



Artículo

ASPECTOS DESTACADOS DEL RD LEY 12/2018 DE 7 DE SEPTIEMBRE DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

Eduardo Tapia

etappad369@g.educaand.es

RESUMEN

La evolución de las TICs, especialmente con el desarrollo de Internet, implica que las redes y sistemas de información desarrollen un papel crítico en nuestra sociedad, siendo imprescindible asegurar su fiabilidad y seguridad de forma que puedan realizar tareas esenciales para el desarrollo normal de las actividades económicas y sociales.

Debido a esta circunstancia, los ciberincidentes que, al afectar a las redes y sistemas de información, perturban estas actividades, representan un grave desafío a nuestra sociedad, pues tanto si son accidentales como si provienen de actos terroristas pueden generar pérdidas económicas, socavar la confianza de la población y, en definitiva, causar graves perjuicios a la economía y a la sociedad, con la posibilidad de afectar a la propia ciberseguridad nacional en la peor de las hipótesis.-

PALABRAS CLAVE : redes, seguridad, ciberseguridad, normativa, legislación.-

INTRODUCCIÓN

El Real Decreto-ley 12/2018, de 7 de Septiembre, de Seguridad de las Redes y Sistemas de Información es una ley española cuyo objetivo es establecer las medidas necesarias para garantizar la seguridad de las redes y sistemas de información, especialmente en los sectores estratégicos y los servicios esenciales. Estos son los aspectos más destacados de la normativa:

1º.- **Ámbito de aplicación:** entre otras áreas, la normativa es aplicable a los operadores de servicios esenciales y a los proveedores de servicios digitales, quienes son identificados mediante una serie de criterios. Los operadores de servicios esenciales tienen un cierto número de obligaciones, como la notificación de

incidentes de seguridad y la realización de auditorías de seguridad, mientras que los proveedores de servicios digitales están obligados a notificar incidentes significativos y mantener registros de actividades relevantes, entre otras responsabilidades.

2º.- Autoridad competente: en esta ley, se asigna a la Agencia Española de Protección de Datos la responsabilidad de ser la autoridad competente en materia de seguridad de redes y sistemas de información en España.

3º.- Coordinación y colaboración: la normativa también incluye disposiciones sobre la promoción de la cooperación entre los distintos actores involucrados en los ámbitos cubiertos por la ley, a nivel nacional e internacional, para mejorar la ciberseguridad.

4º.- Sanciones: las sanciones dependerán de la gravedad de la infracción, y se impondrán multas más altas para castigar infracciones más serias.

En resumen, el Real Decreto-ley 12/2018 se centra en la protección cibernética de quienes son responsables de los sectores clave, estableciendo regulaciones específicas para los operadores de servicios esenciales y los proveedores de servicios digitales y definiendo las leyes para la prevención y el manejo de incidentes de seguridad en las redes y sistemas de información.

¿CUÁLES SON LOS ASPECTOS MÁS DESTACADOS DE ESTA LEY?

- **Ámbito de aplicación.** Una definición clara de las partes a las que se les aplican las disposiciones legales, haciendo hincapié y centrándose en los operadores de servicios esenciales y los proveedores de servicios digitales .
- **Identificación de los operadores de servicios esenciales.** Determina los criterios para la identificación de cuales deben estar sujetos a esta legislación, tales como energía, transporte, servicios financieros, entre otros.
- **Medidas de seguridad para operadores de servicios esenciales y proveedores de servicios digitales.** Obligación de los operadores de servicios esenciales de establecer medidas de seguridad que les sean proporcionales, para la protección de redes y sistemas de información.
- **Notificación de incidentes.** Obligación de los operadores de servicios esenciales y los proveedores de servicios digitales a notificar a las autoridades competentes los incidentes de seguridad ocurridos en sus sistemas.
- **Auditorías.** Realización de auditorías de seguridad a fin de verificar la adecuación y efectividad de las medidas implantadas por el operador de servicios esenciales.
- **Colaboración y coordinación.** La cooperación y coordinación entre los agentes, a nivel nacional e internacional, para mejorar la detección, gestión y respuesta frente a incidentes de seguridad.
- **Papel de la Agencia Española de Protección de Datos (AEPD).** La AEPD será la autoridad de control en la materia, y desarrollará funciones de asesoramiento y control.
- **Sanciones.** Régimen de sanciones en caso de incumplimiento de las obligaciones con multas según la infracción.

Como resultado, en general, el Real Decreto-ley 12/2018 tiene por objeto fortalecer la ciberseguridad de los sectores críticos y fomentar la prevención, la detección y la respuesta a incidentes de seguridad en las redes y sistemas de información de España.

CONCLUSIONES

Sigue el marco legislativo relacionando leyes españolas e internacionales sobre ciberseguridad y protección de datos. Aquí hay algunas otras leyes y regulaciones en las que se basa:

Reglamento General de Protección de Datos , que es una regulación de la Unión Europea estableciendo reglas de protección de datos personales.

Por otro lado, el Real Decreto-ley 12/2018 complementa el Reglamento General de Protección de Datos, ya que se enfoca en la seguridad de las redes y los sistemas de información, proporcionando pautas adicionales y medidas específicas para garantizar la integridad y confidencialidad de la información.

La Ley de Protección de Datos Personales y Garantía de los Derechos Digitales es una disposición local que aborda las regulaciones específicas de la protección de datos personales en España. Esta ley se integra con el Real Decreto-ley 12/2018 al considerar la seguridad de las redes y los sistemas de información en el entorno digital.

La Ley General de Telecomunicaciones en España también es importante para esta discusión, ya que regula el sector de las telecomunicaciones. En esta situación, la conexión entre el Real Decreto-ley 12/2018 radica en la consideración adecuada de las comunicaciones digitales.

La directiva sobre la seguridad de las redes y la información , que es una regulación de la Unión Europea que establece medidas para proporcionar un alto nivel de seguridad de las redes y los sistemas de información.

El Real Decreto-ley 12/2018 implementa las disposiciones de la Directiva NIS en el nivel nacional, lo que garantiza la seguridad de las redes y los sistemas de información en España.

La Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico también puede estar relacionada con el Real Decreto-ley 12/2018 en términos de seguridad digital y protección de servicios.

La interrelación de las regulaciones descritas implica la formación de un sistema integrado para abordar los problemas de ciberseguridad, proteger la privacidad y garantizar un entorno digital seguro en España.

El presente artículo se basa en los contenidos abordados en la asignatura de Normativa de Ciberseguridad del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información. Trabaja la síntesis comprensiva de la correspondiente Ley así como su relación con el resto de la Normativa Nacional y Europea.- No tratándose de un artículo muy extenso para la Ley considerada, es de gran valor su concreción de contenido y descripción de interrelaciones en el Marco Normativo Europeo.-

Espero que este artículo haya sido de su agrado y contribuido a mejorar su conocimiento en el aspecto estudiado.-

REFERENCIAS BIBLIOGRÁFICAS :

«BOE» núm. 218, de 08 de septiembre de 2018 -- Referencia: BOE-A-2018-12257

Eduardo Tapia : Profesor de Secundaria .-