Spread the love

El Boletín Oficial del Estado (BOE) publica 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 texto completa la incorporación del la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea, conocida como Directiva NIS (*Security of Network and Insformation Systems*)

Cabanas, 2016

Recuérdese que a finales del año 2018, la transposición de la citada Directiva NIS se llevó al ordenamiento jurídico español mediante el **Real Decreto-ley 12/2018**, de 7 de septiembre, de seguridad de las redes y sistemas de información. 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, y fija un marco institucional de cooperación que facilita la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la **Unión Europea**

En esta ocasión, el **Real Decreto 43/2021**, de 26 de enero, que publica el **BOE**, establece como ámbito de aplicación la **prestación de 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.** Pero **también la prestación de servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.**

En el artículo 2.2. RD contempla que está sometidos a este nuevo Real Decreto «*los operadores de servicios esenciales establecidos en España. En coherencia con lo ya expresado respecto de NIS, s****e entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades****. Así mismo, 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****.» También «****los proveedores de servicios digitales que tengan su sede social en España y que 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 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.*»

> Por contra, este Real Decreto no se aplica, según establece el artículo 2.3, 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****.». Tampoco a «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.***«

Sanabria

Cabe destacar que en dicho Real Decreto:

1. se establecen **los requisitos de seguridad**, así como **las medidas para el cumplimiento de las obligaciones de seguridad**,
2. contempla en el plano normativo al responsable de la seguridad de la información o RSI, el CISO, que veíamos desarrollado en normas o estándares privados como ISO.
3. se ocupa de la gestión de incidentes de seguridad
4. detalla las **obligaciones de notificación** de los incidentes de los operadores de servicios esenciales: «*Los operadores de servicios esenciales notificarán a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto, según el detalle que se especifica en el apartado 4 de la Instrucción nacional de notificación y gestión de ciberincidentes, que se contiene en el anexo de este real decreto. Asimismo, notificarán los sucesos o incidencias que, por su nivel de peligrosidad, puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido todavía un efecto adverso real sobre aquellos. A estos efectos, se considerarán los incidentes con un nivel de peligrosidad crítico, muy alto o alto, según el detalle que se especifica en el apartado 3 de la citada Instrucción*«, reza el artículo 9.1 de este RD.

El RSI o CISO (para OSE)

En relación con el Responsable de Seguridad de la Información, el artículo 7 del RD 43/2021 insta a que esta figura mantenga «una comunicación real y efectiva con la alta dirección». Además, señala que su posición debe «facilitar el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad». Esta figura, ya sea una persona, unidad u órgano colegiado, deberá contar con medios personales y materiales para desarrollar su función. Ejercerá de punto de contacto y coordinación técnica con la autoridad competente y el CSIRT de referencia. El art 7 es de aplicación únicamente a los OSE

- Recuérdese que la Directiva NIS realiza una armonización de mínimos en relación con los OSE, pero de máximos en relación con lo PSD y que respecto de estos últimos existe un Reglamento (UE) de ejecución:
    - Reglamento de Ejecución (UE) 2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los

proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo

Entre las funciones del RSI/CISO está el elaborar las políticas de seguridad y proponerlas para su aprobación por la organización. Estas políticas han de incluir las **medidas técnicas y organizativas** 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

Se reproduce a continuación el art 7 del RD 43/2021:

Artículo 7. Responsable de la seguridad de la información.

1. Los operadores de servicios esenciales designarán una **persona, unidad u órgano colegiado, responsable de la seguridad de la información** que ejercerá las funciones de punto de *contacto y coordinación técnica con la autoridad competente y CSIRT de referencia* que le corresponda de conformidad con lo previsto en el apartado tercero*. En el supuesto de que el responsable de seguridad de la información sea una unidad u órgano colegiado, se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad.* El plazo para llevar a cabo dicha designación será de tres meses desde su designación como operador de servicios esenciales.
2. Los operadores de servicios esenciales comunicarán a la autoridad competente respectiva la designación del responsable de la seguridad de la información dentro del plazo establecido en el apartado anterior, así como los nombramientos y ceses que afecten a la designación del responsable de la seguridad de la información en el plazo de un mes desde que aquellos se produzcan.
3. El responsable de la seguridad de la información actuará como *punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información, y como punto de contacto especializado para la coordinación de la gestión de los incidentes con el CSIRT de referencia.* Se desarrollarán **bajo su responsabilidad, entre otras, las siguientes funciones:**

   a) **Elaborar y proponer para aprobación** por la organización, de conformidad con lo establecido en el artículo 6.2 de este real decreto, l**as 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.

b) **Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles** periódicos de seguridad.

c) **Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad** considerado en el artículo 6.3 párrafo segundo de este real decreto.

d) Actuar como **capacitador de buenas prácticas** en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

e) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las **notificaciones de incidentes** que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

f) **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.**

g) **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.

4. Los operadores de servicios esenciales garantizarán que el responsable de la seguridad de la información cumpla con los siguientes requisitos:

a) Contar co**n personal con conocimientos especializados** y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de las funciones indicadas en el apartado anterior.

b) Contar con los **recursos n**ecesarios para el desarrollo de dichas funciones.

c) Ostentar una **posición en la organización que facilite el desarrollo de sus funciones,** participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.

d) Mantener la debida **independencia respecto de los responsables de las redes y los sistemas de información.**

5. Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, las funciones y responsabilidades encomendadas al responsable de la seguridad de la información **podrán compatibilizarse con las señaladas para el Responsable de Seguridad del Esquema Nacional de Seguridad**, a lo que dedicamos la siguiente entrada de este blog