Guía Docente: Delitos Informáticos

DATOS GENERALES	
Facultad	Facultad de Ciencias Jurídicas y Económicas
Titulación	Grado en Derecho
Plan de estudios	2012
Especialidad/Mención	Mención en Derecho de las Nuevas Tecnologías
Materia	Derecho de las Nuevas Tecnologias de la Información y las Telecomunicaciones
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Para esta materia no se precisa haber superado previamente materias determinadas; por tanto, los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Daniel Gonzalez Uriel	**Correo electrónico**	daniel.gonzalez.uriel@ui1.es
Área		**Facultad**	Facultad de Ciencias Jurídicas y Económicas

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Comercio electrónico; contratación electrónica y firma electrónica. E-Administración • Delitos Informáticos • Derecho de la Información • Derecho de las Telecomunicaciones • Protección de Datos
Contexto y sentido de la asignatura en la titulación y perfil profesional	Se trata de una asignatura con contenidos necesarios para todo aquel que vaya a ejercer profesionalmente en el mundo del Derecho, dado que se trata de una materia de gran impacto y, por tanto, imprescindible. Los delitos informáticos forman parte del día a día, tanto de las personas físicas como jurídicas y se torna fundamental comprender las obligaciones y límites que conlleva. Mediante esta asignatura se pretende que el alumno posea un conocimiento exhaustivo, claro y profundo de los delitos por medios informáticos, puesto que prácticamente todo sujeto de Derecho (sea persona física o jurídica, nacional o extranjera) puede ver comprometido alguna de estas cuestiones. Esta asignatura está directamente relacionada con los que se encuadran en el denominado Derecho de las Tecnologías de la Información y las Comunicaciones (TIC). Su ubicación dentro de la Mención incorpora la normativa de este Derecho TIC y su interpretación en un mundo globalizado en la denominada Red de Redes: Internet. Esto nos lleva a considerar sin duda la relación con el resto de las asignaturas, puesto que es imposible hoy en día desligar el mundo jurídico de las TIC.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	Generales y básicas • CG-01: Desarrollar la capacidad de analizar e interpretar normas y supuestos de hecho relevantes jurídicamente. • CG-02: Capacidad de organización y planificación. • CG-05: Conocimientos de informática relativos al ámbito de estudio. • CG-06: Saber recabar, gestionar, analizar y elaborar información sobre los elementos necesarios para resolver problemas jurídicos en el contexto del derecho y la realidad social. • CG-07: Resolución de problemas. • CG-08: Trabajar en equipo, tanto en cada una de las diversas materias, como en aquellas tareas que requieren una relación interdisciplinar. • CG-13: Desarrollar la capacidad de un aprendizaje autónomo, sobre la base de saber reflexionar sobre el propio aprendizaje, tanto en la etapa de formación del Grado como posteriormente en la ampliación de conocimientos y saber hacer en el campo del Derecho. • CG-16: Iniciativa y espíritu emprendedor. Específicas • CE-02: Capacidad para utilizar los principios y valores constitucionales como herramienta de trabajo en la interpretación del ordenamiento jurídico.

	• CE-03: Capacidad para identificar y aplicar las fuentes jurídicas básicas, y saber identificar y aplicar todas las fuentes jurídicas de relevancia en una cuestión concreta (legales, jurisprudenciales y doctrinales). • CE-04: Desarrollo de la oratoria jurídica. Capacidad de expresarse apropiadamente ante un auditorio. • CE-05: Capacidad para leer una amplia diversidad de trabajos complejos en relación con el derecho y sintetizar sus argumentos de forma precisa. • CE-06: Capacidad para redactar con fluidez textos jurídicos elaborados, empleando la terminología técnicamente apropiada. • CE-07: Adquirir un amplio dominio de las técnicas informáticas en el tratamiento de texto, en la obtención de la información jurídica (bases de datos de legislación, jurisprudencia y bibliografía), y en la utilización de la red informática para la comunicación de datos). • CE-11: Saber sintetizar los argumentos de forma precisa, sobre la base de conocimientos sólidos de argumentación jurídica. Universidad • CU-04: Utilizar las Tecnologías de la Información y la Comunicación (TIC) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU-05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • CU-06: Aprender a trabajar individualmente de forma activa. • CU-10: Reconocer y saber resolver problemas que afecten a derechos fundamentales de las personas y a valores democráticos. • CU-16: Saber transmitir un informe técnico de la especialidad. • CU-17: Ser capaz de concluir adecuadamente la tesis de la exposición basándose en modelos, teorías o normas, etc. Mención • CM1-01: Capacidad para adaptar una organización a las exigencias normativas en protección de datos de carácter personal, en lo que respecta, entre otros, a la inscripción de ficheros, al momento de la recogida de datos, en la redacción de un documento de seguridad, en la contestación frente a ejercicios de derechos… Asimismo, se adquieren los conocimientos para intervenir en los diversos procedimientos ante las autoridades de protección de datos. • CM1-02: Capacidad para asesorar jurídicamente en los procesos de puesta en marcha de portales en Internet que pretenden realizar comercio electrónico y adaptarlo a la normativa vigente. • CM1-03: Capacidad para llevar a la practica del ejercicio activo del Derecho los conocimientos adquiridos respecto a las categorías que delimitan un delito informático y las particulares circunstancias que los envuelven. • CM1-04: Adquisición de los conocimientos suficientes para manejarse con fluidez, asesorar, e incluso formar a otros, respecto de los servicios que presta la Administración Electrónica en España y las implicaciones normativas consecuentes con los ciudadanos, las empresas, e incluso entre Administraciones Públicas. • CM1-05: Adquisición de los conocimientos necesarios para comprender el funcionamiento de las pautas jurídicas que afectan a las telecomunicaciones, entendidas como la infraestructura sobre la que se desarrollan los sistemas y servicios de la sociedad de la información
Resultados de aprendizaje de la asignatura	• Demostrar conocimientos básicos en materia de las TICs. • Exponer los tipos penales, y sus especialidades, relacionados con las nuevas tecnologías. • Resolver cualquier cuestión conectada con la protección de datos, tanto en

	entidades públicas como privadas. • Implantar y auditar un sistema de protección de datos en cualquier organización. • Redactar contratos informáticos y cláusulas legales de contratación electrónica. • Ordenar legalmente un portal de Internet que realice comercio electrónico. • Explicar los principios regulatorios básicos del sector de las Telecomunicaciones. • Asesorar acerca de la protección de los usuarios de servicios de Telecomunicaciones.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Las categorías que delimitan un delito informático pueden incluir delitos específicos o tradicionales, pero en cualquier caso, destaca la especialidad del particular medio comisivo empleado: las nuevas tecnologías de la información y las comunicaciones.
Contenidos	**Unidad didáctica 1. Generalidades** 1.1. Generalidades 1.2. Su denominación 1.3. Clasificación 1.4. La informática como instrumento en la comisión de un delito 1.4.1. Manipulación de datos 1.4.2. Acceso no autorizado a datos 1.4.3. Malware 1.4.4. Utilización de la herramienta informática con fines fraudulentos 1.4.5. Agresión a la privacidad 1.5. Derechos de autor **Unidad didáctica 2. Características de los delitos informáticos** 2.1. Rapidez y acercamiento en tiempo y en espacio su comisión 2.2. Facilidad para ocultar el hecho 2.3. Facilidad para borrar las pruebas 2.4. Prevención y corrección **Unidad didáctica 3. El Código Penal** 3.1. Introducción 3.2. En la protección de la intimidad 3.3. Delitos contra el patrimonio y contra el orden socioeconómico

3.3.1. De los hurtos

3.3.2. De las defraudaciones

3.3.3. De los daños

3.3.4. De los delitos relativos a la propiedad intelectual e industrial

3.4. De la infidelidad en la custodia de documentos

3.5. De las falsedades documentales

3.6. Otras referencias indirectas

Unidad didáctica 4. La responsabilidad penal de las personas jurídicas

4.1. La obligación del debido control

4.1.1. Artículo 31 bis

4.1.2. Artículo 31 ter

4.1.3. Artículo 31 quater

4.1.4. Artículo 31 quinquies

4.2. El compliance

4.3. Circunstancias atenuantes

4.4. Exención de responsabilidad

4.5. Sanciones y penas

Unidad didáctica 5. Ciberseguridad

5.1. Concepto

5.2. Aspectos jurídicos de la ciberseguridad en España

5.3. Estrategia de ciberseguridad en la Unión Europea

5.4. Directiva 2016/1148/UE

5.5. Incidentes de seguridad

Unidad didáctica 6. Delitos en redes sociales

6.1. Grooming

6.2. Ciberbullying

6.3. Sexting y sexcasting

6.4. Sextorsión

6.5. Suplantación de identidad

	6.6. Porno venganza o revenge porn 6.7. Acoso incesante: stalking 6.8. Responsabilidad penal de los menores 6.9. Enaltecimiento de odio y del terrorismo a través de las redes sociales

METODOLOGÍA	
Actividades formativas	**Actividades de descubrimiento inducido (Estudio del Caso)** Los Estudios de Caso son las actividades en las que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando, en el Aula Virtual una situación real o simulada que le permitirá realizar un primer acercamiento a los diferentes temas de estudio. **Actividades de aplicación práctica (grupal online)** Incluye la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de la asignatura. **Actividades de trabajo autónomo individual (Estudio de la Lección)** Trabajo individual de los materiales utilizados en la asignatura, aunque apoyado por la resolución de dudas y construcción de conocimiento a través de un foro habilitado para estos fines. Esta actividad será la base para el desarrollo de debates, resolución de problemas, etc. **Lectura crítica, análisis e investigación.** Se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. Se incluyen, a modo de ejemplo, recensiones de libros o crítica de artículos y proyectos de investigación. **Tutorías.** Permiten la interacción directa entre docente y alumno para la resolución de dudas y el asesoramiento individualizado sobre distintos aspectos de la asignatura. **Foros.** Los Foros son las actividades en las que se discutirá y argumentará acerca de diferentes temas relacionados con la asignatura y que servirán para guiar el proceso de descubrimiento inducido.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de*

proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.

El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*.

El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera:

Sistema de evaluación convocatoria ordinaria

Opción 1. Evaluación continua

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado.

En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura.

Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Velasco Núñez, E./Sanchis Crespo, C. (2019). *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015.* Valencia: Tirant lo Blanch. Mir Puig, C./Corcoy Bidasolo, M./Mir Puig, s. (dirs.) (2015). *Comentarios al código penal reforma lo 1/2015 y lo 2/2015.* Valencia: Tirant lo Blanch.
Bibliografía complementaria	• Poveda Criados, M. A. (2015). *Delitos en la Red*. Madrid: Fragua. • Mir Puig, S. (2014). *Responsabiliad de la empresa y compliance*. Madrid: Edisofer S.L. • Nieto Martin, A. (2008). *La responsabilidad penal de las personas jurídicas: un modelo legislativo*. Madrid: Iustel. Portal derecho. • VV.AA. (2013). *Compliance y teoría del derecho penal*. Madrid: Marcial Pons. • Saiz Peña, C. A. (2015). *Compliance*. Pamplona: Aranzadi. • Velasco Núñez, E. (2015). Los delitos informáticos. *Práctica penal: cuaderno jurídico*. 81, 4-28. Madrid: SEPIN. • García López, P. (2015). UNE-ISO/IEC 27002: la guía en la era de la ciberseguridad. Madrid: AENOR. • Rubio Alamillo, J. (2015). La informática en la reforma de la Ley de Enjuiciamiento Criminal. *Diario La Ley*. 8663. Madrid. • Gil Antón, A. M. (2015). De los delitos contra la intimidad personal y familiar y delito informático, de acuerdo con la reforma operada por la LO 1/2015, de 30 de marzo, de reforma del Código Penal. *Revista Aranzadi de derecho y nuevas tecnologías*. 39, 27-57. Pamplona. • Álvaro Mendo Estrella, A. (2014). Delitos y redes sociales: mecanismos formalizados de lucha y delitos más habituales. el caso de la suplantación de identidad. *Revista General de Derecho Penal*. 22. Madrid. • Davara Rodríguez, M. A. (2015). *Manual de Derecho Informático.* (11ª Ed.). Pamplona: Editorial Aranzadi.
Otros recursos	Consejos a la hora de denunciar delitos informáticos: https://www.youtube.com/watch?v=cs_sI1xm6nQ Guía de almacenamiento seguro de la información: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf Ciberseguridad para la empresa: https://www.youtube.com/watch?v=EHjmxujXIaQ La ética es la base del compliance: https://www.youtube.com/watch?v=E5LLQsXVh4E Introducción a la ciberseguridad: https://www.youtube.com/watch?v=TM-OT1U3P0k Ciberseguridad en comercio electrónico: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_ciberseguridad_comercio_electronico/guiacomercioincibe0.pdf Ciberseguridad: https://www.youtube.com/watch?v=Z1mWmy-iSmc Compliance penal: https://www.youtube.com/watch?v=uVYL-vm_YO8 Arranca el juicio contra la cúpula española de Anonymous: https://www.youtube.com/watch?v=K6TBebUOMyw

	Gestión de riesgos, una guía de aproximación para el empresario: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf