Jornada de formación continua:

“La Ciberseguridad en la empresa”

El pasado 5 de junio tuvo lugar la jornada mensual de formación en el Institut de Formació Contínua de la UB. La jornada versó sobre la ciberseguridad en las empresas. Bajo el título de “**La Ciberseguridad en la empresa”** Rafael López, Perito Judicial Informático nos introdujo en los principales medidas a tener en cuenta para mitigar los riesgos en un ataque cibernético.

La Jornada fué 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.

Rafael empezó comentando que el compromiso con la seguridad se define por medio de una Política de Seguridad que defina todos aquellos aspectos importantes para la empresa y soportada por el desarrollo de unos procedimientos y normativas.

Un aspecto importante, señaló, es definir el nivel de riesgo asumido por la organización empezando por un análisis de la situación actual en que se encuentra.

Seguidamente señalo todas aquellas medidas mínimas imprescindibles a tener en cuenta a la hora de implementar un Plan de Seguridad, como puede ser el uso del correo electrónico, políticas de contraseñas, uso de software legal permitido, etc. etc.

Los aspectos legales también fue foco de atención por parte de Rafael donde el cumplimiento de las disposiciones legales y normativas es de vital importancia.

Hizo una exposición detallada de los accesos lógicos a los sistemas de información para garantizar la confidencialidad y la integridad de los datos y su uso debido. En este sentido la importancia de conocer en cada momento que quien hace qué en que momento para poder hacer un seguimiento de incidente en caso de producirse.

Mencionó la importancia de la gestión de las copias de seguridad teniendo en cuenta su temporalidad, alcance y pruebas de recuperación.

Tuvo una especial mención sobre el malware y todas sus implicaciones referentes a la ciberseguridad haciendo una descripción de sus características definiendo el antimalware y los antivirus. En este sentido habló de la importancia de mantener las actualizaciones al día y tener una buena gestión del parque informático y todos sus elementos, un solo componente puede acarrear una infección en toda la organización, comentó.

Por último habló de las soluciones a implantar unas de tipo organizativo como pueden ser las políticas de seguridad, las auditorías de seguridad y los test y pruebas de vulnerabilidades, sin olvidar las aplicaciones o herramientas como pueden ser los antimalware, sistemas de detección de intrusos.

Finalmente hubo un coloquio donde se habló de las dificultades de mantener segura una organización compleja como pueden ser los grupos con decenas de empresas o empresas con muchas delegaciones.

Barcelona 8 de junio 2018