Teaching Guide					
Identifying Data					2015/16
Subject (*)	Protección e Seguridade da Información			Code	614111637
Study programme	Enxeñeiro en Informática				
Descriptors					
Cycle	Period	Year		Type	Credits
First and Second Cycle	2nd four-month period	All		Optativa	4
Language	Spanish				
Teaching method	Face-to-face				
Prerequisites					
Department	Tecnoloxías da Información e as Comunicacións				
Coordinador	Santos Del Riego, Antonino		E-mail	antonino.santos@udc.es	
Lecturers	Santos Del Riego, Antonino		E-mail	antonino.santos@udc.es	
Web	psi-udc.blogspot.com/				

General description	Es a finales de los ochenta, principalmente por el uso de la red Internet, cuando la protección y seguridad de la información se transforma en una necesidad. A finales de los 90 las amenazas a los sistemas ?abiertos? a la red Internet se generalizan y la protección y seguridad de la información toma una gran relevancia. En la actualidad, las empresas y la sociedad en general demandan progresivamente un mayor número de expertos en seguridad informática. Hoy en día un profesional de las tecnologías de la información y las comunicaciones, tanto del ámbito de los sistemas como del desarrollo software, sin unos buenos fundamentos en seguridad, estará claramente devaluado. Nuestra profesión no consiste únicamente en la administración de sistemas y desarrollo de software y hardware. En otras palabras, un programa o sistema que simplemente funciona, sin considerar el factor seguridad, puede suponer un gran peligro para una organización. El apagar y encender una máquina puede arreglar un problema, el análisis de las causas y la búsqueda de soluciones constituye una clara diferencia entre un buen y mal profesional. En la asignatura de Protección y Seguridad de la Información, optativa de segundo cuatrimestre, se proporciona al alumno unos fundamentos en seguridad de la información, y con ello un valor añadido sobre otros profesionales del sector. En todo momento nos centramos en aquellos aspectos de interés para su futuro profesional, intentado llevar los contenidos de la asignatura hacia los temas y entornos de relevancia para el mundo empresarial. De nada me sirve que un alumno ?comprenda? el esquema de funcionamiento de los distintos tipos de cortafuegos, si posteriormente no es capaz de hacer una buena configuración sobre alguno de ellos. Nuestra profesión se centra en ?hacer?, no únicamente en ?saber hacer?, y a ser posible en ?hacerlo lo mejor posible?. Y, ¿qué nos piden las empresas?, claramente profesionales que sepan lo que hay que hacer, que lo hagan bien, en el menor de los tiempos y con un coste mínimo. Un profesional en estas condiciones estará en la mejor situación para demandar un salario acorde. Sin duda alguna, ?diseñar? y ?construir? profesionales de este tipo, altamente productivos, es una tarea muy compleja. Pero bueno, no debería ser docente quien no esté dispuesto a intentarlo. Objetivos.: - Adquirir los fundamentos en seguridad necesarios para proporcionar un valor añadido a nuestros futuros profesionales. - Las amenazas que sufre la información durante su proceso, almacenamiento y transmisión son crecientes, multiformes y complejas. Para contrarrestarlas se han desarrollado numerosas medidas de protección, que se implementan mediante los denominados mecanismos de seguridad. La lista de estos mecanismos es ya muy numerosa y en ella se encuentra, entre otros muchos: procesos de identificación y autenticación, control de accesos, control de flujo de información, registros de auditoría, cifrado de información, etc. Sin duda alguna, el mecanismo por excelencia es el de cifrado de la información, que en la forma de protocolos seguros se integra en todo tipo de entornos tecnológicos. Ser consciente de esta realidad, con sus ventajas y limitaciones, proporcionará a los alumnos una base para afrontar una gran parte de las implementaciones tecnológicas a las que se puedan enfrentar en su futuro profesional. - Identificar los aspectos relacionados con la protección y seguridad de la información, proporcionando las habilidades necesarias para ?saber lo que hay que hacer?, ?hacerlo lo mejor posible?, en el menor tiempo y con un coste mínimo. En este contexto será fundamental la exposición y estudio de casos reales, reforzando en el alumno la necesidad de utilizar en todo momento el ?sentido común?, alejando de la toma de decisiones los muchos peligros y factores que pueden ?contaminar?, total o parcialmente, muchos de nuestros desarrollos. - Un alumno que sienta un gran entusiasmo por las tecnologías proporcionará a nuestras empresas unos mayores niveles de productividad, y durante más tiempo. Reforzar esta cualidad en el alumno, y despertarla en los que la puedan tener ligeramente aletargada será uno de los principales objetivos de la asignatura. - Evitar la proliferación de profesionales mediocres que, en el peor de los casos, destruyan todo lo que toquen.

Study programme competences / results	
Code	Study programme competences / results
A1	Aprender de maneira autónoma novos coñecementos e técnicas avanzadas axeitadas para a investigación, o deseño e o desenvolvemento de sistemas e servizos informáticos.
A3	Concibir e planificar o desenvolvemento de aplicacións informáticas complexas ou con requisitos especiais.

A4	Coñecer e aplicar diferentes protocolos de comunicación e sistemas de xestión de rede.
A8	Concibir, despregar, organizar e xestionar un servizo informático complexo.
A9	Dirixir equipos de traballo ligados ao deseño de produtos, procesos, servizos informáticos e outras actividades profesionais.
A10	Saber especificar, deseñar e implementar unha política de seguridade no sistema.
A12	Coñecer a regulación legal da profesión e os seus aspectos éticos, en particular os ligados á propiedade intelectual e á protección de datos.
B1	Aprender a aprender.
B2	Resolver problemas de forma efectiva.
B3	Aplicar un pensamento crítico, lóxico e creativo.
B4	Aprendizaxe autónoma.
B5	Traballar de forma colaborativa.
B6	Comportarse con ética e responsabilidade social como cidadán e como profesional.
B7	Comunicarse de maneira efectiva en calquera contorno de traballo.
B8	Traballar en equipos de carácter interdisciplinar.
B9	Capacidade para tomar decisións.
B10	Capacidade de xestión da informática (captación e análises da información).
B11	Razoamento crítico.
B12	Capacidade para a análise e a síntese.
B13	Capacidade de comunicación.
B14	Coñecemento de idiomas.
B15	Motivación pola calidade.
C1	Expresarse correctamente, tanto de forma oral coma escrita, nas linguas oficiais da comunidade autónoma.
C2	Dominar a expresión e a comprensión de forma oral e escrita dun idioma estranxeiro.
C3	Utilizar as ferramentas básicas das tecnoloxías da información e as comunicacións (TIC) necesarias para o exercicio da súa profesión e para a aprendizaxe ao longo da súa vida.
C4	Desenvolverse para o exercicio dunha cidadanía aberta, culta, crítica, comprometida, democrática e solidaria, capaz de analizar a realidade, diagnosticar problemas, formular e implantar solucións baseadas no coñecemento e orientadas ao ben común.
C5	Entender a importancia da cultura emprendedora e coñecer os medios ao alcance das persoas emprendedoras.
C6	Valorar criticamente o coñecemento, a tecnoloxía e a información dispoñible para resolver os problemas cos que deben enfrontarse.
C7	Asumir como profesional e cidadán a importancia da aprendizaxe ao longo da vida.
C8	Valorar a importancia que ten a investigación, a innovación e o desenvolvemento tecnolóxico no avance socioeconómico e cultural da sociedade.

Learning outcomes			
Learning outcomes	Study programme competences / results		
Definir los riesgos y vulnerabilidades de un sistema de información.	A1 A10 A12	B10	
Identificar los fundamentos de los criptosistemas.	A4 A8	B10 B12	C3
Identificar los mecanismos de seguridad y su integración en las organizaciones.	A3 A8 A10 A12	B2 B3 B6 B8 B9 B10	C3 C6

Utilizar las herramientas de seguridad	A1 A4	B2 B4 B5 B6 B9 B10 B14	C3 C6
Organizar la seguridad de un sistema de información.	A8 A10 A12	B2 B6 B9 B10 B15	C3 C6
Asumir responsabilidades sobre los sistemas de información y tomar decisiones en cuanto a su seguridad.	A9 A12	B3 B6 B7 B9 B15	C4
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.		B2 B3 B6 B7 B9 B10 B15	C4 C6
Enfrentarse a casos ?reales? y ?saber lo que hay que hacer?, ?hacerlo lo mejor posible?, en el menor tiempo y con un coste mínimo.	A3 A8 A10 A12	B2 B3 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15	C1 C2 C3 C4 C5 C6 C7 C8

Evitar la proliferación de profesionales mediocres que, en el peor de los casos, se especialicen en la destrucción de todo lo que tocan.		B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15	C1 C2 C3 C4 C5 C6 C7 C8

Contents	
Topic	**Sub-topic**
Fundamentos.	- Fundamentos de protección y seguridad. - Categorías de ataques. - Ejemplo de categoría de ataque ("sniffing" en redes). - Detección de entidades.
Fundamentos de *virtualización.	
Registro de auditorías.	
Metodologías de seguridad existentes.	
Seguridad a nivel físico.	
Seguridad y dispositivos de almacenamiento.	
Fundamentos de alta disponibilidad, "clustering" y balanceo de carga.	
Fundamentos de "malware".	
Criptografía.	- Hacia la criptografía (cifrado de paquetes, cifrado de servicios y cifrado de datos). - Sistemas criptográficos ?modernos?. - Firma Digital y Autoridades Certificadoras. - Protocolos ?más o menos seguros?. - Control de accesos.
Temario Prácticas.	- Seguridad en el subsistema de red (configuración básica). - Ataque y defensa de la confidencialidad de la red (sniffing). - Seguridad en los dispositivos de almacenamiento. - Protocolos ?más o menos seguros?.

Planning				
Methodologies / tests	**Competencies / Results**	**Teaching hours (in-person & virtual)**	**Student?s personal work hours**	**Total hours**
Laboratory practice		30	22.5	52.5
Multiple-choice questions		1	0	1
Guest lecture / keynote speech		30	30	60
Speaking test		1	0	1
Events academic / information		5	0	5
Personalized attention		1	0	1
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	**Description**
Laboratory practice	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. Al tratarse de una asignatura de segundo y tercer curso, los ejercicios proponen diversos apartados que planteen 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 tomas 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. Finalmente, señalar que las prácticas de laboratorio se desarrollan en grupos de dos alumnos, siendo el profesor el encargado de definirlos. Esta asignación de grupos introducirá al alumno en el mundo de las relaciones laborales con sus compañeros, aspecto de gran importancia para su futuro profesional.
Multiple-choice questions	Esta prueba estará orientada a determinar si el alumno ha asimilado los distintos objetivos de la asignatura.
Guest lecture / keynote speech	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. 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, me permite controlar el grado de asimilación de los conocimientos por parte del mismo. Las lecciones magistrales incluyen, tanto conocimientos extraídos de las fuentes bibliográficas, como los resultantes de mi propia experiencia profesional, fomentando la capacidad de análisis crítico. En todo momento busco que gran parte de los contenidos aportados no requieran del alumno una tarea de memorización. Por las peculiaridades de la materia de protección y seguridad de la información, claramente al alumno le resultaría desalentador el estudio de la misma sin la asistencia del profesor, principalmente por tratarse de alumnos de segundo y tercer curso. Además, la utilización de gran cantidad de fuentes de información, y de la propia experiencia permite ofrecer una visión muy equilibrada de los conocimientos, difícil de obtener directamente de la gran cantidad de libros y, en general, fuentes de información, en dicha materia. Sin duda alguna, esta metodología es muy adecuada para tratar de conseguir un alto grado de motivación en el alumno.
Speaking test	El alumno deberá defender, mediante una prueba oral, cada una de las prácticas de laboratorio. Dicha prueba, de carácter práctico, hará uso de las máquinas virtuales utilizadas en las prácticas de laboratorio.
Events academic / information	Sin duda alguna, todo evento científico-divulgativo, especialmente en temas de seguridad de la información, será una valiosa herramienta para la obtención de los objetivos de la asignatura. Señalar que este tipo de eventos son de especial relevancia en el proceso de motivación en el alumno. Además, esta metodología permite establecer un contacto directo entre los alumnos y los profesionales del sector. De esta forma el alumno puede perfilar distintos aspectos de nuestra realidad profesional.

Personalized attention	
Methodologies	**Description**

Laboratory practice	Prácticas de laboratorio.: Se guía al alumno de forma individualizada en el desarrollo de cada uno de las prácticas de laboratorio. Si bien 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 duda alguna, la identificación de este parámetro es fundamental para determinar que la totalidad de los alumnos progresa durante el desarrollo de la asignatura. Atención personalizada.: Toda cuestión tecnológica planteada por el alumno.

Assessment			
Methodologies	Competencies / Results	Description	Qualification
Multiple-choice questions		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.	100
Guest lecture / keynote speech		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, me 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.	10
Speaking test		Cada grupo de prácticas de laboratorio, y tras considerar que ha superado cada práctica, 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. El mundo de la seguridad de la información está directamente vinculado a un esquema de ataque-defensa.	10
Others			

Assessment comments

Sources of information	
Basic	- (). Cotse net. http://www.cotse.com/ - William Stalling (2004). Fundamentos de Seguridad en Redes. Aplicaciones y estándares. Pearson - (). Packet Storm. http://packetstorm.linuxsecurity.com/ - A. Santos del Riego (2008). Protección y Seguridad de la Información. http://psi-udc.blogspot.com Â

Complementary	- (). AntiOnline. http://www.antionline.com/ - (). Centro de alerta temprana sobre virus y seguridad informática. http://alerta-antivirus.inteco.es/portada/index.php - (). CERT:Computer Emergence Response Team. http://www.cert.org - (). Cisco security. http://www.cisco.com/en/US/products/hw/vpndevc/index.html - (). Common Vulnerabilities and Exposures (CVE). http://www.cve.mitre.org/ - (). Criptored. http://www.criptored.upm.es - (). Delitos Informáticos. http://www.delitosinformaticos.com/ - (). Dr Dobb's Journal. http://www.ddj.com - (). Implementaciones software de algoritos criptográficos. ftp://ftp.funet.fi/pub/crypt/cryptography - (). NIST Computer Security Division. http://csrc.nist.gov/ - (). Security Focus. http://www.securityfocus.com/ - (). vLex: Editorial Jurídica en Internet. http://www.vlex.com

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments
Protección y Seguridad de la Información se podría impartir tanto en segundo como tercero.

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.