Pérez-Llorca

Real Decreto de seguridad de las redes y sistemas de información

MARCO NORMATIVO

i. El RD 43/2021 desarrolla el RDL 12/2018, que fue el encargado de trasponer la Directiva NIS y estableció un marco general para la **seguridad en las redes y en los sistemas de información.**

ii. El RD 43/2021 se aplica, al igual que el RDL 12/2018, a:

a. la prestación de los **servicios esenciales** dependientes en las redes e **Infraestructuras Críticas.**

b. Los **servicios digitales** que correspondan a **mercados en línea, motores de búsqueda en línea y servicios de computación en nube.**

iii. El RD 43/2021 tiene por finalidad desarrollar el RD 182/2018 en lo que afecta a:

a. el **marco estratégico e institucional** de seguridad de las redes y sistemas de información;

b. el cumplimiento de las **obligaciones de seguridad** de los operadores de servicios esenciales y de los proveedores de servicios digitales; y

c. la gestión de **incidentes de seguridad.**

iv. El RD 43/2021 amplía las **autoridades competentes** para los operadores de servicios esenciales que no sean consideradas operadores críticos.

v. Refuerza la **cooperación y coordinación** entre los distintos equipos de CSIRT y estructura la cooperación entre los CSIRT y las autoridades competentes, a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

vi. Recoge la función del **punto de contacto único**, que garantiza la cooperación transfronteriza de las autoridades competentes con:

a. las autoridades competentes de otros Estados Miembros de la Unión Europea;

b. el grupo de cooperación de representantes de los Estados Miembros, la Comisión Europea y la Empresa Nacional de Innovación; y

c. la red de CSIRT.

REQUISITOS DE SEGURIDAD

i. Obligación de los operadores de servicios esenciales y los proveedores de servicios digitales de adoptar **medidas técnicas y de organización** adecuadas y proporcionadas para la gestión de los riesgos que afecten a la seguridad de las redes y sistemas de información.

ii. Las **políticas de seguridad** aprobadas por los operadores de servicios esenciales deberán respetar los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

iii. Las medidas adoptadas se deberán formalizar en la **Declaración de Aplicabilidad** de medidas de seguridad, que deberá suscribir el Responsable de Seguridad de la información del operador.

iv. La figura del **Responsable de Seguridad** de la información puede ser ostentada por una persona u órgano colegiado, deberá tener interlocución directa con la alta dirección del operador, actuará como punto de contacto y coordinación técnica con la autoridad competente y CSIRT de referencia y tendrá, como principales funciones:

a. Elaborar, proponer para aprobación por la organización y supervisar las **políticas de seguridad.**

b. Elaborar el documento de **Declaración de Aplicabilidad** de medidas de seguridad.

c. Recibir, interpretar y supervisar la aplicación de las instrucciones y **guías emanadas de la autoridad competente.**

GESTIÓN DE **INCIDENTES** DE SEGURIDAD

i. Se contempla la obligación de los operadores de servicios esenciales de **notificar los incidentes** que puedan (i) tener efectos perturbadores significativos en los servicios; o (ii) , así como aquellos que puedan afectar a las redes y sistemas de información que sean empleados para la prestación de servicios esenciales. Los operadores de servicios esenciales deberán notificar a la autoridad competente a través del CSIRT de referencia.

ii. Los incidentes están asociados a **distintos niveles de peligrosidad e impacto**. Es obligatorio notificar todos los que se categoricen con un **nivel crítico, muy alto o alto**. El procedimiento de notificación de incidentes se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

SUPERVISIÓN

i. Las **autoridades competentes supervisarán el cumplimiento de las obligaciones** de seguridad y notificación de incidentes de los operadores de servicios esenciales y los proveedores de servicios digitales, incluyendo la obligación de estos de colaborar con la autoridad competente.

ii. Se contempla la posibilidad de que las autoridades competentes lleven a cabo **labores de inspección.**