Seguridad de las redes y sistemas de información

El pasado 26 de enero se publicó el Real Decreto 43/2021 de seguridad de las redes y sistemas de información que desarrolla el Real Decreto-ley 12/2018[1], 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 a la gestión de incidentes de seguridad.

Entre los aspectos que regula la norma, destacan los siguientes:

Ámbito de aplicación

Esta norma es de aplicación a la prestación de servicios esenciales dependientes de las redes y sistemas de información de sectores estratégicos[2] y a la prestación de los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube. Además, están sometidos a este Real Decreto, los operadores de servicios esenciales establecidos en España y a los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea.

Por otra parte, la norma contempla aquellos supuestos que quedan fuera de su ámbito de aplicación: (i) operadores de redes y servicios de comunicaciones electrónicas y prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011[3] y (ii) proveedores de servicios digitales que se constituyan como microempresas o pequeñas empresas.

Responsable de la seguridad de la información

Los operadores de servicios esenciales, en el plazo de tres meses desde su designación como tal, deberán nombrar una persona 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 los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia.

Entre sus funciones, destacan: elaborar las políticas de seguridad; supervisar y desarrollar la aplicación y efectividad de las políticas de seguridad, realizando controles periódicos de seguridad; elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad; comunicar las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicio o suministrar información a la autoridad competente o al CSIRT de referencia, entre otras.

Medidas para el cumplimiento de las obligaciones de seguridad

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios.

En el caso de los operadores de servicios esenciales, deberán además, aprobar políticas de seguridad, atendiendo a los principios de seguridad integral, gestión de riesgos, o segregación de tareas. Estas

políticas deberán prever un análisis y gestión de riesgos, un catálogo de medidas de seguridad, organizativas, tecnológicas y físicas; la adquisición de productos de seguridad o la detección y gestión de incidentes, entre otros.

La relación de medidas adoptadas se formalizará en el documento “Declaración de Aplicabilidad de medidas de seguridad”, deberá remitirse a la autoridad competente en el plazo de seis meses desde la designación del operador como operador de servicios esenciales y deberá revisarse, al menos, cada tres años.

Incidentes de seguridad

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. Además, deberán notificar a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, 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[4].

Otras cuestiones

El Real Decreto designa también, las autoridades competentes en materia de seguridad de las redes y sistemas de información, desarrolla los supuestos de cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia, y de estos con las autoridades competentes; y articula el procedimiento de notificación de incidentes a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. La norma recoge además, 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.

[1] Real Decreto de 7 de septiembre, de seguridad de las redes y sistemas de información

[2] Sectores estratégicos comprendidos 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. Entre ellos: sanidad, transportes, sector financiero y tributario, alimentación, energía o agua

[3] Ley 8/2011, de 28 de abril , por la que se establecen medidas para la protección de las infraestructuras críticas

[4]Efectos perturbadores y/o incidencias con nivel de peligrosidad: incidentes con un nivel de impacto crítico y/o peligrosidad, muy alto o alto, según el detalle que se especifica en la Instrucción nacional de notificación y gestión de ciberincidentes inluida en el anexo de la norma