UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Institut de Ciències de l'Educació

Edifici P, Planta 3, despatx 327A | Av. Doctor Marañón, 44-50
08028 Barcelona, Spain | Tel: 93 401 60 66
a/e: info.ice@upc.edu | http://www.upc.edu/ice

Ciberseguretat avançada (04/07/2017 - 13/07/2017)			
INFORMACIÓ GENERAL			
Titol activitat:	Ciberseguretat avançada - 0007080014		
Tipus activitat:	Curs	**Hores:**	30
Impartit per:	ANTONIO RODRIGUEZ I GARCIA (Factultat d'Informàtica de Barcelona (FIB))		
Sessions:	**Dia**	**Hora**	**Aula**
	04/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	05/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	06/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	07/07/2017	10:00 h - 13:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	10/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	11/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	12/07/2017	10:00 h - 14:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa
	13/07/2017	10:00 h - 13:00 h	INS Nicolau Copèrnic -Carrer Torrent del Batlle, 10 - 08225 Terrassa

INFORMACIÓ DETALLADA

PRESENTACIÓ

La Seguretat en els sistemes d'informació és una de les àrees més importants en el dia a dia de qualsevol entitat, pública o privada. Segon un informe anul·la de CCN-CERT (Centro Criptológico Nacional) en l'any 2015 es van gestionar 18.232 incidents de seguretat informàtica en les Administracions Públiques i en empreses d'interès estratègic, un 41,45% més que l'any 2014. Del total d'incidents, 430 van ser catalogats amb un nivell de risc molt alt o crític, és a dir, es va tenir constància que els atacs van afectar als sistemes de l'organització i a la seva informació sensible.

Aquest curs ens oferirà una visió global de les diferents aspectes que inclou la ciberseguretat per saber

identificar-los i aprendre a utilitzar les eines mes adients en cadascun de ells.

<img src="http://xtec.gencat.cat/web/.content/formacio/Imatges/logo-mecd-fse.jpg" " height="150" width="206">

Aquesta activitat s'emmarca en el "Programa de millora de la qualitat en formació professional" finançat pel Ministerio de Educación, Cultura y Deporte i cofinançat pel Fons Social Europeu.

DESTINATARIS

Professorat de formació professional de la família d'Informàtica i comunicacions

OBJECTIUS

L'objectiu d'aquest curs és proporcionar una visió global dels diferents aspectes que inclou la ciberseguretat per saber identificar-los i aprendre a utilitzar les eines mes adients en cadascun de ells:

• Hacking ètic : Les xarxes informàtiques són susceptibles de rebre atacs informàtics. Les auditories de xarxa periòdiques faciliten informació molt important sobre el nivell de seguretat dels diferents actius de què es disposa. Veurem com s'han de realitzar les auditories de seguretat i coneixerem les diferents eines que ens poden ajudar a dur-les a terme.

• Prevenció i resposta: Apropar a l'alumne a tècniques de detecció, prevenció i resposta envers atacs informàtics. Actualment, els sistemes generen gran quantitat de dades, sent necessari crear entorns que permetin centralitzar la informació per optimitzar l'anàlisi. Es treballaran els aspectes relacionats amb la centralització i gestió d'esdeveniments de seguretat per tal de detectar de forma proactiva possibles atacs.

• Informàtica forense: La detecció, preservació i investigació de proves o evidències electròniques que poden usar-se per defensar l'empresa davant la possible responsabilitat penal es coneix com "computer forensics". Tractarem d'entendre els aspectes legals i tècnics necessaris per portar a terme una anàlisi forense de manera correcta i aprendrem a obtenir evidencies en diferents entorns de treball mitjançant una selecció correcta de les eines.

• Seguretat en el desenvolupament d'aplicacions: Més d'un 80% dels atacs als sistemes informàtics es fan aprofitant vulnerabilitats de les aplicacions web. És per tant imprescindible que els desenvolupadors tinguin coneixements de seguretat i que aquests coneixements estiguin integrats en el dia a dia de la seva feina.

PLA DE TREBALL

El curs es divideix en 4 mòduls ben diferenciats. Tots els mòduls aniran acompanyats d'exercicis que es realitzaran a mesura que es vagin tracten els diferents temes.

La distribució d’hores i dies dels mòduls és la següent:

• Hacking ètic: Dos dies de 4 hores (8 hores total).

• Ciberatacs: Tres dies , 2 dies de 4 hores i un dia de 3 hores (11 hores total).

o Seguretat a la infraestructura: 4 hores.

o Monitoritació: 4 hores.

o Resposta: 3 hores.

• Informàtica forense: Dos dies de 4 hores (8 hores total).

• Seguretat en el desenvolupament d’aplicacions: Un dia de 3 hores (3 hores total).

TEMARI

• **Hacking ètic**

o Information gathering

o Escaneig i identificació de vulnerabilitats

o Anàlisi manual o Anàlisi automatitzat

o Explotació

• **Ciberatacs: Prevenció i resposta**

o Seguretat a la infraestructura

o Monitorització

o Resposta (gestió d’un incident)

• **Informàtica forense**

o Introducció

o Obtenció d’evidències

o Tècniques i eines d’anàlisi

• **Seguretat en el desenvolupament d’aplicacions**

o OWASP Top 10

METODOLOGIA

• La metodologia a utilitzar serà una combinació de teoria i pràctica per tal que els conceptes quedin clars i la pràctica ajudi a consolidar-los.

• Els exercicis pràctics es realitzaran amb màquines virtuals que proporcionarà el professor, amb les eines necessàries instal·lades.

BIBLIOGRAFIA

CERTIFICACIÓ

La certificació a les persones participants estarà supeditada a la prèvia inscripció i acceptació pel mitjà establert (electrònicament a través del web) i a l'assistència a un mínim del 80% de les hores totals de l'activitat.

Els certificats s'obtindran a través del sistema informàtic de la Generalitat de Catalunya (http://xtec.gencat.cat/ca/formacio/la-meva-formacio/els-meus-certificats).