

Guía Docente: Delitos Informáticos

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Ciencias de la Seguridad
Plan de estudios	2016
Materia	Derecho
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se precisa

DATOS DEL PROFESORADO			
Profesor Responsable	Carmen Gonzalez Vaz	Correo electrónico	carmen.gonzalez.vaz@ui1.es
Área		Facultad	Facultad de Criminología
Perfil Profesional 2.0	Linkedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA

Asignaturas de la materia	<ul style="list-style-type: none"> • Código Técnico de la Edificación • Derecho Administrativo de la Seguridad • Derecho de la Seguridad • Derecho Penal de la Seguridad • Fundamentos Comunitarios y Constitucionales • Ley Orgánica 4/2015, de Protección de la Seguridad Ciudadana • Protección de Datos de Carácter Personal y Seguridad • Responsabilidad Civil, Penal y Administrativa • Propiedad industrial e intelectual • Delitos informáticos
Contexto y sentido de la asignatura en la titulación y perfil profesional	<p>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.</p> <p>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.</p> <p>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.</p>

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE

Competencias de la asignatura	<p style="text-align: center;">Generales y básicas</p> <ul style="list-style-type: none"> • CB01: Poseer y comprender conocimientos en un área de estudio que parte de la base de la Educación Secundaria General, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio. • CB02: Saber aplicar sus conocimientos a su trabajo o vocación de una forma profesional y poseer las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio. • CB03: Reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. • CB04: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CB05: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. • CG01: Conocer, saber organizar y planificar los recursos individuales y colectivos disponibles para el ejercicio, en sus distintas modalidades, de la profesión.
--------------------------------------	--

- CG02: Capacidad para asesorar a terceros en cuestiones concretas y específicas que solo la especialización en una materia puede otorgar.
- CG03: Capacidad de gestión de la información, de redacción de informes y/o artículos de investigación con una actitud creativa e innovadora y mediante el empleo de una correcta técnica de investigación.
- CG04: Resolución de problemas en materias relativas a la seguridad.

Específicas

- CE01: Saber aplicar los conocimientos de seguridad en las diferentes posibilidades de desarrollo profesional existentes y poseer las competencias de elaboración, síntesis y defensa de sus propios argumentos para la resolución de los distintos problemas que la inseguridad plantea a través del estudio de casos reales.
- CE02: Capacidad de reunir, seleccionar e interpretar datos relevantes en procedimientos o investigaciones para emitir juicios de valor y opiniones críticas que no solo incluyan una reflexión cualificada sobre temas relevantes relacionados con la seguridad desde la triple vertiente social, científica y ética, sino que también sean capaces de asesorar y realizar propuestas de intervención o actuación en materias relacionadas con la seguridad.
- CE03: Comprender la información, ser capaz de seleccionarla, interpretarla, recordarla y trasladarla a nuevos contextos y realidades de seguridad.
- CE04: Habilidad para identificar problemas de seguridad, investigarlos y formular cuestiones.
- CE09: Comprender el carácter dinámico y evolutivo del crimen y las inseguridades. El futuro titulado deberá ser capaz de comprender la progresiva complejidad y diversificación del delito, el crimen y la inseguridad, de mantener una actitud positiva y racional en el desarrollo de la actividad, y de adoptar decisiones abiertas y reflexivas en la actual sociedad del riesgo cambiante y globalizado.
- CE10: Evaluar las ventajas y los diversos objetivos de las respuestas y de las teorías más relevantes incluyendo la protección a los derechos humanos y a los datos de carácter personal.
- CE11: Comprender el marco legal que regula las actividades relacionadas con la seguridad. Conocer la normativa vigente que afecta a los distintos tipos delictivos y criminales, y ser capaz de planificar y desarrollar la propia actividad de acuerdo con la normativa reguladora. Conocer el sistema regulador de los derechos y deberes en una sociedad democrática y las diferentes instituciones que velan por el mantenimiento de la seguridad.
- CE15: Conocimiento de la normativa regional, estatal y supraestatal que regula las actividades en materia de seguridad, tanto pública como privada.

Universidad

- CU02: Identificar y dar valor a las oportunidades, tanto personales como profesionales, siendo responsables de las actuaciones que se pongan en marcha, sabiendo comprometer los recursos necesarios con la finalidad de realizar un proyecto viable y sostenible para uno mismo o para una organización.
- CU03: Utilizar la expresión oral y escrita de forma adecuada en contextos personales y profesionales.
- CU04: 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.
- CU05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión.
- CU06: Aprender a trabajar individualmente de forma activa.
- CU10: Reconocer y saber resolver problemas que afecten a derechos fundamentales de las personas y a valores democráticos.
- CU11: Comprender y saber actuar ante situaciones en las que proceda defender la

	<p>igualdad, particularmente la de género y la de oportunidades.</p> <ul style="list-style-type: none"> • CU12: Saber cómo se han de adoptar posturas de defensa de la paz y la mediación. • CU13: Aceptar y defender el derecho de los diferentes, llegando incluso ante la desigualdad compensatoria, particularmente en los casos de personas con disminución de su autonomía personal. • CU15: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • CU16: Saber transmitir un informe técnico de la especialidad. • CU17: Ser capaz de concluir adecuadamente la tesis de la exposición basándose en modelos, teorías o normas, etcétera.
<p>Resultados de aprendizaje de la asignatura</p>	<ul style="list-style-type: none"> • Adquirir los conocimientos esenciales para comprender estas materias y poder desenvolverse en ellas con naturalidad. • Conocer los tipos penales y sus procedimientos y las consecuencias jurídicas del delito. • Obtener los elementos de juicio imprescindibles para defender una postura en relación con estas asignaturas. • Conocer, comprender y analizar el concepto y las características del acto administrativo y los fundamentos de las relaciones de la Administración con los ciudadanos. • Identificar una serie de elementos cognoscitivos al futuro profesional para un estudio integral de las áreas que integran el derecho penal y la aplicación de penas y medidas de seguridad. • Analizar la seguridad desde el punto de vista del ordenamiento jurídico-administrativo. • Conocer las fases del proceso penal y sus características principales. • Conocer el marco teórico de protección constitucional de los derechos humanos y su repercusión. • Conocer y analizar los principales instrumentos jurídicos que proporciona el derecho positivo.

PROGRAMACION DE CONTENIDOS

<p>Breve descripción de la asignatura</p>	<p>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.</p>
<p>Contenidos</p>	<p>Unidad didáctica 1. Generalidades, la falta de tipificación y clasificación</p> <p>1.1. Generalidades</p> <p>1.2. Su denominación</p> <p>1.3. Clasificación</p> <p>1.4. La informática como instrumento en la comisión de un delito</p> <p>1.4.1. Manipulación de datos</p> <p>1.4.2. Acceso no autorizado a datos</p> <p>1.4.3. Malware</p>

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

1.1. Rapidez y acercamiento en tiempo y en espacio su comisión

1.2. Facilidad para ocultar el hecho

1.3. Facilidad para borrar las pruebas

1.4. Prevención y corrección

Unidad didáctica 3. El Código Penal

1.1. Introducción

1.2. En la protección de la intimidad

1.3. Delitos contra el patrimonio y contra el orden socioeconómico

1.3.1. De los hurtos

1.3.2. De las defraudaciones

1.3.3. De los daños

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

1.4. De la infidelidad en la custodia de documentos

1.5. De las falsedades documentales

1.6. Otras referencias indirectas

Unidad didáctica 4. La responsabilidad penal de las personas jurídicas

1.1. La obligación del debido control

1.1.1. Artículo 31 bis

1.1.2. Artículo 31 ter

1.1.3. Artículo 31 quater

1.1.4. Artículo 31 quinquies

1.2. El compliance

- 1.3. Circunstancias atenuantes
- 1.4. Exención de responsabilidad
- 1.5. Sanciones y penas

Unidad didáctica 5. Ciberseguridad

- 1.1. Concepto
- 1.2. Aspectos jurídicos de la ciberseguridad en España
- 1.3. Estrategia de ciberseguridad en la Unión Europea
- 1.4. Directiva 2016/1148/UE
- 1.5. Incidentes de seguridad

Unidad didáctica 6. Delitos en redes sociales

- 1.1. Grooming
- 1.2. Cyberbullying
- 1.3. Sexting y sextcasting
- 1.4. Sextorsión
- 1.5. Suplantación de identidad
- 1.6. Porno venganza o revenge porn
- 1.7. Acoso incesante: stalking
- 1.8. Responsabilidad penal de los menores
- 1.9. 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 (grupales 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, reseñas 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 autenticación 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.

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. y Sanchis Crespo, C. (2019). *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*. Tirant lo Blanch.

El siguiente manual estudia todos los elementos de los delitos informáticos, haciendo una gran labor de actualización con las nuevas conductas introducidas con las Leyes Orgánicas 1/2015 y 2/2015. Esta obra sirve al alumno en el estudio de la asignatura gracias al detallado análisis que realiza.

Mir Puig, C./Corcoy Bidasolo, M./Mir Puig, s. (dirs.) (2015). *Comentarios al código penal reforma lo 1/2015 y lo 2/2015*. Tirant lo Blanch.

La presente obra muestra un estudio detallado de los tipos delictivos presentes en el Código Penal, incluyendo doctrina científica y judicial. Gracias a este manual el alumno podrá acceder a un estudio ecléctico, el cual le dará más profundidad y amplitud a sus conocimientos.

Bibliografía complementaria

- Davara Rodríguez, M. A. (2015). *Manual de Derecho Informático*. (11ª Ed.). Aranzadi.

- García López, P. (2015). *UNE-ISO/IEC 27002: la guía en la era de la ciberseguridad*. AENOR.
- 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.
- Poveda Criados, M. A. (2015). *Delitos en la Red*. Fragua.
- 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.
- Mir Puig, S. (2014). *Responsabilidad de la empresa y compliance*. Edisofer S.L.
- Nieto Martín, A. (2008). *La responsabilidad penal de las personas jurídicas: un modelo legislativo*. Iustel.
- Rubio Alamillo, J. (2015). La informática en la reforma de la Ley de Enjuiciamiento Criminal. *Diario La Ley*, 8663. Madrid.
- Saiz Peña, C. A. (2015). *Compliance*. Aranzadi.
- Velasco Núñez, E. (2015). Los delitos informáticos. *Práctica penal: cuaderno jurídico*, 81, 4-28.
- VV.AA. (2013). *Compliance y teoría del derecho penal*. Marcial Pons.

Otros recursos

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=EHjmxujXlaQ>

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/guigestionriesgos.pdf