



DATOS IDENTIFICATIVOS

Seguridade en sistemas informáticos

Materia	Seguridade en sistemas informáticos			
Código	O06G150V01702			
Titulación	Grao en Enxeñaría Informática			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OB	4	1c
Lingua de 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://fatic.uvigo.es			
Descrición xeral	A materia "Seguridade en Sistemas Informáticos" ubícase no cuarto curso do Grao en Enxeñaría 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

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.
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 humanos, 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
D1	I1: Capacidade de análise, síntese e avaliación

D7	I7: Capacidade de buscar, relacionar e estruturar información proveniente de diversas fontes e de integrar ideas e coñecementos
D8	I8: Resolución de problemas
D9	I9: Capacidade de tomar decisións
D10	I10: Capacidade para argumentar e xustificar lxicamente as decisións tomadas e as opinións
D11	P1: Capacidade de actuar autonomamente
D12	P2: Capacidade de traballar en situacións de falta de información e/ou baixo presión
D13	P3: Capacidade de integrarse rapidamente e traballar eficientemente en equipos unidisciplinares e de colaborar nun entorno multidisciplinar
D16	S1: Razoamento crítico
D17	S2: Compromiso ético e democrático
D18	S3: Aprendizaxe autónoma
D19	S4: Adaptación a novas situacións
D20	S5: Creatividade
D21	S6: Liderado
D22	S7: Ter iniciativa e ser resolutivo
D23	S8: Espírito emprendedor e ambición profesional
D24	S9: Ter motivación pola calidade e a mellora continua

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe			
RA1: Coñecer os fundamentos da criptografía moderna	A3	B3 B7	C7 C29 C37	D1 D8 D9
RA2: Coñecer a arquitectura de seguridade dos sistemas operativos actuais e saber configuralos e administralos de modo seguro	A2	B3 B4 B7 B12	C7 C29 C32 C37	D1 D7 D8 D9 D10 D11 D12 D13 D16 D18 D19 D20
RA3: Xestionar unha rede informática dun xeito 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: Coñecer os tipos de ataques informáticos máis habituais e as maneiras de protexerse contra eles	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

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 ameazas no software
- 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 intrusionés
- 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 despliegue 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	18	20	38
Prácticas de laboratorio	21	30	51
Aprendizaxe baseado en proxectos	7	20	27
Traballo tutelado	0	15	15
Presentación	2	5	7
Probas de resposta curta	2	10	12

*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 sesións 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.
Aprendizaxe baseado en proxectos	Proxecto práctico de programación de entidade media-baixa. Tratarase un exercicio individual ou en parellas relacionado coas competencias vinculadas ao uso de ferramentas criptográficas. Consistirá 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 maxistras, requirirá a entrega dunha pequena memoria.
Traballo tutelado	Pequeno traballo de investigación, individual ou en parellas, relacionado con aspectos da seguridade informática non incluídos 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 sesións 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 asistencia 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.
Aprendizaxe baseado en proxectos	Trátase dun traballo autónomo (ou en parellas) que contará coa titorización puntual do profesorado.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticas de laboratorio	Avaliación das competencias revisadas nas sesións de laboratorio relativas a seguridade en redes e sistemas operativos. Cada actividade proposta incluírá 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 incluírán unha descrición breve das tarefas realizadas e a resposta ás mencionadas cuestións/comprobacións. - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	35	A2 B3 C7 D8 B4 C29 D9 B7 C32 D10 C34 D12 D16 D17 D18 D19 D22 D24
Aprendizaxe baseado en proxectos	Avaliación das competencias revisadas no proxecto de programación con APIs criptográficas. Entregarase o código 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. - RESULTADOS APRENDIZAXE: RA1, RA4	10	A2 B3 C7 D1 B4 C29 D7 B7 C37 D10 D11 D13 D20 D22 D24
Traballo tutelado	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	A3 B7 C7 D1 B11 C29 D7 B12 C37 D10 D11 D16 D17 D20 D24
Presentación	Avaliación da presentación do traballo tutelado. Avaliarase a capacidade de síntese e de comunicación das ideas máis relevante, así como o fomento da discusión e a defensa/aclaración das dúbidas ou cuestións presentadas. - RESULTADOS APRENDIZAXE: RA2, RA3, RA4, RA5	5	A3 B7 C7 D10 B11 C29 D19 B12 C37 D20 D21 D22 D23 D24

Probas de resposta curta	Proba escrita onde se avaliarán os contidos e competencias revisados nas sesións maxistras e os aspectos teóricos da súa posta en práctica levada a cabo nas sesións prácticas. O tipo de proba consistirá 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 si os diversos contidos teórico e técnicas presentados no curso.	40	A3 B3 B7	C7 C29 C32 C34 C37	D1 D8 D10
--------------------------	--	----	----------	--------------------	-----------

- RESULTADOS APRENDIZAXE: RA1, RA2, RA3, RA4, RA5

Outros comentarios sobre a Avaliación

CRITERIOS DE AVALIACIÓN PARA ASISTENTES 1ª EDICIÓN DE ACTAS

- Para superar (e liberar) as "Probas de resposta curta" requírese acadar un 40% da puntuación máxima prevista para ese tipo de proba.
- Para superar (e liberar) as "Prácticas de laboratorio" e o "Proxecto" requírese acadar en conxunto un 40% da suma das puntuacións máxima previstas para ambas probas.
- Para superar a materia é preciso acadar os mínimos anteriores (en "Probas de resposta curta" e en "Prácticas de laboratorio" + "Proxecto") e sumar na nota final un mínimo de 5 puntos.
- No caso de constatar un comportamento non ético (copia, plaxio) nalguna das entregas realizadas (total ou parcial), anularase a totalidade da contribución do correspondente elemento de avaliación ("Prácticas de laboratorio", "Proxecto", "Traballo tutelado", "Probas de resposta curta") sobre a cualificación final.

CRITERIOS DE AVALIACIÓN PARA NON ASISTENTES

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

Metodoloxía/Proba 1: Probas de resposta curta

Descrición: Proba escrita onde se avaliarán os contidos e competencias revisados nas sesións maxistras e os aspectos teóricos da súa posta en práctica levada a cabo nas sesións prácticas. O tipo de proba consistirá 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 si 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, CT1, CT8, CT10

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

Metodoloxía/Proba 2: Prácticas de laboratorio

Descrición: Avaliación das competencias revisadas nas sesións de laboratorio relativas a seguridade en redes e sistemas operativos. Cada actividade proposta incluírá 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 incurrán unha descrición breve das tarefas realizadas e a resposta ás mencionadas cuestións/comprobacións.

% Calificación: 35% (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,CT8,CT9,CT10,CT12,CT16,CT17,CT18,CT22,CT24

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

Metodología/Proba 3: Proxectos

Descrición: Avaliación das competencias revisadas no proxecto de programación con APIs criptográficas. Entregarase o código 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.

% Calificación: 15% (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,CE37,CT1,CT7,CT10,CT11,CT13,CT20,CT22,CT24

Resultados de aprendizaxe avaliados: RA1, RA4

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 incluír 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/index.php?id=29>

Bibliografía. Fontes 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 Catalunya,

Manuel J. Lucena Lopez, **Criptografía y Seguridad en Computadores.**,

Antonio Villalon Huerta, **Seguridad en UNIX y Redes**,

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 levaráanse a cabo sobre Java, polo que precisárase 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.
