

Guía Docente: Delitos Informáticos

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Ciencias de la Seguridad
Año verificación	2016
Especialidad/Mención	
Materia/Módulo	Derecho
Carácter	Optativo
Modalidad	Virtual
Período de impartición	Segundo Trimestre
Curso	Cuarto
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No precisa

DATOS DEL PROFESORADO

Profesor Responsable	Óscar Ibáñez Vicente	Correo electrónico	oscar.ibanez@ui1.es
Área		Facultad	Facultad de Criminología
Doctor acreditado	No		
Perfil Profesional 2.0	<p>www.linkedin.com/in/óscar-ibáñez-vicente-721501a5</p> <p>Licenciado en Derecho Especialidad Derecho de la Empresa (Universidad de Zaragoza) Máster en Dirección de Comercio Internacional (ESIC) Doctorado en Derecho (en curso) (Universidad de Murcia)</p> <p>Experiencia Docente:</p> <ul style="list-style-type: none"> - Relaciones Internacionales, Derecho Internacional y Diplomacia en Grado en Traducción y Comunicación Intercultural (Universidad San Jorge) - Derecho Administrativo I en Grado en Derecho (Universidad San Jorge) <p>Experiencia Investigadora:</p> <ul style="list-style-type: none"> - Proyecto de Innovación docente: "El debate académico como estrategia para la formación transversal del jurista", Universidad de Zaragoza, finalizado en 15/06/2022. - Secretaría Técnica del I Congreso Internacional de Innovación Docente en Derecho: "aprendizaje a través del debate jurídico", Universidad de Zaragoza 21/04/2022. <p>Publicaciones:</p> <ul style="list-style-type: none"> -Valve Contra UFC-Que Choisir: Videojuegos digitales frente al derecho. Cuadernos de Derecho Transnacional. 14 - 1, Universidad Carlos III, 01/03/2022. - Schrems contra Facebook y la caída del Privacy Shield: transmisiones internacionales de datos personales a EE.UU. "Europa en un mundo cambiante estrategia Europa 2020 y sus retos sociales : una perspectiva desde el derecho internacional privado". Aranzadi. 		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA

Contexto y sentido de la asignatura

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 para 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.

RESULTADOS DE APRENDIZAJE

Conocimientos o contenidos

- CON03: Conocer la normativa regional, estatal y supraestatal que regula las actividades en materia de seguridad, tanto pública como privada.
- CON08: Aprender a trabajar individualmente de forma activa.

Habilidades o destrezas

- HAB01: 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.
- HAB02: 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.
- HAB03: Comprender la información, ser capaz de seleccionarla, interpretarla, recordarla y trasladarla a nuevos contextos y realidades de seguridad.
- HAB04: Identificar problemas de seguridad, investigarlos y formular cuestiones.
- HAB09: 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.
- HAB10: 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.
- HAB11: 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

	<p>el mantenimiento de la seguridad.</p> <ul style="list-style-type: none"> • HAB15: 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. • HAB16: Utilizar la expresión oral y escrita de forma adecuada en contextos personales y profesionales. • HAB17: 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. • HAB18: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • HAB20: Reconocer y saber resolver problemas que afecten a derechos fundamentales de las personas y a valores democráticos. • HAB21: Comprender y saber actuar ante situaciones en las que proceda defender la igualdad, particularmente la de género y la de oportunidades. • HAB22: Saber cómo se han de adoptar posturas de defensa de la paz y la mediación. • HAB23: 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. • HAB25: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • HAB26: Saber transmitir un informe técnico de la especialidad.
<p>Competencias (básicas y generales)</p>	<ul style="list-style-type: none"> • CG01: Conocer, saber organizar y planificar los recursos individuales y colectivos disponibles para el ejercicio, en sus distintas modalidades, de la profesión. • CG02: Asesorar a terceros en cuestiones concretas y específicas que solo la especialización en una materia puede otorgar. • CG03: Tener la 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: Ser capaz de resolver problemas en materias relativas a la seguridad. • CB1: 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. • CB2: Aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean 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 • CB3: 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. • CB4: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CB5: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

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>
--	--

Contenidos	Unidad didáctica 1. Generalidades
	<ul style="list-style-type: none">1.1. Generalidades1.2. Su denominación1.3. Clasificación1.4. La informática como instrumento en la comisión de un delito<ul style="list-style-type: none">1.4.1. Manipulación de datos1.4.2. Acceso no autorizado a datos1.4.3. Malware1.4.4. Utilización de la herramienta informática con fines fraudulentos1.4.5. Agresión a la privacidad1.5. Derechos de autor
	Unidad didáctica 2. Características de los delitos informáticos <ul style="list-style-type: none">2.1. Introducción2.2. Rapidez y acercamiento en tiempo y en espacio su comisión2.3. Facilidad para ocultar el hecho2.4. Facilidad para borrar las pruebas2.5. Prevención y corrección<ul style="list-style-type: none">Prevención y corrección (II)Prevención y corrección (III)2.6 El perfil del ciberdelincuente<ul style="list-style-type: none">El perfil del ciberdelincuente (II)<ul style="list-style-type: none">2.6.1. Clasificación de los ciberdelincuentes especializados2.6.2. Clasificación de los ciberdelincuentes no especializados
	Unidad didáctica 3. El Código Penal <ul style="list-style-type: none">3.1. Introducción3.2. En la protección de la intimidad3.3. Delitos contra el patrimonio y contra el orden socioeconómico<ul style="list-style-type: none">3.3.1. De los hurtos3.3.2. 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. El extinto principio *Societas delinquere potest*

4.2. La obligación del debido control

4.2.1. Artículo 31 bis

4.2.2. Artículo 31 ter

4.2.3. Artículo 31 quater

4.2.4. Artículo 31 quinquies

4.3. El *compliance*

El *compliance* (II)

El *compliance* (III)

El *compliance* (IV)

4.4. Circunstancias atenuantes

4.5. Exención de responsabilidad

4.6. Sanciones y penas

4.7. El internet de las cosas y el Derecho Penal

4.7.1. Introducción y contexto

4.7.2. La comercialización de información personal. Especial referencia a los casos de Google y Facebook: la colisión con el derecho a la intimidad.

La comercialización de información personal. Especial referencia a los casos de Google y Facebook: la colisión con el derecho a la intimidad (II)

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

Directiva 2016/1148/UE (II)

Directiva 2016/1148/UE (III)

Directiva 2016/1148/UE (IV)

Directiva 2016/1148/UE (V)

Directiva 2016/1148/UE (VI)

5.5. Incidentes de seguridad

5.5.1. La red de equipos de respuesta

5.5.2. Grupo de cooperación

5.5.3. Estrategia nacional de seguridad en las redes y sistemas de información

5.6. Amenazas cibernéticas. Especial referencia al ciberterrorismo y al ciberespionaje

5.6.1. Ciberterrorismo

Delitos informáticos (arts. 197 bis y 197 ter y 264 a 264 *quater*) con fines terroristas (art. 573.2 CP)

Delito de autocapacitación terrorista (art. 575.2 CP)

La contranarrativa como arma contra el ciberterrorismo

5.6.2. Ciberespionaje

Unidad didáctica 6. Delitos en redes sociales

6.1. Grooming

6.2. Cyberbullying

6.3. Sexting y sexting

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

Métodos y actividades formativas del proceso de enseñanza-aprendizaje

Las **actividades formativas** de la asignatura de Delitos informáticos se dividen en cuatro categorías:

- **Crítica de un artículo relacionado con la UD** donde se analiza el estado de la ciencia y se adquieren competencias para estudiar y cuestionar trabajos sobre la materia objeto de estudio.
- **Cuestionario** con preguntas tipo test con una única respuesta válida.
- **Estudios de Casos** donde se analizan supuestos reales con el propósito de llevar a la práctica los aspectos teóricos sustanciales aplicables en la materia.
- **Foro de debate** entre los distintos alumnos sobre un tema determinado de los estudiados en la unidad didáctica correspondiente.
- **Trabajo colaborativo** relacionado con los contenidos de la unidad didáctica. Se trata de un trabajo de investigación en el que los distintos alumnos trabajarán en grupos, de manera colaborativa, no independiente.

Prueba de Evaluación de Competencias (PEC)

En el caso de optar por la opción de evaluación (PEC + examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

Para contestar a cada una de las preguntas, el alumno debe tener en cuenta el contenido tratado en las unidades, así como el tenor de las leyes que regulan la materia, así como la Constitución.

La estructuración de los casos responde a la necesidad de que el estudiante llegue a comprender cuestiones complejas, que involucren distintos temas jurídicos, pero siempre teniendo como marco el contenido de la asignatura.

La prueba consistirá en el análisis de un supuesto práctico y la respuesta de cinco preguntas de desarrollo relacionadas con el mismo. En la misma se deberán plasmar los conocimientos adquiridos en las unidades didácticas 1 a 6. Cada una de las preguntas tendrá un valor del 20 por 100 del total de la nota del ejercicio.

La extensión mínima del documento será de 20 páginas y la extensión máxima de 25 páginas sin contar la portada y las referencias bibliográficas.

Asimismo, existirá un examen de repaso de las UD 1 a 6 en la que se formularán preguntas tipo test sobre las citadas unidades, con un valor total del 5 por 100 de la nota total.

EVALUACIÓN

Sistema evaluativo

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 u online (EX)**, según la modalidad elegida por el estudiante, 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 u online (EX)**, según la modalidad elegida por el estudiante.

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**, 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 u online (EX)**, según la modalidad elegida por el estudiante, 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.

Corcoy Bidasolo, M.; Mir Puig, S. y Vera Sánchez, J. S. (dirs.) (2015). *Comentarios al*

Código Penal tras la 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 intimidación 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

COMENTARIOS ADICIONALES