DORA entra en el siguiente capítulo con el segundo lote de productos de políticas



Publicado el 16 de diciembre de 2023 por [**Editor**](https://www.xbrl.org/news/dora-enters-next-chapter-with-second-batch-of-policy-products/)

Las Autoridades Europeas de Supervisión (AES) inician una consulta pública sobre el segundo lote de mandatos políticos en virtud de la Ley de Resiliencia Operacional Digital (DORA). Promulgada el 16 de enero de 2023, DORA estará en pleno funcionamiento a partir del 17 de enero de 2025, armonizando las reglas de resiliencia operativa para 21 tipos de entidades financieras.

La legislación integral aborda aspectos críticos como la gestión de riesgos de TIC, la notificación de incidentes, las pruebas de resiliencia digital y la gestión de riesgos de TIC de terceros. Este paquete integral incluye cuatro borradores de estándares técnicos regulatorios (RTS), un conjunto de borradores de estándares técnicos de implementación (ITS) y dos conjuntos de directrices (GL).

Al reconocer el aumento en el uso de las TIC en las entidades financieras, DORA tiene como objetivo fortalecer la resiliencia operativa digital para mitigar los riesgos cibernéticos y las interrupciones transfronterizas. Aporta un marco unificado, aplicable a diversas entidades financieras, que cubre áreas cruciales como la gestión de riesgos de TIC, la notificación de incidentes y la gestión de riesgos de terceros. Desde una perspectiva de supervisión, DORA aumenta la conciencia sobre los riesgos cibernéticos y fomenta la cooperación entre las autoridades competentes para gestionar eficazmente las TIC y los riesgos cibernéticos. Desde la perspectiva de la Supervisión de la UE, DORA introduce un marco para supervisar los riesgos sistémicos y de concentración vinculados a las TIC.

Hay mucho en qué profundizar con esta actualización: puede acceder a todas las consultas [aquí](https://www.eba.europa.eu/publications-and-media/press-releases/esas-launch-joint-consultation-second-batch-policy-mandates), y la nota introductoria proporciona un punto de partida ideal. punto para comprender las diversas cuestiones. DORA es un nuevo e importante conjunto de obligaciones operativas y de cumplimiento para las instituciones financieras con sede en la UE.

[DORA](https://www.xbrl.org/tag/dora/) [ESAS](https://www.xbrl.org/tag/esas/) [UE](https://www.xbrl.org/tag/eu/) [TIC](https://www.xbrl.org/tag/ict/)

Las ESA lanzan una consulta conjunta sobre el segundo lote de mandatos políticos en virtud de la Ley de Resiliencia Operacional Digital

Las Autoridades Europeas de Supervisión (EBA, EIOPA y ESMA, las ESA) lanzaron hoy una consulta pública sobre el segundo lote de mandatos políticos en virtud de la Ley de Resiliencia Operacional Digital (DORA). El paquete de hoy incluye cuatro proyectos de normas técnicas regulatorias (RTS), un conjunto de proyectos de normas técnicas de implementación (ITS) y dos conjuntos de directrices (GL). Estos instrumentos de política tienen como objetivo garantizar un marco legal coherente y armonizado en las áreas de notificación de incidentes importantes relacionados con las TIC, pruebas de resiliencia operativa digital, gestión de riesgos de terceros de TIC y supervisión de proveedores externos de TIC críticos. La consulta se extenderá hasta el 4 de marzo de 2024.

* **8 de diciembre de 2023**

**Las Autoridades Europeas de Supervisión (EBA, EIOPA y ESMA, las ESA) lanzaron hoy una consulta pública sobre el segundo lote de mandatos políticos en virtud de la Ley de Resiliencia Operacional Digital (DORA). El paquete de hoy incluye cuatro proyectos de normas técnicas regulatorias (RTS), un conjunto de proyectos de normas técnicas de implementación (ITS) y dos conjuntos de directrices (GL). Estos instrumentos de política tienen como objetivo garantizar un marco legal coherente y armonizado en las áreas de notificación de incidentes importantes relacionados con las TIC, pruebas de resiliencia operativa digital, gestión de riesgos de terceros de TIC y supervisión de proveedores externos de TIC críticos. La consulta se extenderá hasta el 4 de marzo de 2024.**

A través de DORA, las ESA tienen el mandato de desarrollar conjuntamente un total de 13 instrumentos políticos, presentados en dos lotes. Este segundo lote comprende lo siguiente:

* RTS e ITS sobre contenido, cronogramas y plantillas sobre notificación de incidentes
* GL sobre costos agregados y pérdidas por incidentes importantes
* RTS sobre subcontratación de funciones críticas o importantes
* RTS sobre armonización de la supervisión
* GL sobre cooperación en materia de supervisión entre las AES y las autoridades competentes
* RTS sobre pruebas de penetración dirigidas por amenazas (TLPT)

Puede encontrar más información sobre el borrador de los productos de la política en la [nota introductoria](https://www.eba.europa.eu/sites/default/files/2023-12/4cc26834-758f-4ef0-a1e5-6cef36a76774/DORA%20public%20consultation%20on%20the%20second%20batch%20of%20policy%20products_overview%20document.pdf).

**Proceso de consulta**

Los comentarios sobre esta consulta se pueden enviar a las ESA a través de las páginas de consulta:

* [Consulta sobre proyectos conjuntos de normas técnicas sobre notificación de incidentes graves](https://ec.europa.eu/eusurvey/runner/DORA_RTS_ITS_MAJOR_INCIDENTS)
* [Consulta sobre el proyecto conjunto de directrices sobre la estimación de costos y pérdidas anuales agregados causados ​​por incidentes importantes relacionados con las TIC](https://ec.europa.eu/eusurvey/runner/DORA_GL_COSTS_LOSSES_MAJOR_ICT_INCIDENTS)
* [Consulta sobre el borrador conjunto de RTS sobre subcontratación de servicios TIC que respaldan funciones críticas o importantes](https://ec.europa.eu/eusurvey/runner/DORA_RTS_ELEMENTS_SUBCONTRACTING_ICT_SERVICES_CRIT_IMP_FUNCTIONS)
* [Consulta sobre el proyecto conjunto de RTS sobre la armonización de las condiciones que permiten la realización de las actividades de supervisión.](https://ec.europa.eu/eusurvey/runner/RTS_Oversight_Harmonistation)
* [Consulta sobre un proyecto conjunto de directrices sobre cooperación en materia de supervisión e intercambio de información entre las AES y las autoridades competentes](https://ec.europa.eu/eusurvey/runner/GL_OVS_Cooperation)
* [Consulta sobre el borrador conjunto de RTS que especifica elementos relacionados con las pruebas de penetración dirigidas por amenazas](https://ec.europa.eu/eusurvey/runner/EUSurveyDORA_RTSonTLPT)

Tenga en cuenta que la fecha límite para la presentación de comentarios es el 4 de marzo de 2024. Todas las contribuciones recibidas se publicarán una vez finalizada la consulta, a menos que se solicite lo contrario.

**Audiencia pública**

Se organizará una audiencia pública en forma de seminario web el 23 de enero de 2024 de 09:00 a 18:00 CET. Las ESA invitan a las partes interesadas a registrarse mediante el [formulario de registro](https://ec.europa.eu/eusurvey/runner/Joint_ESAs_public_event_on_DORA_January2024) antes de las 16:00 CET del 19 de enero de 2023. ​Los detalles del acceso telefónico se comunicarán a los participantes registrados a su debido tiempo.

**Base jurídica, antecedentes y próximos pasos**

DORA, que entró en vigor el 16 de enero de 2023 y se aplicará a partir del 17 de enero de 2025, tiene como objetivo mejorar la resiliencia operativa digital de las entidades en todo el sector financiero de la UE y armonizar aún más los requisitos clave de resiliencia operativa digital para todas las entidades financieras de la UE.

Las ESA esperan presentar los proyectos de normas técnicas a la Comisión Europea y publicar las directrices antes del 17 de julio de 2024.



Ley de Resiliencia Operativa Digital (DORA):

consulta pública sobre la segunda tanda de productos políticos

1. Las tecnologías de la información y la comunicación (TIC) son compatibles con sistemas complejos utilizados para las actividades cotidianas del sector financiero. El uso extendido de los sistemas TIC aumenta la eficiencia de los procesos internos y la experiencia de usuario para los clientes, sin embargo, también introduce riesgos y vulnerabilidades, que pueden hacer que las entidades financieras estén expuestas a ciberataques o incidentes. Si no se gestionan adecuadamente, los riesgos de las TIC podrían provocar perturbaciones en los servicios financieros que a menudo se ofrecen a través de las fronteras y pueden tener efectos de gran alcance en otras empresas, sectores o incluso en el resto de la economía. El riesgo de que se produzcan estas perturbaciones transfronterizas e intersectoriales pone de relieve la importancia de la resiliencia operativa digital del sector financiero.

2. Como medida para mejorar la resiliencia operativa digital global del sector financiero de la UE, el 27 de diciembre de 2022 se publicó en el Diario Oficial de la Unión Europea1 la Ley de Resiliencia Operativa Digital (DORA), que entró en vigor el 16 de enero de 2023. El DORA se aplicará a partir del 17 de enero de 2025.

3. El DORA armoniza las normas relativas a la resiliencia operativa del sector financiero aplicables a 21 tipos diferentes de entidades financieras, que abarcan temas importantes como: la gestión del riesgo relacionado con las TIC; gestión y notificación de incidentes relacionados con las TIC; pruebas de la resiliencia operativa digital de los sistemas de TIC; y la gestión de los riesgos de terceros relacionados con las TIC. Además, DORA es lex specialis de la Directiva SRI2 y del artículo 11 y de los capítulos III, IV y VI de la Directiva RCE3.

4. Desde el punto de vista supervisor, el DORA tiene por objeto aumentar la concienciación supervisora sobre los riesgos cibernéticos y los incidentes relacionados con las TIC a los que se enfrentan las FE y mejorar la cooperación entre las autoridades competentes del sector financiero, pero también entre las autoridades de diferentes sectores y jurisdicciones en relación con las TIC y la gestión del riesgo cibernético.

5. El DORA también introduce un marco para supervisar los riesgos sistémicos y de concentración que plantea la dependencia del sector financiero de proveedores terceros de servicios de TIC y un marco de supervisión a escala de la UE para los proveedores esenciales de servicios de TIC que tiene por objeto garantizar que los riesgos de TIC que plantean estos proveedores esenciales a las entidades financieras se gestionen adecuadamente.

6. Para poner en práctica la solicitud, el DORA encomienda a las Autoridades Europeas de Supervisión (AES) que preparen conjuntamente, a través del Comité Mixto, un conjunto de productos políticos con dos plazos principales de presentación: el 17 de enero de 2024 (primer lote) y el 17 de junio de 2024 (segundo lote), como se destaca en la imagen siguiente.



7. Además de los mandatos políticos conferidos a las AES por el DORA, estas han emitido el 29 de septiembre de 2023 un dictamen técnico4 a la Comisión Europea para responder a la convocatoria de asesoramiento5 para apoyar la preparación de actos delegados que complementen el texto del DORA en relación con los criterios para designar a los proveedores terceros de servicios de TIC como esenciales y las tasas que dichos proveedores tendrán que pagar para ser supervisados.

8. En el cuadro que figura a continuación se resumen los plazos para la elaboración de políticas de todos los productos del DORA y su consulta pública:



9. La publicación de hoy se centra en la segunda tanda de mandatos de política que incluyen documentos de consulta sobre las siguientes normas:

i. RTS e ITS sobre el contenido, los plazos y las plantillas para la notificación de incidentes relacionados con las TIC (artículo 20)

El borrador de la RTS sobre los detalles de la notificación de incidentes graves en el marco de DORA abarca tres aspectos distintos:

a) el contenido de los informes de incidentes graves relacionados con las TIC;

b) los plazos para la presentación de una notificación inicial y de informes intermedios y finales para cada incidente grave;

c) establecer el contenido de la notificación en caso de ciber amenazas significativas.

El proyecto de estrategia técnica refleja la proporcionalidad y garantiza la coherencia con el enfoque de notificación de incidentes adoptado en la Directiva (UE) 2022/2555 (SRI 2).

Por lo que se refiere a los plazos de presentación de informes, el proyecto de RTS propone plazos armonizados para las entidades financieras incluidas en el ámbito de aplicación del DORA. En consecuencia, los plazos propuestos para la notificación de incidentes graves son los siguientes:

• El informe inicial dentro de las 4 horas posteriores al momento de la clasificación del incidente como grave, pero a más tardar 24 horas desde el momento de la detección del incidente.

• Un informe intermedio dentro de las 72 horas posteriores a la clasificación del incidente como grave, o cuando se hayan recuperado las actividades habituales y la actividad vuelva a la normalidad.

• El informe final se presentará a más tardar 1 mes después de la clasificación del incidente como grave.

Por lo que se refiere al contenido de las notificaciones de incidentes graves, el proyecto de RTS tiene por objeto lograr el equilibrio adecuado entre permitir que las autoridades competentes reciban la información esencial relacionada con cada incidente y, al mismo tiempo, no suponer una carga de notificación para las entidades financieras. En relación con el contenido de las notificaciones de ciber amenazas significativas (que deben notificarse de forma voluntaria), el proyecto de RTS introduce un contenido breve, sencillo y conciso de las notificaciones.

El borrador de ITS cubre aspectos relacionados con los requisitos generales de presentación de informes e introduce el formato y las plantillas para informar sobre incidentes graves y amenazas cibernéticas significativas en el marco de DORA. Con respecto a la plantilla, el proyecto de ITS introduce una plantilla única que abarca la notificación inicial, los informes intermedios y finales. La plantilla y los detalles técnicos de apoyo están diseñados de manera similar a los requisitos de información prudencial. El borrador de ITS también proporciona un glosario de datos, las características de los campos de datos e instrucciones sobre cómo rellenarlos.

ii. Directrices sobre los costes y pérdidas agregados derivados de incidentes graves relacionados con las TIC (artículo 11, apartado 1)

En el proyecto de directrices se especifica la estimación de los costos y pérdidas anuales agregados causados por incidentes graves relacionados con las TIC. El cálculo de los costes y pérdidas anuales con arreglo a las Directrices está en consonancia con la evaluación de los costes y pérdidas de cada incidente con arreglo a las normas técnicas de notificación de incidentes. En particular, las Directrices introducen un informe que abarca los costes y pérdidas brutos, las recuperaciones financieras y los costes y pérdidas netos por incidentes graves relacionados con las TIC.

En las Directrices también se propone centrar el período de referencia para la agregación en un ejercicio contable, a fin de basarse en las cifras disponibles de los estados financieros validados.

iii. RTS sobre ensayos de penetración con hilo conductor (art. 26, apartado 11)

El artículo 26 del DORA obliga a determinadas entidades financieras a realizar al menos cada 3 años pruebas avanzadas mediante TLPT. El artículo 26, apartado 11, del DORA encomienda a las AES, «de acuerdo con el BCE», que elaboren proyectos de normas técnicas de regulación «de conformidad con el marco TIBER-UE» para especificar con mayor detalle los criterios utilizados para identificar a las entidades financieras que deben llevar a cabo TLPT, los requisitos y normas que rigen el uso de evaluadores internos, los requisitos relativos al alcance, la metodología de ensayo y el enfoque para cada fase del ensayo. los resultados, las etapas de cierre y remediación y el tipo de supervisión y otra cooperación pertinente necesaria para la aplicación de la TLPT y para la facilitación del reconocimiento mutuo.

iv. RTS sobre subcontratación de funciones críticas o importantes (Art.30.5)

El artículo 30, apartado 5, del DORA exige a las AES que elaboren, a través del Comité Mixto, proyectos de normas técnicas de regulación para especificar con mayor detalle los elementos a que se refiere el artículo 30, apartado 2, letra a), que una entidad financiera debe determinar y evaluar al subcontratar servicios de TIC que soporten funciones esenciales o importantes o partes materiales de las mismas.

El borrador de la RTS proporciona especificaciones adicionales sobre cómo determinar y evaluar cuándo se pueden realizar subcontratos de servicios de TIC que respaldan funciones críticas o importantes. De conformidad con el mandato, el proyecto de RTS se centra en los servicios de TIC que respaldan funciones críticas o importantes, o partes materiales de las mismas, prestados por subcontratistas de TIC. El proyecto de estrategia técnica sigue el ciclo de vida de los acuerdos entre las entidades financieras y los proveedores terceros de servicios de TIC cuando subcontratan servicios de TIC que apoyan funciones esenciales o importantes, y establece requisitos clave para las entidades financieras sobre el uso de servicios subcontratados que respaldan funciones esenciales o importantes o partes materiales de las mismas, que abarca: la evaluación de riesgos antes de permitir que se subcontraten servicios de TIC que apoyen funciones esenciales o importantes; requisitos sobre los arreglos contractuales; sobre el seguimiento de los acuerdos de subcontratación; sobre la información de los cambios sustanciales; y sobre los derechos de salida y rescisión.

v. Directrices sobre la cooperación en materia de supervisión entre las AES y las autoridades competentes (artículo 32, apartado 7)

El artículo 32, apartado 7, del DORA exige a las AES que publiquen directrices sobre la cooperación entre las AES y las autoridades competentes que abarquen:

o los procedimientos y condiciones detallados para la asignación y ejecución de tareas entre las autoridades competentes y las AES; y

o los detalles sobre los intercambios de información necesarios para que las autoridades competentes garanticen el seguimiento de las recomendaciones dirigidas a los proveedores terceros esenciales de servicios de TIC.

El proyecto de directrices se refiere únicamente a la cooperación y el intercambio de información entre las AES y las autoridades competentes. Por lo tanto, la cooperación con las entidades financieras, los proveedores terceros esenciales de servicios de TIC, las autoridades competentes en virtud de la Directiva (UE) 2022/2555, entre las autoridades competentes, entre las AES y con otras instituciones de la UE queda fuera del ámbito de aplicación de las directrices.

El proyecto de directrices abarca las cuatro esferas siguientes:

o Consideraciones generales: abarca temas como el idioma, los medios de comunicación, los puntos de contacto y la diferencia de opiniones entre las AES y las autoridades competentes.

o Designación de proveedores terceros esenciales de servicios de TIC: abarca los intercambios de información entre el supervisor principal, las autoridades competentes y el Foro de Supervisión en relación con la designación de proveedores terceros esenciales de servicios de TIC.

o Actividades de supervisión: abarca los procedimientos y el intercambio de información relacionados con el plan anual de supervisión, las investigaciones generales y las inspecciones in situ y las autoridades competentes que adoptan medidas relativas a los proveedores externos esenciales de servicios de TIC de acuerdo con el supervisor principal.

o Seguimiento de las recomendaciones: abarca los intercambios de información entre el supervisor principal y las autoridades competentes para garantizar el seguimiento de las recomendaciones y la decisión de las autoridades competentes de exigir a las entidades financieras que suspendan o rescindan su contrato con el proveedor tercero esencial de servicios de TIC.

vi. RTS sobre armonización de la supervisión (art. 41, apartado 1) El artículo 41, apartado 1, del DORA exige a las AES que elaboren, a más tardar el 17 de julio de 2024, un proyecto de RTS en el que se especifique:

a) la información que debe facilitar un proveedor tercero de servicios de TIC en la solicitud de designación de una solicitud voluntaria como crítica;

b) el contenido, la estructura y el formato de la información que deben presentar, divulgar o comunicar los proveedores terceros de servicios de TIC al supervisor principal de conformidad con el artículo 35, apartado 1, incluida la plantilla para facilitar información sobre los acuerdos de subcontratación;

d) los detalles de la evaluación por parte de las autoridades competentes de las medidas adoptadas por los proveedores terceros esenciales de servicios de TIC sobre la base de las recomendaciones de la OA de conformidad con el artículo 42, apartado 3.

Cabe señalar que el mandato del Equipo Mixto de Examen6 se finalizará con arreglo a un calendario diferente con la participación del Grupo de Alto Nivel sobre Supervisión del DORA (HLGO), recientemente constituido.

El objetivo principal del proyecto de RTS es armonizar los requisitos en materia de normativa y establecer condiciones de supervisión eficientes frente a los proveedores de servicios terceros esenciales, las entidades financieras y las autoridades de supervisión en toda la Unión, con el fin de evitar la fragmentación legislativa, garantizando al mismo tiempo la estabilidad del sector financiero.

Consulta pública y próximos pasos

10. La consulta pública sobre todos los mandatos incluidos en la segunda tanda durará hasta el 4 de marzo de 2024. Además, para presentar los documentos de consulta y sus fundamentos, y para aclarar las cuestiones planteadas por las partes interesadas, las AES organizarán una audiencia pública en línea el 23 de enero de 2024.

11. En cada documento de consulta se incluyen detalles sobre la forma de proporcionar información sobre los distintos productos de política.

12. Sobre la base de los comentarios recibidos en la consulta pública, los instrumentos jurídicos se finalizarán y se presentarán a la Comisión Europea a más tardar el 17 de julio de 2024.

Antecedentes

13. El DORA es un Reglamento intersectorial que se aplica a más de 20 tipos diferentes de entidades financieras y a un número de autoridades competentes (CA) más del doble, con el fin de garantizar un enfoque intersectorial, proporcionado y armonizado en el desarrollo de la legislación de nivel 2, las AES han decidido constituir el Comité Mixto Subcomité de Operaciones Digitales

Resiliencia (JC SC DOR)7 para contribuir y coordinar, cuando sea necesario, la contribución de las AES al proceso regulador de la UE en relación con la resiliencia operativa digital. Más de 50 autoridades, incluidas las autoridades nacionales, el Banco Central Europeo y ENISA, participan en el trabajo conjunto sobre el desarrollo de los productos políticos establecidos en el DORA8.

1. Reglamento (UE) 2022/2554, de 14 de diciembre de 2022, relativo a la resiliencia operativa digital del sector financiero (DORA)

2. Véase el considerando 28 de la Directiva (UE), de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (Directiva SRI II)

3. Véanse el considerando 21 y el artículo 8 de la Directiva (UE) 2022/2557, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (RCE)

4. <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2023/JC%20technical%20advice%20on%20DORA/1062226/JointESAs%E2%80%99%20response%20to%20the%20Call%20for%20advice%20on%20the%20designation%20criteria%20and%20fees%20for%20the%20DORA%20oversight%20framework_final.pdf>

5. Las AES inician un debate sobre los criterios aplicables a los proveedores de servicios externos esenciales de TIC y las tasas de supervisión (europa.eu)

6. El texto de la habilitación es el siguiente: «Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación para especificar: c) los criterios para determinar la composición del equipo de examen conjunto que garantice una participación equilibrada de los miembros del personal de las AES y de las autoridades competentes pertinentes, su designación, tareas y modalidades de trabajo».

7. Mandato del Subcomité de Resiliencia Operativa Digital (europa.eu) del Comité Mixto de las Autoridades Europeas de Supervisión

8. Los siguientes productos de actuación se elaborarán únicamente en consulta con ENISA: RTS sobre el marco de gestión de riesgos de las TIC (art. 15) y marco simplificado de gestión de riesgos (art. 16). En consulta con ENISA y el BCE, se elaborarán los siguientes productos de actuación: RTS sobre los criterios para la clasificación de los incidentes relacionados con las TIC (art. 18, apartado 3), RTS para especificar la notificación de incidentes graves relacionados con las TIC (art. 20.a), STI para establecer los detalles de notificación de incidentes graves relacionados con las TIC (art. 20.b) y el informe de viabilidad sobre una mayor centralización de la notificación de incidentes mediante la creación de un centro de la UE para la notificación de incidentes graves relacionados con las TIC (art. 21). Por último, las AES desarrollarán, de acuerdo con el BCE, las normas técnicas para especificar las pruebas de penetración basadas en amenazas (art. 26.1)

