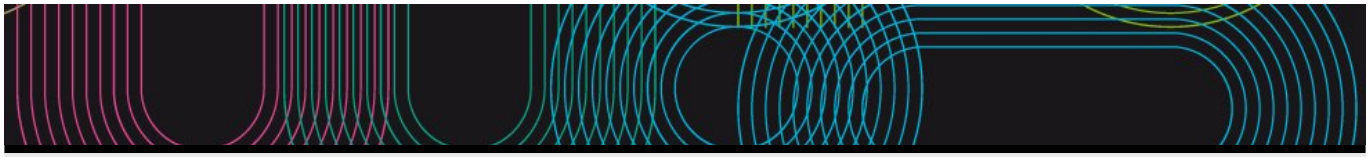

DATOS IDENTIFICATIVOS				
Seguridade en sistemas informáticos				
Materia	Seguridade en sistemas informáticos			
Código	O06G151V01401			
Titulación	Grao en Enxeñaría Informática			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OB	4	1c
Lingua de impartición	#EnglishFriendly Castelán Galego			
Departamento	Informática			
Coordinador/a	Ribadas Pena, Francisco José			
Profesorado	Ribadas Pena, Francisco José			
Correo-e	ribadas@uvigo.es			
Web	http://moovi.uvigo.gal			
Descrición xeral	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. A lingua de impartición da materia e das titorías será indistintamente castelán e/ou galego. Respecto ao material empregado nas clases, usaránse recursos en castelán, galego e, en menor medida, inglés. Materia do programa English Friendly. Os/as estudantes internacionais poderán solicitar ao profesorado: a) materiais e referencias bibliografías para o seguimento da materia en inglés, b) atender as titorías en inglés, c) probas e avaliacións en inglés.			

Resultados de Formación e Aprendizaxe	
Código	
A2	Que os estudantes saiban aplicar os seus coñecementos ó seu traballo ou vocación dunha forma profesional e posúan as competencias que adoitan demostrarse por medio da elaboración e defensa de argumentos e a resolución de problemas dentro da súa área de estudo.
A3	Que os estudantes teñan a capacidade de reunir e interpretar datos relevantes (normalmente dentro da súa área de estudo) para emitir xuízos que inclúan unha reflexión sobre temas relevantes de índole social, científica ou ética.
B3	Capacidade para deseñar, desenvolver, avaliar e asegurar a accesibilidade, ergonomía, usabilidade e seguridade dos sistemas, servizos e aplicacións informáticas, así como da información que xestionan.
B4	Capacidade para definir, avaliar e seleccionar plataformas hardware e software para o desenvolvemento e a execución de sistemas, servizos e aplicacións informáticas, de acordo cos coñecementos adquiridos.
B7	Capacidade para coñecer, comprender e aplicar a lexislación necesaria durante o desenvolvemento da profesión de Enxeñeiro Técnico en Informática e manexar especificacións, regulamentos e normas de obrigado cumprimento.
B9	Capacidade para resolver problemas con iniciativa, toma de decisións, autonomía e creatividade. Capacidade para saber comunicar e transmitir os coñecementos, habilidades e destrezas da profesión de Enxeñeiro Técnico en Informática.
B11	Capacidade para analizar e valorar o impacto social e medioambiental das solucións técnicas, comprendendo a responsabilidade ética e profesional da actividade de Enxeñeiro Técnico en Informática.
B12	Coñecemento e aplicación de elementos básicos de economía e de xestión de recursos humáns, organización e planificación de proxectos, así como a lexislación, regulación e normalización no ámbito dos proxectos informáticos, de acordo cos coñecementos adquiridos.

C7	Capacidade para deseñar, desenvolver, seleccionar e avaliar aplicacións e sistemas informáticos, asegurando a súa fiabilidade, seguridade e calidade, conforme aos principios éticos e á lexislación e normativa vixente
C29	Capacidade de identificar, avaliar e xestionar os riscos potenciais asociados que puidesen presentarse
C32	Capacidade para seleccionar, deseñar, despregar, integrar, avaliar, construír, xestionar, explotar e manter as tecnoloxías de hardware, software e redes, dentro dos parámetros de custo e calidade adecuados
C34	Capacidade para seleccionar, deseñar, despregar, integrar e xestionar redes e infraestruturas de comunicacións nunha organización
C37	Capacidade para comprender, aplicar e xestionar a garantía e seguridade dos sistemas informáticos
D4	Capacidade de análise, síntese e avaliación
D7	Capacidade de buscar, relacionar e estruturar información provinte de diversas fontes e de integrar ideas e coñecementos.
D8	Capacidade de traballar en situacións de falla de información e/ou baixo presión
D9	Capacidade de integrarse rápidamente e traballar eficientemente en equipos unidisciplinares e de colaborar nun entorno multidisciplinar
D11	Razoamento crítico
D12	Liderado
D13	Espíritu emprendedor e ambición profesional
D14	Ter motivación pola calidade e a mellora continua

Resultados previstos na materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe			
RA2: Coñecer a arquitectura de seguridade dos sistemas operativos actuais e saber configuralos e administralos de modo seguro	A2	B3 B4 B7 B9 B12	C7 C29 C32 C37	D7 D9 D11 D14
RA3: Xestionar unha rede informática dun xeito seguro	A3	B3 B4 B7 B9 B11 B12	C7 C29 C32 C34 C37	D7 D8 D9 D14
RA4: Coñecer os tipos de ataques informáticos máis habituais e as maneras de protexerse contra eles	A2 A3	B3 B7 B9 B11 B12	C7 C29 C34 C37	D7 D8 D12 D13 D14
RA5: Saber xestionar un problema de seguridade	A2 A3	B3 B7 B9 B11 B12	C7 C29 C32 C34 C37	D4 D7 D8 D11 D12 D13 D14

Contidos

Tema	
BLOQUE I. Seguridade da información	.
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
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
CONTIDOS PREVISTOS NAS PRÁCTICAS	- Uso de APIs de cifrado - Análise de seguridade en redes, sistemas e servizos - Deseño e despregue de solucións de seguridade perimetral - Análise de seguridade en aplicacións web e deseño de contramedidas

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	20	20	40
Prácticas de laboratorio	26	52	78
Traballo tutelado	0	15	15
Presentación	1	3	4
Exame de preguntas obxectivas	2	10	12
Traballo	1	0	1

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Lección maxistral	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 e á criptografía. Consistirán na revisión de diversas ferramentas de seguridade e do seu uso en entornos similares aos reais. A avaliación destas prácticas realizarase mediante cuestionarios entregables (tanto teóricos como experimentais) específicos para cada unha de elas. AVALIACION CONTINUA Caracter: Obrigatorio Asistencia: Non obrigatoria AVALIACION GLOBAL Caracter: Obrigatorio
Traballo tutelado	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. AVALIACION CONTINUA Caracter: Obrigatorio Asistencia: Non obrigatoria AVALIACION GLOBAL Caracter: Non obrigatorio
Presentación	Presentación pública e discusión dos aspectos máis relevantes e conclusións 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. AVALIACION CONTINUA Caracter: Non obrigatorio Asistencia: Non obrigatoria

Atención personalizada

Metodoloxías	Descrición

Traballo tutelado	Trátase dun traballo de investigación autónomo (ou en parellas) que contará coa titorización puntual do profesorado, xunto con guías de elaboración.
Prácticas de laboratorio	Trátase dun traballo autónomo (ou en parellas) que contará coa titorización puntual do profesorado, xunto con guías específicas.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe			
Prácticas de laboratorio	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. 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. - PUNTUACIÓN MÍNIMA: 4 puntos sobre 10 - RESULTADOS APRENDIZAXE: RA1, RA2, RA3, RA4, RA5	45	A2	B3 B4 B7	C7 C29 C32 C34	D7 D8 D9 D11 D12 D14
Presentación	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. - PUNTUACIÓN MÍNIMA: non hai mínimo - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	5	A3	B7 B11 B12	C7 C29 C37	D4 D7 D13
Exame de preguntas obxectivas	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 tipo test ou de resposta curta sobre conceptos concretos. A súa finalidade será comprobar a asimilación dos mesmos e a capacidade do alumnado para relacionar entre sí os diversos contidos teórico e técnicas presentados no curso. - PUNTUACIÓN MÍNIMA: 4 puntos sobre 10 - RESULTADOS APRENDIZAXE: RA1, RA2, RA3, RA4, RA5	40	A3	B3 B7	C7 C29 C32 C34 C37	D4 D7 D8
Traballo	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. - PUNTUACIÓN MÍNIMA: non hai mínimo - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	10	A3	B7 B11 B12	C7 C29 C37	D4 D7 D9 D11

Outros comentarios sobre a Avaliación

(1) SISTEMA DE AVALIACIÓN CONTÍNUA

PROBA 1: *Proxecto de cifrado coa API de Java*

Descripción: Avaliación do código e a memoria do proxecto de desenvolvemenTeo emprgando a API de cifrado JCA.

Metodoloxía(s): Prácticas de laboratorio

% Calificación: 10%

% Mínimo: 4 puntos sobre 10

Competencias avaliadas: B3, C7, C32

Resultados aprendizaxe avaliados: RA1

PROBA 2: *Prácticas guiadas*

Descripción: Avaliación dos entregables e cuestións correspondentes ás prácticas de seguridad en redes e S.O.

Metodoloxía(s): Prácticas de laboratorio

% Calificación: 35%

% Mínimo: 4 puntos sobre 10

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

Resultados aprendizaxe avaliados: RA2, RA3, RA4, RA5

PROBA 3:*Traballo tutelado*

Descripción: Avaliación da memoria do traballo de investigación tutelado

Metodoloxía(s): Traballo

% Calificación: 10%

% Mínimo: non hai mínimo

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

Resultados aprendizaxe avaliados: RA2, RA3, RA4, RA5

PROBA 4: *Presentación*

Descripción: Avaliación da presentación do traballo de investigación tutelado

Metodoloxía(s): Presentación

% Calificación: 5%

% Mínimo: no hay mínimo

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

Resultados aprendizaxe avaliados: RA2, RA3, RA4, RA5

PROBA 5:*Exame final*

Descripción: Exame tipo test sobre os contenidos teóricos da materia

Metodoloxía(s): Exame de preguntas obxectivas

% Calificación: 40%

% Mínimo: 4 puntos sobre 10

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

Resultados aprendizaxe avaliados: RA1, RA2, RA3, RA4, RA5

ACLARACIÓNS ADICIONAIS

- Para superar a materia é preciso alcanzar os mínimos indicados nas probas anteriores e sumar na nota final ponderada un mínimo de 5 puntos sobre 10.

- No caso de constatar un comportamiento non ético (copia, plaxio) nalgunha das entregas realizadas (total ou parcial), anularáse a totalidad da contribución do correspondiente elemento de avaliación sobre la cualificación final

(2) SISTEMA DE AVALIACIÓN GLOBAL

Procedemento para a elección da modalidad de avaliación global:

- Asúmese por defecto a modalidad de avaliación contínua.
- Os alumnos que opten pola avaliación global deberán comunicalo via Moovi, mediante os mecanismos que se habiliten e no prazo estipulado, una vez superado un mes dedde o comenzo do cuatrimestre

PROBA 1: *Proxecto de cifrado coa API de Java*

Descripción: Avaliación do código e da memoria do proxecto de desenvolvemento empreagndo a API de cifrado JCA.

Metodoloxía(s): Prácticas de laboratorio

% Calificación: 10%

% Mínimo: 5 puntos sobre 10

Competencias avaliadas: B3, C7, C32

Resultados aprendizaxe avaliados: RA1

PROBA 2: *Prácticas guiadas*

Descripción: Avaliación dos entregables e cuestions correspondeentes as prácticas de seguridade en redes y S.O.

Metodoloxía(s): Prácticas de laboratorio

% Calificación: 35%

% Mínimo: 4 puntos sobre 10

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

Resultados aprendizaxe avaliados: RA2, RA3, RA4, RA5

PROBA 3: *Exame final*

Descripción: Exame tipo test sobre ls contidos teóricos da materia

Metodoloxía(s): Exame de preguntas obxectivas

% Calificación: 55%

% Mínimo: 5 puntos sobre 10

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

Resultados aprendizaxe avaliados: RA1, RA2, RA3, RA4, RA5

ACLARACIÓNS ADICIONAIS

- Para superar a materia é preciso alcanzar os mínimos indicados nas probas anteriores e sumar na nota final ponderada un mínimo de 5 puntos sobre 10.
- No caso de constatar un comportamento non ético (copia, plaxio) nalgunha das entregas realizadas (total ou parcial), anularáse a totalidade da contribución do correspondente elemento de avaliaicón

sobre la calificación final

(3) CRITERIOS DE AVALIACIÓN PARA A CONVOCATORIA EXTRAORDINARIA E FIN DE CARREIRA

Empregaránse os sistemas de avaliación continua e global expostos anteriormente.

Nestas convocatorias, os alumnos so deberán realizar as probas nas que non teñan obtido a cualificación mínima indicada.

(4) PROCESO DE CALIFICACIÓN DE ACTAS

No caso dos alumnos que superen parte dos elementos avaliados, pero non acaden o mínimo preciso para aprobar a materia completa, a calificación a incluir nas respectivas actas calcularase coma o mínimo entre el promedio ponderado das partes superadas e 4,9.

(5) DATAS DE AVALIACIÓN

As datas oficiais de exame das diferentes convocatorias, aprobadas oficialmente pola Xunta de Centro da ESEI, atópanse publicadas na páxina web da ESEI https://esei.uvigo.es/docencia/horarios/.

(6) EMPREGO DE DISPOSITIVOS MÓBILES

Lémbrase a todo o alumnado a prohibición do uso de dispositivos móbiles en exercicios e prácticas, en cumprimento do artigo 13.2.d) do Estatuto do Estudante Universitario, relativo aos deberes do estudantado universitario, que establece o deber de "Absterse da utilización ou cooperación en procedementos fraudulentos nas probas de avaliación, nos traballos que se realicen ou en documentos oficiais da universidade."

(7) CONSULTA/SOLICITUDE DE TITORÍAS

As titorías pódense consultar a través da páxina persoal do profesorado, accesible a través de https://esei.uvigo.es/docencia/profesorado/

Bibliografía. Fontes 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

Recomendacións

Outros comentarios

Presuponse un coñecemento básico sobre as cuestión típicas relacionadas coa administración de sistemas GNU/Linux e un coñecemento básico sobre redes TCP/IP.

A maior parte das referencias e recursos externos (tutoriais, manual, ferramentas) só están dispoñibles en inglés, polo que é recomendable un nivel mínimo de soltura na lectura e comprensión de documentos técnicos en inglés.

Os proxectos de programación levaránse a cabo sobre Java, polo que precísarase unha base mínima nesa linguaxe.

As prácticas de seguridade en rede farán uso de máquinas virtuais sobre VirtualBox (www.virtualbox.org), polo que é

recomendable coñecer previamente os aspectos básicos desta ferramenta.