfuerzo del regulador por lograr la homogeneización y normalización en materia de riesgo TIC, ...

En enero de 2023, la Comisión Europea publicó la versión final del Reglamento DORA, que establece un marco regulador europeo único para la gestión de los riesgos derivados de las TIC y los proveedores, ampliando el perímetro tradicional a nuevos actores del sector financiero.

Septiembre 2020

Presentación de la propuesta de Reglamento DORA por parte de la Comisión el 24 de septiembre de 2020.

Diciembre 2022

Publicación en el Diario Oficial de la Unión Europea el 27 de diciembre de 2022 del **reglamento relativo a la resiliencia operativa digital en el sector financiero (Reglamento DORA),** estableciendo así un **código normativo único** para prevenir y mitigar los eventos de riesgo tecnológico y ciberamenzas que sufran las distintas entidades de la industria financiera europea.

Finales 2023

Publicación primeros RTS / ITS de desarrollo de la norma:

- *RTS sobre gestión de riesgos de las TIC.*
- *RTS sobre gestión simplificada de riesgos de las TIC.*
- *RTS sobre clasificación de incidentes relacionados con las TIC y ciberamenazas.*
- *RTS sobre estrategia de gestión de riesgos de las TIC frente a terceros.*
- *ITS sobre el registro de información de acuerdos contractuales de servicios de TIC.*

Mediados 2024

Finalización publicación RTS / ITS:

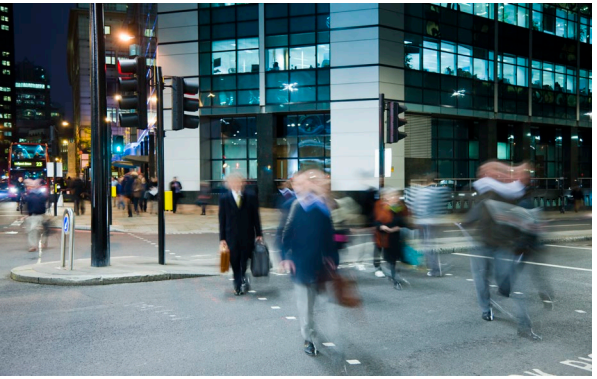
- *RTS sobre notificación de incidentes graves relacionados con las TIC y ciberamenazas.*
- *ITS sobre plantillas para la notificación de incidentes graves relacionados con las TIC y ciberamenazas.*
- *RTS sobre pruebas avanzadas basadas en pruebas de penetración dirigidas por amenazas.*
- *RTS sobre la descripción de los servicios de TIC prestados por terceros proveedores y sobre el uso de la subcontratación.*
- *RTS sobre la realización de la supervisión de proveedores de servicios críticos de TIC a terceros.*
- *Directrices sobre la estimación de los costes anuales agregados y las pérdidas causadas por incidentes graves relacionados con las TIC.*

Enero 2025

Entrada en aplicación de la norma

...ha llegado para regular la resiliencia a nivel europeo, ampliando el perímetro de supervisión a todos los players del sector financiero, incluyendo las entidades de seguros y reaseguros...

Las entidades financieras deben disponer de capacidades integrales que permitan una gestión sólida y eficaz de los riesgos de las TIC, así como de mecanismos y políticas específicos para gestionar todos los incidentes relacionados con las TIC y notificar aquellos incidentes importantes.



¿Cuál es el objetivo que persigue dora?

- Establecer un **marco para la gestión del riesgo en el ámbito de las tecnologías y la comunicación (TIC),** unificando y mejorando la gestión de riesgos TIC a nivel europeo.
- Definir los **criterios** para la **clasificación**, **gestión** y **notificación** de los incidentes relacionados con las TIC.
- Establecer **pruebas exhaustivas** recurrentes en los sistemas de TIC.
- Establecer requisitos para la gestión y supervisión de los **riesgos derivados de la dependencia de proveedores** de servicios TIC en el sector financiero.

¿Cuáles es el perímetro de dora?

- **El alcance de aplicación** de la norma es **universal** y de **obligado cumplimiento** para **todos** los **actores** del **sector financiero** a nivel europeo.
- **Se amplia,** por tanto**, el perímetro** tradicional, yendo **más allá de las Entidades Financieras tradicionales** incluyendo a un **amplio rango de los *players* del sector financiero.**

Entidades bajo perímetro

- ***Entidades de crédito***
- ***Entidades de pago***
- ***Proveedores de servicios de información sobre cuentas***
- ***Entidades de dinero electrónico***
- ***Empresas de servicios de inversión***
- ***Proveedores de servicios de criptoactivos***
- ***Depositarios centrales de valores***
- ***Entidades de contrapartida central***
- ***Centros de negociación***
- ***Registros de operaciones***
- ***Gestores de fondos de inversión alternativos y sociedades de gestión***
- ***Proveedores de servicios de suministro de datos***
- ***Empresas de seguros y reaseguros***
- ***Intermediarios de seguros, de reaseguros y de seguros complementarios***
- ***Fondos de pensiones de empleo***
- ***Agencias de calificación crediticia***
- ***Administradores de índices de referencia cruciales***
- ***Proveedores de servicios de financiación participativa***
- ***Registros de titulizaciones***
- ***Proveedores terceros de servicios de TIC***

...centrando el foco de la regulación en torno a cinco grandes bloques de contenido que involucran a numerosos equipos dentro de las entidades

Gobierno y Organización

- **Disponer de marcos internos de gobernanza y control que garanticen una gestión eficaz de todos los riesgos de TIC.**
- **Implicar a la Alta Dirección y al Consejo, establecer roles y funciones, diseñar circuitos de aprobación y control así como disponer de una función de control y gestión del riesgo.**

Gestión de riesgos TIC

- **Contar con un proceso de gestión del riesgo de TIC** (identificación activa, protección y prevención, detección, comunicación) **sólido y completo.**
- **Garantizar un alto nivel de resiliencia operativa digital que se ajuste a las necesidades, tamaño y complejidad de las entidades.**

Gestión, clasificación y notificación de incidentes

- **Identificar, registrar y clasificar los incidentes relacionados con las TIC.**
- **Notificar los incidentes más graves a las autoridades y a los clientes cuando tenga impacto en sus intereses.**
- **Presentar informes, así como comunicar a sus clientes cuando el incidente tenga un impacto en sus intereses financieros.**

Pruebas de resiliencia operativa digital

- **Establecer, mantener y revisar un programa de pruebas de resiliencia operativa digital sólido y completo como parte del marco de gestión de riesgos TIC.**
- **Realizar pruebas apropiadas de todos los sistemas y aplicaciones de TIC, así como pruebas de penetración guiadas por amenazas sobre las funciones esenciales o importantes.**

Riesgo de terceros

- **Gestionar el riesgo de terceros relacionados con las TIC como un elemento integrante del marco de gestión del riesgo de TIC de las entidades financieras.**
- **Establecer los criterios para determinar los proveedores terceros esenciales de servicios TIC, así como el marco de supervisión por parte de las autoridades de la UE.**

El reglamento DORA se va a reforzar con la publicación de distintas Normas Técnicas de Regulación (RTS), habiéndose publicado un primer lote en versión draft…

Capítulo II
Marco de riesgo TIC

- **RTS sobre el marco de Gestión de Riesgos de las TIC (Art.15);**
- **RTS sobre el marco simplificado de Gestión de Riesgos (Art.16.3);**
- Directrices sobre la estimación de costes/pérdidas agregadas causadas por incidentes importantes relacionados con las TIC (Art. 11.1).

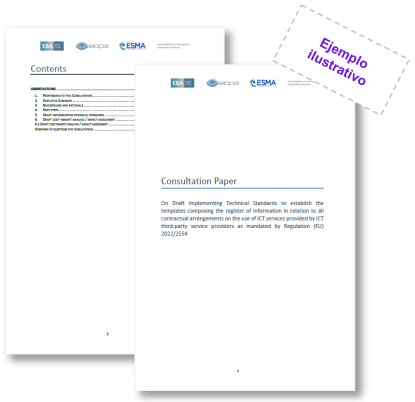
Los RTS(*) resaltados son aquellos relativos al <u>primer lote</u>, cuya versión final se publicará el 17 de Enero de 2024.

Capítulo III
Clasificación e informes de gestión de incidentes TIC

- **RTS sobre criterios para la clasificación de los incidentes relacionados con las TIC (Art. 18.3);**
- RTS para especificar la notificación de los principales incidentes relacionados con las TIC (Art. 20.a);
- ITS para establecer los detalles de notificación de los principales incidentes relacionados con las TIC (Art. 20.b);
- Informe de viabilidad sobre una mayor centralización de la notificación de incidentes mediante el establecimientos de un centro único de la UE para los incidentes relacionados con las TIC (Art. 21).

Capítulo IV
Pruebas de Resiliencia Operativa Digital

- RTS para especificar pruebas de penetración dirigidas por amenazas (Art. 26.1).



Capítulo V
Gestión de Riesgos de Terceros

- **ITS para establecer las plantillas de registro de información (Art.28.9);**
- **RTS para especificar la política sobre los servicios TIC realizados por terceros (Art.28.10);**
- RTS para especificar los elementos a determinar y evaluar al subcontratar servicios TIC que respalden una función crítica o esencial (Art.30.5).

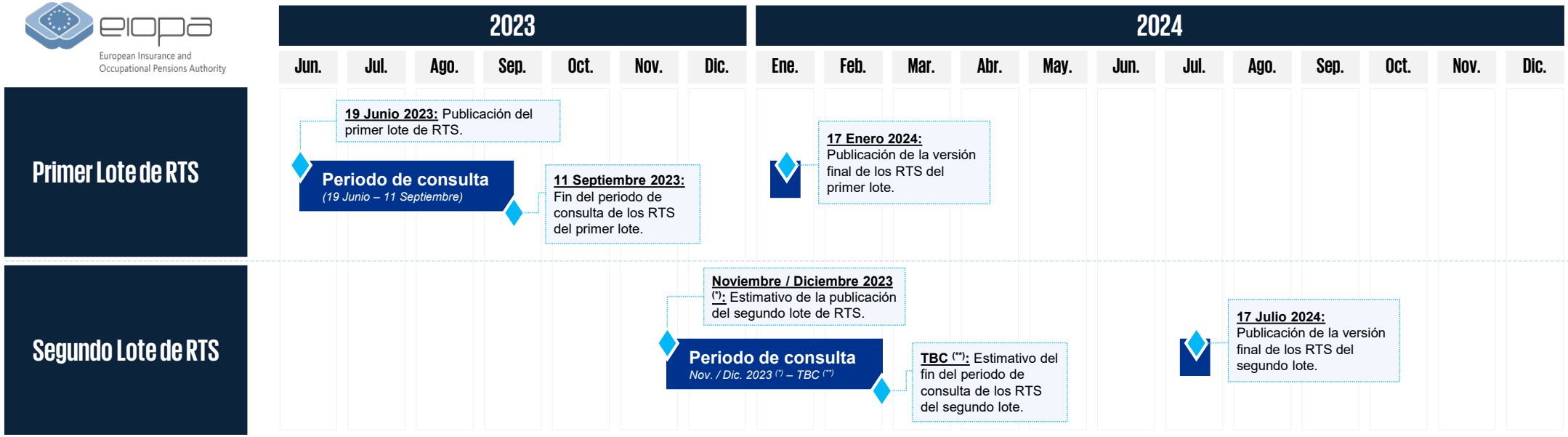
El contenido del DORA se ha visto reforzado con la publicación de la versión *draft* de un primer lote de RTS, publicados el 19 de junio de 2023; comenzando entonces su periodo de consulta a la EBA, para la publicación de sus versiones definitivas el 17 de enero de 2024. Del mismo modo, la versión *draft* del segundo lote de RTS está prevista que se publique a finales de 2023, comenzando entonces su período de consulta para la publicación de sus versiones finales el 17 de julio de 2024.

(*) Una Norma Técnica de Regulación (RTS) es "un acto delegado, técnico, elaborado por una Autoridad Europea de Supervisión. Debe desarrollar, especificar y determinar las condiciones para una armonización coherente de las normas incluidas en el acto legislativo de base".

...que se irá completando con la publicación del resto de RTSs en versión consultiva y definitiva de acuerdo al siguiente calendario

Plazos para la consulta pública y publicación de la versión final de RTS

No exhaustivo



(*) Pendiente de confirmación de la fecha exacta de publicación de la versión draft, así como del comienzo del periodo de consulta, de los RTS del segundo lote.

(**) Pendiente de confirmación. Periodo sujeto a la publicación del comienzo del periodo de consulta de los RTS del segundo lote.

Primer lote de RTS:

- RTS sobre el marco de gestión de riesgos de las TIC (Art.15);
- RTS sobre el marco simplificado de gestión de riesgos (Art.16.3);
- RTS sobre criterios de clasificación de incidentes relacionados con las TIC (Art. 18.3);
- ITS para establecer las plantillas de registro de información (Art.28.9);
- RTS para especificar la política sobre servicios TIC prestados por terceros (Art.28.10).

Segundo lote de RTS:

- Guía para la estimación de los costes/pérdidas agregados causados por incidentes graves relacionados con las TIC (Art. 11.1);
- RTS para especificar la notificación de incidentes graves relacionados con las TIC (Art. 20.a);
- ITS para establecer los detalles de la notificación de incidentes graves relacionados con las TIC (Art. 20.b);
- Informe de viabilidad sobre una mayor centralización de la notificación de incidentes mediante el establecimiento de un centro único de la UE para la notificación de incidentes graves relacionados con las TIC (Art. 21);
- RTS para especificar las pruebas de penetración dirigidas por amenazas (Art. 26.1);
- RTS para especificar los elementos que deben determinarse y evaluarse al subcontratar servicios de TIC que apoyen una función crítica o importante (Art.30.5).

A continuación, se presenta el resumen ejecutivo del contenido de los RTSs e ITS publicados (versión draft) en el primer lote

Capítulo II

RTS del marco de gestión de riesgos TIC *(Artículo 15)* **& RTS del marco simplificado de gestión de riesgos TIC** *(Artículo 16(3)):*

- Debido a las interrelaciones de ambos dos RTS, **las dos propuestas de regulación técnica se han agrupado en un solo borrador de normas técnicas** para abordar de manera integral la gestión de riesgos TIC.
- Los requisitos principales para las Entidades Financieras pivotan sobre las siguientes puntos: (I) **Políticas, procedimientos, protocolos y herramientas de seguridad sobre las TIC**; (II) **Política de RRHH y Control de accesos**; (III) **Detección y respuesta a incidentes relacionados con las TIC**; (IV) **Gestión de Continuidad del Negocio de las TIC**; (V) **Informes de la revisión del marco de gestión de riesgos TIC**; y (VI) **Proporcionalidad**.
- El RTS especifica **un marco simplificado de gestión de riesgos de TIC** aplicable solo a 5 categorías de Entidades Financieras más pequeñas o menos interrelacionadas.

Capítulo III

RTS sobre el criterio para la clasificación de los incidentes relacionados con las TIC *(Artículo 18(3))*:

- Requisitos armonizados para las Entidades Financieras sobre:
  - (I) **La clasificación de los incidentes relacionados con las TIC** por parte de las Entidades Financieras (EE.FF.);
  - (II) **El enfoque de clasificación y los umbrales de materialidad** para la determinación de los principales incidentes relacionados con las TIC para ser comunicados por las EE.FF. a las Autoridades Competentes (AA.CC.);
  - (III) **Los criterios y los umbrales a aplicar en la clasificación** de las ciberamenazas significativas; y
  - (IV) **Los criterios que aplicarán las AA.CC. con el fin de evaluar la relevancia de los incidentes importantes relacionados con las TIC** para las AA.CC. pertinentes en los Estados Miembro de acogida y los detalles de la información que se compartirán con ellas.

Capítulo V

ITS para establecer las plantillas para el registro de información *(Artículo 28(9)):*

- **Plantillas armonizadas para el registro de información** que deben mantener las Entidades Financieras que abarquen todos **los acuerdos contractuales sobre el uso de servicios de TIC prestados por terceros proveedores de servicios de TIC a nivel de Entidad local, consolidado y sub-consolidado.**
- Las plantillas han sido diseñadas teniendo en cuenta la triple finalidad del registro de información: (I) **el registro de información forma parte del marco de gestión de riesgos TIC de las Entidades Financieras**; (II) el registro de información permite la supervisión **eficaz de las Entidades Financieras**, incluyendo (III) la **designación de terceros proveedores** de servicios como críticos a nivel de la UE por parte de las AES en el contexto del marco de supervisión.
- Para simplificar el establecimiento de los registros, el proyecto de **ITS contiene dos conjuntos diferentes de plantillas (a nivel de entidad local, y a nivel de sub-consolidado y consolidado, para grupos empresariales).**

RTS para especificar la política sobre los servicios de TIC prestados por terceros proveedores de TIC *(Artículo 28 (10)):*

- Requisitos durante todas las etapas que deben asumir **las Entidades Financieras en relación con el ciclo de vida de la gestión de los acuerdos de terceros en TIC.**
- Especificación del contenido de la política relativa a la utilización de servicios de TIC de apoyo a funciones críticas o importantes abordando los siguientes aspectos: (I) **la fase precontractual**; (II) **la aplicación, supervisión y gestión de los cambios y modificaciones contractuales para la utilización de servicios de TIC en apoyo de funciones críticas o importantes**; (III) **la estrategia de salida y los procesos de terminación de la relación con el proveedor.**

Principales retos y dificultades a los que se enfrentan las entidades del sector asegurador a la hora de desarrollar su capacidad de resiliencia operativa en consonancia con la nueva normativa

Principales retos del sector asegurador para su adherencia a DORA

01. Funciones esenciales o importantes

Definición de las funciones esenciales o importantes. Cuántas, con qué grado de detalle, cómo impulsar la rendición de cuentas y gestionarlas en todas las unidades de negocio o países.

02. Marco de gestión de riesgos de TIC

Mayor armonización de las herramientas, protocolos, procesos y políticas de gestión de riesgos de las TIC. Evolución del marco de gestión de riesgos de las TIC para garantizar la resiliencia operativa digital.

03. *Third-parties & Fourth-parties*

Resiliencia de principio a fin (*end-to-end)* con *third-parties* y *fourth-parties* con requerimientos sólidos respecto a al evaluación y monitorización de los proveedores, incluyendo las cadenas de subcontratación y los proveedores intragrupo. *Claras* dependencias en proveedores críticos, por ejemplo, de tecnología y *cloud*.

04. Medición de la resiliencia

Cómo medir la capacidad de resiliencia de la entidad definiendo las métricas de resiliencia, las pruebas, la calidad de los datos, los cuadros de mando y las herramientas/automatización, etc.

05. Integración en BaU

Integración en las prácticas habituales (BaU). Priorización de las inversiones, compromiso de los empleados, implicación real de los consejos de administración, implicación de los servicios, integración en el ADN de todo el personal, etc.

¿Cómo os podemos ayudar con DORA en el sector asegurador?

KPMG dispone de una gran experiencia en la prestación de distintos servicios para apoyar a las Entidades en lograr su alineamiento con los distintos requerimientos de DORA.

Análisis de Impacto de la norma

KPMG dispone de una amplia experiencia en la realización de **diagnósticos / análisis gap sobre la situación actual de la entidadades respecto al cumplimiento de los requerimientos del reglamento DORA** y las normas que lo desarrollan, que permiten **entender el punto de partida en cuanto a las necesidades y desarrollos a realizar en las entidades.**

Documentación cuestionario DGS

La experiencia de KPMG en el análisis y evaluación del reglamento DORA, le convierte en un gran **soporte para dar completitud a los cuestionarios de Resiliencia Operativa Digital solicitados por la Dirección General de Seguros** a las entidades.

Establecimiento programa de trabajo / *roadmap*

KPMG dispone de experiencia contrastada en el **diseño de planes directores que permitan la implementación de las líneas de acción que aseguren el alineamiento con la norma**. El diseño de un ***roadmap* que incorpore el plan de proyecto multidisciplinar y global** es fundamental a la hora de implementar con éxito los diferentes elementos que articulan la gestión de la resiliencia a lo largo de la Entidad.

Acompañamiento en el desarrollo de líneas de acción

KPMG dispone de **equipos especialistas** en las distintas materias cubiertas por la norma (gestión y control de proveedores, ciberseguridad, riesgos, etc.) **que permiten afrontar con solvencia la implantación y desarrollo de las distintas líneas de acción definidas en el *Roadmap*.**

Contactos

Alberto Esteban
Socio responsable de FS-Strategy de KPMG en España
T: +34 648 02 99 23
E: albertoesteban@kpmg.es

Mikel Campo
Socio de FS - Insurance Consulting Strategy
T: +34 686 41 61 06
E: mikelcampo@kpmg.es

Alberto Igartua
Senior Manager FS Consulting
T: +34 638 16 88 87
E: aigartua@kpmg.es

Laura Loranca
Manager FS Consulting
T: +34 680 44 16 62
E: lauraloranca@kpmg.es

kpmg.es

Document Classification: KPMG Public