CONCLUSIONES DESAYUNO PRESENTACIÓN

GUÍA DE ACTUACIÓN ANTE INCIDENTES DE SEGURIDAD QUE REQUIERAN NOTIFICACIÓN

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)

Grupo de Trabajo de Seguridad y Calidad

5 de octubre de 2017

El 5 de octubre de 2017 tuvo lugar, en la sede de **Red.es** y con el patrocinio de **GMV**, un desayuno de trabajo en el que se presentó la **"Guía de actuación ante incidentes de seguridad que requieran notificación"** elaborada por el **Grupo de Calidad y Seguridad de AUTELSI**, en el marco del Foro para el debate sobre el desarrollo de la Sociedad de la Información para la divulgación del conocimiento en materia de TIC.

Presentación de la Guía

Francisco Lázaro, como Presidente del Grupo de Calidad y Seguridad de AUTELSI, presentó la Guía, exponiendo las razones que llevaron al Grupo a la realización de la misma, los objetivos que se perseguían con su elaboración y cómo se ha estructurado.

Recientemente el panorama regulatorio en materia de ciberseguridad ha cambiado de forma notable, con la aparición de una serie de normas que implican el deber de comunicación de incidencias y que exigirán, a los operadores de servicios esenciales y a los organismos y entidades pertenecientes al Sector Público y privado de los estados miembros de la Unión Europea, la notificación de incidentes significativos que sufran en las redes y servicios de información ante las autoridades competentes para cada caso:

- RGPD: Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Este reglamento será de obligado cumplimiento a partir del 25 de mayo de 2018.

- LPIC: Ley del 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas.

- NIS: 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.

- RD 3/2010: Real Decreto por el que se regula el Esquema nacional de Seguridad en el ámbito de la administración electrónica. Última modificación el 4 de noviembre de 2015 con el RD 951/2015.

La adopción de este conjunto de normativa constituye un hito importante para el refuerzo de la resiliencia en materia de ciberseguridad. En las mismas, se establecen requisitos en materia de notificación y seguridad en todos los sectores que son vitales para nuestra economía y nuestra sociedad y que, además, dependen en gran medida de las TIC, tales como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad y la infraestructura digital.

Por esta razón, el Grupo de Calidad y Seguridad de AUTELSI identificó como del máximo interés para las Entidades Asociadas la elaboración de esta "Guía de Actuación ante Incidentes de Seguridad que requieran notificación".

Esta "Guía de actuación" **va dirigida** tanto al sector público como al sector privado español con independencia del tamaño o sector de actividad de la empresa.

El **objetivo de la guía** es dar soporte a los profesionales de la seguridad de la información, a los distintos componentes del comité de crisis/seguridad o responsables en esta materia para que puedan informar, a tiempo, dichas situaciones con un criterio homogéneo a los organismos correspondientes. También pretende servir de elemento de sensibilización y de acercamiento de dicha problemática a los distintos órganos de Dirección de las empresas y entes públicos.

La guía se **estructura** para dar respuesta a las siguientes cuestiones:

- Introducción
- ¿Por qué debemos notificar?
- Tabla resumen
- ¿Qué normativas son las que establecen la obligación de notificar y desde cuándo?
- ¿Qué es un incidente o brecha de seguridad?
- ¿Por qué debe notificar?
- ¿Qué incidentes deben notificarse?
- ¿Quién debe notificar el incidente?
- ¿A quién debe notificarse?
- ¿Qué información se notifica?
- ¿Cómo se notifica: a través de qué canales de notificación y formatos?
- ¿Cuándo debe notificarse y en qué plazo?
- ¿Cuál es la sanción si no se notifica?
- ¿Qué debo tener preparado por si ocurre?
- ¿Y antes?

Conclusiones del debate

Tras la presentación de la Guía, se abrió un interesante debate entre las autoridades de regulación y las empresas reguladas participantes en el desayuno, centrándose en temas como:

- La importancia de las notificaciones
- Las sanciones
- La confianza de las empresas
- La protección de datos de ciudadanos y clientes
- Las capacidades de respuesta
- Los canales de colaboración entre los diferentes agentes y la coordinación entre autoridades.

Las principales conclusiones a las que llegaron fueron:

- La Guía viene a dar respuesta a una creciente necesidad de información que las empresas tienen en relación con el conjunto de obligaciones en materia de Ciberseguridad.
- La necesidad de realizar jornadas como la presente, donde autoridades, empresas y organismos aporten información y debatan sobre estas u otras cuestiones de Ciberseguridad.
- La necesidad de tener “una ventanilla única” de notificación.
- La necesidad de sumar capacidades de respuesta.