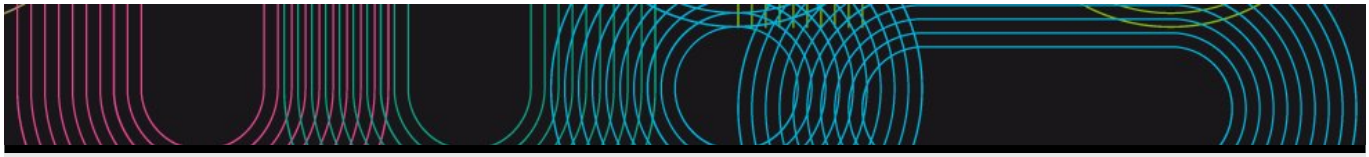

DATOS IDENTIFICATIVOS				
Seguridade en sistemas informáticos				
Materia	Seguridade en sistemas informáticos			
Código	O06G150V01702			
Titulacion	Grao en Enxeñaría Informática			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	4	1c
Lingua impartición	Castelán Galego			
Departamento	Informática			
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			
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.			

Competencias	
Código	
CB2	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.
CB3	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.
CG3	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.
CG4	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.
CG7	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.
CG9	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.
CG11	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.
CG12	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.
CE7	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
CE29	Capacidade de identificar, avaliar e xestionar os riscos potenciais asociados que puidesen presentarse

CE32	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
CE34	Capacidade para seleccionar, deseñar, despregar, integrar e xestionar redes e infraestruturas de comunicacións nunha organización
CE37	Capacidade para comprender, aplicar e xestionar a garantía e seguridade dos sistemas informáticos
CT4	Capacidade de análise, síntese e avaliación
CT7	Capacidade de buscar, relacionar e estruturar información provinte de diversas fontes e de integrar ideas e coñecementos.
CT8	Capacidade de traballar en situacións de falla de información e/ou baixo presión
CT9	Capacidade de integrarse rápidamente e traballar eficientemente en equipos unidisciplinares e de colaborar nun entorno multidisciplinar
CT11	Razoamento crítico
CT12	Liderado
CT13	Espíritu emprendedor e ambición profesional
CT14	Ter motivación pola calidade e a mellora continua

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias			
RA1: Coñecer os fundamentos da criptografía moderna	CB3	CG3 CG7	CE7 CE29 CE37	CT4 CT11
RA2: Coñecer a arquitectura de seguridade dos sistemas operativos actuais e saber configuralos e administralos de modo seguro	CB2	CG3 CG4 CG7 CG9 CG12	CE7 CE29 CE32 CE37	CT7 CT9 CT11 CT14
RA3: Xestionar unha rede informática dun xeito seguro	CB3	CG3 CG4 CG7 CG9 CG11 CG12	CE7 CE29 CE32 CE34 CE37	CT7 CT8 CT9 CT14
RA4: Coñecer os tipos de ataques informáticos máis habituais e as maneras de protexerse contra eles	CB2 CB3	CG3 CG7 CG9 CG11 CG12	CE7 CE29 CE34 CE37	CT7 CT8 CT12 CT13 CT14
RA5: Saber xestionar un problema de seguridade	CB2 CB3	CG3 CG7 CG9 CG11 CG12	CE7 CE29 CE32 CE34 CE37	CT4 CT7 CT8 CT11 CT12 CT13 CT14

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 desplregue 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.
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.
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.

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	Competencias Avaliadas

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. - RESULTADOS APRENDIZAXE: RA1, RA2, RA3, RA4, RA5	45	CB2	CG3 CG4 CG7	CE7 CE29 CE32 CE34	CT7 CT8 CT9 CT11 CT12 CT14
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. - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	5	CB3	CG7 CG11 CG12	CE7 CE29 CE37	CT4 CT7 CT13
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. - RESULTADOS APRENDIZAXE: RA1, RA2, RA3, RA4, RA5	40	CB3	CG3 CG7	CE7 CE29 CE32 CE34 CE37	CT4 CT7 CT8
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. - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	10	CB3	CG7 CG11 CG12	CE7 CE29 CE37	CT4 CT7 CT9 CT11

Outros comentarios sobre a Avaliación

CRITERIOS DE AVALIACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS

- Para superar (e liberar) o "Exame de preguntas obxectivas" requírese acadar un 40% da puntuación máxima prevista para este tipo de proba.
- Para superar (e liberar) as "Prácticas de laboratorio" requírese acadar un 40% da puntuación máxima previstas para estas probas.
- Para superar a materia é preciso acadar os mínimos anteriores (en "Exame de preguntas obxectivas" e en "Prácticas de laboratorio") e sumar na nota final un mínimo de 5 puntos.
- No caso de constatar un comportamento non ético (copia, plaxio) nalgunha das entregas realizadas (total ou parcial), anularase a **totalidade** da contribución do correspondente elemento de avaliación ("Prácticas de laboratorio", "Traballo tutelado", "Exame de preguntas obxectivas") sobre a cualificación final.

CRITERIOS DE AVALIACIÓN PARA NON ASISTENTES

- No caso do alumnado non asistente o esquema de avaliación non incluirá o "Traballo tutelado" nin a "Presentación/Exposición".
- As "Prácticas de laboratorio" serán exclusivamente individuais.
- Para superar a materia será preciso acadar un mínimos do 50% en cada proba e sumar na nota final un mínimo de 5 puntos.
- No caso de constatar un comportamento non ético (copia, plaxio) nalgunha das entregas realizadas (total ou parcial), anularase a **totalidade** da contribución do correspondente elemento de avaliación ("Prácticas de laboratorio", "Exame de preguntas obxectivas") sobre a cualificación final.

Metodoloxía/Proba 1: "Exame de preguntas obxectivas"

Descripción: 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 ou de tipo test 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.

% Calificación: 50% (*Para liberar esta parte da avaliación debe obterse unha calificación igual o superior a 5 puntos sobre 10)*.

Competencias avaliadas: CB3, CG3, CG7, CE7, CE29, CE32, CE34, CE37, CT7, CT8

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

Metodología/Proba 2: Prácticas de laboratorio

Descripción:

Avaliación das competencias revisadas no proxecto de programación con APIs criptográficas. Entregarase o códido desenvolvido xunto cunha 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.

% Calificación: 50% (*Para liberar esta parte da avaliación debe obterse unha calificación igual ou superior a 5 puntos sobre 10)*.

Competencias avaliadas: CB2,CG3,CG4,CG7,CE7,CE29,CE32,CE34,CT7,CT8,CT9,CT11,CT12,CT14

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

CRITERIOS DE AVALIACIÓN PARA 2ª EDICIÓN DE ACTAS E FIN DE CARREIRA

Para os alumnos "asistentes" empregarase o mesmo esquema de avaliación descrito na sección "CRITERIOS DE AVALIACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS".

- Os alumnos só deberán superar as partes non liberadas na primeira edición das actas
- Dado que na "segunda convocatoria" non é posible a avaliación de "Presentacións/exposicións", os alumnos que non fixeran a súa presentación no periodo de clases regular non poderán optar a contar con esa porción da nota.

Para os alumnos "non asistentes" empregarase o mesmo esquema de avaliación descrito na sección "CRITERIOS DE AVALIACIÓN PARA NON ASISTENTES".

PROCESO DE CALIFICACIÓN DE ACTAS

No caso dos alumnos que superen parte dos elementos avaliados, pero non alcancen o mínimo preciso para aprobar a materia completa, a calificación a incluir nas respectivas actas calcularase como o mínimo entre a media ponderada das partes superadas e 4,9.

DATAS DE AVALIACIÓN

O calendario de probas de avaliación aprobado oficialmente pola Xunta de Centro da ESEI atópase publicado na páxina web http://www.esei.uvigo.es

Bibliografía. Fontes de información

Bibliografía Básica

W. Stallings, **Cryptography and Network Security: Principles and Practice**, 978-0134444284, 7th edition, Prentice Hall, 2017

W. Stallings, L. Brown, **Computer Security: Principles and Practice**, 978-0134794105, 4rd edition, Prentice Hall, 2017

J. L. García Rambla, **Ataques en redes de datos IPv4 e IPv6**, 978-8461792788, 2da edición, 0xWORD, 2014

Bibliografía Complementaria

Carlos Álvarez Martín y Pablo González Pérez, **Hardening de servidores GNU / Linux**, 978-8461715183, 2ª ed., 0xWORD, 2014

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

Recomendacións

Materias que continúan o temario

Teoría de códigos/O06G150V01971

Materias que se recomenda ter cursado previamente

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

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.

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada polo COVID-19, a Universidade de Vigo establece unha planificación extraordinaria que se activará no momento en que as administracións e a propia institución determíneno atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou parcialmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun modo máis áxil e eficaz ao ser coñecido de antemán (ou cunha ampla antelación) polo alumnado e o profesorado a través da ferramenta normalizada e institucionalizada das guías docentes.

=== ESCENARIO 1: DOCENCIA MIXTA ===
No caso dunha situación excepcional na cal non se poida empregar o aforamento completo das aulas nas que se imparta docencia realizarase unha docencia mixta, na que parte do alumnado poderá asistir presencialmente ás clases, mentres que outra parte do alumnado poderá seguir as clases de forma online a través do Campus Remoto.

En tal situación, manteranse as metodoloxías e sistemas de avaliación.
As avaliacións trataranse de facer de forma presencial sempre que sexa posible. No caso de non ser posible, realizaranse a través de Campus Remoto, Faitic e/ou outros servizos da Universidade de Vigo. En tal caso, comunicarase ao alumnado con suficiente antelación.

Respecto das titorías, estas faranse, preferentemente, de forma online.
Co fin de poder facer unha mellor organización, os alumnos deberán comunicar ao profesorado o seu desexo de realizar unha titoría de forma previa a través dun correo electrónico.

=== ESCENARIO 2: DOCENCIA NON PRESENCIAL ===
No caso dunha situación excepcional na cal non se poida impartir docencia presencial, impartiranse as clases de forma online a través do Campus Remoto.

En tal situación, manteranse as metodoloxías e sistemas de avaliación.
As avaliacións realizaranse a través de Campus Remoto, Faitic e/ou outros servizos da Universidade de Vigo. Estes cambios comunicaranse ao alumnado con suficiente antelación.

Respecto das titorías, faranse de forma online e, co fin de poder facer unha mellor organización, os alumnos deberán comunicar ao profesorado o seu desexo de realizar unha titoría de forma previa a través dun correo electrónico.

En casos excepcionais nos que un alumno xustifique a existencia dunha situación que lle impida seguir a materia de forma normal (p.ex. problemas de conectividade, problemas de conciliación, etc.), poderá acordar co profesorado a adaptación das datas das probas de avaliación, así como dos medios para realizalas. En calquera caso, manteranse os sistemas de avaliación previstos.