



"Nuestra estructura legal y jurisdiccional es todo lo contrario al funcionamiento intrínseco de Internet y las redes sociales"

04.07.2017 Entrevistamos a Carlos Alberto Sáiz Peña, vicepresidente de ISMS Forum España.

- El pasado 11 de mayo ISMS Forum reunió en el Círculo de Bellas Artes de Madrid a más de 600 profesionales de la ciberseguridad y la protección de datos en la XIX Jornada Internacional de Seguridad de la Información de ISMS Forum. ¿Podemos decir que este evento supone el mayor congreso privado nacional para profesionales del Sector? ¿A qué atribuiría el enorme éxito de esta edición?

En primer lugar, dar las gracias a los más de 600 asistentes, 60 ponentes, patrocinadores, mediapartners y a todo el apoyo institucional que hemos tenido. Respondiendo a tu pregunta, trabajamos para que nuestros Encuentros tengan un enfoque diferente, sean únicos y tengan cada vez mayor aceptación entre los profesionales de seguridad de la Información. Haber organizado ya 19 Encuentros Internacionales y el momento de interés que hay en asuntos de Privacidad y Ciberseguridad ha causado una gran afluencia de personas en esta edición, que ha sido espectacular en formato, contenido y calidad de los ponentes.

- Para quién de nuestros lectores y seguidores de LAW & TIC no conozca aún ISMS Forum Spain ¿podría presentárnosla?

ISMS Forum Spain es la Asociación Española para el Fomento de la Seguridad. Es una organización sin ánimo de lucro fundada en enero de 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de la comunidad implicada en el sector, tanto organizaciones como profesionales. En nuestros 10 años de vida (sí, estamos de aniversario) ya tenemos 900 socios y más de 150 empresas asociadas, por lo que constituimos una importante red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España.

- Y un día después aconteció WannaCry. ¿WannaCry marca un antes y un después en el ámbito de las ciberamenazas o simplemente se trata de una constatación más de una realidad vigente de la que no somos o no queremos ser conscientes de su existencia?

Creo que poco a poco somos todos más conscientes de lo que significa el ciberespacio y de las amenazas con las que tenemos que convivir. Apenas unos días después de WannaCry, hemos conocido Petya, que quizá sea más peligroso y sofisticado aún. Todos tenemos una responsabilidad para que la ciberseguridad sea una realidad, desde el Estado a cada uno

de los ciudadanos. Desde ISMS Forum intentamos promover una Cultura de Ciberseguridad y lanzamos proyectos para que los profesionales, las compañías, las administraciones públicas y los propios usuarios estén mejor preparados para afrontar lo que denominamos como “Jungla Digital”.

- Respecto a los dispositivos conectados (IoT) ¿realmente nos enfrentamos a un futuro inseguro tal como pronosticaba en la Jornada Bruce Schneier?

En pocos años viviremos rodeados de dispositivos conectados a Internet que harán mejorar nuestro rendimiento laboral, el tráfico en las ciudades, los servicios médicos y asistenciales, y el día a día de nuestro entorno doméstico. Pero lógicamente eso conlleva que millones de dispositivos móviles estarán emitiendo información y datos sobre nosotros y que se manejarán con herramientas y apps de todo tipo ubicadas en entornos Cloud. Las amenazas son muchas y las necesidades para protegernos como individuos de usos inadecuados también lo son. Para ello, debemos empezar a ser conscientes de la necesidad de exigir en la industria que la seguridad esté embebida en los productos y servicios que nos venden, es decir, aplicar de verdad el concepto de “security by default”.

- ¿Qué retos en materia de ciberseguridad traerá consigo la entrada en vigor del RGPD en mayo del próximo año?

Se trata de una norma que pretende establecer un sistema de protección de los datos personales de manera homogénea en todos los países de Europa, e incluso para compañías extranjeras que quieran operar en el mercado europeo. Creo que existen dos grandes retos respecto a la ciberseguridad: el primero, la necesidad de gestionar el cumplimiento normativo con un enfoque a riesgos, realizando evaluaciones de impacto de privacidad antes de tratar los datos y aplicando las medidas de seguridad proporcionales, y el segundo, cumplir con el nuevo requisito de notificar las violaciones de datos a la Autoridad de Control, y al usuario cuyos datos se hayan visto afectados.

- A su juicio ¿qué instrumentos normativos considera que faltan o requieren mejorarse por parte del Legislador en el sector de la Ciberseguridad?

Actualmente tenemos normativa sobre Protección de datos personales, el Esquema Nacional de Seguridad, Firma Electrónica, Protección de Infraestructuras Críticas, la futura Directiva NIS para la protección de las redes, el Código Penal para penalizar las conductas ilícitas... Considero que existen dos aspectos en los que mejorar mucho: a) la coordinación normativa y jurisdiccional internacional que permita soluciones homogéneas y más flexibles a problemas globales que afectan a múltiples usuarios en varios países y b) soluciones de ciberderecho para los ciberproblemas creando sistemas disciplinarios y sanciones que puedan aplicar nuevas figuras como los cibertribunales. Nuestra estructura legal y jurisdiccional es todo lo contrario al funcionamiento intrínseco de Internet y las redes sociales. Debemos buscar sistemas de resolución alternativa de conflictos ágiles, digitales y seguros.

- En la Jornada, la Agencia Española de Protección de Datos junto con ISMS Forum presentaron el Código de Buenas Prácticas en Protección de Datos para proyectos de Big Data. ¿Qué utilidad aporta este Código y por qué hay que hacerse con él?

Tanto el sector privado como el público deben estar preparados para la implementación de la nueva regulación europea a mayo 2018. Muchísimas organizaciones realizan proyectos y crean servicios que implican ingentes tratamientos de datos, estructurados y desestructurados, y que provienen de diferentes fuentes. Es el llamado Big Data. Utilizar grandes cantidades de información no es un problema en sí mismo, pero hay que hacerlo aportando las garantías necesarias para una correcta protección de los datos de las personas interesadas. Hemos trabajado durante 1 año en un Grupo de Trabajo con muchos expertos y en colaboración con la AEPD para desarrollar esta guía.

- Para terminar, ¿cuáles son las próximas citas de ISMS Forum Spain y por qué habrá que asistir?

Los próximos eventos que tenemos en ISMS Forum Spain son el 27 de septiembre, el VI de la Ciberseguridad, el 18 de octubre el evento del II Foro de Movilidad e Internet de las Cosas en Caixa Forum de Madrid (Paseo del Prado, 36) y el 28 de noviembre en el Instituto de Empresa de la c/María de Molina tendremos la última cita de este año 2017 con el VII encuentro de Cloud Security Alliance. Invitamos a todos los profesionales interesados a asistir para enterarse de las últimas novedades del sector.

Disponible en http://tecnologia.elderecho.com/tecnologia/ciberseguridad/estructura-jurisdiccional-funcionamiento-intrinseco-Internet_14_1108195001.html