GUÍA DOCENTE
2021 - 2022

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Ética: privacidad y hacking
Código	DOI-MCS-521
Impartido en	Máster Universitario en Ingeniería de Telecomunicación [Segundo Curso] Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	1,5 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Organización Industrial
Responsable	Javier Camacho Ibáñez
Descriptor	Este módulo tiene por objetivo conseguir que el alumno reflexione sobre la dimensión ética del uso de los datos y recursos en la era de la economía digital. Por una parte se introduce al estudiante en los conceptos básicos del razonamiento ético, para que pueda aplicarlo a dos áreas muy concretas relacionadas con la ciberseguridad: la privacidad y el hacking ético. En un entorno donde todas las organizaciones compiten por conseguir datos para optimizar los diferentes sistemas de inteligencia artificial y otros algoritmos para la toma de decisiones, el acceso, uso, cesión y conservación de estos datos supone un reto en un entorno legal desigual, donde compiten varios derechos fundamentales, tales como la seguridad y la privacidad. El hacking ético se presenta en su sentido más amplio, es decir, no solo como la acción consentida de intentar penetrar en un sistema de seguridad, sino como cualquier uso no violento de la tecnología, a favor de una causa, política o de otro tipo. El Hacking

Datos del profesorado	
Profesor	
Nombre	Javier Camacho Ibáñez
Departamento / Área	Departamento de Gestión Empresarial
Correo electrónico	jcamacho@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Competencias - Objetivos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

1. Introducción a la Ética
2. Razonamiento ético
3. Privacidad en la Era de la Economía Digital

4. Aspectos fundamentales de la privacidad en las organizaciones
5. Definición y tipos de Hacking Ético
6. Tests de intrusion/penetración
7. Descubrimiento de vulnerabilidades y programas de recompensas
8. Whisteblowing y hacking ético
9. Hacktivismo

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Calificaciones

Examen final: 40%

Trabajos (grupo/individuales): 60%

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Blanken-Webb, J., Palmer, I., Deshaies, S. E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). A Case Study-based Cybersecurity Ethics Curriculum. In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).

Coleman, E. G. (2012). Coding freedom: The ethics and aesthetics of hacking. Princeton University Press.

Coleman, G. (2014). Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous. Verso books.

Dennedy, Michelle, Jonathan Fox, and Tom Finneran. The privacy engineer's manifesto: getting from policy to code to QA to value. Apress, 2014.

Engelmann, Severin & Chen, Mo & Fischer, Felix & Kao, Ching-Yu & Grossklags, Jens. (2019). Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines "Good" and "Bad" Behavior. 69-78. 10.1145/3287560.3287585.

Mac Síthigh, D., & Siems, M. (2019). The Chinese social credit system: A model for other countries?. The Modern Law Review, 82(6), 1034-1071.

Maurushat, Alana. Ethical Hacking. University of Ottawa Press, 2019.

Narayanan, Arvind, and Vitaly Shmatikov. "How to break anonymity of the netflix prize dataset." arXiv preprint cs/0610105 (2006).

Ohm, Paul. "Broken promises of privacy: Responding to the surprising failure of anonymization." UCLA l. Rev. 57 (2009): 1701.

Richterich, A. (2018). The Big Data Agenda. University of Westminster Press.

Ryffel, T., Trask, A., Dahl, M., Wagner, B., Mancuso, J., Rueckert, D., & Passerat-Palmbach, J. (2018). A generic framework for privacy preserving deep learning. arXiv preprint arXiv:1811.04017.

Wong, K. L. X., & Dobson, A. S. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures

in Westernised democracies. Global Media and China, 4(2), 220-232.