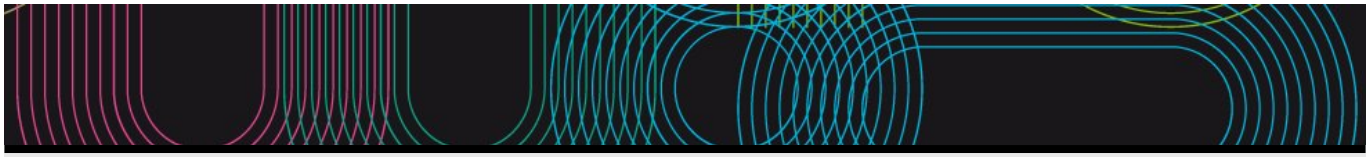

DATOS IDENTIFICATIVOS				
Seguridad en sistemas informáticos				
Asignatura	Seguridad en sistemas informáticos			
Código	O06G151V01401			
Titulacion	Grado en Ingeniería Informática			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	4	1c
Lengua Impartición	#EnglishFriendly Castellano Gallego			
Departamento	Informática			
Coordinador/a	Ribadas Pena, Francisco José			
Profesorado	Ribadas Pena, Francisco José			
Correo-e	ribadas@uvigo.es			
Web	http://moovi.uvigo.gal			
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. El idioma de impartición de la materia y de las tutorías será indistintamente castellano y/o gallego. Respecto al material empleado en clase, se usarán recursos en castellano, gallego y, en menor medida, inglés. Materia del programa English Friendly: Los/as estudiantes internacionales podrán solicitar al profesorado: a) materiales y referencias bibliográficas para el seguimiento de la materia en inglés, b) atender las tutorías en inglés, c) pruebas y evaluaciones en inglés.			

Resultados de Formación y Aprendizaje	
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.
B9	Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.
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
D4	Capacidad de análisis, síntesis y evaluación
D7	Capacidad de buscar, relacionar y estructurar información proveniente de diversas fuentes y de integrar ideas y conocimientos.
D8	Capacidad de trabajar en situaciones de falta de información y/o bajo presión
D9	Capacidad de integrarse rápidamente y trabajar eficientemente en equipos unidisciplinares y de colaborar en un entorno multidisciplinar
D11	Razonamiento crítico
D12	Liderazgo
D13	Espíritu emprendedor y ambición profesional
D14	Tener motivación por la calidad y la mejora continua

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje			
RA2: Conocer la arquitectura de seguridad de los sistemas operativos actuales y saber configurarlos y administrarlos de un modo seguro	A2	B3 B4 B7 B9 B12	C7 C29 C32 C37	D7 D9 D11 D14
RA3: Gestionar una red informática de un modo seguro	A3	B3 B4 B7 B9 B11 B12	C7 C29 C32 C34 C37	D7 D8 D9 D14
RA4: Conocer los tipos de ataques informáticos más habituales y las maneras de protegerse contra ellos	A2 A3	B3 B7 B9 B11 B12	C7 C29 C34 C37	D7 D8 D12 D13 D14
RA5: Saber gestionar un problema de seguridad	A2 A3	B3 B7 B9 B11 B12	C7 C29 C32 C34 C37	D4 D7 D8 D11 D12 D13 D14

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	20	20	40
Prácticas de laboratorio	26	52	78
Trabajo tutelado	0	15	15
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 y a la criptografía. 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 entregables (tanto teóricos como experimentales) específicos para cada una de ellas. EVALUACION CONTINUA Caracter: Obligatorio Asistencia: No obligatoria EVALUACION GLOBAL Caracter: Obligatorio
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. EVALUACION CONTINUA Caracter: Obligatorio Asistencia: No obligatoria EVALUACION GLOBAL Caracter: No obligatorio
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. EVALUACION CONTINUA Caracter: No obligatoria Asistencia: No obligatoria

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 código 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. - PUNTUACIÓN MÍNIMA: 4 puntos sobre 10 - RESULTADOS DE APRENDIZAJE: RA1, RA2, RA3, RA4, RA5	45	A2	B3 B4 B7	C7 C29 C32 C34	D7 D8 D9 D11 D12 D14
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. - PUNTUACIÓN MÍNIMA: no hay mínimo - RESULTADOS DE APRENDIZAJE: RA2, RA3, RA4, RA5	5	A3	B7 B11 B12	C7 C29 C37	D4 D7 D13
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 preguntas tipo test o cuestiones de respuesta corta 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. - PUNTUACIÓN MÍNIMA: 4 puntos sobre 10 - RESULTADOS DE APRENDIZAJE: RA1, RA2, RA3, RA4, RA5	40	A3	B3 B7	C7 C29 C32 C34 C37	D4 D7 D8
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. - PUNTUACIÓN MÍNIMA: no hay mínimo - RESULTADOS DE APRENDIZAJE: RA2, RA3, RA4, RA5	10	A3	B7 B11 B12	C7 C29 C37	D4 D7 D9 D11

Otros comentarios sobre la Evaluación

(1) SISTEMA DE EVALUACIÓN CONTÍNUA

PRUEBA 1: *Proyecto de cifrado con API de Java*

Descripción: Evaluación del código y la memoria del proyecto de desarrollo empleando el API de cifrado JCA.

Metodología(s): Prácticas de laboratorio

% Calificación: 10%

% Mínimo: 4 puntos sobre 10

Competencias evaluadas: B3, C7, C32

Resultados aprendizaje evaluados: RA1

PRUEBA 2: *Prácticas guiadas*

Descripción: Evaluación de los entregables y cuestiones correspondientes a las prácticas de seguridad en redes y S.O.

Metodología(s): Prácticas de laboratorio

% Calificación: 35%

% Mínimo: 4 puntos sobre 10

Competencias evaluadas: A2,B3,B4,B7,C7,C29,C32,C34,D7,D8,D9,D11,D12,D14

Resultados aprendizaje evaluados: RA2, RA3, RA4, RA5

PRUEBA 3:*Trabajo tutelado*

Descripción: Evaluación de la memoria del trabajo de investigación tutelado

Metodología(s): Trabajo

% Calificación: 10%

% Mínimo: no hay mínimo

Competencias evaluadas: A3,B7,B11,B12,C7,C29,C37,D4,D7,D9,D11

Resultados aprendizaje evaluados: RA2, RA3, RA4, RA5

PRUEBA 4: *Presentación*

Descripción: Evaluación de la presentación del trabajo de investigación tutelado

Metodología(s): Presentación

% Calificación: 5%

% Mínimo: no hay mínimo

Competencias evaluadas: A3,B7,B11,B12,C7,C29,C37,D4,D7,D13

Resultados aprendizaje evaluados: RA2, RA3, RA4, RA5

PRUEBA 5:*Examen final*

Descripción: Examen tipo test sobre los contenidos teóricos de la materia

Metodología(s): Examen de preguntas objetivas

% Calificación: 40%

% Mínimo: 4 puntos sobre 10

Competencias evaluadas: A3,B3,B7,C7,C29,C32,C34,C37,D4,D7,D8

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

ACLARACIONES ADICIONALES

- Para superar la materia es preciso alcanzar los mínimos indicados en las pruebas anteriores y sumar en la nota final ponderada un mínimo de 5 puntos sobre 10.
- 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 sobre la calificación final

(2) SISTEMA DE EVALUACIÓN GLOBAL

Procedimiento para la elección de la modalidad de evaluación global:

- Se asume por defecto la modalidad de evaluación contínua.
- Los alumnos que opten por la evaluación global deberán comunicarlo via Moovi, emleando los mecanismos que se habiliten y en el plazo estipulado, una vez superado el plazo de un mes desde el comienzo del cuatrimestre

PRUEBA 1: *Proyecto de cifrado con API de Java*

Descripción: Evaluación del código y la memoria del proyecto de desarrollo empleando el API de cifrado JCA.

Metodología(s): Prácticas de laboratorio

% Calificación: 10%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: B3, C7, C32

Resultados aprendizaje evaluados: RA1

PRUEBA 2: *Prácticas guiadas*

Descripción: Evaluación de los entregables y cuestiones correspondientes a las prácticas de seguridad en redes y S.O.

Metodología(s): Prácticas de laboratorio

% Calificación: 35%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: A2,B3,B4,B7,C7,C29,C32,C34,D7,D8,D9,D11,D12,D14

Resultados aprendizaje evaluados: RA2, RA3, RA4, RA5

PRUEBA 3: *Examen final*

Descripción: Examen tipo test sobre los contenidos teóricos de la materia

Metodología(s): Examen de preguntas objetivas

% Calificación: 55%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: A3,B3,B7,C7,C29,C32,C34,C37,D4,D7,D8

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

ACLARACIONES ADICIONALES

- Para superar la materia es preciso alcanzar los mínimos indicados en las pruebas anteriores y sumar en la nota final ponderada un mínimo de 5 puntos sobre 10.
- 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 sobre la calificación final

(3) CRITERIOS DE EVALUACIÓN PARA CONVOCATORIA EXTRAORDINARIA Y FIN DE CARRERA

Se emplearán los sistemas de evaluación continua y global expuestos anteriormente.

En estas convocatorias, los alumnos sólo deberán realizar las pruebas en las cuales no hubieran obtenido la calificación mínima indicada.

(4) 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.

(5) 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

(6) EMPLEO DE DISPOSITIVOS MOVILES

Se recuerda a todo el alumnado la prohibición del uso de dispositivos móviles en ejercicios y prácticas, en cumplimiento del artículo 13.2.d) del Estatuto del Estudiante Universitario, relativo a los deberes del estudiantado universitario, que establece el deber de "Abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad."

(7) CONSULTA/SOLICITUD DE TUTORÍAS

Las tutorías pueden consultarse a través de la página personal del profesorado, accesible a través de https://esei.uvigo.es/docencia/profesorado/

Fuentes de información

Bibliografía Básica

W. Stallings, **Cryptography and Network Security: Principles and Practice**, 978-1292158587, 7th edition, Prentice Hall, 2017

W. Stallings, L. Brown, **Computer Security: Principles and Practice**, 978-0134794105, 4rd edition, Prentice Hall, 2018

J. L. García Rambla, **Ataques en redes de datos IPv4 e IPv6**, 978-8409240630, 2da edición, 0xWORD, 2014

Bibliografía Complementaria

Carlos Álvarez Martín y Pablo González Pérez, **Hardening de servidores GNU / Linux**, 978-84-09-24061-6, 4ª edición, 0xWORD, 2020

Darril Gibson, **Microsoft Windows Security Essentials**, 978-1118016848, 1st Edition, John Wiley & Sons, 2011

Recomendaciones

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.