ISACA
Barcelona Chapter

Jornada de formación continua:

“Com fer front a un ciber atac. La importància de l'assegurança de risc cibernètic”

El passat 5 de febrer de l'2019 va tenir lloc la jornada mensual de formació a l'Auditori de IL3. Institut de Formació Contínua. La jornada va versar sobre com fer front a un atac cibernètic sota el títol "**Com fer front a un ciber atac. La importància de l'assegurança de risc cibernètic**". Carmen Segovia, directora de línies Financeres per a Catalunya i Balears i Responsable Nacional de Ciber risk va ser la ponent de la xerrada.

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 va expressar la necessitat de **protegir la informació** que gestiona l'empresa en els seus sistemes i també tenir en compte els sistemes dels seus proveïdors externs com a punt de partida per poder assumir les conseqüències econòmiques assegurables i que es deriven d'un **Fallada de seguretat o Fallada de sistemes**.

Des d'un punt de vista d'una asseguradora, Carmen va expressar la seqüència de com s'ha d'afrontar una ciberextorsiór:

1. Intervenció d'un equip de resposta davant incidents / Forensic.
2. Assessorament legal en cas de compromís de dades de caràcter personal.
3. Assessorament en gestió de crisi si es filtra i es fa pública aquesta situació.

En aquest ordre de coses, s'ha de fer una **valoració de les despeses** ocasionades per l'extorsió en què pot haver estat provocat per un ransomware. Aquí apareixen les despeses de recuperació de les dades, despeses incorregudes per **reprendre els sistemes**, assessorament per a la gestió, negociació i el possible **pagament del rescat, pèrdua de beneficis** / Pèrdua de Beneficis derivada del dany reputacional o Fons de recompensa: suma oferta que porti a l'arrest i condemna del ciberextorsionador.
A això caldria afegir despeses de **defensa jurídica** i la indemnització en cas de ser responsables legals de la pèrdua ocasionada.

En aquesta mateixa línia, Carmen va exposar dos casos més sobre la situació en què hi ha un **compromís de dades** i com fer front a aquest esdeveniment on apareixen les diferents fases per afrontar-lo, la relació amb els afectats, **l'acompanyament davant del regulador** i tots aquells **procediments necessaris** per fer front a les responsabilitats hagudes. També va destacar la **gestió de la sanció administrativa** en matèria de protecció de dades (G.D.P.R.).

Finalment, Carmen, va plantejà el cas d'una caiguda dels sistemes de forma involuntària, negligent o per **atac de DDoS** i els perjudicis que comporta i la manera d'afrontar-lo durant i després de la caiguda.

Carmen es va referir a la manera en què les asseguradores fan front a aquest tipus d'esdeveniments per **calcular la prima de l'assegurança**, on un aspecte molt important és el nivell de les mesures de seguretat implementades i la criticitat de les dades.

Al final de la ponència es va entaular un interessant i intens debat sobre la possibilitat **d'assegurar les infraccions**, la necessitat de denunciar l'extorsió i com es pot valorar la prima de l'assegurança.

Com sempre la jornada va finalitzar amb un refrigeri i un networking on es va seguir intercanviant opinions sobre la conferència que Carmen va oferir.

Barcelona 8 de febrer 2019