Real Decreto 43/2021, de 26 de enero, de seguridad de las redes y sistemas de información

Real Decreto 43/2021, de 26 de enero, que desarrolla el Real Decreto- ley 12/2018, que regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales.

Febrero 2021

Ponte en contacto con PwC Tax & Legal:

Assumpta Zorraquino Rico
Socia responsable de Regulación Digital de PwC Tax & Legal
roberta.poza.cid@pwc.com

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información.

1. Objeto de desarrollo de la norma

En 2016, se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems).

La transposición de la citada Directiva NIS al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018 (RDL), que regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información.

El nuevo Real Decreto 43/2021 desarrolla el RDL en lo relativo al establecimiento de un marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y a la gestión de los incidentes de seguridad.

2. Servicios a los que es de aplicación el RD

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
b) Los servicios digitales que sean **mercados en línea, motores de búsqueda en línea y servicios de computación en nube.**

3. Operadores a los que es de aplicación el RD

a) Los operadores de servicios esenciales establecidos en España.
b) Los proveedores de servicios digitales que tenga su sede social en España y que constituya su establecimiento principal en la UE, así como los que no estando, designen en España a su representante en la Unión.

Publicación del Real Decreto 43/2021, de 26 de enero, que desarrolla el Real Decreto- ley 12/2018, que regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información"

Este Real Decreto **no se aplicará a:**

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.
b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

4. Marco estratégico e institucional

En lo relativo al marco estratégico e institucional, el RD en su art. 3 relaciona cuáles son las autoridades competentes por sectores de actividad.

Seguidamente, regula la cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia, y de estos con las autoridades competentes, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

5. Requisitos de seguridad

El Capítulo III establece los requisitos de seguridad (medidas técnicas y organizativas) que deberán adoptar los operadores de servicios esenciales y los proveedores de servicios digitales para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y sistemas propios, como de proveedores externos.

Para los operadores esenciales, la relación de medidas adoptadas se formalizará en un acuerdo denominado **Acuerdo de Aplicabilidad** de medidas de seguridad que deberá remitirse a la autoridad competente en el plazo de seis meses desde la designación de operador esencial y revisarse, al menos, cada 3 años.

En la elaboración de las políticas de seguridad de redes y sistemas de información se tendrán en cuenta los **riesgos que se deriven del tratamiento de los datos personales,** de acuerdo con el art 24 RGPD.

6. Gestión de incidentes de seguridad

Los operadores de servicios esenciales deberán notificar **los incidentes que puedan tener efectos perturbadores significativos** en dichos servicios, clasificándolos en función de su criticidad con un nivel de impacto crítico, muy alto o alto.

También deberán ser objeto de notificación los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido un efecto adverso real sobre aquellos.

La notificación de un ciberincidente atendiendo los requisitos de este Real Decreto no excluye ni sustituye la notificación de los mismos hechos a otras organismos, como por ej. a la AEPD.

7. Anexo

El Real Decreto incorpora en su Anexo una Instrucción de notificación y gestión de ciberincidentes, relativa a:

1) Obligatoriedad de notificación.
2) Tabla con la Clasificación / Taxonomia de los ciberincidentes, Descripción y ejemplos prácticos, alineada con la aprobada por la Agencia de la Unión Europea de Ciberserguridad (ENISA).
3) Nivel de peligrosidad del ciberincidente (Crítico, Muy alto, Alto, Medio, Bajo). El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información, así como para los servicios prestados o la continuidad de negocio en caso de haberla.
4) Nivel de impacto del incidente (Crítico, Muy alto, Alto, Medio, Bajo, Sin Impacto).
5) Información a notificar a la autoridad competente. (Qué notificar y su descripción).
6) Ventana temporal de reporte.
7) Definiciones y conceptos.

8. Entrada en vigor

El Real Decreto entró en vigor el día siguiente de su publicación en el BOE del pasado jueves 28 de enero de 2021.