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

Legal Alert

Enero de 2021

kpmgabogados.es
kpmg.es

Principales novedades del Real Decreto 43/2021 sobre seguridad de las redes y sistemas de información

El Consejo de Ministros aprobó, el pasado 26 de enero de 2021, el Real Decreto 43/2021 que desarrolla el Real Decreto-ley 12/2018 (en adelante, "Ley NIS"), de 7 de septiembre, de seguridad de las redes y sistemas de información, habiéndose publicado en el Boletín Oficial del Estado el 28 de enero.

Este real decreto tiene por objeto desarrollar la Ley NIS, en lo relativo (i) al marco estratégico e institucional de seguridad de las redes y sistemas de información, (ii) la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y (iii) a la gestión de los incidentes de seguridad.

Consta de cinco capítulos, quince artículos, seis disposiciones adicionales, una disposición transitoria, tres disposiciones finales y un anexo relativo a la Instrucción nacional de notificación y gestión de ciberincidentes.

A continuación, se desarrollan las principales novedades introducidas por el Real Decreto 43/2021 y que tienen impacto sobre el sector financiero.

Quedan sometidos a este real decreto:

- Los operadores de servicios esenciales establecidos en España. Asimismo, este real decreto será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

- Los proveedores de servicios digitales que tengan sede social en España cuando constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148

El real decreto, en su artículo 3, pormenoriza **la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información** prevista en el artículo 9.1.a) 2.º del Real Decreto-ley 12/2018, de 7 de septiembre.

En este sentido, el precitado artículo establece que las autoridades competentes en el sector financiero son:

1.º El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones.
2.º El Banco de España, para las entidades de crédito.
3.º La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

Este real decreto también presenta importantes novedades **en relación con la figura del punto de contacto único** (art.5) derivada de la Directiva 2016/1148, en concreto, se desarrollan sus funciones de enlace.

Por otra parte, el artículo 6 de este real decreto desarrolla las previsiones derivadas de la Ley NIS relativas a las **medidas necesarias para el cumplimiento de las obligaciones de seguridad por parte de los operadores de servicios esenciales**, que habrán de concretarse en una declaración de aplicabilidad de medidas de seguridad a suscribir por el responsable de seguridad de la información del operador, que deberá remitir a la autoridad competente en el plazo de seis meses desde la designación del operador, al que se dedica el artículo 7, en el que se incluye una relación de sus funciones. En cuanto a la designación del responsable la seguridad, deberá hacerse en todo caso, dentro de los tres meses siguientes a la designación de la entidad como operador de servicios esenciales.

artículo 7, en el que se incluye una relación de sus funciones. En cuanto a la designación del responsable la seguridad, deberá hacerse en todo caso, dentro de los tres meses siguientes a la designación de la entidad como operador de servicios esenciales.

Por lo que se refiere a la **notificación de incidentes**, desarrolla el real decreto, en sus artículos 8 y 9, las obligaciones de gestión y notificación por parte de los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de 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, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción nacional de notificación y gestión de ciberincidentes que se contiene en el anexo.

Asimismo, establece la obligación para estos operadores y proveedores de resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios.

Por su parte, el **procedimiento de notificación de incidentes** (arts. 10 y 11) se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, estableciéndose, para los operadores de servicios esenciales y los proveedores de información, la obligación de notificar el incidente tan pronto como dispongan de información para determinar que se dan las circunstancias de notificación. En adición a lo anterior, se articula también el sistema a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad (art. 12), su comunicación en caso de tener carácter presuntamente delictivo (art. 13) y la disponibilidad de la información (consulta con otras autoridades – art. 14 –).

En materia de supervisión de requisitos de seguridad, el real decreto desarrolla en su artículo 15 la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir, asimismo, la colaboración de los CSIRT de referencia.

Finalmente, la disposición adicional sexta especifica la información sobre incidentes que tengan lugar en el sistema financiero, estableciendo la obligación para los CSIRT de informar al titular de la Secretaría de Estado de Economía y Apoyo a la Empresa, a través de la Secretaría General del Tesoro y Financiación Internacional, de los incidentes que puedan tener efectos perturbadores significativos en servicios esenciales del sistema financiero.

A estos efectos, se entenderá que tienen efectos perturbadores significativos cuando su umbral o nivel de impacto sea crítico, muy alto o alto, según lo señalado en el anexo.

Obligaciones para los sujetos obligados:

1. Cooperación entre los CSIRT y las Autoridades Competentes a través de la Plataforma Nacional de Notificación y Seguimiento de Ciber incidentes.

2. **Designar, en el plazo de tres meses,** a una persona, unidad u órgano colegiado responsable de la seguridad de la información, que hará de punto de contacto y de coordinación y **deberá desarrollar**, bajo su responsabilidad, **las siguientes funciones**:

(i) Elaborar y proponer para aprobación por la organización las políticas de seguridad.
(ii) Supervisar y desarrollar la aplicación de las políticas de seguridad, supervisar su efectividad y llevar a cabo controles.
(iii) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.
(iv) Actuar como capacitador de buenas prácticas en seguridad.
(v) Remitir a la autoridad competente, a través del SIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios.
(vi) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente.
(vii) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

El responsable de la seguridad de la información, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

- **En referencia al régimen específico del Banco de España:**

En la disposición adicional tercera del real decreto se recoge el régimen jurídico aplicable al Banco de España, teniendo en cuenta su especial configuración jurídica como entidad de Derecho público con personalidad jurídica propia y plena capacidad pública y privada, que, en el desarrollo de su actividad y para el cumplimiento de sus fines, actúa con autonomía respecto a la Administración General del Estado, y como parte integrante del Sistema Europeo de Bancos Centrales (SEBC) y del Mecanismo Único de Supervisión (MUS).

Esta especial configuración jurídica supone que el marco de seguridad de las redes y sistemas de información solo le resulte de aplicación en la medida en que no interfiera con su naturaleza, funciones e independencia.

Entrada en vigor: 29 de enero de 2021.
Adjuntamos un enlace al Real Decreto: Ir.

Contactos

Alfonso Gonzalez-Espejo
Socio
KPMG Abogados, S.L.P.
Tel. +34 91 451 31 53
agonzalezespejo@kpmg.es

Manuel Aguilar
Senior Manager
KPMG Abogados, S.L.P.
Tel. +34 91 451 32 72
manuelaguilar@kpmg.es

Oficinas de KPMG en España

A Coruña

Calle de la Fama, 1
15001 A Coruña
T: 981 21 8241
Fax: 981 20 02 03

Alicante

Edificio Oficentro
Avda. Maisonnave, 19
03003 Alicante
T: 965 92 0722
Fax: 965 22 75 00

Barcelona

Torre Realia
Plaça de Europa, 41
08908 L´Hospitalet de Llobregat
Barcelona
T: 932 53 2900
Fax: 932 80 49 16

Bilbao

Torre Iberdrola
Plaza Euskadi, 5
48009 Bilbao
T: 944 79 7300
Fax: 944 15 29 67

Girona

Edifici Sèquia
Sèquia, 11
17001 Girona
T: 972 22 0120
Fax: 972 22 22 45

Las Palmas de Gran Canaria

Edificio San Marcos
Dr. Verneau, 1
35001 Las Palmas de Gran Canaria
T: 928 33 2304
Fax: 928 31 91 92

Madrid

Torre de Cristal
Paseo de la Castellana, 259 C
28046 Madrid
T: 91 456 3400
Fax: 91 456 59 39

Málaga

Larios, 3
29005 Málaga
T: 952 61 1460
Fax: 952 30 53 42

Oviedo

Ventura Rodríguez, 2
33004 Oviedo
T: 985 27 6928
Fax: 985 27 49 54

Palma de Mallorca

Edifici Ca´n de Segura
Avda. del Comte de Sallent, 2
07003 Palma de Mallorca
T: 971 72 1601
Fax: 971 72 58 09

Pamplona

Edificio Iruña Park
Arcadio M. Larraona, 1
31008 Pamplona
T: 948 17 1408
Fax: 948 17 35 31

San Sebastián

Avenida de la Libertad, 17-19
20004 San Sebastián
T: 943 42 2250
Fax: 943 42 42 62

Sevilla

Avda. de la Palmera, 28
41012 Sevilla
T: 954 93 4646
Fax: 954 64 70 78

Valencia

Edificio Condes de Buñol
Isabel la Católica, 8
46004 Valencia
T: 963 53 4092
Fax: 963 51 27 29

Vigo

Arenal, 18
36201 Vigo
T: 986 22 8505
Fax: 986 43 85 65

Zaragoza

Centro Empresarial de Aragón
Avda. Gómez Laguna, 25
50009 Zaragoza
T: 976 45 8133
Fax: 976 75 48 96