Consulta pública conjunta de las ESAs sobre el primer paquete de proyectos de normas técnicas de desarrollo del Reglamento 2022/2554, sobre la resiliencia operativa digital en el sector financiero (DORA)

Enlace a los documentos:

Consultation paper on draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under article 15 and 16.3 of Regulation 2022/2554

Consultation paper on draft Regulatory Technical Standards on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation 2022/2554

Consultation paper on draft Implementation Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third party service providers as mandated by Regulation 2022/2554

Consultation paper on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandate by Regulation 2022/2554

1.- A quién va dirigido (partes interesadas):

Esta consulta va dirigida a todos los participantes del mercado, incluidos los terceros proveedores de servicios de TIC (Tecnología de la Información y la Comunicación) que presten sus servicios a entidades financieras.

La CNMV agradecería a todas las partes interesadas mencionadas anteriormente que le remitieran una copia de sus respuestas a la consulta a la dirección que se indica a continuación: Documentosinternacional@cnmv.es

2.- Nota Informativa

ESMA ha publicado, el 19 de junio de 2023, cuatro consultas públicas sobre un paquete de proyectos de normas técnicas de desarrollo del Reglamento 2022/2554, sobre la resiliencia operativa digital en el sector financiero (DORA).

1) Consulta pública sobre el proyecto de normas técnicas de regulación para lograr una mayor armonización de las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC de conformidad con los artículos 15 y 16.3 del Reglamento 2022/2554

Las ESAs han agrupado los mandatos de los artículos 15 y 16.3 debido a su interrelación para abordar los marcos de gestión de riesgo de TIC de manera integral.

Las normas técnicas de desarrollo del artículo 15 (marco general de gestión de riesgo relacionado con las TIC) especifican los requisitos que todas las entidades financieras deben cumplir en relación con los aspectos siguientes:

> i) las políticas, procedimientos, protocolos y herramientas en materia de seguridad de las TIC, incluidos requisitos de gobernanza, de gestión de riesgos y de gestión de activos de TIC, técnicas de encriptación y criptografía, seguridad de la operativa de ICT, seguridad de la red, proyecto y cambio en la gestión, seguridad física y concienciación/formación sobre seguridad;
>
> ii) la política de recursos humanos y los nuevos componentes de los controles de los derechos de gestión del acceso lógico y físico a los activos de información y activos de TIC;
>
> iii) los mecanismos para la rápida detección de actividades anómalas y criterios para activar los procesos de detección de incidentes relacionados con las TIC y los planes de respuesta a los mismos; y
>
> iv) la política de continuidad de la actividad en materia de TIC.

También especifican también el contenido y el formato del informe sobre la revisión del marco de gestión de riesgo relacionado con las TIC que debe realizarse al menos anualmente (periódicamente en el caso de microempresas) o en caso de incidentes graves.

Estas normas técnicas son complementarias a los requisitos establecidos en los artículos 5-16 del Reglamento DORA y, por lo tanto, deben leerse juntamente con ellos.

Las normas técnicas de desarrollo del artículo 16 (marco simplificado de gestión de riesgo de TIC) son de aplicación únicamente a cinco categorías de entidades financieras: ESIs pequeñas y no interconectadas, entidades de pago exentas conforme a la Directiva 2015/2366, entidades exentas conforme a la Directiva 2013/36 cuando el Estado Miembro no ha aplicado la opción del art. 2.4 (excluir del ámbito de aplicación), entidades de dinero electrónico exentas confirma la Directiva 2009/110 y fondos de pensiones de empleo pequeños. Estas normas técnicas complementan los requisitos establecidos en el artículo 16 en las áreas siguientes: marco de gestión de riesgo de TIC, elementos de los sistemas, protocolos y herramientas para minimizar el riesgo de TIC, la política de continuidad de la actividad en materia de TIC y el informe de revisión de gestión del riesgo de TIC.

En cuanto al principio de proporcionalidad, la propuesta de ESMA combina las dos opciones de política legislativa que describe el proyecto de análisis de impacto: opción A para el marco general de riesgos: un principio general (tener en cuenta elementos de complejidad o riesgo) aplicable a todas las entidades financieras en el ámbito del Reglamento de DORA pero no sujetas al artículo 16 para hacer la evaluación de proporcionalidad; y opción B para el marco simplificado de gestión de riesgo: identificar requisitos específicos a aplicar de manera diferenciada, por ejemplo, la frecuencia en la revisión o diferentes niveles de detalle a incluir en las políticas de ICT o en aspectos procedimentales.

Consulta pública sobre el proyecto de normas técnicas de regulación para especificar los criterios para la clasificación de los incidentes relacionados con las TIC, los umbrales de importancia relativa para determinar los incidentes graves y las ciberamenazas importantes en el Reglamento 2022/2554 (art. 18.3)

Las normas técnicas establecen requisitos armonizados para las entidades financieras sobre:

i) los criterios para la clasificación de incidentes relacionados con las TIC por parte de entidades financieras;

ii) los criterios y los umbrales de importancia relativa para determinar los incidentes graves relacionados con las TIC de los que las entidades financieras deben informar a las autoridades competentes;

iii) los criterios y los umbrales de importancia relativa a aplicar a la hora de clasificar las ciberamenazas como importantes o significativas; y

iv) los criterios a aplicar por las autoridades competentes con el fin de evaluar la relevancia de los principales incidentes relacionados con las TIC para autoridades competentes pertinentes en los Estados miembros de acogida y los detalles de la información para ser compartida con ellas.

El objetivo de estas normas técnicas es armonizar y agilizar el régimen de notificación de incidentes relacionados con las TIC en la UE.

El documento considera dos tipos de criterios para clasificar los incidentes: i) primarios, que son los criterios siguientes: "clientes, contrapartes financieras y operaciones afectadas", "pérdidas de datos" y "servicios críticos afectados"; y ii) secundarios, que incluyen los criterios siguientes: "impacto reputacional", "duración y tiempo de inactividad del servicio", "distribución geográfica" e impacto económico". En cuanto los umbrales, algunos de ellos son apropiados sólo para entidades de gran tamaño.

Para la clasificación de incidentes como graves, se propone que se alcancen los umbrales de importancia relativa para dos criterios primarios o para un criterio primario y dos secundarios. los incidentes recurrentes con la misma causa raíz aparente, naturaleza e impacto que, individualmente no son graves pero que acumulativamente cumplen con los criterios de clasificación, deben ser clasificado como graves.

Para la clasificación de las ciberamenazas como importantes, el documento propone un enfoque basado en la probabilidad de que se materialice la amenaza, de que afecte a servicios críticos y de que si se materializa pueda cumplir las condiciones para ser un incidente grave.

Finalmente, la ESAs proponen que la evaluación de la relevancia para las autoridades competentes en otros países miembros esté basada en la importancia del impacto en la jurisdicción respectiva notificándose entre las autoridades todos los detalles de los incidentes graves.

<u>Consulta púbica sobre el proyecto de normas técnicas de implementación para establecer las plantillas normalizadas para el registro de información en relación con todos los acuerdos contractuales relativos al uso de servicios de TIC prestados por terceros proveedores de servicios de TIC conforme al Reglamento 2022/2554 (art. 28.9)</u>

Para garantizar el adecuado seguimiento del riesgo de terceros de las TIC en el sector financiero, las entidades financieras adoptarán una estrategia que permita el control permanente de todas las actividades de los terceros proveedores de servicios de TIC. Para lograr este objetivo, las entidades financieras mantendrán y actualizarán el registro de

información en relación a todos los acuerdos contractuales relativos al uso de servicios de TIC prestados por terceros proveedores de servicios de TIC.

Las normas técnicas contienen plantillas normalizadas para el registro de información que deben mantener y actualizar las entidades financieras, a nivel de la entidad y a nivel sub consolidado y consolidado, en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC.

Las plantillas se han diseñado teniendo en cuenta la triple finalidad del registro de información: i) es parte de la gestión de riesgos de TIC dentro del marco de gestión del riesgo relacionado con la TIC; ii) facilita la supervisión efectiva de las entidades financieras: y iii) facilita la designación de proveedores de servicios de terceros como críticos por las ESAs a nivel de la UE en el contexto del marco de supervisión.

Para simplificar la elaboración de los registros por parte de las entidades financieras, el proyecto de normas técnicas contiene dos conjuntos diferente de plantillas para los registros, el primero, a nivel de entidad individual y, el segundo, a nivel subconsolidado y consolidado.

Las plantillas tienen como objetivo asegurar un nivel mínimo de información que es común a todos los acuerdos contractuales sobre el uso de servicios TIC y han sido diseñadas teniendo en cuenta una perspectiva de gestión y remisión de la información a incluir para garantizar la coherencia y la armonización y evitar la duplicidad en el procesamiento de datos con fines informativos. Las normas técnicas no contienen especificaciones sobre el proceso de intercambio de información entre las entidades financieras y las autoridades competentes ni de éstas con el Foro de Supervisión. Las entidades financieras complementarán la información requerida por las plantillas adaptándola a sus propósitos internos e individuales de gestión de riesgos.

Desde el punto de vista de la proporcionalidad, el documento indica que el conjunto de plantillas es proporcionado ya que la cantidad de información a incluir depende del grado de dependencia de los servicios proporcionados por terceros proveedores de servicios de TIC. Por lo tanto, una entidad financiera que dependa de un número significativo de TIC de terceros proveedores de servicios tendrá que reportar más información que una menos dependiente. Además, las entidades financieras están obligadas a proporcionar cierta información adicional, como información complementaria sobre la evaluación de riesgos, la cadena de suministro de TIC o sobre la subdelegación si el servicio de TIC prestado se refiere a una función crítica o importante.

Consulta pública sobre el proyecto de normas técnicas de regulación para especificar el contenido detallado de la política sobre el uso de servicios de TIC en relación con los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC conforme al Reglamento 2022/2554 (art. 28.10)

Las entidades financieras adoptarán y revisarán, como parte de su marco de gestión de riesgos de TIC, una estrategia sobre el riesgo relacionado con los proveedores de servicios de que incluirá una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores de servicios de TIC.

Las normas técnicas tienen por objetivo que la entidad mantenga el control de sus riesgos operacionales, la seguridad de la información y la continuidad del negocio a lo largo de la vida del acuerdo contractual con los terceros proveedores de servicios de TIC. Para ello, las normas

técnicas establecen los requisitos para las entidades financieras en cada una de las fases en relación con el ciclo de vida de la gestión de los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC: i) la fase precontractual: planificación de los acuerdos contractuales, incluidos la evaluación del riesgo, los procesos de diligencia debida y el proceso de aprobación de cambios nuevos o materiales de esos acuerdos contractuales con terceros; ii) la implementación, seguimiento y gestión de los acuerdos contractuales; y iii) la estrategia de salida y los procesos para la finalización de los acuerdos que aseguren la continuidad del negocio en caso de prestación inadecuado o fallo del servicio.

Próximos pasos. Las ESAs tendrán en cuenta los comentarios recibidos para redactar las normas técnicas que deberán remitir a la Comisión Europea a más tardar el 17 de enero de 2023.

3.- Solicitud de comentarios

El período de consulta finaliza el **11 de septiembre de 2023.**

Los interesados deben enviar sus aportaciones a través de la web de ESMA **www.esma.europa.eu.** En la página ***Consultations*** (ponga el cursor sobre la palabra para acceder a la página donde se encuentran los cuatro cuestionarios online de respuesta).

El 13 de julio de 9:00-18:00 tendrá lugar una audiencia pública a la que las ESAs invitan a todas las partes interesadas. Para asistir a la audiencia pública, es necesario registrarse antes del 10 de julio a las 16:00 a través del formulario (ponga el cursor sobre la palabra para acceder al formulario).

Asimismo, como ya se ha indicado arriba, la CNMV agradecería a las partes interesadas que le remitieran una copia de sus respuestas a la consulta a la dirección que se indica a continuación: Documentosinternacional@cnmv.es

CNMV
Dirección de Asuntos Internacionales
c/ Edison 4
28006 Madrid