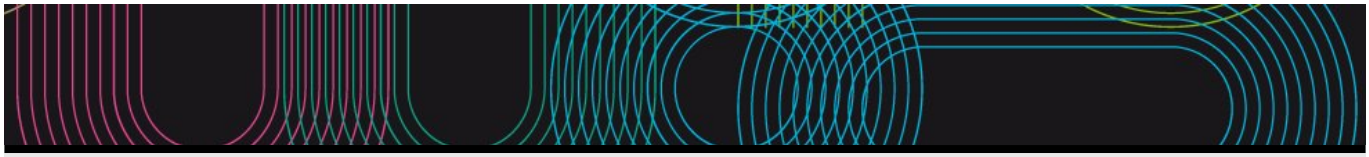

DATOS IDENTIFICATIVOS				
Seguridad en sistemas informáticos				
Asignatura	Seguridad en sistemas informáticos			
Código	O06G150V01702			
Titulacion	Grado en Ingeniería Informática			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	4	1c
Lengua Impartición	Gallego			
Departamento	Informática			
Coordinador/a	Ribadas Pena, Francisco Jose			
Profesorado	Ribadas Pena, Francisco Jose			
Correo-e	ribadas@uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	(*)A materia "Seguridade en Sistemas Informáticos" ubícase no cuarto curso do Grao en Enxeñería Informática. Trátase dunha materia obrigatoria que pretende integrar, complementar e ampliar competencias e contidos relacionados coa seguridade informática xa traballados polos alumnos noutras materias previas relacionadas cos sistemas operativos e coas redes de computadoras. Dado que a seguridade informática é un campo moi amplo e variado, o obxectivo fundamental da materia é servir de introducción a esta rama da informática e dar unha visión xeral, á vez que práctica, dos aspectos máis relevantes da seguridade informática, de xeito que sirvan ao alumno como punto de partida no caso de que decida orientar a súa carreira profesional neste campo.			

Competencias de titulación	
Código	
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
A29	Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse
A32	Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados
A34	Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización
A37	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
B1	Capacidad de análisis, síntesis y evaluación
B7	Capacidad de buscar, relacionar y estructurar información proveniente de diversas fuentes y de integrar ideas y conocimientos
B8	Resolución de problemas
B9	Capacidad de tomar decisiones
B10	Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones
B11	Capacidad de actuar autónomamente
B12	Capacidad de trabajar en situaciones de falta de información y/o bajo presión
B13	Capacidad de integrarse rápidamente y trabajar eficientemente en equipos unidisciplinares y de colaborar en un entorno multidisciplinar
B16	Razonamiento crítico
B17	Compromiso ético y democrático
B18	Aprendizaje autónomo
B19	Adaptación a nuevas situaciones
B20	Creatividad
B21	Liderazgo
B22	Tener iniciativa y ser resolutivo
B23	Espíritu emprendedor y ambición profesional
B24	Tener motivación por la calidad y la mejora continua

Competencias de materia		
Resultados previstos en la materia	Resultados de Formación y Aprendizaje	
(*)Coñecer o papel da seguridade dentros dos sistemas de información	A7 A29 A32 A34 A37	B1 B7 B16
(*)Coñecer os fundamentos da criptografía moderna e aplicar os métodos criptográficos na protección dos datos.	A29 A32 A37	B1 B7 B8 B10 B16 B18 B20 B22
(*)	A7 A29 A32 A34 A37	B1 B7 B8 B9 B10 B11 B12 B16 B17 B18 B19 B20 B21 B22 B24
(*)Xestionar unha rede informática dun xeito seguro, identificando as vulnerabilidades típicas e empregando as técnicas e ferramentas axeitadas.	A7 A29 A32 A34 A37	B1 B7 B8 B9 B10 B11 B12 B13 B16 B17 B18 B19 B20 B21 B22 B24
(*)Coñecer as vulnerabilidades e os tipos de ataques informáticos máis habituais e as técnicas e ferramentas para protexerse dos mesmos.	A7 A29 A34 A37	B1 B11 B12 B13 B16 B18 B19 B20 B22 B24

(*)Saber xetionar un incidente de seguridade conforme a recomendacións e boas prácticas establecidas.	A7 A29 A37	B1 B8 B9 B10 B11 B12 B16 B17 B18 B19 B20 B21 B22 B23 B24

Contenidos	
Tema	
(*)TEMA 1. Contexto da seguridade nos sistemas informáticos	(*)1.1 Conceptos e terminoloxía 1.2 Niveis da seguridade: física, lóxica, organizativa 1.3 Normas e recomendacións
(*)BLOQUE I. Seguridade da información	(*).
(*)TEMA 2. Criptografía	(*)2.1 Fundamentos e evolución 2.2 Cifrado simétrico 2.3 Cifrado asimétrico 2.4 Infraestructuras criptográficas: certificados, firma dixital, PKI
(*)TEMA 3. Seguridade no desenvolvemento de aplicacións	(*)3.1 Tipos de vulnerabilidades e amenazas no sotfware 3.2 Explotación de vulnerabilidades 3.3 Programación segura
(*)BLOQUE II. Seguridade en sistemas operativos	(*).
(*)TEMA 4. Administración segura de SS.OO.	(*)4.1 Mecanismos de autenticación. 4.2 Ferramentas de monitorización 4.3 Vulnerabilidades típicas 4.4 Resposta ante incidentes
(*)BLOQUE III. Seguridade en redes	(*).
(*)TEMA 5. Protocolos seguros	(*)5.1 Vulnerabilidades en redes TCP/IP 5.2 Seguridade a nivel de rede: IPSec 5.3 Seguridade a nivel de transporte: SSL/TLS 5.4 Seguridade a nivel de aplicación: SSH
(*)TEMA 6. Protección perimetral	(*)6.1 Firewalls: tipos e topoloxías 6.2 Sistemas de detección de intrusións 6.3 Redes privadas virtuais 6.4 Análise da seguridade en redes

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Sesión magistral	18	20	38
Prácticas de laboratorio	21	30	51
Proyectos	7	20	27
Trabajos tutelados	0	15	15
Presentaciones/exposiciones	2	5	7
Pruebas de respuesta corta	2	10	12
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías	
	Descripción
Sesión magistral	(*) Exposición por parte do profesor dos contidos previstos na guía docente da materia e discusión e consultas por parte do alumnado. Inclúense como parte destas sesión maxistrais actividades como estudo de casos prácticos e exemplos, presentación de estudos e/ou investigacións, revisión e avaliación de ferramentas de seguridade.
Prácticas de laboratorio	(*) Traballos prácticos a realizar no laboratorio de prácticas. Tratarase dunha colección de exercicios guiados (individuais ou en parellas) relacionados fundamentalmente coas competencias vinculadas á administración segura de sistemas operativos e redes. Consistirán na revisión de diversas ferramentas de seguridade e do seu uso en entornos similares aos reais. A avaliación destas prácticas realizarase mediante cuestionarios (tanto teóricos como experimentais) específicos para cada unha de elas.

Proyectos	(*) Proxecto práctico de programación de entidade media-baixa. Traáarase un exercicio individual ou en parellas relacionado coas competencias vinculadas ao uso de ferramentas criptográficas. Consistirán na implementación dunha pequena aplicación que faga uso de APIs criptográficas de uso habitual. A avaliación deste proxecto comprobará o coñecemento e uso adecuado dos algoritmos criptográficos vistos nas sesións maxistrais, requerirá a entrega dunha pequena memoria.
Trabajos tutelados	(*) Pequeno traballo de investigación, individual ou en parellas, relacionado con aspectos da seguridade informática non incluidos nos contidos principais da materia. A temática pode ser proposta polo alumnado ou polo profesor. Trátase dun traballo autónomo que contará coa titorización puntual do profesorado. O resultado do traballo plasmarase nunha memoria coa estrutura que se determine xunto cunha presentación pública nas sesión presencias da materia.
Presentaciones/exposiciones	(*) Presentación pública e discusión dos aspectos máis relevantes e conclusión do traballo tutelado realizado polo alumno/s. Na temporización desta actividade inclúese a asitencia e participación nas presentacións realizadas por outros alumnos dos seus traballos.

Atención personalizada

Metodologías	Descripción
Trabajos tutelados	
Prácticas de laboratorio	
Proyectos	

Evaluación

	Descripción	Calificación
Prácticas de laboratorio	(*)Avaliación das competencias revisadas nas sesións de laboratorio relativas a seguridade en redes e sistemas operativos. Cada actividade proposta incluirá unha serie de cuestións teóricas e/ou comprobacións prácticas relacionadas co contido de cada práctica. A avaliación destes traballos farease mediante a realización e entrega dun "caderno de prácticas" onde se incuirán unha descripción breve das tarefas realizadas e a resposta ás mencionadas cuestións/comprobacións.	35
Proyectos	(*) Avaliación das competencias revisadas no proxecto de programación con APIs criptográficas. Entregarase o cógido desenvolvido xunta con unha pequena memoria explicativa. Avaliarase a idoneidade e o uso eficaz das diversas técnicas criptográficas que sexa preciso empregar, xunto coa calidade da implementación realizada.	10
Trabajos tutelados	(*) Avaliación da memoria do traballo de investigación tutelado. Avaliarase a capacidade de síntese e a completitude e adecuada presentación das ideas e conceptos relativos ao tema escollido.	10
Presentaciones/exposiciones	(*)Avaliación da presentación do traballo tutelado. Avaliarase a capacidade de síntese e de comunicación das ideas másis relevante, así como o fomento da discusión e a defensa/aclaración das dúbidas ou cuestións presentadas.	0,5
Pruebas de respuesta corta	(*)Proba escrita onde se avaliarán os contidos e competencias revisados nas sesións maxistrais e os aspectos teóricos da súa posta en práctica levada a cabo nas sesión prácticas. O tipo de proba consitirá nun conxunto de cuestións de resposta curta sobre conceptos concretos. A súa finalidade será comprobar a asimilación dos mesmos e a capacidade di alumnado para relacionar entre sí os diversos contidos teórico e técnicas presentados no curso.	40

Otros comentarios sobre la Evaluación

Fuentes de información

Recomendaciones

Asignaturas que continúan el temario

Codificación y criptografía/O06G150V01961

Asignaturas que se recomienda haber cursado previamente

Derecho: Fundamentos éticos y jurídicos de las TIC/O06G150V01102
Sistemas operativos II/O06G150V01405
Centros de datos/O06G150V01601
Redes de computadoras II/O06G150V01505