Guia docente				
Datos Identificativos				2014/15
Asignatura (*)	Legislación y Seguridad Informática		Código	614G01024
Titulación	Grao en Enxeñaría Informática			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Grado	1º cuatrimestre	Tercero	Obligatoria	6
Idioma	CastellanoGallego			
Prerrequisitos				
Departamento	Dereito Público EspecialTecnoloxías da Información e as Comunicacións			
Coordinador/a	Santos Del Riego, Antonino	Correo electrónico	antonino.santos@udc.es	
Profesorado	Ballesteros Soriano, Alfonso	Correo electrónico	alfonso.ballesteros@udc.es	
	Carballal Mato, Adrián		adrian.carballal@udc.es	
	Santos Del Riego, Antonino		antonino.santos@udc.es	
	Vázquez Naya, José Manuel		jose.manuel.vazquez.naya@udc.es	
Web	psi-udc.blogspot.com/			

Descripción general	É a finais dos oitenta, principalmente polo uso da rede Internet, cando a seguridade da información transfórmase nunha necesidade. A finais dos 90 as ameazas aos sistemas "abertos" á rede Internet xeneralízanse e a seguridade da información toma unha gran relevancia. Na actualidade, as empresas, os gobernos e a sociedade en xeral demandan un maior número de expertos en seguridade informática. Hoxe en día un profesional das tecnoloxías da información e as comunicacións, tanto do ámbito dos sistemas como do desenvolvemento do software, sen uns bos fundamentos en seguridade, estará claramente devaluado. A nosa profesión non consiste unicamente na administración de sistemas e desenvolvemento de software e hardware. Noutras palabras, un programa ou sistema que simplemente funciona, sen considerar o factor seguridade, pode supor un gran perigo para unha organización. O apagar e acender unha máquina pode arranxar un problema, a análise das causas e a procura de solucións constitúe unha clara diferenza entre un bo e mal profesional. Na materia de Lexislación e Seguridade Informática proporciónase ao alumno uns fundamentos en seguridade da información, e con iso un valor engadido sobre outros "profesionais" do sector. En todo momento centrámonos naqueles aspectos de interese para o seu futuro profesional, tentado levar os contidos da materia cara aos temas e contornas de relevancia para o mundo empresarial. A nosa profesión céntrase en "facer", non unicamente en "saber facer", e se é posible en "facelo o mellor posible". E, que nos piden as empresas?, claramente profesionais que saiban o que hai que facer, que o fagan ben, no menor dos tempos e cun custo mínimo. Sen ningunha dúbida, "deseñar" e "construír" profesionais deste tipo, altamente produtivos, é unha tarefa moi complexa. Obxectivos.: - Adquirir os fundamentos en seguridade necesarios para proporcionar un valor engadido aos nosos futuros profesionais. - As ameazas que sofre a información durante o seu proceso, almacenamento e transmisión son crecentes, multiformes e complexas. Para contrarrestalas desenvolvéronse numerosas medidas de protección, que se implementan mediante os denominados mecanismos de seguridade. A lista destes mecanismos é xa moi numerosa e nela atópase, entre outros moitos: procesos de identificación e autenticación, control de accesos, control de fluxo de información, rexistros de auditoría, cifrado de información, etc. Ser consciente desta realidade, coas súas vantaxes e limitacións, proporcionará aos alumnos unha base para afrontar unha gran parte das implementaciones tecnolóxicas ás que se poidan enfrontar no seu futuro profesional. - Identificar os aspectos relacionados coa seguridade da información, tanto desde o punto de vista técnico como legal, proporcionando as habilidades necesarias para "saber o que hai que facer", "facelo o mellor posible", no menor tempo e cun custo mínimo. Neste contexto será fundamental a exposición e estudo de casos reais, reforzando no alumno a necesidade de utilizar en todo momento o "sentido común", afastando da toma de decisións os moitos perigos e factores que poden "contaminar", total ou parcialmente, moitos dos nosos desenvolvementos. - Analizar os aspectos prácticos da contorna legal no que se desenvolverá a futura actividade profesional dos nosos alumnos, con especial referencia ás súas obrigacións en materia de datos de carácter persoal e seguridade informática. - Un alumno que senta un gran entusiasmo polas tecnoloxías proporcionará ás nosas empresas uns maiores niveis de produtividade, e durante máis tempo. Reforzar esta calidade no alumno, e espertala nos que a poidan ter lixeiramente aletargada será un dos principais obxectivos da materia.

Competencias de la titulación	
Código	Competencias de la titulación
A5	Conocimiento de la estructura, organización, funcionamiento e interconexión de los sistemas informáticos, los fundamentos de su programación, y su aplicación para la resolución de problemas propios de la ingeniería.
A7	Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.
A24	Conocimiento de la normativa y la regulación de la informática en los ámbitos nacional, europeo e internacional.
A36	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
A47	Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

A50	Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.
A58	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
B1	Capacidad de resolución de problemas
B3	Capacidad de análisis y síntesis
B4	Capacidad para organizar y planificar
B5	Habilidades de gestión de la información
B6	Toma de decisiones
B7	Preocupación por la calidad
C3	Utilizar las herramientas básicas de las tecnologías de la información y las comunicaciones (TIC) necesarias para el ejercicio de su profesión y para el aprendizaje a lo largo de su vida.
C4	Desarrollarse para el ejercicio de una ciudadanía abierta, culta, crítica, comprometida, democrática y solidaria, capaz de analizar la realidad, diagnosticar problemas, formular e implantar soluciones basadas en el conocimiento y orientadas al bien común.
C5	Entender la importancia de la cultura emprendedora y conocer los medios al alcance de las personas emprendedoras.
C6	Valorar críticamente el conocimiento, la tecnología y la información disponible para resolver los problemas con los que deben enfrentarse.
C7	Asumir como profesional y ciudadano la importancia del aprendizaje a lo largo de la vida.
C8	Valorar la importancia que tiene la investigación, la innovación y el desarrollo tecnológico en el avance socioeconómico y cultural de la sociedad.

Resultados de aprendizaje			
Competencias de materia (Resultados de aprendizaje)	Competencias de la titulación		
Definir los riesgos y vulnerabilidades de un sistema de información.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C3 C7
Identificar los fundamentos de la certificación digital.	A58		C3
Identificar los mecanismos de seguridad y su integración en las organizaciones.	A5 A7 A47 A50 A58	B1 B6 B7	C3 C7
Utilizar las herramientas de seguridad.			C3
Organizar la seguridad de un sistemas de información.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C3 C7
Asumir responsabilidades sobre los sistemas de información y tomar decisiones en cuanto a su seguridad.	A5 A7 A36 A47 A50 A58	B4 B5 B6	C7
Aplicar el "sentido común" en la toma de decisiones, identificando los muchos peligros y factores que pueden "contaminar", total o parcialmente, muchos de nuestros desarrollos.		B6 B7	C6 C7

Enfrentarse a casos "reales" y "saber lo que hay que hacer", "hacerlo lo mejor posible", en el menor tiempo y con un coste mínimo.	A5 A7 A36 A47 A50 A58	B1 B6 B7	C7
Evitar la proliferación de profesionales mediocres que, en el peor de los casos, se especialicen en la destrucción de todo lo que tocan.		B1 B6 B7	C4 C5 C6 C7 C8
Conocer la regulación legal de la sociedad de la información y de la protección de datos de carácter personal, con especial atención a la seguridad informática.	A7 A24 A47 A58		
Comportarse con ética y responsabilidad social como ciudadano y profesional.			C4
Razonamiento crítico, en especial en relación con los valores y los derechos.	A7 A24 A47	B3 B6	C6
Capacidad para el análisis y la síntesis.		B1 B3 B5 B6	C6

Contenidos	
Tema	**Subtema**
Fundamentos y categorías de ataques.	
La trilogía ("host discovery", "port scanning", "fingerprinting")	
Ocultación.	
?Sniffing?.	
[D]DoS.	
Seguridad a nivel físico.	
Monitorización y filtrado en seguridad de la información.	
Certificados digitales y autoridades de certificación.	
Metodologías y auditorías de seguridad.	
La regulación jurídica de la informática.	- Derecho. Elementos y conceptos jurídicos básicos. - Ética profesional y deontología. - Autorregulación. Códigos de conducta, códigos de práctica, códigos tipo.
La prestación de servicios y la tutela de los derechos en la sociedad de la información.	- La prestación de servicios en la sociedad de la información. Servicios de intermediación. Servicios de certificación. - La contratación electrónica y la contratación informática. - Las comunicaciones comerciales electrónicas. - La firma electrónica. - La Administración electrónica. - La resolución judicial de conflictos. - Las soluciones extrajudiciales. La autorregulación. El arbitraje electrónico.

La protección de los datos de carácter personal.	- Introducción y delimitaciones conceptuales. - Constitución, derechos fundamentales y protección de datos. - La legislación española de protección de datos de carácter personal. Disposiciones generales. Principios. Sujetos. Derechos. Obligaciones. Medidas de seguridad. Procedimientos. - Autorregulación y protección de datos personales. - Criminalidad informática y datos personales.
Temario Prácticas y Seminarios.	- Seguridad (fundamentos y configuraciones básicas). - Categorías de ataques e identificación de recursos. - Seguridad a nivel físico. - Autoridades de certificación - Auditorías de seguridad.

Planificación			
Metodologías / pruebas	Horas presenciales	Horas no presenciales / trabajo autónomo	Horas totales
Prácticas de laboratorio	18	27	45
Prueba de respuesta múltiple	0.5	0	0.5
Sesión magistral	27	40.5	67.5
Seminario	10	15	25
Análisis de fuentes documentales	3	3.6	6.6
Estudio de casos	2	2.4	4.4
Atención personalizada	1	0	1
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos			

Metodologías	
Metodologías	Descripción
Prácticas de laboratorio	Las clases prácticas permiten sacar el máximo provecho en la retroalimentación, refuerzo y asimilación de los objetivos. Los desarrollos prácticos se inician con una práctica básica, y se eleva su dificultad paulatinamente. En todo momento se presenta al alumno el conjunto de ideas y técnicas que permiten el desarrollo práctico de los conocimientos transmitidos en las sesiones magistrales. En las prácticas se proponen diversos apartados que plantean una batería de dificultades tratadas durante el estudio del tema. Se buscará la interrelación entre los distintos apartados, aportando un contexto de ejercicio completo, para lograr en el alumno una visión de conjunto, revelando los nexos existentes entre cuestiones que podrían parecer lejanas. En todas las clases prácticas se utilizan máquinas virtuales sobre computadoras como herramienta básica para la resolución de los ejercicios. El alumno podrá seleccionar e instalar aquellas herramientas que considere más oportunas en cada caso. De esta forma, se le requerirá, desde un primer momento, que se enfrente a toma de decisiones, analizando las ventajas y desventajas en todos y cada uno de los casos. En este punto inicial, será fundamental un asesoramiento personalizado, que permita un análisis realista sobre las decisiones tomadas, facilitando la retroalimentación de nuevos parámetros no considerados a priori.
Prueba de respuesta múltiple	Esta prueba estará orientada a determinar si el alumno ha asimilado los distintos objetivos de la asignatura.

Sesión magistral	Transmisión de información y conocimientos clave de cada uno de los temas. Se potencia en ciertos momentos la participación del alumno. Como parte de la metodología, un enfoque crítico de la disciplina llevará a los alumnos a reflexionar y descubrir las relaciones entre los diversos conceptos, formar una mentalidad crítica para afrontar los problemas y la existencia de un método, facilitando el proceso de aprendizaje en el alumno. También será fundamental la transmisión de los conceptos y conocimientos éticos y jurídicos básicos en seguridad de la información. Su singularidad hace que se dedique cierto tiempo a la exposición del lenguaje específico que soporta los conceptos, y que sirve de principal medio de comunicación y argumentación ética y jurídica. Esto permitirá al alumno comprender el lenguaje y los conceptos que integran los aspectos éticos y jurídicos de la informática. Para luchar contra la posible pasividad del alumno, en ciertos momentos se plantean pequeñas cuestiones, que hagan reflexionar al alumno, complementando dichos aspectos con referencias bibliográficas que le permitan enriquecer el conocimiento adquirido. Este intercambio con el alumno, como parte de la lección magistral, nos permite controlar el grado de asimilación de los conocimientos por parte del mismo. Las lecciones magistrales incluyen, tanto conocimientos extraídos de las referencias de la asignatura, como los resultantes de nuestras propias experiencias profesionales, fomentando la capacidad de análisis crítico. En todo momento se busca que cierta parte de los contenidos aportados no requieran del alumno una tarea de memorización. Esta metodología tratará de conseguir un alto grado de motivación en el alumno.
Seminario	Los seminarios se configurarán como una extensión de las prácticas de laboratorio. A diferencia de estas, se potenciará el desarrollo práctico en grupos, frente al trabajo individual en las prácticas de laboratorio. El trabajo en común con los alumnos nos permitirá valorar el progreso de la clase hacia los objetivos marcados.
Análisis de fuentes documentales	Lectura y examen crítico de los principales documentos éticos y jurídicos de la informática. Sirven de introducción general a los temas. Proporcionan una explicación histórica y sistemática de su significado. Son de gran importancia en el contexto del resto de metodologías utilizadas en la asignatura.
Estudio de casos	El análisis ético y jurídico de la informática tiene unas características específicas. Con el estudio de casos se pretende examinar la estructura y los contenidos de los problemas presentes en los casos, tanto de manera individual como en grupo. Es una forma de aprendizaje de contenidos y también metodológica, en la que el estudiante aprende a analizar, deliberar y llegar a conclusiones fundamentadas y razonables con los argumentos éticos y jurídicos. Resulta de gran utilidad para ejercitar las destrezas y habilidades argumentativas.

Atención personalizada	
Metodologías	**Descripción**
Seminario Prácticas de laboratorio	Prácticas de laboratorio.: Se guía al alumno de forma individualizada en el desarrollo de cada una de las prácticas de laboratorio. Aunque en el desarrollo de la primera práctica existen grandes diferencias en las necesidades de cada alumno, progresivamente se van homogeneizando en cuanto a sus necesidades de atención personalizada. Sin ninguna duda, la identificación de este parámetro es fundamental para determinar que la totalidad de los alumnos progresa durante el desarrollo de la materia. Seminarios.: Mediante el trabajo conjunto en desarrollos prácticos con pequeños grupos formados en cada seminario. Atención personalizada.: Toda cuestión tecnológica expuesta por el alumno, en persona, tutorías, email., etc.

Evaluación		
Metodologías	**Descripción**	**Calificación**

Seminario	Cada grupo formado en los seminarios, y tras considerar que ha superado cada ejercicio propuesto, deberá pasar una pequeña prueba oral. También se plantearán pequeñas cuestiones, que hagan reflexionar al alumno, y nos permitan controlar el grado de asimilación de los conocimientos por parte del mismo.	10
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio, y tras considerar que ha superado cada práctica, siempre antes del plazo establecido para cada práctica-seminario, deberá pasar una pequeña prueba oral. En ella el profesor plantea un par de pequeñas pruebas que los alumnos deberán resolver sobre las máquinas virtuales del laboratorio de prácticas, defendiendo sus desarrollos de forma oral.	20
Sesión magistral	Para luchar contra la posible pasividad del alumno, en ciertos momentos de las sesiones magistrales se plantean pequeñas cuestiones, que hagan reflexionar al alumno. Este intercambio con el alumno, como parte de la lección magistral, nos permite controlar el grado de asimilación de los conocimientos por parte del mismo. Para potenciar la participación de alumno estás cuestiones tienen asignado una pequeña puntuación, según el grado de dificultad (puntuación complementaria fuera de guía).	0
Prueba de respuesta múltiple	Esta prueba incluye los contenidos y, en general, todo aspecto relacionado con los objetivos de la asignatura. En ella se plantean diversas cuestiones relacionadas tanto con los contenidos de las sesiones magistrales como de las prácticas de laboratorio, dándole un mayor peso a las primeras.	70
Otros		

Observaciones evaluación
Para aprobar la asignatura será necesario tener superadas las prácticas de laboratorio y los seminarios. En la convocatoria de julio, en su defecto, a la prueba de respuesta múltiple se le añadirá una prueba de la parte práctica, que deberá ser superada por separado.

Fuentes de información	
Básica	- Lorenzo COTINO, Julián VLAERO (coords.) (2010). Administración electrónica. Valencia: Tirant lo Blanch - Gonzalo F. GÁLLEGO HIGUERAS (2010). Código de Derecho informático y de las nuevas tecnologías. Madrid: Civitas - Javier ORDUÑA, Gonzalo AGUILERA (dir.) (2009). Comercio, Administración y Registros electrónicos. Madrid: Civitas - Manuel CASTELLS (2009). Comunicación y poder. Madrid: Alianza - (). Criptored. http://www.criptored.upm.es/ - debian.org (). Debian. http://www.debian.org/ - José Luis PIÑAR MAÑAS (dir.) (2011). electrónica y ciudadanos. Madrid: Civitas - José APARICIO SALOM (2009). Estudio sobre la Ley Orgánica de protección de datos de carácter personal. Pamplona: Aranzadi - Antonio TRONCOSO (2010). La protección de datos personales. En busca del equilibrio. Valencia: Tirant lo Blanch - A. Santos del Riego (). Legislación [Protección] y Seguridad de la Información. http://psi-udc.blogspot.com - Miguel Ángel DAVARA RODRÍGUEZ (2008). Manual de Derecho informático. Pamplona: Aranzadi - Willian Stallings (2014). Network Security Essentials. Applications and Standards. Prentice Hall - Packet Storm (). Packet Storm. http://packetstormsecurity.org/ - Miguel PEGUERA POCH (coord.) (2010). Principio de Derecho de la sociedad de la información. Cizur Menor: Aranzadi - yolinux (). yolinux. http://www.yolinux.com/

Complementária	- (). (in)secure magazine. http://www.net-security.org/insecure-archive.php - (). AntiOnline. http://www.antionline.com/ - (). CERT:Computer Emergence Response Team. http://www.cert.org - (). Common Vulnerabilities and Exposures (CVE). http://www.cve.mitre.org/ - (). Delitos Informáticos. http://www.delitosinformaticos.com/ - Pedro DE MIGUEL ASENSIO (2011). Derecho privado de internet. Madrid: Civitas - Lawrence LESSIG (2001). El código y otras leyes del ciberespacio. Madrid, Taurus - Fernando MIRÓ LLINARES (2005). Internet y delitos contra la propiedad intelectual. Valencia: Tirant lo Blanch - Esther MORÓN LERMA (2002). Internet y Derecho penal. Pamplona: Aranzadi - Pekka HIMANEN (2002). La ética del hacker y el espíritu de la era de la información. Barcelona, Destino - Antoni FARRIOLS I SOLA (2006). La protección de datos de carácter personal en los centros de trabajo. Madrid: Cinca - Justo GÓMEZ NAVAJAS (2005). La protección de los datos personales. Cizur Menor, Thomson Civitas - (). Linux Journal. http://www.linuxjournal.com/ - (). NIST Computer Security Division. http://csrc.nist.gov/ - (). Security art work. http://www.securityartwork.com/ - (). Security by default. http://www.securitybydefault.com/ - (). Security Focus. http://www.securityfocus.com/

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías