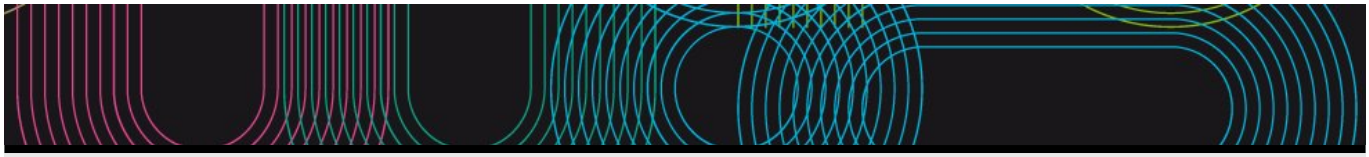

DATOS IDENTIFICATIVOS				
Seguridad en sistemas informáticos				
Asignatura	Seguridad en sistemas informáticos			
Código	O06G150V01702			
Titulacion	Grado en Ingeniería Informática			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	4	1c
Lengua Impartición	Castellano Gallego			
Departamento	Informática			
Coordinador/a	Ribadas Pena, Francisco José			
Profesorado	Darriba Bilbao, Víctor Manuel Ribadas Pena, Francisco José			
Correo-e	ribadas@uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	La materia "Seguridad en Sistemas Informáticos" se ubica en el cuarto curso del Grado en Ingeniería Informática. Se trata de una materia obligatoria que pretende integrar, complementar y ampliar competencias y contenidos relacionados con la seguridad informática ya trabajados por los alumnos en otras materias previas relacionadas con los sistemas operativos y con las redes de computadoras. Dado que la seguridad informática es un campo muy amplio y variado, el objetivo fundamental de la materia es servir de introducción la esta rama de la informática y dar una visión general, al tiempo que práctica, de los aspectos más relevantes de la seguridad informática, de modo que sirvan al alumno como punto de partida en caso de que decida orientar su carrera profesional en este campo.			

Competencias	
Código	
A2	Que los estudiantes sepan 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.
A3	Que los estudiantes tengan la capacidad de 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.
B3	Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
B4	Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos
B7	Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.
B11	Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.
B12	Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como la legislación, regulación y normalización en el ámbito de los proyectos informáticos, de acuerdo con los conocimientos adquiridos.
C7	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
C29	Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse
C32	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
C34	Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización
C37	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
D1	I1: Capacidad de análisis, síntesis y evaluación

D7	I7: Capacidad de buscar, relacionar y estructurar información proveniente de diversas fuentes y de integrar ideas y conocimientos
D8	I8: Resolución de problemas
D9	I9: Capacidad de tomar decisiones
D10	I10: Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones
D11	P1: Capacidad de actuar autónomamente
D12	P2: Capacidad de trabajar en situaciones de falta de información y/o bajo presión
D13	P3: Capacidad de integrarse rápidamente y trabajar eficientemente en equipos unidisciplinares y de colaborar en un entorno multidisciplinar
D16	S1: Razonamiento crítico
D17	S2: Compromiso ético y democrático
D18	S3: Aprendizaje autónomo
D19	S4: Adaptación a nuevas situaciones
D20	S5: Creatividad
D21	S6: Liderazgo
D22	S7: Tener iniciativa y ser resolutivo
D23	S8: Espíritu emprendedor y ambición profesional
D24	S9: Tener motivación por la calidad y la mejora continua

Resultados de aprendizaje

Resultados previstos en la materia	Resultados de Formación y Aprendizaje			
RA1: Conocer los fundamentos de la criptografía moderna	A3	B3 B7	C7 C29 C37	D1 D8 D9
RA2: Conocer la arquitectura de seguridad de los sistemas operativos actuales y saber configurarlos y administrarlos de un modo seguro	A2	B3 B4 B7 B12	C7 C29 C32 C37	D1 D7 D8 D9 D10 D11 D12 D13 D16 D18 D19 D20
RA3: Gestionar una red informática de un modo seguro	A3	B3 B4 B7 B11 B12	C7 C29 C32 C34 C37	D1 D8 D9 D10 D11 D12 D16 D17 D18 D19 D20 D21 D22 D23 D24
RA4: Conocer los tipos de ataques informáticos más habituales y las maneras de protegerse contra ellos	A2 A3	B3 B7 B11 B12	C7 C29 C34 C37	D1 D7 D8 D9 D10 D11 D12 D13 D16 D17 D19 D20 D21 D22 D23

RA5: Saber gestionar un problema de seguridad	A2 A3	B3 B7 B11 B12	C7 C29 C32 C34 C37	D1 D7 D8 D9 D10 D11 D12 D13 D16 D17 D18 D19 D20 D21 D22 D23

Contenidos	
Tema	
BLOQUE I. Seguridad de la información	.
TEMA 1. Contexto de la seguridad en los sistemas informáticos	1.1 Conceptos y terminología 1.2 Niveles de la seguridad: física, lógica, organizativa 1.3 Normas y recomendaciones
TEMA 2. Criptografía	2.1 Fundamentos y evolución 2.2 Cifrado simétrico 2.3 Cifrado asimétrico 2.4 Infraestructuras criptográficas: certificados, firma digital, PKI
TEMA 3. Seguridad en el desarrollo de aplicaciones	3.1 Tipos de vulnerabilidades y amenazas en el sotfware 3.2 Explotación de vulnerabilidades 3.3 Programación segura
BLOQUE II. Seguridad en sistemas operativos	.
TEMA 4. Administración segura de SS.OO.	4.1 Mecanismos de autenticación. 4.2 Herramientas de monitorización 4.3 Vulnerabilidades típicas 4.4 Respuesta ante incidentes
BLOQUE III. Seguridad en redes	.
TEMA 5. Protocolos seguros	5.1 Vulnerabilidades en redes TCP/IP 5.2 Seguridad a nivel de red: IPSec 5.3 Seguridad a nivel de transporte: SSL/TLS 5.4 Seguridad a nivel de aplicación: SSH
TEMA 6. Protección perimetral	6.1 Firewalls: tipos y topologías 6.2 Sistemas de detección de intrusos 6.3 Redes personales virtuales 6.4 Análisis de la seguridad en redes
CONTENIDOS DE LAS PRÁCTICAS	- Uso de APIs de cifrado - Análisis de seguridad en redes, sistemas e servicios - Diseño y despliegue de soluciones de seguridad perimertal - Análisis de seguridad en aplicaciones web y diseño de contramedidas

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	18	20	38
Prácticas de laboratorio	28	50	78
Trabajo tutelado	0	17	17
Presentación	1	3	4
Examen de preguntas objetivas	2	10	12
Trabajo	1	0	1

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías	
	Descripción
Lección magistral	Exposición por parte del profesor de los contenidos previstos en la guía docente de la materia y discusión y consultas por parte del alumnado. Se incluyen como parte de estas sesión magistrales actividades como estudio de casos prácticos y ejemplos, presentación de estudios y/o investigaciones, revisión y evaluación de herramientas de seguridad.

Prácticas de laboratorio	Trabajos prácticos a realizar en el laboratorio de prácticas. Se tratará de una colección de ejercicios guiados (individuales o en parejas) relacionados fundamentalmente con las competencias vinculadas a la administración segura de sistemas operativos y redes. Consistirán en la revisión de diversas herramientas de seguridad y de su uso en entornos similares a los reales. La evaluación de estas prácticas se realizará mediante cuestionarios (tanto teóricos como experimentales) específicos para cada una de ellas.
Trabajo tutelado	Pequeño trabajo de investigación, individual o en parejas, relacionado con aspectos de la seguridad informática no incluidos en los contenidos principales de la materia. La temática puede ser propuesta por el alumnado o por el profesor. Se trata de un trabajo autónomo que contará con la tutorización puntual del profesorado. El resultado del trabajo se plasmará en una memoria con la estructura que se determine junto con una presentación pública en las sesión presencias de la materia.
Presentación	Presentación pública y discusión de los aspectos más relevantes y conclusión del trabajo tutelado realizado por el alumno/s. En la temporización de esta actividad se incluye la asistencia y participación en las presentaciones realizadas por otros alumnos de sus trabajos.

Atención personalizada

Metodologías	Descripción
Trabajo tutelado	Se trata de un trabajo autónomo (o en parejas) que contará con la tutorización puntual del profesorado y guías de elaboración específicas.
Prácticas de laboratorio	Se trata de un trabajo autónomo (o en parejas) que contará con la tutorización puntual del profesorado y guías específicas.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Prácticas de laboratorio	Evaluación de las competencias revisadas en el proyecto de programación con APIs criptográficas. Se entregará el códido desarrollado junta con una pequeña memoria explicativa. Se evaluará la idoneidad y el uso eficaz de las diversas técnicas criptográficas que sea preciso emplear, junto con la calidad de la implementación realizada. Evaluación de las competencias revisadas en las sesiones de laboratorio relativas la seguridad en redes y sistemas operativos. Cada actividad propuesta incluirá una serie de cuestiones teóricas y/o comprobaciones prácticas relacionadas con el contenido de cada práctica. La evaluación de estos trabajos se hará mediante la realización y entrega de un "cuaderno de prácticas" donde se incluirán una descripción breve de las tareas realizadas y la respuesta a las mencionadas cuestiones/comprobaciones. - RESULTADOS DE APRENDIZAJE: RA2, RA3, RA4, RA5	45	A2	B3 B4 B7	C7 C29 C32 C34	D8 D9 D10 D12 D16 D17 D18 D19 D22 D24
Presentación	Evaluación de la presentación del trabajo tutelado. Se evaluará la capacidad de síntesis y de comunicación de las ideas más relevantes, así como el fomento de la discusión y la defensa/aclaración de las dudas o cuestiones presentadas. - RESULTADOS DE APRENDIZAJE: RA2, RA3, RA4, RA5	5	A3	B7 B11 B12	C7 C29 C37	D10 D19 D20 D21 D22 D23 D24
Examen de preguntas objetivas	Prueba escrita donde se evaluarán los contenidos y competencias revisados en las sesiones magistrales y los aspectos teóricos de su puesta en práctica llevada a cabo en las sesión prácticas. El tipo de prueba consistirá en un conjunto de cuestiones de respuesta corta o de tipo test sobre conceptos concretos. Su finalidad será comprobar la asimilación de los mismos y la capacidad dice alumnado para relacionar entre si los diversos contenidos teórico y técnicas presentados en el curso. - RESULTADOS DE APRENDIZAJE: RA1, RA2, RA3, RA4, RA5	40	A3	B3 B7	C7 C29 C32 C34 C37	D1 D8 D10
Trabajo	Evaluación de la memoria del trabajo de investigación tutelado. Se evaluará la capacidad de síntesis y la completitud y adecuada presentación de las ideas y conceptos relativos al tema escogido. - RESULTADOS DE APRENDIZAJE: RA2, RA3, RA4, RA5	10	A3	B7 B11 B12	C7 C29 C37	D10 D11 D16 D17 D20 D24

Otros comentarios sobre la Evaluación

CRITERIOS DE EVALUACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS

- Para superar (y liberar) las "Examen de preguntas objetivas" se requiere alcanzar un 40% de la puntuación máxima prevista para ese tipo de prueba.
- Para superar (y liberar) las "Prácticas de laboratorio" se requiere alcanzar un 40% de la puntuaciones máxima previstas para estas pruebas.
- Para superar la materia es preciso alcanzar los mínimos anteriores (en "Examen de preguntas objetivas" y en "Prácticas de laboratorio ") y sumar en la nota final un mínimo de 5 puntos.
- En el caso de constatar un comportamiento no ético (copia, plagio) en alguna de las entregas realizadas (total o parcial), se anulará la totalidad de la contribución del correspondiente elemento de evaluación ("Prácticas de laboratorio", "Trabajo tutelado", "Examen de preguntas objetivas") sobre la calificación final.

CRITERIOS DE EVALUACIÓN PARA NO ASISTENTES

- En el caso del alumnado no asistente el esquema de evaluación no incluirá el "Trabajo tutelado" ni "la Presentación/Exposición".
- Las "Prácticas de laboratorio" serán exclusivamente individuales.
- Para superar la materia será preciso alcanzar los mínimos indicados en cada prueba y sumar en la nota final un mínimo de 5 puntos.
- En el caso de constatar un comportamiento no ético (copia, plagio) en alguna de las entregas realizadas (total o parcial), se anulará la totalidad de la contribución del correspondiente elemento de evaluación ("Prácticas de laboratorio", "Examen de preguntas objetivas") sobre la calificación final.

Metodología/Prueba 1: Pruebas de respuesta corta

Descripción: Prueba escrita donde se evaluarán los contenidos y competencias revisados en las sesiones magistrales y los aspectos teóricos de su puesta en práctica llevada a cabo en las sesión prácticas. El tipo de prueba consistirá en un conjunto de cuestiones de respuesta corta o de tipo test sobre conceptos concretos. Su finalidad será comprobar la asimilación de los mismos y la capacidad del alumnado para relacionar entre sí los diversos contenidos teórico y técnicas presentados en el curso.

% Calificación: 50% (*Para liberar esta parte de la evaluación debe obtenerse una calificación igual o superior a 5 puntos sobre 10)*.

Competencias evaluadas: CB3, CG3, CG7, CE7, CE29, CE32, CE34, CE37, CT1, CT8, CT10

Resultados de aprendizaje evaluados: RA1, RA2, RA3, RA4, RA5

Metodología/Prueba 2: Prácticas de laboratorio

Descripción: Evaluación de las competencias revisadas en las sesiones de laboratorio relativas la seguridad en redes y sistemas operativos. Cada actividad propuesta incluirá una serie de cuestiones teóricas y/o comprobaciones prácticas relacionadas con el contenido de cada práctica. La evaluación de estos trabajos se realizará mediante la realización y entrega de un "cuaderno de prácticas" donde se incluirá una descripción breve de las tareas realizadas y la respuesta a las mencionadas cuestiones/comprobaciones.

% Calificación: 45% (*Para liberar esta parte de la evaluación debe obtenerse una calificación igual o superior a 5 puntos sobre 10)*.

Competencias evaluadas: CB2,CG3,CG4,CG7,CE7,CE29,CE32,CE34,CT8,CT9,CT10,CT12,CT16,CT17,CT18,CT22,CT24

Resultados de aprendizaje evaluados: RA1, RA2, RA3, RA4, RA5

CRITERIOS DE EVALUACIÓN PARA 2ª EDICIÓN DE ACTAS Y FIN DE CARRERA

Para los alumnos asistentes se empleará el mismo esquema de evaluación descrito en la sección CRITERIOS DE EVALUACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS.

- Los alumnos solo deberán superar las partes no liberadas en la primera edición de las actas

- Dado que en la segunda convocatoria no es posible a evaluación de "Presentaciones/exposiciones", los alumnos que no habían hecho su presentación en el periodo de clases regular no podrán optar a contar con esa porción de la nota.

Para los alumnos "no asistentes" se empleará el mismo esquema de evaluación descrito en la sección "CRITERIOS DE EVALUACIÓN PARA NO ASISTENTES".

PROCESO DE CALIFICACIÓN DE ACTAS

En el caso de los alumnos que superen parte de los elementos evaluados, pero no alcancen el mínimo preciso para aprobar la materia completa, la calificación a incluir en las respectivas actas se calculará como el mínimo entre el promedio ponderado de las partes superadas y 4,9.

FECHAS DE EVALUACIÓN

El calendario de pruebas de evaluación aprobado oficialmente por la Junta de Centro de la ESEI se encuentra publicado en la página web http://www.esei.uvigo.es

Fuentes de información
Bibliografía Básica
W. Stallings, **Cryptography and Network Security: Principles and Practice**, 5th edition, Prentice Hall, 2011
W. Stallings, L. Brown, **Computer Security: Principles and Practice**, 2nd edition, Prentice Hall, 2012
J. L. García Rambla, **Ataques en redes de datos IPv4 e IPv6**, 2da edición, 0xWORD, 2014
Bibliografía Complementaria
Carlos Álvarez Martín y Pablo González Pérez, **Hardening de servidores GNU / Linux**, 2ª ed., 0xWORD, 2014
Darril Gibson, **Microsoft Windows Security Essentials**, 1st Edition, John Wiley & Sons, 2011
Varios autores, **Aspectos avanzados de seguridad en redes**, Universitat Oberta de Cataluña,
Manuel J. Lucena Lopez, **Criptografia y Seguridad en Computadores.**,
Antonio Villalon Huerta, **Seguridad en UNIX y Redes**,

Recomendaciones
Asignaturas que continúan el temario
Teoría de códigos/O06G150V01971

Asignaturas que se recomienda haber cursado previamente

Sistemas operativos II/O06G150V01405
Centros de datos/O06G150V01601
Redes de computadoras II/O06G150V01505

Otros comentarios

Se presupone un conocimiento básico sobre las cuestión típicas relacionadas con la administración de sistemas GNU/Linux y un conocimiento básico sobre redes TCP/IP.

La mayor parte de las referencias y recursos externos (tutorialess, manuales, herramientas) sólo están disponibles en inglés, por lo que es recomendable un nivel mínimo de soltura en la lectura y comprensión de documentos técnicos en inglés.

Los proyectos de programación se llevarán a cabo sobre Java, por lo que se precisa una base mínima en dicho lenguaje.

Las prácticas de seguridad en redes harán uso de máquinas virtuales sobre VirtualBox (www.virtualbox.org), por lo que es recomendable conocer previamente los aspectos básicos de esta herramienta.