Consulta conjunta de las Autoridades Europeas de Supervisión (AES) sobre el segundo paquete de mandatos en virtud de la Ley de Resiliencia Operacional Digital (DORA)

Consulta conjunta de las AES sobre el segundo paquete de mandatos en virtud de la Ley de Resiliencia Operacional Digital

1.- A quién va dirigida

La consulta pública está dirigida a participantes en los mercados.

2.- Nota Informativa

DORA armoniza las reglas relacionadas con la resiliencia operativa para el sector financiero que se aplican a 21 tipos diferentes de entidades financieras, cubriendo temas importantes como: gestión de riesgos TIC; gestión y notificación de incidentes TIC; pruebas de la resiliencia operativa digital de los sistemas TIC; y la gestión de riesgos TIC de terceros.

Para hacer operativa la aplicación, DORA exige a las Autoridades Europeas de Supervisión (AES) que preparen conjuntamente, a través del Comité Conjunto (JC), un conjunto de normas. Para el primer paquete de mandatos, el plazo de presentación a la Comisión Europea está fijado para el 17 de enero de 2024 y la consulta pública ya ha finalizado.

Esta publicación se centra en el segundo paquete de mandatos de normas que se presentarán antes del 17 de junio de 2024 e incluye documentos de consulta sobre los siguientes estándares:

1) RTS e ITS sobre contenido, cronogramas y plantillas para la notificación de incidentes relacionados con las TIC (Artículo 20)

El borrador de RTS sobre los detalles de notificación de incidentes importantes bajo DORA cubre 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, informes intermedios y finales para cada incidente mayor;

c) el contenido de la notificación de ciberamenazas significativas.

El borrador de ITS cubre aspectos relacionados con los requisitos generales de presentación de informes e introduce el formato y las plantillas para informar incidentes importantes y amenazas cibernéticas importantes bajo DORA.

Documento de consulta sobre el borrador de RTS e ITS sobre notificación de incidentes importantes bajo DORA.

Formulario de respuesta para las RTS e ITS sobre notificación de incidentes mayores.

2) Directrices sobre costes y pérdidas agregados derivados de incidentes importantes relacionados con las TIC (Artículo 11(1))

El proyecto de Directrices especifica la estimación de los costes y pérdidas anuales agregados causados por incidentes importantes relacionados con las TIC.

Documento de consulta sobre el borrador de Directrices sobre costos y pérdidas.

Formulario de respuesta para las Directrices sobre costes y pérdidas causados por incidentes importantes relacionados con las TIC.

3) RTS sobre pruebas de penetración basadas en amenazas (TLPT) (Art.26(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, de DORA exige a las AES, "de acuerdo con el BCE", que desarrollen proyectos de normas técnicas regulatorias "de conformidad con el marco TIBER-UE" para especificar con más detalle los criterios utilizados para identificar las entidades financieras obligadas a realizar TLPT, los requisitos y estándares que rigen el uso de probadores internos, los requisitos en relación con el alcance, la metodología de prueba y el enfoque para cada fase de las pruebas, resultados, etapas de cierre y remediación y el tipo de supervisión y otra cooperación relevante necesaria para la implementación de TLPT y para facilitar el reconocimiento mutuo.

Documento de consulta sobre el borrador de RTS sobre TLPT.

Formulario de respuesta para las RTS de pruebas de penetración basadas en amenazas (TLPT).

4) RTS sobre subcontratación de funciones críticas o importantes (Art.30(5))

Los proyectos de normas técnicas de regulación especifican con más 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 TIC que respalden funciones críticas o importantes o partes materiales de las mismas. Los RTS cubren requisitos relacionados con: la evaluación de riesgos antes de permitir que se subcontraten servicios TIC que respaldan funciones críticas o importantes; requisitos sobre los acuerdos contractuales; sobre el seguimiento de los acuerdos de subcontratación; sobre información de cambios materiales; y sobre derechos de salida y terminación.

Documento de consulta sobre el proyecto de RTS sobre subcontratación.

Formulario de respuesta para las RTS sobre subcontratación de servicios TIC.

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

Las directrices cubren: los procedimientos y condiciones detallados para la asignación y ejecución de tareas entre las autoridades competentes y las AES y los detalles sobre los intercambios de información que son necesarios para que las autoridades competentes garanticen el seguimiento de las recomendaciones dirigidas a terceros proveedores críticos de servicios TIC.

La cooperación con entidades financieras, terceros proveedores de servicios de TIC críticos, autoridades competentes en virtud de la Directiva (UE) 2022/2555, entre autoridades competentes, entre las AES y con otras instituciones de la UE está fuera del alcance de las directrices.

Documento de consulta sobre el proyecto de directrices sobre cooperación en materia de supervisión.

Formulario de respuesta para las GL sobre cooperación en materia de supervisión e intercambio de información entre las AES y las autoridades competentes.

6) RTS sobre armonización de la supervisión (Art.41(1))

El objetivo principal del borrador del RTS es armonizar los requisitos en todas las regulaciones y establecer condiciones de supervisión eficientes frente a terceros proveedores de servicios críticos, entidades financieras y autoridades de supervisión en toda la Unión con el fin de evitar la fragmentación legislativa, al mismo tiempo que garantizar la estabilidad del sector financiero. Estas especifican:

a) la información que debe proporcionar un tercero proveedor de servicios TIC en la solicitud para que una solicitud voluntaria sea designada como crítica;

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

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

Cabe señalar que el mandato del Equipo Conjunto de Examen se finalizará según un cronograma diferente con la participación del Grupo de Alto Nivel sobre Supervisión de DORA (HLGO), recientemente constituido.

Documento de consulta sobre el borrador de RTS sobre armonización de la supervisión.

Formulario de respuesta para las RTS sobre armonización de supervisión.

3.- Envío de comentarios

La fecha límite de esta consulta es el **4 de marzo de 2024.**

Los interesados pueden enviar sus comentarios a través del enlace proporcionado al principio de este documento o los enlaces individuales facilitados en cada apartado. Allí encontrará más información junto con los documentos de consulta y los formularios de respuesta. Todos los documentos están disponibles en inglés.

Asimismo, se ruega se remita a la CNMV una copia de las respuestas remitidas por correo electrónico a la siguiente dirección: **documentosinternacional@cnmv.es**

Dirección de Asuntos Internacionales

CNMV

c/ Edison 4

28006 Madrid