CUATRECASAS

Real Decreto 43/2021: El desarrollo del marco legal de ciberseguridad en España

Legal Flash de Propiedad Intelectual y Derecho Digital

2 de marzo de 2021

La ciberseguridad se ha convertido en uno de los ámbitos de cumplimiento normativo que mayor importancia ha adquirido para las empresas, atendiendo tanto a la creciente frecuencia de este tipo de incidentes, así como a los desarrollos normativos que se van sucediendo a este respecto.

El *Real Decreto 43/2021*, en vigor desde el pasado 27 de enero, tiene por objeto desarrollar el *Real Decreto-ley 12/2018*, de seguridad de las redes y sistemas de información, en vigor desde el 8 de septiembre de 2018. Se trata de la principal norma en materia de Ciberseguridad, que alinea el derecho español con el marco armonizado europeo conforme a la *Directiva 2016/1148* (más conocida como Directiva NIS).

En este legal flash reseñamos los puntos clave del *Real Decreto 43/2021*, entre los que cabe destacar que esta norma:

- Establece las principales obligaciones y procedimientos para asegurar una óptima gestión de riesgos de seguridad en redes y sistemas de información en sectores críticos.
- Señala las funciones del responsable de seguridad de la información para los operadores obligados.
- Determina las autoridades competentes para los operadores de servicios esenciales privados que no sean operadores críticos.

Real Decreto 43/2021: El desarrollo del marco legal de Ciberseguridad en España

El *Real Decreto 43/2021* tiene por objeto complementar algunos aspectos *del Real Decreto-ley 12/2018*, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al 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 la gestión de incidentes de seguridad. Supone un avance en la adecuación de la normativa española a la *Directiva 2016/1148* (Directiva NIS).

¿A quién se aplica?

El *Real Decreto 43/2021* se aplicará a dos categorías distintas de operadores:

- **Prestadores de servicios esenciales** establecidos en España, dependientes de las redes y sistemas de información comprendidos en sectores estratégicos.

    - De acuerdo con la *Ley 8/2011,de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*, se incluyen en esta categoría los siguientes sectores estratégicos: administraciones públicas; espacio; industria nuclear; industria química; instalaciones de investigación; agua; energía; salud; tecnologías de la información y comunicaciones; transporte; alimentación; así como el sistema financiero y tributario.

    - Son factores para determinar qué es un «servicio esencial» en virtud de la *Directiva 2016/1148* (Directiva NIS): (i) si un incidente potencial tendría un efecto perturbador significativo y, (ii) si la prestación del servicio esencial depende de redes y sistemas de información.

    - El Real Decreto será también de aplicación a los prestadores de servicios esenciales residentes o domiciliados en otro Estado que ofrezcan sus servicios a través de un establecimiento permanente situado en España.

- **Operadores de servicios digitales** que incluyan mercados en línea, motores de búsqueda y servicios de computación en nube.

Obligaciones de los operadores y prestadores

Este nuevo Real Decreto concreta algunas de las principales obligaciones y procedimientos a seguir por los operadores de servicios esenciales y los prestadores de servicios digitales, a fin de asegurar una óptima gestión de riesgos de seguridad en redes y sistemas de información en sectores estratégicos, así como para asegurar una adecuada coordinación entre los distintos actores implicados en este tipo de situaciones de riesgo. Destacan, entre otros puntos, los siguientes:

- Definición de medidas técnicas y organizativas para la adecuada gestión de los riesgos de ciberseguridad, tanto si se trata de redes y sistemas propios, como de proveedores externos.

- Gestión y resolución de incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. Obligación que alcanza tanto a incidentes detectados por el propio operador o prestador como a los señalados por el CSIRT de referencia o la autoridad competente.

Asimismo, el Real Decreto establece obligaciones adicionales para los prestadores de servicios esenciales, tales como:

- La aprobación de unas políticas de seguridad de redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

    - La propia norma establece que dichas políticas deberán tratar los aspectos clave en seguridad tales como el análisis y gestión de riesgos (incluyendo los de terceros o proveedores), el listado de medidas de seguridad, organizativas, tecnológicas y físicas, los planes de recuperación y aseguramiento de la continuidad de las operaciones, o la interconexión de sistemas.

    - Dichas medidas deberán formalizarse en un documento denominado **Declaración de Aplicabilidad de medidas de seguridad**, del que deberá remitirse una copia a la autoridad competente en el plazo de 6 meses desde la designación de la entidad como operador de servicios esenciales y, deberá revisarse, al menos, cada 3 años.

    - Las citadas medidas tomarán como referencia las recogidas en el anexo II del *Real Decreto 3/2010, de 8 de enero*, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, sin perjuicio de poder tener en cuenta otros estándares reconocidos internacionalmente.

- Designación de un responsable de seguridad.

  - Podrá ser una persona, unidad u órgano colegiado que dentro de la compañía en cuestión actuará como responsable de la seguridad de la información, además de punto de contacto y coordinación con la autoridad competente.

  - El responsable de seguridad deberá **contar con conocimientos especializados y experiencia en materia de ciberseguridad, tanto desde el punto de vista técnico como jurídico.**

  - Los operadores sujetos a este nuevo Real Decreto deberán **notificar a dicha autoridad la identidad de su responsable de seguridad dentro de los 3 meses** siguientes a su designación como operador de servicios esenciales.

  - Asimismo, deberán notificar los ceses y nuevos nombramientos de su responsable de seguridad dentro del mes siguiente al correspondiente cese o nombramiento.

  - Esta figura pretende ser la referencia, dentro del operador en cuestión, en el ámbito de la seguridad de redes y sistemas de información. En este sentido, se establece que, entre otras funciones, el responsable de seguridad deberá:

    (i) elaborar y proponer para aprobación las políticas de seguridad, así como la correspondiente Declaración de Aplicabilidad;

    (ii) supervisar y desarrollar la adopción e implementación de las medidas técnicas y organizativas definidas en las citadas políticas de seguridad;

    (iii) remitir a la autoridad competente las notificaciones de incidentes, sin dilación indebida; o

    (iv) interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente.

  - Para desarrollar estas funciones el responsable de seguridad se podrá apoyar en servicios prestados por terceros.

- Notificación de incidentes de seguridad.

  - El Real Decreto establece una obligación general de notificación a la autoridad competente aquellos incidentes que puedan tener "efectos perturbadores significativos" en los servicios que preste el operador en cuestión o que, atendiendo a su nivel de peligrosidad, puedan afectar a las redes y sistemas de

información empleados para la prestación de los servicios esenciales, incluso si no han tenido un efecto relevante en las actividades del operador.

- Dicho deber de notificación se entenderá sin perjuicio de otras obligaciones legales similares tales como, por ejemplo, la prevista en el artículo 33 del *Reglamento (UE) 2016/679, General de Protección de Datos*, en el sentido de notificar a la autoridad relevante una brecha de seguridad que haya comprometido información de carácter personal.

- Los prestadores de servicios esenciales realizarán dichas notificaciones a través del responsable de seguridad de la información designado.

- El Real Decreto prevé la creación de una Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, gestionada por el *Centro Criptográfico Nacional* en colaboración con el *Instituto Nacional de Ciberseguridad* y el *Mando Conjunto de Ciberdefensa*.

- En este contexto, ante un incidente de seguridad de redes o sistemas de información -tales como brechas de información, sistemas infectados con *malware*, compromiso de sistemas o aplicaciones, los operadores de servicios esenciales deberán notificar obligatoriamente a la autoridad competente a fin de comunicar la concurrencia de dichos Ciberincidentes.

- Las notificaciones incluirán, en cuanto esté disponible, la información que permita determinar cualquier efecto transfronterizo del incidente.

- En el caso de que no se regule de modo diferente en los actos de ejecución previstos en el artículo 16.9 de 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*, lo establecido en el Real Decreto respecto al procedimiento de notificación de incidentes será de aplicación a los proveedores de servicios digitales.

- El cumplimiento de las obligaciones anteriormente mencionadas podrá ser acreditado mediante la certificación en un esquema de seguridad que, previa consulta al CSIRT de referencia, sea reconocido por la autoridad competente.

¿A quién hay que notificar? Autoridades competentes

Las autoridades competentes supervisarán en su ámbito de actuación el cumplimiento de las obligaciones de seguridad y de notificación de incidentes que sean de aplicación a los operadores de servicios esenciales y a los proveedores de servicios digitales.

- Sin perjuicio de la clasificación que se describe a continuación, el Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para mejorar la coordinación las actuaciones de las autoridades competentes y optimizar los recursos dedicados a la gestión de los incidentes que afecten a la seguridad de las redes y sistemas de información.

- Son autoridades competentes para los operadores de **servicios esenciales que no sean operadores críticos** de acuerdo con la *Ley 8/2011*, y que no estén incluidos en el ámbito de aplicación de la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*, las siguientes:

Sector	Autoridades competentes
Transporte	Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.
Energía	Ministerio para la Transición Ecológica y el Reto demográfico, a través de la Secretaría de Estado de Energía.
Tecnologías de la información y las telecomunicaciones	Ministerio de Economía y Empresa, Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Sistema financiero y tributario	i. 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. ii. Banco de España, para las entidades de crédito. iii. Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

Espacio	Ministerio de Defensa, a través de la Secretaría de Estado de Defensa.
Industria química	Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.
Instalaciones de investigación	Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación.
Salud	Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.
Agua	Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.
Alimentación	i. Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación. ii. Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad. iii. Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio. iv. El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN).
Industria nuclear	i. Ministerio para la Transición Ecológica, a través de la Secretaría de Estado de Energía. ii. Consejo de Seguridad Nuclear.

- El Real Decreto se entenderá sin perjuicio de las competencias y funciones atribuidas al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, en lo relativo a tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito, y de acuerdo con la *Ley 13/1994, de 1 de junio, de Autonomía del Banco de España*.

- Son autoridades competentes para los operadores de **servicios esenciales designados como operadores críticos** conforme a la *Ley 8/2011*, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación, o **que sin ser**

operadores críticos estén incluidos en el ámbito de aplicación de la *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*, las siguientes:

Tipo de operador	Autoridad competente
Operador crítico	Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).
Operadores de servicios esenciales y proveedores de servicios digitales del sector público	Ministerio de Defensa, a través del Centro Criptológico Nacional.

Régimen sancionador

- Las autoridades competentes podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control. Entre ellas, controlar el cumplimiento de las normas e instrucciones técnicas, verificar el cumplimiento de las funciones del responsable de seguridad o realizar comprobaciones, inspecciones, pruebas o revisiones del cumplimiento de medidas de seguridad.

- Las sanciones aplicables a las infracciones de este Real Decreto serán las ya previstas en el *Real Decreto-ley 12/2018* categorizadas en una escala de gravedad por leves, graves y muy graves. La cuantía de las sanciones partirá desde una amonestación o multa para las muy leves (p. ej. no someterse a una auditoría de seguridad) hasta **1.000.000 euros** para las muy graves (p. ej. el incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio).

¿Y ahora, qué? Próximos pasos

- Si desea más información a la contenida en el documento respecto a las obligaciones y deberes que le son exigibles, puede dirigirse a su contacto habitual en Cuatrecasas.

- Desde Cuatrecasas, consideramos que la información y los distintos sistemas asociados son activos críticos que deben ser protegidos adecuadamente para asegurar el correcto

funcionamiento de la empresa, y que también incluyen a sus empleados, directivos, socios y administradores.

- De este modo, nuestro equipo de abogados especializado en cuestiones de ciberseguridad asesora con el objetivo de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, así como el cumplimiento de las diferentes normas vigentes en cada momento, incluidas las obligaciones derivadas del presente Real Decreto.

- Acompañamos a nuestros clientes en todo el ciclo de vida de la ciberseguridad en su vertiente jurídica, ayudándoles a diseñar e integrar las políticas, protocolos y procedimientos de ciberseguridad, incluyendo planificación frente a incidencias, formación y educación.

- Además, ofrecemos asesoramiento en materia de cumplimiento normativo, contratación y riesgos en la cadena de suministros, incluyendo evaluación de contratistas y normativas contractuales en materia cibernética, integrando aspectos de protección de datos y asuntos relativos a la seguridad informática en el contexto de *due diligence, joint ventures,* proyectos y subcontrataciones.

Contactos

Soraya Sáenz de Santamaría
Socia
soraya.saenzdesantamaria@cuatrecasas.com
915 247 199

Albert Agustinoy
Socio
albert.agustinoy@cuatrecasas.com
933 127 184

Omar Puertas
Socio
omar.puertas@cuatrecasas.com
932 905 484