Jornada de formación continua:

# “Introducción a la Ciberseguridad en sistemas mHealth y la protección de datos”

El 7 de febrero la Jornada de formación mensual se tituló “Introducción a la Ciberseguridad en sistemas mHealth y la protección de datos” y estuvo a cargo de Marina Gibert, Knowledge Engineering and Machine Learning Group, Departamento de Estadística e Investigación operativa de la UPC y de Juan Francisco Fernández Carrasco, Ingeniero de Backend en Websays.

La Jornada fue patrocinada por Deloitte, Auren, Innevis, Víntegris, ItAdvisory, Andornet, OptimumTIC y con el apoyo institucional de Coettc, COEINF, Consejo General de Economistas, IAITG, ISMS, itSMF, UAB, ATI, Telecos.cat, CCJCC, CESICAT, BQB, Andorra Telecom y el Instituto Municipal de Informática Hábitat Urbano - Ayuntamiento de Barcelona.

Los ponentes explicaron como el eHealth ha pasado a ser mHealth, un escenario en el que se mezclan el Big data con los smart sensors, los datos en frío y el acceso en tiempo real a todo. La ubicuidad de los móviles y las baterías más eficientes de los sensores han facilitado que se esté desarrollando el mHealth, que Gartner prevé que en el período de 2019 a 2024 llegará a la meseta de productividad.

Los ponentes nos describieron la anatomía del sistema de mHealth en la que se encuentra el paciente, el profesional médico, así como otros profesionales, personal de IT, servicios en la nube y personas del entorno del paciente, todos pueden compartir y proporcionar datos.

Los retos del mHealth son la privacidad y la fiabilidad. Y es que hay que tener en cuenta que de estos aspectos dependerá la salud y la vida de las personas.

Se describieron algunos escenarios de riesgo según el tipo de dispositivo y se puso como ejemplo real el de una bomba de insulina que transmitía datos a un mando a distancia sin cifrar, lo que hizo que se tuviera que retirar del mercado o un administrador de viales que tenía los puertos abiertos y, por tanto, era susceptible de que se asumiera el control sobre el mismo.

Las herramientas para luchar contra las vulnerabilidades son especialmente la criptografía, la autenticación, la auditoría, la anonimización, la formación, la federación de identidades o el MDMs en los móviles de los usuarios.

Otras medidas en las que se está trabajando de cara al futuro con el cifrado homomórfico y la autenticación basada en riesgo.

La sesión termino con un networking, acompañado de un refrigerio, donde se siguió hablando de las distintas maneras de cómo afrontar los retos de la privacidad, la fiabilidad i aprovechar todo el potencial del mHealth.

Barcelona 7 de febrero 2017