ISACA
Barcelona Chapter

Jornada de formación continua:

"Cómo hacer frente a un ciber ataque. La importancia del seguro de riesgo cibernético"

El pasado 5 de febrero del 2019 tuvo lugar la jornada mensual de formación en el Auditorio de IL3. Institut de Formació Contínua. La jornada versó sobre cómo hacer frente a un ataque cibernético bajo el título "**Cómo hacer frente a un ciber ataque. La importancia del seguro de riesgo cibernético".** Carmen Segovia, Directora de Línees Financeres per a Catalunya i Balears i Responsable Nacional de Ciber risk fue la ponente de la charla.

La Jornada fue patrocinada por Deloitte, Auren, Prosegur, Víntegris, Andornet, OptimumTIC, ITACA y con el suporte institucional de Coettc, COEINF, Consejo General de Economistas, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, CESICAT , BQB, Andorra Telecom i l'Institut Municipal d'Informàtica Hàbitat Urbà - Ajuntament de Barcelona.

Carmen expresó la necesidad de **proteger la información** que gestiona la empresa en sus sistemas y también tener en cuenta los sistemas de sus proveedores externos como punto de partida para poder asumir las consecuencias económicas asegurables y que se derivan de un **Fallo de Seguridad o un Fallo de Sistemas**.

Desde un punto de vista de una aseguradora, Carmen expresó la secuencia de cómo se debe afrontar una ciberextorsió, a saber:

1. Intervención de un equipo de respuesta ante incidentes / Forensic.
2. Asesoramiento legal en caso de compromiso de datos de carácter personal.
3. Asesoramiento en gestión de crisis si se filtra y se hace pública esta situación.

En este orden de cosas, se debe hacer una **valoración de los gastos** ocasionados por la extorsión en la que puede haber sido provocado por un ransomware. Aquí aparecen los, gastos de recuperación de los datos, gastos incurridos para **reanudar los sistemas**, asesoramiento para la gestión, negociación y el posible **pago del rescate**, **pérdida de Beneficios** / Pérdida de Beneficios derivada del daño reputacional o Fondo de recompensa: suma ofrecida que lleve al arresto y condena del ciberextorsionador.
A ello habría que añadir gastos de **Defensa Jurídica** y la indemnización en caso de ser responsables legales de la pérdida ocasionada.

En esta misma línea, Carmen expuso dos casos más sobre la situación en que existe un **compromiso de datos** y como hacer frente a este evento donde aparecen las distintas fases para afrontarlo, la relación con los afectados, el **acompañamiento frente al regulador** y todos aquellos **procedimientos necesarios** para hacer frente a las responsabilidades habidas. También destacó la **gestión de la sanción administrativa** en materia de protección de datos (G.D.P.R.).

Por último, Carmen, planteo el caso de una caída de los sistemas de forma involuntaria, negligente o por **ataque de DDoS** y los perjuicios que conlleva y la manera de afrontarlo durante y después de la caída.

Carmen se refirió a la manera en que las aseguradoras hacen frente a este tipo de eventos para **calcular la prima del seguro**, donde un aspecto muy importante es el nivel de las **medidas de seguridad** implementadas y la criticidad de los datos.

Al final de la ponencia se entabló un interesante e intenso debate sobre la posibilidad de **asegurar las infracciones**, la necesidad de denunciar la extorsión y cómo se puede valorar la prima del seguro.

Como siempre la jornada finalizó con un refrigerio y un networking donde se siguió intercambiando opiniones sobre la conferencia que Carmen ofreció.

Barcelona 8 de febrero 2019