ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa - Real Decreto - Ley 12/2018: Seguridad de las redes y sistemas de información.

Madrid, 27 de febrero de 2019

El 7 de septiembre entró en vigor **el Real Decreto Ley 12/2018**, (transposición de la Directiva NIS (UE) 2016/1148, de 6 de julio de 2016), la cual tiene por objetivo **garantizar y aumentar los niveles de seguridad de los sistemas y redes en la UE**. Para este objetivo, se ha configurado un esquema de prevención y acción ante los incidentes de ciberseguridad que ha conllevado a la designación de autoridades competentes, formación de equipos de respuesta a incidentes y el establecimiento de nuevas obligaciones para los Operadores de Servicios Críticos y Proveedores Esenciales de Servicios Digitales a los que les aplica la ley.

¿A quién afecta el RD NIS?

a. A los **(i) Operadores de 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 y designados en cada sector a través de los planes estratégicos sectoriales o **(ii)** cuyas **infraestructuras** hayan sido designadas como **críticas** de acuerdo a lo establecido por dicha ley. Los sectores afectados son: energía, agua, finanzas, salud, energía nuclear, espacio, TIC, investigación, transporte, química, alimentación y administración (servicios esenciales para el estado).

b. A los **Proveedores de Servicios Digitales** que ocupen al menos **50 personas y cuyo volumen de negocios anual sea igual o mayor a 10 millones de euros**, y que prestan alguno de los servicios descritos a continuación:

   I. **Mercados online (Online Marketplace):** Aquellos servicios en línea que permiten a consumidores y a empresarios celebrar contratos de compraventa o de prestación de servicios. Esta definición se aplicaría en exclusiva a plataformas que permitan que terceros (empresas o particulares) ofrezcan y adquieran productos y servicios a través de la misma.
   II. **Motores de búsqueda (Search Engines):** Son servicios que permiten realizar búsquedas de información específica en internet, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, obteniendo como respuesta aquellos enlaces en los que puede encontrarse información relacionada con el contenido solicitado.
   III. **Computación en la nube (Cloud Services):** Son servicios que ofrecen al usuario la utilización de recursos informáticos adaptables a la demanda del usuario, los cuales pueden ser accedidos a través de una conexión a internet o una red WAN. Dentro de los servicios en Cloud se pueden encontrar tres modelos de servicios: Infrastructure as a Service **(IaaS)**, Platform as a Service **(PaaS)** y Software as a Service **(SaaS)**.

El artículo 7 del RD 12/2018 impone a los Proveedores de Servicios Digitales sujetos a la normativa (es decir los detallados anteriormente) la **obligación de realizar una notificación**

formal de inicio de actividad a la Secretaría de Estado para el Avance Digital a los tres meses del inicio de su actividad.

La Secretaría de Estado para el Avance Digital ha habilitado un trámite en su sede para poder hacer dicha notificación que deberá contener, entre otros, los datos identificativos de la sociedad, la actividad realizada, así como datos identificativos a nivel societario.

Obligación de notificar

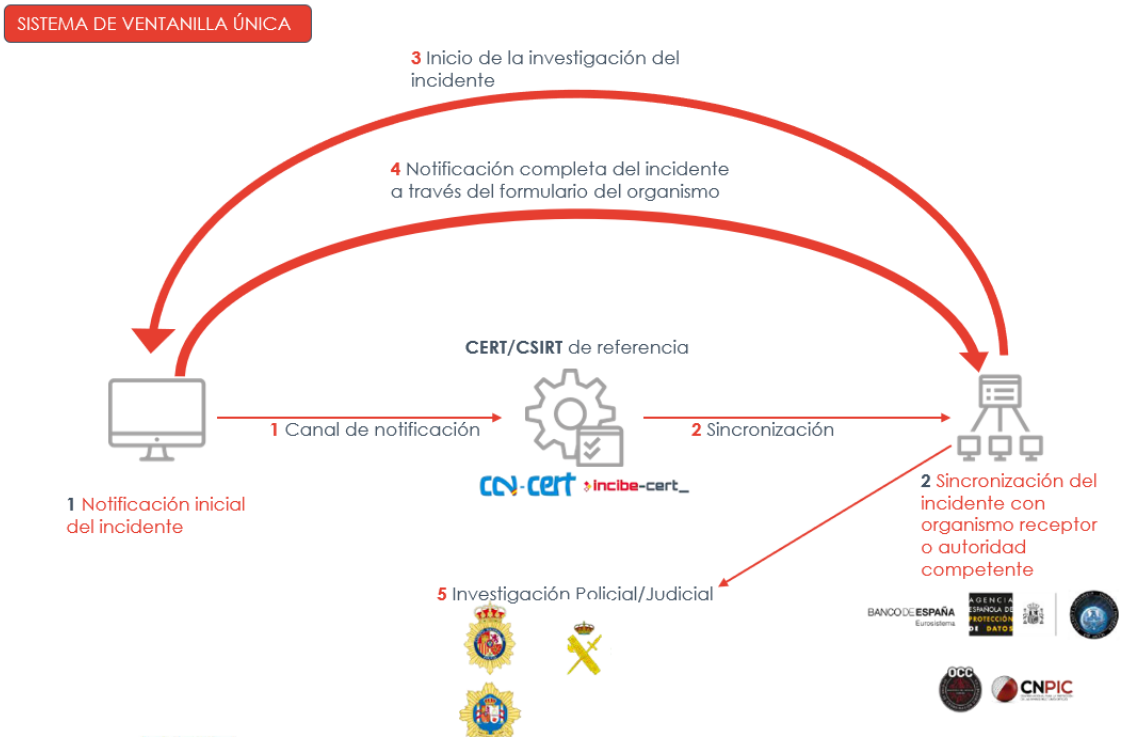
La principal obligación impuesta a los sujetos afectados por esta normativa es la **notificación de cualquier anomalía** que tenga un efecto negativo en la confidencialidad, integridad, autenticidad o disponibilidad de los sistemas, generando una interrupción o reducción de la calidad en los servicios relacionados a los sistemas de información. A estos efectos, se debe analizar el **nivel de peligrosidad inherente** al incidente para determinar la potencial amenaza que supondría la materialización del mismo y el **nivel de impacto** determinado en base a las consecuencias que efectivamente ha sufrido la organización afectada y a las medidas de seguridad implementadas.

Cada proveedor deberá evaluar la manera en que ha sido designado y que obligaciones debe cumplir a los efectos de determinar cuál es su autoridad competente y su CSIRT de referencia, siendo en todo caso **el CCN-CERT el designado para el sector público** y el **INCIBE-CERT el correspondiente para el sector privado**.

Sistema de ventanilla única

El sistema de notificación de incidentes de ciberseguridad indicado en esta guía parte con una gran ventaja de cara a la coordinación de los requisitos de los diferentes organismos y normativas. Así las cosas, **la notificación por este sistema de ventanilla única implicará que el CSIRT de referencia que reciba dicha notificación traslade la misma a la autoridad nacional competente**:

- Si afecta a la **Defensa Nacional**, al **ESPDEFCERT**
- Si afecta a una **Infraestructura Crítica** de la Ley PIC 8/2011, al **CNPIC**
- Si afecta a **la normativa de protección de datos**, a la **AEPD**
- Si es un **incidente de AAPP bajo el ENS** de peligrosidad MUY ALTA o CRÍTICA, al **CCN-CERT**
- Si es un incidente de obligatorio reporte según el RD Ley 12/2018, a la **autoridad nacional competente correspondiente.**



Medidas de seguridad

Con respecto a las medidas de seguridad a implementar por estos operadores, si bien, se está a la espera del reglamento de desarrollo de esta norma, el propio texto define que dichas medidas de seguridad deberán dar cobertura (como mínimo) a los siguientes aspectos:

- a la **seguridad de los sistemas e instalaciones**;
- a la **gestión de incidentes**;
- a la **gestión de la continuidad de las actividades**;
- a la **supervisión, auditorías y pruebas**;
- al **cumplimiento de las normas internacionales.**

Régimen sancionatorio

Para finalizar, el incumplimiento del contenido de este Real Decreto podrá conllevar a las siguientes sanciones:

Infracciones muy graves

Multa de 500.001 hasta 1.000.000 euros.

Infracciones graves

Multa de 100.001 hasta 500.000 euros.

Infracciones leves

Multa hasta 100.000 euros

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

Área de Tecnologías de la Información y Ciberseguridad de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60