Guia docente				
Datos Identificativos				2013/14
Asignatura (*)	Seguridad en los sistemas Informáticos		Código	614G01079
Titulación	Grao en Enxeñaría Informática			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Grado	1º cuatrimestre	Cuarto	Obligatoria	6
Idioma	Castellano			
Prerrequisitos				
Departamento	Tecnoloxías da Información e as Comunicacións			
Coordinador/a	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es	
Profesorado	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es	
Web	campusvirtual.udc.es			
Descripción general	La seguridad en los sistemas de información es crucial en todos y cada uno de los servicios ofertados por la denominada sociedad de la información. Incluso en este ámbito, todavía en desarrollo, los requisitos de seguridad cambian a un ritmo vertiginoso. Puesto que cada vez más información está accesible, cada vez se requieren controles de seguridad más estrictos. El avance tecnológico en este caso funciona de catalizador en ambas direcciones: por un lado favorece el acceso a nuevos tipos y a mayor cantidad de información (lo que requiere un aumento de los controles de seguridad) y por otro lado posibilita la implantación de mecanismos de seguridad más refinados (que posibilitan el acceso seguro a nuevos tipos de información). La asignatura está planteada para proporcionar al alumno el conocimiento necesario de los conceptos básicos y técnicas empleadas para la protección de los sistemas de información, desde el punto de vista físico, lógico y administrativo. Estos conceptos básicos incluirán, como paso de inicio, la evolución de los diferentes métodos y algoritmos de cifrado. Debido al enorme auge de los diversos medios electrónicos de intercambio de información (correo electrónico, páginas web, e-commerce, firma digital, etc.) un aspecto fundamental cuando se trabaja en este ámbito será tener la formación suficiente en la seguridad de este tipo de sistemas. Para el correcto funcionamiento de los servicios referidos se exige la existencia de una infraestructura (redes de comunicaciones y sistemas operativos) que funcione de modo seguro y confiable. Por lo tanto será necesario conocer los aspectos fundamentales de los componentes, protocolos de funcionamiento, configuración, etc. de dicha infraestructura. Dichos conocimientos serán los que le permitan entender y solucionar los riesgos actuales, y los que inevitablemente surgirán en el futuro, que afectan a todo sistema de información. Objetivos: - Familiarizarse con el proceso de la seguridad - Identificar los riesgos de los sistemas de información - Conocer distintos mecanismos para dotar de seguridad a un sistema de información - Comprender los conceptos fundamentales de la criptografía - Entender qué es, cómo se define y cómo se aplica una política de seguridad			

Competencias de la titulación	
Código	Competencias de la titulación
A4	Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.
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.
A6	Conocimiento adecuado del concepto de empresa, marco institucional y jurídico de la empresa. Organización y gestión de empresas.

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.
A11	Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas.
A14	Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.
A16	Conocimiento de las características, funcionalidades y estructura de los sistemas operativos y diseñar e implementar aplicaciones basadas en sus servicios.
A24	Conocimiento de la normativa y la regulación de la informática en los ámbitos nacional, europeo e internacional.
A29	Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
A36	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
A38	Capacidad para diseñar, desplegar, administrar y gestionar redes de computadores.
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
B2	Trabajo en equipo
B3	Capacidad de análisis y síntesis
B4	Capacidad para organizar y planificar
B5	Habilidades de gestión de la información
B7	Preocupación por la calidad
B8	Capacidad de trabajar en un equipo interdisciplinar
C1	Expresarse correctamente, tanto de forma oral como escrita, en las lenguas oficiales de la comunidad autónoma.
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.
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.

Resultados de aprendizaje			
Competencias de materia (Resultados de aprendizaje)	Competencias de la titulación		
Resumir los fundamentos de los criptosistemas	A5 A7 A29 A36 A47 A50 A58	B5 B7	
Definir los riesgos y vulnerabilidades de un sistema de información	A4 A6 A7 A11 A14 A16	B2 B3 B7 B8	C1 C3 C6
Analizar los nuevos avances en seguridad y sus repercusiones		B3 B7	C6 C7

Utilizar las herramientas de seguridad	A11 A24 A38 A58		C3
Organizar la seguridad de un sistema de información	A7 A36 A47 A58		C3
Expresar de forma clara y efectiva la necesidad, implantación, ventajas y desventajas de las medidas de seguridad		B2 B3 B7	C1 C3
Asumir la existencia de vulnerabilidades en los sistemas de información e intentar su minimización			C4 C6
Colaborar con otros profesionales (administradores de sistemas, redes, bases de datos, aplicaciones, etc.) en la puesta en marcha y mantenimiento de las medidas de seguridad		B1 B2 B4	

Contenidos	
Tema	**Subtema**
Análisis de Riesgos y Medidas de Seguridad	Análisis de Riesgos Gestión del Riesgo Medidas de Seguridad
Criptografía	Sistemas criptográficos clásicos Sistemas criptográficos de clave secreta Sistemas criptográficos de clave pública Firma digital
Malware	Virus Troyanos Rootkits Exploits
Análisis forense	Fases del Análisis Forense Herramientas HW y SW
Normativa	ISO 27001
Estudios de casos	Estudio de casos reales de ataques a sistemas de información.
Prácticas	Prueba de distintas herramientas de seguridad, relacionadas con los temas de teoría.

Planificación			
Metodologías / pruebas	**Horas presenciales**	**Horas no presenciales / trabajo autónomo**	**Horas totales**
Sesión magistral	15	22.5	37.5
Prácticas de laboratorio	12	24	36
Seminario	7.5	15	22.5
Trabajos tutelados	3	18	21
Estudio de casos	3	3	6
Presentación oral	5	5	10
Prueba mixta	1.5	7.5	9
Eventos científicos y/o divulgativos	2	0	2
Atención personalizada	6	0	6
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos			

Metodologías	
Metodologías	**Descripción**
Sesión magistral	Introducción conceptos y aspectos clave de cada uno de los temas
Prácticas de laboratorio	Búsqueda información para los trabajos tutelados y realización de trabajos de apoyo a la teoría.
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.
Trabajos tutelados	Trabajos académicos relativos al contenido teórico de la asignatura
Estudio de casos	Estudio de casos reales de temas relacionados con la seguridad de sistemas
Presentación oral	Presentación trabajos tutelados
Prueba mixta	Realización examen
Eventos científicos y/o divulgativos	Asistencia a eventos de interés (conferencias, seminarios, etc.)

Atención personalizada	
Metodologías	**Descripción**
Trabajos tutelados Prácticas de laboratorio Seminario	Resolución de dudas. Tutorización personalizada trabajos individuales.

Evaluación		
Metodologías	**Descripción**	**Calificación**
Trabajos tutelados	Realización de trabajos tutelados: Criterios evaluación: calidad trabajos y presentaciones, participación activa en las defensas de los compañeros, actitud	20
Prácticas de laboratorio	Realización de prácticas Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica	20
Prueba mixta	Asimilación de Conceptos Teóricos, relativos a los bloques de teoría, prácticas de laboratorio y trabajos tutelados). Nota mínima exigida: 5	50
Seminario	Realización de prácticas en grupos reducidos Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica	10
Otros		

Observaciones evaluación

<p> El proceso de evaluación será continuo a lo largo de la realización de la materia. La evaluación se compondrá de varios apartados distintos: asimilación conceptos teóricos, realización de prácticas y exposición de trabajos que se valorarán según la ponderación indicada a continuación.

La nota final de la asignatura vendrá determinada por una evaluación ponderada de los tres bloques que formoan parte de ella:

1) El 45% de la nota vendrá dada por la realización de los trabajos tutelados. Los criterios a valorar serán la calidad de los trabajos presentados, la claridad y calidad de las presentaciones realizda, la participación activa en las defensas de los trabajos de los compañeros o la actitud

2) El 35% de la nota vendrá dada por las prácticas de laboratorio. Se perseguirá realizar una evaluación continua, o en todo caso, valorar el aprovechamiento de las horas de laboratorio y la defensa de las prácticas realizadas.

3) El 20% restante de la nota vendrá dado por la realización de un examen teórico. En este examen, tipo test, se valorará la asimilación de los contenidos de la asignatura, mediante preguntas relativas a los bloques de teoría, práctica y trabajos tutelados. Será necesaria una nota mínima de un 5 en este examen para poder aprobar la asignatura.

</p>

Fuentes de información	
Básica	- Jorge Ramió (1999). Aplicaciones Criptográficas. UPM - S. Harris (2010). CISSP All in one. 5ª Edición. Mc-Graw Hill - W. Stallings (2004). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. 2ª Edición. Pearson Educación - M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). Official ISC2 Guide to the SSCP CBK. 2ª Edición. Ed. Harold F. Tripton
Complementária	- Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://wwwdi.ujaen.es/~mlucena - Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly - Information Security Forum (). The Standard of good Practice for Information Security. http://www.isfsecuritystandard.com

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Legislación y Seguridad Informática/614G01024
Otros comentarios
Otros materiales de apoyo: Se proporcionarán al alumno las diapositivas empleadas para el desarrollo de las clases, así como referencias bibliográficas en las que pueda profundizar en el estudio de determinados puntos del temario.