

ECIJA

Segundo paquete
normativo en el
marco de la Ley
de Resiliencia
Operativa Digital

NOTA INFORMATIVA

Segundo paquete normativo en el marco de la Ley de Resiliencia Operativa Digital

Las novedades del segundo paquete normativo son: cuatro proyectos definitivos de normas técnicas de regulación (RTS), un conjunto de normas técnicas de ejecución (ITS) y dos Directrices.

El día de 17 de julio de 2024 la Junta de Supervisores de las ESAs (EBA, EIOPA y ESMA,) público el segundo paquete normativo en el marco de la Ley de Resiliencia Operativa Digital o Digital Operational Resilience Act (en adelante, "**Reglamento DORA**"). Este conjunto normas aprobadas incluyen cuatro proyectos definitivos de normas técnicas de regulación (en adelante, "RTS"), un conjunto de normas técnicas de ejecución (en adelante, "ITS") y dos directrices son las novedades del segundo paquete normativo.

JULIO 2024

Las RTS e ITS aprobadas son las siguientes:

- RTS e ITS sobre el contenido, formato, plantillas y plazos para la notificación de incidentes graves relacionados con las TIC y ciberamenazas significativas.
- RTS sobre la armonización de las condiciones que permiten llevar a cabo las actividades de supervisión.
- RTS especificando los criterios para determinar la composición del equipo conjunto de examen (JET).
- RTS sobre pruebas de penetración basadas en amenazas (TLPT)

Estas tienen por objeto desarrollar cuestiones del Reglamento DORA tales como la notificación de incidentes relacionados con las TIC y las pruebas de penetración basadas en amenazas. A su vez, se incluye algunos requisitos sobre el diseño del marco de supervisión.

Entre las cuestiones de mayor interés destaca la **concreción de los plazos para notificar los incidentes de graves de conformidad con el art 19 del Reglamento DORA**. En la norma de técnica se indica que: el **Informe inicial** deberá notificarse en un plazo de **4 horas** desde que se clasifico el incidente como grave **y en un plazo no superior a 24 horas** desde que se detectó el incidente.

Por su parte, el **informe intermedio** será notificado en un **plazo máximo de 72 horas** desde que se clasifico el incidente como grave o cuando se haya recuperado las actividades normales y la actividad haya vuelto a la normalidad. En cuanto al **informe final se establece un plazo de 1 mes** desde que se clasifico el incidente como grave a menos que el incidente no se haya resuelto. A su vez, se establece que en aquellos supuestos en los que el plazo para presentar cualquiera de los informes coincide con un fin de semana, el informe se presentara el día siguiente laborable en un plazo de una hora a partir de una hora habitual de inicio.

JULIO 2024

Otra de las cuestiones fundamentales desarrolladas por las RTS es la relativa a **la identificación de las entidades financieras obligadas a realizar pruebas de penetración basadas en amenazas**. La norma técnica de regulación prevé un listado de las entidades obligadas a cumplir con la mencionada obligación.

Nuevas directrices

En cuanto a las Directrices aprobadas se incluye:

- Directrices sobre la estimación de los costes/pérdidas agregadas causados por incidentes graves relacionados con las TIC
- Directrices sobre cooperación en materia de supervisión.

Próximos pasos

Con la aprobación de las RTS ahora corresponde a la Comisión Europea revisar estas normas para su posterior adopción en los próximos meses.

Área de Protección de Datos de ECIJA

info@ecija.com

Tel: + 34 91.781.61.60

Calle Serrano, 69.
28006 Madrid
www.ecija.com

