COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2022 - 2023

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	F. Javier Gómez Lanz
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

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Competencias - Objetivos

Resultados de Aprendizaje

Análisis de las principales claves que un abogado debe tener en torno a la ciberseguridad y delitos online.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

BLOQUE I

DELITOS EN LA RED

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

- Introducción a la delincuencia en la red.
- Rasgos criminológicos que caracterizan a este fenómeno delictivo
- Concepto de "ciberdelito"
- Taxonomía de ciberdelitos propuesta por el Convenio de Budapest.
- El nuevo "Derecho penal del riesgo": autoría, la responsabilidad por omisión, la responsabilidad de las personas jurídicas o los problemas de jurisdicción y ley aplicable.
- Respuesta penal al fenómeno de la cibercriminalidad en el marco del derecho sustantivo. Las figuras delictivas de más frecuente aplicación en este ámbito – estafas informáticas, daños informáticos y delitos contra bienes jurídicos personalísimos cometidos con apoyo o sirviéndose de las tecnologías de la información y la comunicación - con especial referencia a los problemas que plantea su interpretación y aplicación práctica, y soluciones aportadas por la jurisprudencia y la doctrina emanada al respecto.
- Estudio del agente encubierto online, técnica de investigación que resulta cada vez más esencial para el esclarecimiento de los ciberdelitos frente al uso por parte de los ciberdelincuentes de mecanismos de comunicación más sofisticados para la comisión del delito - mensajería instantánea; foros ocultos en la Dark Web, compartición de archivos nube...etc. -. Este un fenómeno, en el que también incide la aparición de los sistemas de cifrado punto a punto de las comunicaciones, complica extraordinariamente la investigación de estas conductas que, en ocasiones, solo pueden ser investigadas a través de esta figura.
- Marco teórico-normativo que regula la producción y aportación de evidencias digitales en procedimientos judiciales de los diversos órdenes jurisdiccionales criterios de admisibilidad autenticidad eficacia probatoria.
- Producción y enjuiciamiento de distintos medios de prueba digital: correos electrónicos, mensajería instantánea, metadatos, fotografías digitales, código fuente, hash y dirección IP, Código IMEI.
- Aproximación a dos de los métodos más extendidos de autenticación de prueba y su tratamiento judicial: wayback machine y blockchain.
- Medios tecnológicos de investigación penal:

-Prueba digital en el proceso penal: principios generales; Interceptaciones telefónicas y telemáticas; Investigación penal con datos e IA;

-Micrófonos ambiente; Geolocalizadores; Filmación del espacio público; registro de dispositivos almacenadores de información; registro remoto de equipos informáticos; medidas de aseguramiento de la información.

- Investigación penal tecnológica con prueba en el extranjero: Investigación penal tecnológica en el extranjero: aspectos

introductorios; Convenio de ciberdelincuencia de Budapest; 2º protocolo al Convenio de Budapest.

BLOQUE II

CIBERSEGURIDAD

El 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.

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.

- Seguridad de los sistemas de información: Conceptos de ciberseguridad y seguridad de la información. Seguridad, almacenaje y transmisión de la información. Ciberseguridad y seguridad de la información
- Breve resumen del panorama actual. Entorno de la seguridad de la información. Ejemplos de ataques en 2021. Estadísticas y ejemplos prácticos
- Marco legal esencial. Ámbito europeo. Ámbito estatal. Conceptos legales esenciales sobre ciberseguridad y ciberamenaza
- Principales obligaciones de las administraciones públicas – Esquema de Seguridad Nacional. Obligaciones de las administraciones públicas. Principios básicos del Esquema de Seguridad Nacional. Estrategia nacional de ciberseguridad
- Cinco leyes (pero no legales) de la ciberseguridad
- Seguridad de las redes y de los sistemas de información. Ámbito objetivo de la regulación. Infraestructuras críticas. Servicios digitales. Ámbito subjetivo de la regulación. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales. Funciones de las autoridades competentes. Marco sancionador.

BLOQUE III

CIBERSEGUROS/SEGUROS DE RIESGOS CIBERNÉTICOS

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.

- Definición Ciber riesgo
- Origen y desarrollo de los seguros de riesgos cibernéticos.

- Naturaleza jurídica y riesgo cubierto
- Estructura de la póliza
- Coberturas
- Extensiones
- Exclusiones
- Delimitación temporal de la cobertura
- Límites
- Concurrencia de seguros
- Como se activa la póliza: respuesta ante un incidente cibernético.
- Caso Práctico: Brecha de seguridad, cuando comunicar y cuando no a la Agencia Española de Protección de Datos.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Aplicación de los conocimientos teórico-prácticos adquiridos durante la exposición del profesor a escenarios profesionales reales.

Evaluación y valoración de las implicaciones interdisciplinares de carácter tecnológico y organizativo.

Valoración dentro del marco jurídico vigente las distintas vías de solución de los conflictos en defensa de los derechos de los clientes en el marco de un ejercicio del Derecho que también es tecnológico.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Peso (%)
Evaluación final	70%
Participación activa	20%
Asistencia	10%

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

GAMELLA CARBALLO, S., 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, F.; PUJOL CAPILLA, P. 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.

ORTIZ PRADILLO, J.C., "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. El proceso penal en la sociedad de la información", Ed. La Ley, 2012.

DELGADO, J., Investigación Tecnológica y prueba digital en todas las jurisdicciones. Ed. Wolters Kluwer, 2016.

GUTIERREZ MAYO, E., "Delitos informáticos. paso a paso", Ed. Colex, 2021.

VELASCO, E., "Delitos tecnológicos. Cuestiones penales y procesales", Ed. La Ley, 2021.

FERNÁNDEZ TERUELO, G., "Derecho penal e internet", Ed. Lex Nova, Valladolid, 2011.

ALMENAR PINEDA, F., "Ciberdelincuencia", Ed. Juruá, 2018.

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