COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2021 - 2022

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Ciberseguridad y delitos en la red
Código	E000010680
Nivel	Postgrado Oficial Master
Cuatrimestre	Semestral
Créditos	3,0 ECTS
Carácter	Obligatoria
Departamento / Área	Facultad de Derecho
Responsable	ofelia Tejerina
Horario de tutorías	Previa Petición

Datos del profesorado	
Profesor	
Nombre	Francisco Javier Gómez Lanz
Departamento / Área	Departamento de Derecho Público
Despacho	Alberto Aguilera 23 [ED-431]
Correo electrónico	jglanz@icade.comillas.edu
Teléfono	2835
Profesor	
Nombre	Jaime Bragado Iturriaga
Departamento / Área	Centro de Innovación del Derecho (CID - ICADE)
Correo electrónico	jbragado@icade.comillas.edu
Profesor	
Nombre	María Isabel Crespo Vitorique
Departamento / Área	Centro de Innovación del Derecho (CID - ICADE)
Profesor	
Nombre	Ofelia Tejerina Rodríguez
Departamento / Área	Centro de Innovación del Derecho (CID - ICADE)
Correo electrónico	otejerina@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Prerequisitos

No se establece ninguno

Competencias - Objetivos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

BLOQUE I

CIBERSEGURIDAD

El último informe del Parlamento Europeo «sobre la democracia digital en la Unión Europea: posibilidades y retos» (2016-2017) (4), se recordaba a los Estados miembros que la iniciativa ciudadana europea es un derecho político de los ciudadanos, y que es «una herramienta única e innovadora para definir la agenda política en aras de una democracia participativa en la Unión Europea, que permite a los ciudadanos ser parte activa en los proyectos y procesos que les atañen, y cuyo potencial debe, sin duda, explotarse al máximo y mejorarse de forma significativa». Esta iniciativa no podría hoy ser viable si no se entendiera incluida en el entorno digital. Dice por ello también que «el refuerzo de la legitimidad democrática de las instituciones debe ser uno de los objetivos prioritarios de la UE», y que no se puede hablar de democracia ni de seguridad sin «potenciar el empleo de las nuevas tecnologías en la vida institucional y política». Las infraestructuras críticas, las administraciones y el poder ejecutivo, son objetivo de ciberataques a escala mundial.

La ciberseguridad no solo es un aspecto que cuidar desde el interviniente más fuerte, sino que debe atender a todos y cada uno de los escalafones que pueden verse afectados. Así, se protege como materia de ciberseguridad, la libertad de información, que puede ser atacada para manipular el destino de un Estado cambiando la percepción social de la realidad, hasta las empresas que dominan el mercado como los servicios públicos.

BLOQUE II

La seguridad de los sistemas informáticos es ampliamente analizada, desde su perspectiva legal. La normativa exige responsabilidades en caso de que se produzcan daños, a veces irreversibles, con la correspondiente indemnización, a veces reparables, con la correspondiente indemnización y satisfacción del daño. Para solucionar estos problemas es preciso además saber contar con las evidencias electrónicas necesarias. Los ciberataques pueden ser de muy diferentes magnitudes, y tanto la tecnología de protección como la formación del empleado deben ser puestas a punto y actualizadas periódicamente. El caso de las infraestructuras críticas es un caso especial, que puede ser objeto incluso de ataques de ciberterrorismo.

BLOQUE III

CIBERSEGUROS

Se analizan los riesgos cibernéticos y las distintas responsabilidades que se derivan de los mismos, para pasar a centrarnos en el estudio de la estructura y principales características de las pólizas de riesgos cibernéticos, sin olvidar el aspecto práctico de la materia pues realizaremos un caso práctico de brecha de seguridad con la intervención del equipo de respuesta rápida de la póliza, para finalizar dando una visión actual del mercado asegurador español de riesgos cibernéticos

BLOQUE IV

DELITOS EN LA RED – CIBEREVIDENCIAS

En el curso se abordan, en primer lugar, los rasgos criminológicos que caracterizan a este fenómeno delictivo para, a continuación, analizar el propio concepto de "ciberdelito", así como la taxonomía de ciberdelitos propuesta por el Convenio de Budapest. Tras exponer cómo se trata de una manifestación paradigmática del nuevo "Derecho penal del riesgo", se presentan algunas cuestiones de Parte general del Derecho Penal que resultan singularmente complejas en este sector, tales como la autoría, la responsabilidad por omisión, la responsabilidad de las personas jurídicas o los problemas de jurisdicción y ley aplicable.

Se analiza la respuesta penal en nuestro derecho frente a las nuevas formas de criminalidad propiciadas por el uso perverso de las nuevas tecnologías. En el marco del derecho penal sustantivo se estudiarán los nuevos tipos delictivos introducidos para la persecución y castigo de las acciones criminales que se valen de las TIC para atacar a los propios sistemas y dispositivos informáticos así como la información contenida en los mismos y también otras conductas delictivas donde el empleo de las TIC en general, y de internet en particular para la comisión del delito ha tenido y tienen una especial incidencia dando lugar a modificaciones legislativas que han adaptado la respuesta penal a las peculiaridades de estas nuevas formas de delincuencia.

En el ámbito del derecho procesal, se examinarán las medidas de investigación tecnológica para obtención de la evidencia electrónica y su incorporación al proceso que han sido introducidas en la reforma de la LECrim mediante LO 13/2015.

El objetivo de la asignatura es también conocer, por un lado, el marco teórico normativo que regula la producción y aportación de evidencias digitales en procedimientos judiciales de los diversos órdenes jurisdiccionales, con especial énfasis en los criterios de admisibilidad, autenticidad y eficacia probatoria. Por otro lado, la asignatura ofrece diversos ejemplos prácticos con casos reales sobre la producción y enjuiciamiento de distintos medios de prueba digital (correos electrónicos, mensajería instantánea, metadatos, fotografías digitales, código fuente, hash y dirección IP, Código IMEI). En último lugar, la asignatura ofrece una aproximación a dos de los métodos más extendidos de autenticación de prueba y su tratamiento judicial: wayback machine y blockchain.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

PARTICIPACIÓN Y EVALUACIÓN CONTINUA: participación activa en la búsqueda de un resultado cooperativo 10%.

PRUEBAS DE APLICACIÓN 90%: Resolución y entrega de exámenes y/o casos practicos en grupo o individuales

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

"Haz clic aquí para matarlos a todos. Un manual de supervivencia". Schneier, B. Ed. Planeta (2019).

"Internet Organised Crime Threat Assessment (IOCTA) 201". Europol. 2018. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

Recomendación UIT-T X.1205: Aspectos generales de la ciberseguridad. Unión Internacional de Telecomunicaciones. 2009.

"Roadmap on the cooperation between CSIRTS and Legal Enforcement". ENISA. 2019. Disponible en: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

"El Derecho sui generis del fabricante de bases de datos". Bouza López, Miguel Ángel. Ed. Reus. (2001).

"Código de Derecho de la Ciberseguridad". Disponible en: https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=2&nota=0

Análisis de los vectores de ataque del Internet de las cosas (IoT). Grupo de trabajo de amenazas y sensibilización del Centro de Estudios en Movilidad e IoT (CEM) de ISMS FORUM SPAIN. Autores: Pedro Cabrera, Manager (Ernst & Young), Raúl García (Cybersecurity Tecnical Coordinator, Grupo SIA); Alberto Pérez (Responsable de Auditoría de Seguridad IntellSoc, Mnemo) y Raúl Siles (Fundador y Analista de Seguridad, DinoSec). Versión 0.7, de 16 de octubre de 2016.

"OWASP Internet of Things Project". OWASP. 13 Oct 2016. Disponible en: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

"Tort Liability for Vendors of Insecure So ware: Has the Time Finally Come?" Michael D. Scott. MARYLAND LAW REVIEW [VOL. 67:425 2008].

"Reasonableness and Rationality in Negligence Theory". Gregory C. Keating, 48 STAN. L. REV. 311, 344 (1996).

"Holding Internet Service Providers Accountable". Doug Lichtman & Eric Posner, 14 SUP. CT. ECON. REV. 221, 222 (2006).

"Tort Liability For Software Developers: A Law & Economics Perspective". T. Randolph Beard, Phd. George S. Ford, Phd. Thomas M. Koutsky, Esq. Lawrence J. Spiwak, Journal Of Computer & Information Law [Vol. XXVII 2009].

"Who is Liable for Software Errors? Proposed New Product Liability Law in Australia", Roger Clarke. Disponible en: http://www.anu.edu.au/people/Roger.Clarke/SOS/PaperLiaby.html

"Insecure software is eating the world: promoting cybersecurity in an age of ubiquitous software-embedded systems". Daley, John. 19 STAN. TECH. L. REV. 533 (2016).

"Convenio sobre la ciberdelincuencia" - Budapest el 23 de noviembre de 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

"Claves de la investigación en redes sociales". Barrera, Silvia. Grupo Editorial Círculo Rojo (2016).

"Derecho probatorio". Abel Lluch, Xavier. Ed. Bosch Procesal (2012).

"Nuevas tecnologías e investigación penal. Estudios sobre prueba penal". Vol. III. Abel Lluch, Xavier. Ed. La ley. (2013)

"Nuevos horizontes del derecho procesal". Bulnes, Mar Jimeno. Ed. Bosch (2019).

"Intervención policial de mensajes SMS y eficacia de las juntas provinciales de Policía Judicial". Magro Servet, Vicente. Diario la Ley nº 6764. (2007).

"Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. El proceso penal en la sociedad de la información". Ortiz Pradillo, Juan Carlos. Ed. La Ley (2012).

Investigación Tecnológica y prueba digital en todas las jurisdicciones. Ed. Wolters Kluwer. Delgado, Joaquín. (2016).

"The Tort of Negligent Enablement of Cybercrime". Michael L. Rustad & Thomas H. Koenig, BERKELEY TECH. L.J. 1553, 1559 (2005).

"Delitos informáticos. paso a paso". Escarlata Gutiérrez Mayo. Ed. Colex. 2021.

"Delitos tecnológicos. Cuestiones penales y procesales" Eloy Velasco. Ed. La Ley. 2021.

"Derecho penal e internet". Fernández Teruelo, G. Ed. Lex Nova, Valladolid, 2011

"Internet y Derecho Penal". Morón Lerma, E. Ed. Aranzadi, 2002.

"Ciberdelincuencia" Almenar Pineda, F., Ed. Juruá, 2018.

DELGADO MARTÍN, Joaquín, Investigación tecnológica y prueba digital en todas las jurisdicciones. La Ley, 2018.

GAMELLA CARBALLO, Sandra, Redes sociales y otros medios de prueba digital. WhatsApp, Facebook, Twitter, Skype, correo electrónico, Google Maps, GPS y cámaras de videovigilancia. Sepin - Servicio de Propiedad, 2019.

PINTO PALACIOS, Fernando; PUJOL CAPILLA, Purificación. La prueba en la era digital. La Ley, 2017.

ELGUERO MERINO, J.M., "El seguro de riesgos cibernéticos", en MONTERRROSO CASADO, E. (Dir.), MUÑOZ VILLARREAL, A. (Coord.), Inteligencia artificial y riesgos cibernéticos responsabilidades y aseguramiento. Valencia: Tirant lo Blanch, 2019, pp. 375-409.

MUÑOZ VILLARREAL, A., "Ciberiesgos y Seguros: los riesgos de los criptoactivos y su aseguramiento" en BARRIO ANDRÉS, M. (Coord.) Criptoactivos: Retos y desafíos normativos, Madrid, La Ley- Wolters Kluwer, 2020, pp. 311-320.

NAVALÓN LÓPEZ, M.J., "Los ciberseguros y el aseguramiento de la actividad de tratamiento de datos", en JIMENO MUÑOZ, J. (Coord.), Insurtech y nuevas tendencias de la responsabilidad civil, Madrid, Sepin, 2019, pp. 251-270.

VEIGA COPO, A. B., Seguro y tecnología. El impacto de la digitalización en el contrato de seguro. Estudios y Comentarios, Madrid, Civitas, 2020.