Pérez-Llorca

Nota Jurídica

Febrero 2021

ÚLTIMAS NOVEDADES EN MATERIA DE SEGURIDAD EN LAS REDES Y EN SISTEMAS DE INFORMACIÓN

Analizamos en esta nota jurídica el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (el **"RD 43/2021"**), que regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales. El RD 43/2021 ha sido publicado en el Boletín Oficial del Estado el pasado 28 de enero, y ha entrado en vigor el 29 de enero.

Hasta ahora, esta materia venía regulándose en (i) 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 (la **"Directiva NIS"** por sus siglas en inglés); y (ii) el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que se encargó de la trasposición de la citada Directiva NIS al ordenamiento jurídico español (el **"RDL 12/2018"**).

Además, al RD 43/2021 y al RDL 12/2018 se les aplica complementariamente la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (la **"Ley 8/2011"**).

1. La finalidad de desarrollo normativo del RD 43/2021

El RDL 12/2018 estableció un marco general para la seguridad en las redes y en los sistemas de información utilizados para los prestadores de servicios esenciales[1] y los servicios digitales que sean mercados en línea[2], motores de búsqueda[3] en línea y servicios de computación en

[1] Son servicios esenciales según el artículo 2 de la Ley 8/2011 aquellos necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

[2] Es un mercado en línea según el artículo 2 de la Ley 8/2011 aquel servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en un sitio web específico del servicio de mercado en línea, o en un sitio web de un empresario que utilice servicios informáticos proporcionados al efecto por el proveedor del servicio de mercado en línea.

[3] Es un motor de búsqueda en línea según el artículo 2 de la Ley 8/2011 aquel servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y

nube[4], instaurando nuevos instrumentos tendentes a incrementar la protección frente a amenazas que pueda afectar a las redes y sistemas de información, creando un marco estratégico e institucional de la seguridad de las redes y sistemas de información, y potenciando la cooperación entre las autoridades públicas. Además, estableció una serie de obligaciones en materia de seguridad para los operadores y reguló la notificación de incidentes, poniendo especial énfasis en aquellos que tenían un impacto transfronterizo.

El RD 43/2021 tiene por finalidad desarrollar el RDL 12/2018 en aquello que concierne a:

(i) el marco estratégico e institucional de seguridad de las redes y sistemas de información;

(ii) el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales; y

(iii) la gestión de incidentes de seguridad, desarrollando las obligaciones de notificación por parte de los operadores de servicios esenciales de (i) los incidentes que pudieran tener efectos perturbadores en dichos servicios; y (ii) los incidentes que puedan afectar a las redes y sistemas de información que sean utilizados para la prestación de servicios esenciales.

El RD 43/2021 tiene el mismo ámbito de aplicación que el RDL 12/2018. De este modo, dichas normas se aplican a:

(i) la prestación de los servicios esenciales dependientes en las redes y sistemas de información de sectores estratégicos y Ministerios u Organismos del sistema competentes[5]; y

(ii) los servicios digitales que correspondan a mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

Desde un punto de vista territorial, se encuentran sujetos al RD 43/2021 tanto los operadores de servicios esenciales que estén establecidos en España, como aquellos proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, como aquellos que, sin estar establecidos en la Unión Europea, hayan escogido en España su representante en la Unión Europea para el cumplimiento de la Directiva NIS.

---

que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

[4] Es un servicio de computación en nube según el artículo 2 de la Ley 8/2011 aquel servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

[5] Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos se encuentran definidos en el anexo de la Ley 8/2011.

2. Principales novedades del RD 43/2021

El RD 43/2021 amplía (a las ya reguladas por el RDL 12/2018) las autoridades competentes para supervisar a los operadores de servicios esenciales que no sean consideradas operadores críticos, es decir, que no sean organismos responsables de las inversiones o del funcionamiento diario de una instalación, de una red, de un sistema, o de un equipo físico o de tecnología de la información designada como infraestructura crítica[6].

A modo de ejemplo, algunas de las autoridades competentes serán las siguientes, en función del sector al que pertenezcan:

(i) Transporte: el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.

(ii) Tecnologías de la información y las telecomunicaciones: el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

(iii) Industria química: el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

(iv) Salud: el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

Además, el RD 43/2021 refuerza en su artículo 4 la cooperación y coordinación entre los distintos equipos de respuesta a incidentes de seguridad informática (**"CSIRT"** –*Computer Security Incident Response Team*–), y estructura la cooperación entre los CSIRT y las autoridades competentes, a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

El RD43/2021 también dedica su artículo 5 a recoger la función del punto de contacto único, que garantiza la cooperación transfronteriza de las autoridades competentes con (i) las autoridades competentes de otros Estados Miembros de la Unión Europea; (ii) el grupo de cooperación formado por representantes de los Estados Miembros, la Comisión Europea y la Empresa Nacional de Innovación; y (iii) la red de CSIRT.

[6] Según las definiciones del artículo 2 de la Ley 8/2011, se considera infraestructura crítica a aquella que tiene carácter estratégico y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su destrucción supondría un grave impacto en los servicios esenciales.

A. Requisitos de seguridad

En el RD 43/2021 se recoge la obligación de los operadores de servicios esenciales y los proveedores de servicios digitales de adoptar todas aquellas medidas técnicas y de organización que resulten adecuadas y proporcionadas para la gestión de los riesgos que afecten a la seguridad de las redes y sistemas de información que sean utilizados para prestar sus servicios.

Las políticas de seguridad en las redes y sistemas de información que aprueben 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. Además, las medidas que se adopten se deberán formalizar en la Declaración de Aplicabilidad de medidas de seguridad, que deberá suscribir el responsable de seguridad de la información del operador. La figura del responsable de seguridad de la información se ve reforzada gracias al RD 43/2021, pudiendo ser ostentada por una persona u órgano colegiado, si bien en este último caso se deberá designar a un representante persona física, cuyo nombramiento deberá comunicarse a la autoridad competente en el plazo de tres meses desde su designación.

Dicho responsable de seguridad 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 (artículo 7 del RD 43/2021) y tendrá, como principales funciones, las siguientes:

(i) Elaborar, proponer para aprobación por la organización y supervisar las **políticas de seguridad**, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios, de conformidad con lo dispuesto en el artículo 6.

(ii) Elaborar el documento de **Declaración de Aplicabilidad** de medidas de seguridad considerado en el artículo 6.3 párrafo segundo del RD 43/2021.

(iii) Recibir, interpretar y supervisar la aplicación de las instrucciones y **guías emanadas de la autoridad competente**, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

B. Gestión de incidentes de seguridad

El artículo 8 del RD 43/2021 también contempla el encargo a los operadores de servicios esenciales y a los proveedores de servicios digitales de gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información que sean utilizados para la prestación del servicio.

Además, en su artículo 9 se establecen las obligaciones en materia de notificación de incidentes que (i) puedan tener efectos perturbadores significativos en los servicios esenciales por parte de los operadores de servicios esenciales; o que (ii) puedan afectar a las redes y sistemas de información que sean empleados para la prestación de servicios esenciales. Los operadores de servicios esenciales deberán notificarlos a la autoridad competente, a través del CSIRT de referencia.

De este modo, los incidentes se asociarán a distintos niveles de peligrosidad e impacto, estando obligados a notificar todos aquellos 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.

C. Supervisión

En materia de supervisión y control, la norma establece que serán las autoridades competentes las que supervisarán el cumplimiento de las obligaciones de seguridad y notificación de incidentes a las que estén sujetos los operadores de servicios esenciales y los proveedores de servicios digitales, incluyendo la obligación de estos de colaborar con la autoridad competente en dicha supervisión. Asimismo, el RD 43/2021 también contempla la posibilidad de que las autoridades competentes lleven a cabo labores de inspección.

Para más información,
pueden ponerse en contacto con:

Andy Ramos Gil de la Haza
Counsel de Propiedad Intelectual, Industrial y Tecnología
aramos@perezllorca.com
T: + 34 91 423 20 72