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

Nota informativa

Madrid, 28 de julio de 2016

Nueva directiva relativa a la seguridad de las redes y sistemas de información en la unión europea

Nota Informativa sobre la nueva Directiva (UE) destinada a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 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, entrará en vigor el próximo 7 de agosto, y deberá ser transpuesta por los Estados miembros antes del día 9 de mayo de 2018.

La seguridad de las redes y sistemas de información es un elemento primordial del comercio entre los Estados miembros y desempeña un papel crucial en la sociedad actual. Cualquier incidente que derive en alteraciones del nivel de seguridad de las redes y sistemas de información puede generar considerables **pérdidas financieras, dañar la confianza del usuario y causar grandes perjuicios económicos.**

Para dar inmediata respuesta a los potenciales incidentes, la Directiva **integra una serie de requisitos mínimos** dirigidos a los Estados miembros que se agrupan en grandes categorías: ***(i)*** desarrollo de capacidades y planificación; ***(ii)*** intercambio de información; ***(iii)*** cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y ***(iv)*** cooperación y requisitos comunes de seguridad para los proveedores de servicios digitales ***(v)*** deber de supervisión ***(vi)*** establecimiento de un régimen sancionador.

En esta línea es importante destacar los siguientes aspectos, en relación a las obligaciones y deberes de los Estados miembros:

I. Identificación de operadores de servicios esenciales por los Estados miembros. Creación de una lista de operadores de servicios esenciales identificados.

Los criterios para la **identificación** de operadores de servicios esenciales son los que se exponen a continuación:

- si presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales;
- si la prestación de dicho servicio depende de las redes y sistemas de información, y
- si un incidente puede tener efectos perturbadores significativos en la prestación de dicho servicio.

II. Factores a seguir para la determinación del **efecto perturbador significativo** de los incidentes:

- el número de usuarios que confían en los servicios prestados por la entidad de que se trate;

- la dependencia de otros sectores sobre el servicio prestado por esa entidad;
- la repercusión que puedan tener los incidentes;
- la cuota de mercado de la entidad;
- la extensión geográfica con respecto a la zona que pueda verse afectada, y
- la importancia de la entidad para mantener un nivel suficiente del servicio.

III. Deber de los Estados Miembros de **adoptar una estrategia de seguridad** de las redes y sistemas de información y de **designar una o más autoridades competentes** en materia de seguridad de las redes y sistemas de información.

IV. Deber de los Estados Miembros de **designar Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)**.

V. El **establecimiento de un Grupo de cooperación** a fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros.

Por otra parte, se establecen obligaciones que afectarán a los operadores de servicios esenciales y a los operadores de servicios digitales:

I.- ¿Qué requisitos en materia de seguridad y notificación de incidentes serán obligatorios para los **operadores de servicios esenciales (Anexo I de la Directiva)**?

- Adopción de medidas de seguridad adecuadas al riesgo que plantean.
- Todas las medidas serán implementadas con el objeto de garantizar su **continuidad**.
- Deberán notificar sin dilación indebida a la autoridad competente o al CSIRT los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan. Esa notificación incluirá la información necesaria (número de usuarios, duración del incidente, extensión geográfica) para que la autoridad competente o el equipo de respuesta a incidentes de seguridad informática (CSIRT) puedan determinar la importancia de cualquier impacto transfronterizo.
- Una vez recibida la notificación correspondiente, la autoridad competente o el CSIRT informará al resto de Estados miembros afectados e incluso podrá informar al público sobre determinados incidentes, cuando la concienciación pública sea necesaria para evitar un incidente o gestionar uno que ya se haya producido.

II. ¿Qué **medidas técnicas y organizativas** en materia de seguridad y notificación de incidentes deberán adoptar los **proveedores de servicios digitales (mercado en línea, motor de búsqueda en línea y servicios de computación en nube)**? Serán, como mínimo las adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que se utilizan en el marco de la oferta de servicios en la Unión Europea, y además tendrá en cuenta lo siguiente:

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

Por último, cabe destacar que los Estados miembros deberán:

- Velar por que las autoridades competentes adopten medidas, si fuera necesario, mediante **supervisión a posteriori cuando tengan pruebas del incumplimiento de las obligaciones previstas.**

- **Establecer un régimen sancionador** con sanciones efectivas, proporcionadas y disuasorias.

Quedamos a su disposición para cualquier cuestión o duda que pudiera surgir, reciba un cordial saludo.

ECIJA Área de Ciberseguridad

César Zárate – Asociado Sénior
czarate@ecija.com
91.781.61.60