Escola de Enxeñaría de Telecomunicación

Páxina web

www.teleco.uvigo.es

Presentación

A Escola Enxeñaría de Telecomunicación, con acreditación institucional dende o 28/01/2019 (RD 420/2015), oferta un grao e catro másteres totalmente adaptados ao Espazo Europeo de Educación Superior, verificados pola ANECA axustándose ás Ordes Ministeriais CIN/352/2009 e CIN/355/2009.

Grao en Enxeñaría de Tecnoloxías de Telecomunicación (GETT) - Bachelor□s Degree in Telecommunication Technologies Engineering

(Acreditado EUR-ACE®, 15/04/2019; Plan de Excelencia Ultreia 2020 da Xunta de Galicia).

O Grao en Enxeñaría de Tecnoloxías de Telecomunicación habilita para o exercicio das profesións reguladas de enxeñería técnica. As profesións reguladas son aquelas para que o exercicio require cumprir unha condición especial que, xeralmente, é estar en posesión dun determinado título académico. Na actualidade, réxense polo Real Decreto 1837/2008. O Espazo Europeo de Educación Superior (EEES) determinou que as atribucións profesionais pódense adquirir coa titulación de grao (Enxeñeiros e Enxeñeiras Técnicos) ou coa titulación de mestrado universitario (Enxeñeiros e Enxeñeiras).

O GETT foi seleccionado para participar no Plan de Excelencia do Sistema Universitario de Galicia Ultreia 2020, no que se recolle un conxunto de accións que teñen como obxectivo que as universidades galegas poidan dar un novo salto de calidade. Ao abeiro deste plan, a partir do curso 2018/19 **ofértase un itinerario en inglés para que, os alumnos e alumnas que o desexen, podan cursar nesta lingua ata o 80% dos créditos da titulación**.

http://teleco.uvigo.es/images/stories/documentos/gett/diptico-uvigo-eet-grao-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/gett

Máster en Enxeñaría de Telecomunicación

Determinadas profesións reguladas necesitan un nivel de estudos maior e así, para poder exercelas, requírese ter cursado un mestrado universitario habilitante. O Mestrado en Enxeñaría de Telecomunicación é un mestrado con atribucións profesionais plenas de Enxeñeiro e Enxeñeira de Telecomunicación, regulado pola Orde Ministerial CIN/355/2009 de 9 de febreiro de 2009 e publicado no BOE nº 44 de 20/02/2009.

http://teleco.uvigo.es/images/stories/documentos/met/diptico-uvigo-eet-master-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/mit

Mestrados Interuniversitarios

A oferta educativa actual do centro complétase con diferentes mestrados interuniversitarios interrelacionados co sector empresarial.

Master Interuniversitario en Ciberseguridade; www: https://www.munics.es/

Máster Interuniversitario en Matemática Industrial: www: http://m2i.es

Equipo directivo

EQUIPO DIRECTIVO DO CENTRO

Director: Íñigo Cuíñas Gómez (teleco.direccion@uvigo.es)

Subdirección de Relaciones Internacionais: Enrique Costa Montenegro (teleco.subdir.internacional@uvigo.es)

Subdirección de Extensión: Francisco Javier Díaz Otero (teleco.subdir.extension@uvigo.es)

Subdirección de Organización Académica: Manuel Fernández Veiga (teleco.subdir.academica@uvigo.es)

Subdirección de Calidade: Loreto Rodríguez Pardo (teleco.subdir.calidade@uvigo.es)

Secretaría e Subdirección de Infraestruturas: Miguel Ángel Domínguez Gómez (teleco.subdir.infraestructuras@uvigo.es)

COORDINACIÓN DO GRAO EN ENXEÑARÍA DE TECNOLOXÍAS DE TELECOMUNICACIÓN

Coordinadora Xeral: Rebeca Díaz Redondo (teleco.grao@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_grao.pdf

COORDINACIÓN DO MESTRADO EN ENXEÑARÍA DE TELECOMUNICACIÓN

Coordinador Xeral: Manuel Fernández Iglésias (teleco.master@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master.pdf

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN CIBERSEGURIDADE

Coordinada Xeral: Ana Fernández Vilas (camc@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master_ciberseguridade.pdf

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN MATEMÁTICA INDUSTRIAL

Coordinadora Xeral: Elena Vázquez Cendón (USC)

Coordinador UVIGO: José Durany Castrillo (durany@dma.uvigo.es)

http://www.m2i.es/?seccion=coordinacion

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN VISIÓN POR COMPUTADOR

Coordinador Xeral: Xose Manuel Pardo López (USC)

Coordinador UVIGO: José Luis Alba Castro (jalba@gts.uvigo.es)

https://www.imcv.eu/legal-notice/

Máster Universitario en Ciberseguridade

Materias

Curso 1

Código	Nome	Cuadrimestre	Cr.totais

V05M175V01101	Xestión da seguridade da información	1c	6
V05M175V01102	Seguridade da información	1c	6
V05M175V01103	Seguridade en comunicacións	2c	6
V05M175V01104	Seguridade de aplicacións	1c	6
V05M175V01105	Redes Seguras	1c	6
V05M175V01201	Conceptos e leis en ciberseguridade	2c	3
V05M175V01202	Fortificación de sistemas operativos	1c	5
V05M175V01203	Tests de intrusión	2c	5
V05M175V01204	Análise de malware	2c	5
V05M175V01205	Seguridade como negocio	2c	3
V05M175V01206	Seguridade en dispositivos móbiles	2c	3
V05M175V01207	Análise forense de equipos	2c	3
V05M175V01208	Seguridade ubicua	2c	3
V05M175V01209	Ciberseguridade en contornas industriais	2c	3
V05M175V01210	Xestión de incidentes	2c	3

DATOS IDENTIFICATIVOS				
Xestión da seguridade da información				
Materia	Xestión da seguridade da información			
Código	V05M175V01101			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	1	1c
Lingua impartición	Castelán Galego			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel Dafonte Vázquez, José Carlos Fernández Vilas, Ana			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Nesta asignatura introdúcense os conceptos fundamentais relacionados coa xestión da seguridade da información (e.g. vulnerabilidade, ameaza, risco) e estúdanse as metodoloxías, ferramentas e especificacións que se ocupan da análise de riscos e do desenvolvemento de sistemas de xestión de seguridade da información.			

Competencias	
Código	
CB2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
CB3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
CG1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CG2	Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións.
CE5	Deseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
CE7	Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análisis de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
CE13	Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Coñecer os conceptos fundamentais relacionados coa Xestión da Seguridade da Información: vulnerabilidade, ameaza, risco, contramedida, política de seguridade, plan de seguridade, auditoría	CB2 CB3 CT4 CT5
Coñecer as diferentes metodoloxías de Xestión de Seguridade da Información, comúnmente aceptadas	CG1 CG2 CE5 CT5
Coñecer as ferramentas propias para levar a cabo tarefas relacionadas coa análise de riscos e a auditoría de seguridade, así como saber cales son as máis adecuadas a cada contorna	CG1 CG2 CE7 CE13 CT5

Contidos
Tema

Fundamentos	Conceptos básicos: Confidencialidade, Integridade, Dispoñibilidade, ameaza, risco, etc. Marco legal da ciberseguridade Normalización: estándares e especificacións Centros de operacións de seguridade
Análise de riscos, xestión e certificación	ISO 27005 e ISO 31000 Metodoloxías e ferramentas de análises de riscos Estratexia Nacional de Seguridade
Sistemas de Xestión de Seguridade da Información	ISO27000, 27001 y 27002 Esquema Nacional de Avaliación e Certificación das Tecnoloxías da Información Clasificación de información Formación e concienciación
Impacto de negocio	Roles de ciberseguridade Secuencia típica dun ataque Resilencia Xestión da continuidade do negocio Plan de continxencia
Auditoría de seguridade	Obxectivos de control Marcos e estándares para a auditoría Auditoría de seguridade dos datos persoais Delegado de protección de datos

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	19	29	48
Traballo tutelado	0.5	10	10.5
Prácticas de laboratorio	18	57	75
Exame de preguntas obxectivas	1.5	3	4.5
Estudo de casos	3	9	12

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

Metodoloxía docente

	Descrición
Lección maxistral	Presentación por parte do profesorado do temario da materia. Con esta metodoloxía trabállanse as competencias: CE5, CE7, CE13, CT4 e CT5.
Traballo tutelado	Cada alumno de forma individual realizará un traballo sobre un dos temas da asignatura a presentar no grupo A. Con esta metodoloxía traballaranse as competencias CG1, CG2, CT4 e CT5.
Prácticas de laboratorio	No laboratorio desenvolveranse prácticas guiadas e suscitaranse casos de estudo prácticos. Con esta metodoloxía traballaranse as competencias CB2, CB3, CG1, CG2, CE5, CE7, CE13 e CT5.

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	O profesorado da asignatura proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial ou en liña (durante a propia sesión magistral, ou durante o horario establecido para as titorías). O horario de titorías establecerase ao principio do curso e publicarase na páxina web da asignatura.
Prácticas de laboratorio	O profesorado da materia proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas de laboratorio. As dúbidas atenderanse de forma presencial (durante as prácticas, ou durante o horario establecido para titorias). O horario de titorias establecerase ao principio do curso e publicarase na páxina web da asignatura.
Traballo tutelado	O profesorado da materia proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas de laboratorio. As dúbidas atenderanse de forma presencial (durante as prácticas, ou durante o horario establecido para titorias). O horario de titorias establecerase ao principio do curso e publicarase na páxina web da asignatura.

Avaliación

	Descrición	Cualificación	Competencias Avaliadas

Traballo tutelado	Cada alumno de forma individual realizará un traballo sobre un dos temas da asignatura a presentar no grupo A	10		CG1 CG2		CT4 CT5
Exame de preguntas obxectivas	Exame de coñecementos teóricos e de desenvolvemento práctico	50		CG1 CG2	CE5 CE7 CE13	CT4 CT5
Estudo de casos	Desenvolveranse exercicios de casos prácticos sobre a análise de riscos e a realización de plans de seguridade	40	CB2 CB3		CE5 CE7 CE13	CT5

Outros comentarios sobre a Avaliación

Os estudantes poden decidir ser evaluados segundo un modelo de avaliación continua ou ben de avaliación única. Tódolos alumnos que entreguen o primeiro dos estudos de casos están optando pola avaliación continua. Unha vez os estudantes opten polo modelo de avaliación continua a súa cualificación non poderá ser nunca "Non presentado".

A cualificación será o resultado de aplicar a media ponderada entre os resultados: (i) exame escrito (50%), (ii) estudio de casos (40%) 3 (iii) traballo tutelado (10%).

Exame escrito:

Terá lugar nas datas publicadas no calendario oficial. Incluirá preguntas sobre os contidos e os casos prácticos.

Parte práctica:

1- Modelo de avaliación continua. Sendos informes de 2 casos prácticos e 2 avaliacións de informes de compañeiros que se entregarán nas semanas indicadas no documento que se facilitará aos alumnos o primeiro día de clase. Un informe será sobre análise de riscos e o outro sobre o desenvolvemento dun plan de seguridade (SGSI). Cada informe tenrá un peso na nota final do 15% e cada avaliación do 5%. Os informes desenvolveranse en grupo e todos os alumnos do mesmo grupo recibirán ea mesma cualificación. As avaliacións realizaranse de forma individual. Tamén é necesario realizar un traballo tutelado sobre un tema da asignatura a presentar no grupo A.

2- Modelo de avaliación única. Entrega individual de 2 informes dos dous casos prácticos na mesma data do exame escrito publicado no calendario oficial. Neste caso non se realizará a avaliación de informes de compañeiros e cada informe tenrá un peso na nota final do 25%.

Na avaliación en segunda oportunidade os estudantes serán avaliados utilizando a modalidade de avaliación única.

Si se detectase plaxio en calquera das probas de avaliación, a cualificación final da asignatura será de "suspenso (0)", feito que se comunicará á dirección da escola para adoptar as medidas oportunas.

Bibliografía. Fontes de información

Bibliografía Básica

Campbell, Tony, **Practical Information Security Management: A Complete Guide to Planning and Implementation**, Apress, 2016

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012).**, AENOR, 2015

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices. (ISO 22313:2012).**, AENOR, 2015

UNE-EN ISO, **Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)**, AENOR, 2017

UNE-EN ISO, **Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).**, AENOR, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000:2018)**, ISO/IEC, 2018

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Guidance (ISO/IEC 27003:2017)**, ISO/IEC, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016)**, ISO/IEC, 2016

ISO/IEC, **Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2011)**, ISO/IEC, 2011

Bibliografía Complementaria

Gómez Fernández, Luis y Fernández Rivero, Pedro Pablo, **Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS**, AENOR, 2015

Fernández Sánchez, Carlos Manuel y Piatiini Velthuis, Mario, **Modelo para el gobierno de las TIC basado en las normas ISO**, AENOR, 2012

ISO, **Risk management -- Principles and guidelines (ISO/IEC 31000:2009)**, ISO, 2009

Alan Calder Steve Watkins, **IT Governance: An International Guide to Data Security and ISO27001/ISO27002**, 5, Kogan Page, 2012

Alan Calder, **Nine Steps to Success - North American edition: An ISO 27001:2013 Implementation Overview**, 1, IT Governance Publishing, 2017

Edward Humphreys, **Implementing the ISO / IEC 27001 ISMS Standard**, 2, Artech House, 2016

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
Facilitaranse as presentacións para os grupos A a través de Faitic.

No caso dos grupos B o profesorado titor poderá establecer canles de comunicación co alumnado a través de Campus Remoto, Faitic ou outras ferramentas.

As titorías relalizaranse por medios telemáticos (correo electrónico, Campus Remoto, foros de Faitic, etc.) baixo cita previa.

=== ADAPTACIÓN DA AVALIACIÓN ===
En caso de activación de docencia non presencial, no se realizarán cambios en el modelo de evaluación.

DATOS IDENTIFICATIVOS				
Seguridade da información				
Materia	Seguridade da información			
Código	V05M175V01102			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	1	1c
Lingua impartición	Inglés			
Departamento	Dpto. Externo Enxeñaría telemática Teoría do sinal e comunicacións			
Coordinador/a	Fernández Veiga, Manuel			
Profesorado	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
Correo-e	mveiga@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Nesta materia se estúdanse as técnicas de criptografía e criptoanálise, a xeración de números e funcións aleatorias, os métodos de integridade de mensaxes, o cifrado autenticado, o cifrado asimétrico, os métodos de privacidade e anonimato da información, os esquemas de computación segura e a estenografía. Todas as anteriores son ferramentas básicas para a protección da información en redes e sistemas.			

Competencias	
Código	
CB2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
CB5	Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo
CE1	Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras.
CE4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
CE10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Coñecer os conceptos de cifrado Shannon, seguridad perfecta e seguridad semántica	CE1 CE10
Coñecer e saber utilizar os métodos de cifrado en fluxo	CE1 CE4 CE10
Coñecer e saber utilizar os métodos de cifrado en bloque, as función pseudoaleatorias e os estándares DES e AES	CE1 CE4 CE10
Comprender, saber construed e saber utilizer as funcións de hash, as función hash universais e con ellas os mecanismos de integridade da información	CE1 CE4 CE10
Comprender e saber utilizar os principios do cifrado de clave pública e os correspondentes esquemas criptográficos: Diffie-Hellman, RSA, ElGamal. Comprender e saber utilizar as firmas dixitais	CE1 CE4 CE10
Coñecer os fundamentos das técnicas de cifrado avanzado: cifrado con curvas elípticas e cifrado sobre retículas	CB2 CB5 CE1 CE4 CE10
Coñecer e saber utilizar os protocolos de intercambio de claves e de comunicación interactivas seguras	CB5 CE1 CE4 CE10

Coñecer, comprender e saber utilizar as técnicas de anonimización dos datos	CB5 CE1 CE4 CE10
Coñecer, comprender e saber aplicar as técnicas básicas de esteganografía, marcados de agua e forensía dixital	CB2 CB5 CE1 CE4 CE10
Coñecer e comprender as ideas básicas da computación segura	CB2 CB5 CE1 CE4 CE10

Contidos	
Tema	
1. Cifrado	Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap
2. Cifrado en fluxo	Xeneradores seudoaleatorios simples e compostos. Ataques. Casos de estudo
3. Cifrado en bloques	Cifrado en bloques. Seguridade. DES. AES. Función seudoaleatorias. Contrución de PRF e cifrado en bloques.
4. Integridade	Códigos de autenticación e integridade de mensajes. Definición de seguridad. MAC con claves. Función seudoaleatorias e MAC. Función hash. Hashing universal e resistente a colisión. Casos de estudio
5. Cifrado autenticado	Definición. Composición. Ataques. Exemplos e casos de estudo
6. Cifrado con clave pública	Definición. Seguridade semántica. Función ducha dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas dixitais. Casos de estudo.
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículos e cifrado sobre retículas. RLWE. Ataques cuánticos. Cifrado homomórfico
8. Protocolos de identificación	Definición. Contraseñas (dun so uso). Challenge.response. Sigma-protocolos. Esquemas de Okamoto y Schnorr. Casos de estudo.
9. Anonimización	Definición. t-integridade, divergência, análise
10. Ocultación de datos e forensía dixital	Definicións. Marcado de auga mediante espectro ensanchado. Codificación de papel sucio. Forensía dixital.
11. Computación segura	Función computables. Computación segura a días vías e a varias vías. Computación interactiva. Computación homomórfica. Aplicacións.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Resolución de problemas	0	24	24
Prácticas de laboratorio	18	36	54
Lección maxistral	17	51	68
Exame de preguntas de desenvolvemento	2	0	2
Resolución de problemas e/ou exercicios	1	0	1
Proxecto	1	0	1

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

Metodoloxía docente	
	Descrición
Resolución de problemas	Os estudantes resolverán problemas e exercícios sobre o material do curso. Con esta metodología trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT5.
Prácticas de laboratorio	Os estudantes desenvolverán no laboratorio prácticas de seguridade da información con ordenador, e un proxecto de programación sobre cifrado, forma, anonimato ou forenses. As prácticas e proyectos estarán supervisados polos profesores. Con esta metodología trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT4.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso. Con esta metodología trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT5.

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	Ofrecerase atención individual aos estudantes que precisen orientación para o estudo, explicacións adicionáis sobre os contados da disciplina, aclaración ou guía sobre resolución de problemas
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e ejercicios planteados las clases ou trabajados de exit autónomo
Prácticas de laboratorio	Responderanse individualmente as cuestión relativas ás prácticas de laboratorio e ao desenvolvimiento do proyecto

Avaliación

	Descrición	Cualificación	Competencias Avaliadas	
Exame de preguntas de desenvolvemento	Exame escrito. Resolución de cuestión, ejercicios ou problemas.	50	CB2 CB5	CE1 CE4 CE10
Resolución de problemas e/ou exercicios	2 ou 3 conjungos de problemas, ejercicios ou cuestión ao longo do curso, para resolución individual polos estudantes. Entrega por escrito	20	CB2 CB5	CE1 CE4 CE10
Proxecto	Desenvolvimento dun prospecto de implementación dun sistema de protección da información. Probas funcionais e de rendimiento.	30	CB2 CB5	CE1 CE4 CE10

Outros comentarios sobre a Avaliación

Déixanse a discreción dos alumnos dous métodos de avaliación alternativos na materia: avaliación continua e avaliación única.

A avaliación continua consistirá na realización dun exame final (50% da cualificación) e no desenvolvemento de proxectos de enxeñaría a escala (50% da cualificación) que se presentará antes do último día hábil anterior ao período oficial de exames. A avaliación única consistirá na realización dun exame fina escrito (60% da cualificación) e no desenvolvemento de proxectos de enxeñaría a escala (40% da cualificación) que se presentará antes do último día hábil anterior ao período oficial de exames. As probas escritas das modalidades de avaliación única e continua non serán necesariamente iguais.

Os alumnos optarán por unha ou outra modalidade de avaliación ata a data do exame escrito do curso.

Quen non superen a materia na primeira oportunidade da convocatoria dispoñen dunha segunda oportunidade ao final do curso na que se reavaliarán os seus coñecementos cunha proba escrita ou se reavaliará o seu proxecto se se mellorou ou modificou. Os pesos de cada unha das probas (exame e proxecto) serán os mesmos que no período ordinario de avaliación conforme á modalidade que se elixiu.

A cualificación das probas só fornece efecto no curso académico en que se obteñan, con independencia do itinerario de avaliación escollido.

Bibliografía. Fontes de información

Bibliografía Básica

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2018

Bibliografía Complementaria

O. Goldreich, **Foundation of cryptography, vol. I**, Cambridge University Press, 2007

O. Goldreich, **Foundation of cryptography, vol. ii**, Cambridge University Press, 2009

J. Katz, Y. Lindell, **Introduction to modern cryptography**, 2, CRC Press, 2015

A. Menezes, P. van Oorschot, S. Vanstone., **Handbook of applied cryptography**, CRC Press, 2001

C. Dwork, A. Roth, **The algorithmic foundations of differential privacy**, NOW Publishers, 2014

W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, **Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures**, Wiley, 2016

I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, **Digital watermarking and steganography**, 2, Morgan Kaufmann, 2008

A. El-Gamal, Y. Kim, **Network Information Theory**, Cambridge University Press, 2011

Recomendacións

Outros comentarios

A materia impártese en inglés. É recomendable ser capacidade para o razoamento matemático

Plan de Continxencias

Descrición

No caso de que a docencia tiñese que ser temporalmente interrumpida ou cancelada por motivos de saúde pública, todas as actividades da materia (clases, tarefas, exames, entregas) passarás a desenvolverse online coas ferramentas que dispoñan as universidades, e terán a mesma ponderación que a que figura nos outros apartados desta guía docente.

DATOS IDENTIFICATIVOS				
Seguridade en comunicacións				
Materia	Seguridade en comunicacións			
Código	V05M175V01103			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Fernández Iglesias, Diego Rodríguez Pérez, Miguel Rodríguez Rubio, Raúl Fernando			
Correo-e	rrubio@det.uvigo.es			
Web				
Descrición xeral	Esta materia realiza un repaso polas capas da arquitectura de comunicacións de Internet, mostrando as súas principais debilidades desde o punto de vista da seguridade, e proporcionando as técnicas e ferramentas necesarias para mitigalas. Os estudantes coñecerán en detalle os protocolos de rede que provén de seguridade á transmisión da información, e as implicacións derivadas do lugar que ocupan dentro da arquitectura en que se organiza o software de comunicacións.			

Competencias	
Código	
CB2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
CB4	Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
CB5	Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo
CG1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CG3	Capacidade para o razonamiento crítico e a evaluación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
CG5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
CE1	Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras.
CE2	Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
CE4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Comprender que outros protocolos, sendo auxiliares (non relativos ao mundo da seguridade), presentan vulnerabilidades explotables; e poderán describir os ataques máis comúns que tratan de aproveitalas, e os seus posibles contramedidas	CB5 CE4 CT4 CT5
Saber identificar que solución/protocolo é o axeitado para asegurar unha contorna determinada	CB5 CG1 CG3 CG5 CE1 CE2 CE4 CT4 CT5

Coñecer as solucións que se esconden tras certos servizos de rede e/ou aplicacións universalmente utilizadas	CB5 CE2 CE8 CT4 CT5
Ser capaces de configurar as diferentes ferramentas (paquetes software) que os distintos sistemas operativos/plataformas achégannos para activar a seguridade nas comunicacións.	CB2 CB5 CG5 CT4 CT5
Adquirir a capacidade de redactar informes técnicos xustificando a idoneidade dunha solución de ciberseguridade para un problema ou contorna determinada	CB4 CG1 CG3

Contidos	
Tema	
Arquitectura e protocolos de Internet	Conceptos fundamentais.
Seguridade no nivel de enlace	Seguridade en redes cableadas/Ethernet: Control de acceso e autenticación baseada en portos Confidencialidade en redes Ethernet Seguridade en redes sen fíos/WiFi: WPA/2/3 seguridade persoal WPA/2/3 seguridade empresarial
Seguridade no nivel de rede	IPsec Protocolos de seguridade Xestión dinámica de chaves Mecanismos de autenticación
Asegurando a infraestrutura de Internet	Encamiñamento seguro Seguridade en DNS Seguridade en TCP
Seguridade na transmisión dos datos	O protocolo TLS Suites criptográficas Infraestrutura WebPKI Validación de certificados
Seguridade en redes móbiles	Arquitectura do sistema Asociación e autenticación do terminal/usuario Privacidade

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	21	21	42
Prácticas de laboratorio	19	19	38
Prácticas con apoio das TIC	0	58	58
Exame de preguntas de desenvolvemento	2	0	2
Informe de prácticas, prácticum e prácticas externas	0	10	10
*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.			

Metodoloxía docente	
	Descrición
Lección maxistral	As sesións maxistrais seguen o esquema habitual para este tipo de docencia. Nestas sesións trabállanse as competencias CG3, CE1, CE2, CE4, CE8
Prácticas de laboratorio	Realizaranse varias sesións prácticas guiadas polos profesores onde se asentarán os conceptos apresos nas clases teóricas. En ditas prácticas utilizaranse dispositivos de rede reais (routers e switches) e/ou software de virtualización que permitirá ao alumno a súa instrución e adestramento na súa propia casa. De forma natural, as actividades definidas poderán incluír apartados/retos adicionais que complementarán o traballo autónomo do estudante, que se describe no seguinte item. Os alumnos deben adquirir nas prácticas as competencias CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Prácticas con apoio das TIC	Máis aló das prácticas guiadas, o alumno terá que despregar/configurar/implementar algunhas solucións particulares, para certos escenarios, de forma autónoma. Nestas actividades trabállanse as competencias CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	Durante as horas de titoría os docentes realizarán unha atención personalizada para fortalecer ou orientar ao alumno na comprensión dos conceptos teóricos explicados nas clases maxistrais ou nas sesións demostrativas de carácter práctico; e para corrixir ou reorientar os pequenos traballos prácticos optativos derivados de devanditas clases de laboratorio.
Prácticas de laboratorio	Esta actividade é interactiva por definición, polo que se espera que as cuestións flúan con naturalidade entre docentes e estudantes, podendo involucrar a outros estudantes nas respostas buscadas.
Prácticas con apoio das TIC	Aínda que o traballo autónomo está orientado a que o estudante resolva pola súa conta situacións/retos que se atopará nos sistemas reais, nas horas de titoría os docentes poderán orientalo cuestionando as solucións elixidas ou suxerindo camiños alternativos.

Avaliación

	Descrición	Cualificación	Competencias Avaliadas
Prácticas de laboratorio	Serán cualificadas como apto/non apto. O alumno será apto se asiste a todas as sesións deste tipo. Se por algún motivo perdera algunha, deberá suplila realizando algunha práctica complementaria que o profesor definirá no seu momento. Nalgunhas das sesións/actividades poderase solicitar ao alumno un traballo autónomo adicional (e o seu informe asociado) que se avaliará cuantitativamente dentro do ítem máis xeral que denominamos "Prácticas autónomas a través de TIC"	0	CB2 CG5 CE4 CT4 CB4 CE8 CT5 CB5
Prácticas con apoio das TIC	Os estudantes terán que realizar, ante os profesores, a demostración práctica que mostre a resolución dos distintos retos técnicos abordados, enfrontándose a preguntas sobre as solucións adoptadas e o seu grao de finalización. Esta defensa/entrevista terá lugar, por termo xeral, tras a entrega da última tarefa encargada e antes do periodo oficial de exames de cada convocatoria; consensuándose a data concreta entre alumnos e profesores con antelación suficiente. Todo reto ou actividade autónoma esixirá un informe escrito, cuxa estrutura, composición e claridade terán o seu peso na valoración final.	40	CB2 CG5 CE1 CT4 CB4 CE4 CT5 CB5 CE8
Exame de preguntas de desenvolvemento	Realizarase un exame escrito ao final do cuadrimestre, onde se avaliarán tanto os conceptos teóricos impartidos nas sesións maxistrais, como os fundamentos prácticos derivados das clases/traballos prácticos acometidos.	60	CB4 CE1 CT4 CE2 CE4
Informe de prácticas, prácticum e prácticas externas	O traballo autónomo do alumno deberá ser recollido nos informes de prácticas pertinentes, e a súa valoración formará parte da valoración integral daquel.	0	CB4 CG1 CT4 CG3 CT5

Outros comentarios sobre a Avaliación

A avaliación da materia poderá seguir a canle de avaliación continua ou ben avaliación única. Un alumno elixirá avaliación continua ao entregar a solución e informe do primeiro reto ou traballo autónomo que se lle esixa durante o devir normal do curso. As porcentaxes expresadas no epígrafe anterior só reflicten o máximo conseguible en cada tipo de proba na modalidade de avaliación continua; e son só orientativos. A forma de avaliación detallada exprésase a continuación:

Para a avaliación continua (primeira oportunidade), a nota final será a media xeométrica ponderada entre a nota do traballo autónomo (TA, 40%) e a cualificación correspondente ao exame de preguntas de desenvolvemento (E, 60%). A nota TA será a media aritmética das cualificacións asociadas a cada un dos retos/prácticas autónomas que o alumno terá que resolver ao longo do cuadrimestre.

NOTA FINAL(EC)=(TA^0.4)x(E^0.6)

Se as prácticas de laboratorio foron cualificadas como non aptas, a nota será a mínima entre a nota do exame escrito (E) e 3.

Os alumnos que opten pola avaliación única deberán presentarse a un exame final que consistirá de tres partes: unha proba escrita análoga á proba de avaliación continua (E), unha proba de aptitude no laboratorio e un ou varios traballos prácticos (T). A nota final, neste caso, é a media xeométrica ponderada entre a nota de teoría (E, 80%) e o traballo práctico (T, 20%), coa condición de que se supere a proba de aptitude. Se o alumno non supera a proba de aptitude, a nota final será o mínimo entre E e 3.

NOTA FINAL(EU)=(T^0.2)x(E^0.8)

Finalmente, para a segunda oportunidade (xuño/xullo), o alumno poderá proseguir co modo de avaliación que xa elixira (conservándoselle a nota da parte -E ou TA/T- que superase, e afrontando unicamente a parte suspensa - con posibles modificacións nas especificacións dos traballos prácticos), ou encarar desde cero unha avaliación que terá as mesmas características que o exame final que acabamos de describir. A proba de aptitude só será necesaria se non asistiu a todas as sesións do laboratorio.

Bibliografía. Fontes de información

Bibliografía Básica

I. Ristic, **Bulletproff SSL and TLS, ser. Computers/Security**, London: Fesity Duck, 2015

A. Liska and G. Stowe, **DNS Security: Defending the Domain Name System**, Boston: Syngress, 2016

Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya, **RADIUS / AAA / 802.1x**, RA-MA Editorial, 2008

Graham Bartlett, Amjad Inamdar, **IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS**, CISCO PRESS, 2016

Bibliografía Complementaria

D. J. D. Touch, **Defending TCP Against Spoofing Attacks**, IETF, 2007

R. R. Stewart, M. Dalal, and A. Ramaiah, **Improving TCP□s Robustness to Blind In-Window Attacks**, IETF, 2010

D. J. Bernstein, **SYN cookies**,

P. McManus, **Improving syncookies**, 2008

C. Pignataro, P. Savola, D. Meyer, V. Gill, and J. Heasley, **The Generalized TTL Security Mechanism (GTSM)**, IETF, 2007

D. J. D. Touch, R. Bonica, and A. J. Mankin, **The TCP Authentication Option**, IETF, 2010

S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, **DNS Security Introduction and Requirements**, IETF, 2005

R. Arends, R. Austin, M. Larson, D. Massey, S. Rose, **Resource Records for the DNS Security Extensions**, IETF, 2005

R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, **Protocol Modifications for the DNS Security Extensions**, IETF, 2005

Cloudflare Inc., **How DNSSEC works**,

P. E. Hoffman and P. McManus, **DNS Queries over HTTPS (DOH)**, IETF, 2018

E. Jones and O. L. Moigne, **OSPF security vulnerabilities analysis**, IETF, 2006

M. Khandelwal and R. Desetti, **OSPF security: Attacks and defenses**, 2016

J. Durand, I. Pepelnjak, and G. Doering, **BGP operations and security**, IETF, 2015

R. Kuhn, K. Sriram, and D. Montgomery, **Border gateway protocol security**, NIST, 2007

C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, **Making route flap damping usable**, IETF, 2014

Y. Rekhter, J. Scudder, S. S. Ramachandra, E. Chen, and R. Fernando, **Graceful restart mechanism for BGP**, IETF, 2007

IEEE 802.1 Working Group, **IEEE Std 802.1X - 2010. Port-Based Network Access Control**, IEEE Computer Society, 2010

Security Task group of IEEE 802.1, **IEEE Std 802.1AE. Medium Access Control Security**, IEEE Computer Society, 2018

S. Kent, K. Seo, **Security Architecture for the Internet Protocol**, IETF, 2005

S. Kent, **IP Authentication Header**, IETF, 2005

S. Kent, **IP Encapsulating Security Payload**, IETF, 2005

C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, **Internet Key Exchange Protocol Version 2 (IKEv2)**, IETF, 2014

J. Cichonski, J. M. Franklin, M. Bartock, **Guide to LTE Security**, NIST Special Publication 800-187,

Recomendacións

Materias que se recomenda ter cursado previamente

Redes Seguras/V05M175V01105
Seguridade da información/V05M175V01102

Plan de Continxencias

Descrición

Non se prevé que sexa necesario realizar ningún cambio na planificación docente da materia. Todas as tarefas previstas poden ser desenvolvidas de xeito remoto cos equipos con que normalmente contan os estudiantes.

DATOS IDENTIFICATIVOS				
Seguridade de aplicacións				
Materia	Seguridade de aplicacións			
Código	V05M175V01104			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	1	1c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	López Nores, Martín			
Profesorado	Bellas Permuy, Fernando López Nores, Martín Losada Pérez, José			
Correo-e	mlnores@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530005&any_academic=2018_19&idioma_assig=cast			
Descrición xeral	Desenvolver aplicacións seguras non é unha tarefa trivial. Coñecer as vulnerabilidades que habitualmente sofren as aplicacións, os mecanismos de autenticación, autorización e control de acceso, así como a incorporación da seguridade ó ciclo de vida de desenrolo, é esencial para poder construír e manter aplicacións seguras con éxito. En esta materia estúdanse de forma práctica todos estes aspectos, con especial énfase no desenvolvemento de aplicacións e servizos web			

Competencias
Código

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

Plan de Continxencias
Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS

Redes Seguras

Materia	Redes Seguras			
Código	V05M175V01105			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	6	OB	1	1c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Rodríguez Pérez, Miguel			
Profesorado	Nóvoa de Manuel, Francisco Javier Rodríguez Pérez, Miguel Rodríguez Rubio, Raúl Fernando			
Correo-e	miguel@det.uvigo.gal			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530006&any_academic=2018_19&idioma_assig=cast			
Descrición xeral	A materia Redes Seguras ten como obxectivo principal que os estudantes aprendan a deseñar e implementar infraestruturas de rede capaces de proporciona-los servizos de seguridade precisos nun contorno corporativo moderno. Deberán coñecer as arquitecturas de seguridad de referencia e seren quen de configuralas en mantelas, utilizando para iso tecnoloxías como VPN, IDS/IPS e Firewalls entre outros. A materia esta concebida para que as prácticas de laboratorio, con equipos físicos e virtuáis teñan unha importancia capital no proceso de aprendizaxe			

Competencias

Código

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS				
Conceptos e leis en ciberseguridade				
Materia	Conceptos e leis en ciberseguridade			
Código	V05M175V01201			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OB	1	2c
Lingua impartición	Castelán Galego Inglés			
Departamento	Dereito público Dpto. Externo			
Coordinador/a	Rodríguez Vázquez, Virgilio			
Profesorado	Faraldo Cabana, Patricia Rodríguez Vázquez, Virgilio			
Correo-e	virxilio@uvigo.es			
Web				
Descrición xeral	Nesta materia farase unha aproximación á normativa relativa á ciberseguridade. A continuación realizarase un estudo criminolóxico dos principais delitos informáticos. O bloque central está formado por unha revisión sistemática da regulación dos delitos informáticos contida no Código Penal español. Ademais, analizarase a xurisprudenza existente nesta materia.			

Competencias	
Código	
CB3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
CE3	Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CT1	Ter capacidade para comprender o significado e aplicación da perspectiva de xénero nos distintos ámbitos de coñecemento e na práctica profesional co obxectivo de acadar unha sociedade máis xusta e igualitaria.
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.	CB3
Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información	CE3
Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade.	CE8
Ter capacidade para comprender o significado e aplicación da perspectiva de xénero nos distintos ámbitos de coñecemento e na práctica profesional co obxectivo de acadar unha sociedade máis xusta e igualitaria.	CT1
Ter capacidade para comunicarse oralmente e por escrito en inglés.	CT5

Contidos	
Tema	
1. Introducción ao Dereito sobre ciberseguridade. Revisión das normativas en materia de seguridade informática e xestión de riscos.	1.1. A normativa da UE. 1.2. A Lei de Seguridade Nacional: a estratexia de ciberseguridade nacional e o esquema de seguridade nacional. 1.3. O Regulamento (UE) 2016/679 de 27 de abril de 2016, Regulamento Xeral de Protección de Datos (RXPD). A Lei Orgánica de Protección de Datos e o Regulamento de desenvolvemento. 1.4. O Código Penal en materia de delitos informáticos.
2. Aproximación criminolóxica aos delitos informáticos.	2.1. Fontes estatísticas: principais organismos nacionais e internacionais. 2.2. Análise dos principais informes sobre cibercriminalidade. 2.3. Identificación dos principais recursos tecnolóxicos utilizados.

3. A vulneración da ciberseguridade a través de conductas delictivas.	3.1. Precisións terminolóxicas: delitos informáticos e cibercrime. 3.2. A utilización das TIC para cometer delitos e cando as TIC son o obxeto do delito. 3.3. O Código Penal español, LO 10/1995, de 23 de novembro, a Directiva Europea 2013/40/UE do Parlamento Europeo e do Consello, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de información, Convenio sobre cibercriminalidade ou Convenio de Budapest, do Consello de Europa, de 23 de novembro de 2001.
4. As principais conductas delictivas que afectan á ciberseguridade.	4.1. Delitos de descubrimento e revelación de segredos (I). Riscos frecuentes: ransomware e o roubo de información. 4.2. Delitos de descubrimento e revelación de segretos (II). Acceso e interceptación ilícita. O acceso a ficheiros ou soportes informáticos, electrónicos ou telemáticos. Especial atención ao responsable dos ficheiros ou soportes. A interceptación de transmisións de datos informáticos. A utilización de malware (virus, troianos e spyware). 4.3. Delitos de descubrimento e revelación de segretos (III). Producir, adquirir, importar ou facilitar programas informáticos para cometer os delitos anteriores, ou contrasinais de ordenador ou códigos de acceso. 4.4. Delitos contra a intimidade e o dereito á propia imaxe: o uso indebido de cookies. 4.5. Delitos contra a propiedade (I). Estafas valéndose dalgunha manipulación informática. Producir, posuír ou facilitar programas informáticos destinados a ese fin. 4.6. Delitos contra a propiedade (II). Defraudación utilizando sinal de telecomunicacións allea. Uso de terminal de telecomunicacións sen consentimento do titular. 4.7. Delitos contra a propiedade (III). Danos en datos informáticos, programas informáticos ou documentos electrónicos. Danos a sistemas informáticos. Danos a sistemas informáticos dunha infraestructura crítica (breve referencia aos operadores de infraestructuras críticas, aos plans de seguridade do operador e aos plans de protección específicos). Obstaculizar ou interromper o funcionamento dun sistema informático alleo. Fabricar, posuír ou facilitar a terceiros programas informáticos con tal fin. Especial referencia á responsabilidade penal das persoas xurídicas. 4.8. Delitos contra a propiedade intelectual e industrial. A través da prestación de servizos da sociedade da información ou a través dun portal de acceso a internet. 4.9. Delitos relativos ao mercado e aos consumidores. Descubrimento de segredos de empresa a través das TIC. Acceso intelixible a un servizo de radiodifusión sonoro ou televisivo, a servizos interactivos prestados a distancia por vía electrónica. 4.10. Delitos contra a fe pública: falsedades electrónicas.
5. Delitos cometidos contra as persos utilizando as TIC.	5.1. Delitos contra a liberdade. Ameazas e coaccións utilizando redes sociais ou outras TIC. Ciberstalking. 5.2. Delitos contra a liberdade e indemnidade sexuais. Child grooming e pornografía infantil. 5.3. Delitos contra a intimidade e a privacidade. 5.4. Delitos contra a honra. Lesión da reputación dixital.
6. O ciberterrorismo.	6.1. Concepto. 6.2. Delitos informáticos realizados cunha finalidade específica do art. 573 do Código Penal. 6.3. Delito de colaboración con organización ou grupo terrorista a través da prestación de servizos tecnolóxicos.
7. Delitos relativos á Defensa nacional e outros.	Breve aproximación.
8. Análise da xurisprudenza española en relación con delitos informáticos.	8.1. Especial atención á jurisprudenza do Tribunal Supremo. 8.2. Acordos do pleno non xurisdiccional da Sala Segunda do Tribunal Supremo relativos a delitos informáticos. 8.3. O Ministerio Fiscal e a Fiscalía especialista en materia de criminalidade informática.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	13	32	45
Prácticas de laboratorio	5	22	27
Exame de preguntas obxectivas	2	0	2
Resolución de problemas e/ou exercicios	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/a dos contidos sobre a materia obxecto de estudo, bases teóricas e/ou directrices dun traballo, exercicio que o/a estudante ten que desenvolver.
Prácticas de laboratorio	Actividades de aplicación dos coñecementos a situacións concretas e de adquisición de habilidades básicas e procedementais relacionadas coa materia obxecto de estudo.

Atención personalizada	
Metodoloxías	**Descrición**
Lección maxistral	O alumnado será atendido nos horarios de titorías que serán publicados na web do Máster. Poderá atenderse, previa cita -concertada mediante correo electrónico-, ou ben a través de correo electrónico ou ben a través de despacho virtual no campus remoto-integra da Universidad de Vigo.
Prácticas de laboratorio	O alumnado será atendido nos horarios de titorías que serán publicados na web do Máster. Poderá atenderse, previa cita -concertada mediante correo electrónico-, ou ben a través de correo electrónico ou ben a través de despacho virtual no campus remoto-integra da Universidad de Vigo.

Avaliación				
	Descrición	Cualificación	Competencias Avaliadas	
Exame de preguntas obxectivas	O sistema de avaliación continua consistirá en tres exames escritos: os dous primeiros, de resolución de probas obxetivas parciais (□exames de preguntas obxectivas□, tipo test, aos que se refire este apartado da Guía), e o terceiro, de "resolución de problemas" (referido no seguinte apartado da guía). Os exames correspondentes á "resolución de preguntas obxectivas", probas tipo test: - celebraranse ao longo do curso, en horario de clase maxistral. A planificación das diferentes probas de avaliación intermedia aprobarase nunha Comisión Académica de Máster Interuniversitaria (CAMI) e estará dispoñible ao principio do cuadrimestre. - cada exame comprenderá a parte do temario que respectivamente se indique ao inicio do cuadrimestre por parte do coordinador da materia - consistirán en probas tipo test, para cuxa cualificación, de 0 a 2,5 puntos cada unha delas, as respostas correctas suman 0,1 e as incorrectas restanm 0,05, non puntuando as deixadas en branco -Ámbolos dous exames ponderaranse ao 50% para a cualificación final, correspondendo o outro 50% á "resolución de problemas" (que se describe no apartado seguinte). Para superar a materia polo sistema de avaliación continua é necesario que a nota resultante dos tres exames, de acordo coa ponderación indicada, sexa igual ou superior a 5 puntos. Quen acuda á primeira proba parcial (ao primeiro exame de preguntas obxectivas, tipo test), manifestando así o seu interese por acollerse a este sistema de avaliación continua, será avaliado nesta oportunidade de acordo cos criterios previamente establecidos e non terá dereito a ser avaliado mediante un exame final que constitúa o 100% da cualificación da materia. Polo tanto, realizada a primeira proba parcial, non é posible renunciar ao sistema de avaliación continua. Se realizada a primeira proba parcial, a alumna ou alumno non se presentase á seguinte ou seguintes, a cualificación destas será de 0 puntos.	50	CB3 CE3 CE8	CT1

Resolución de problemas e/ou exercicios	O sistema de avaliación continua consistirá en tres exames escritos: os dous primeiros, de resolución de probas obxetivas parciais (exames de preguntas obxectivas, tipo test, aos que se refire o apartado anterior da Guía), e o terceiro, de "resolución de problemas" (referido neste apartado da guía). O devandito exame correspondente á "resolución de problemas": - celebrarase na data oficial de exame final da convocatoria ordinaria: primeira oportunidade, segundo o calendario oficial aprobado pola Comisión Académica do Máster no curso 2019-2020 - consistirá na resolución dun ou varios casos prácticos e calificarase de 0 a 5 puntos - Os problemas que plantexen os casos prácticos poden afectar a cuestións comprendidas na totalidade do temario -Ponderarase ao 50% para a cualificación final, correspondendo o outro 50% aos dous exames anteditos de preguntas obxectivas, de tipo test. Para superar a materia polo sistema de avaliación continua é necesario que a nota resultante dos tres exames, de acordo coa ponderación indicada, sexa igual ou superior a 5 puntos. Quen acuda á primeira proba parcial, manifestando así o seu interese por acollerse a este sistema de avaliación continua, será avaliado nesta oportunidade de acordo cos criterios previamente establecidos e non terá dereito a ser avaliado mediante un exame final que constitúa o 100% da cualificación da materia. Polo tanto, realizada a primeira proba parcial, non é posible renunciar ao sistema de avaliación continua. Se realizada a primeira proba parcial, a alumna ou alumno non se presenta á seguinte ou seguintes, a cualificación destas será de 0 puntos.	50	CB3	CE3 CE8	CT1 CT5

Outros comentarios sobre a Avaliación

1. PRIMEIRA OPORTUNIDADEa) SISTEMA DE AVALIACIÓN CONTINUADescríbese nos apartados anteriores.
b) SISTEMA DE EXAME FINAL

Para quen non opte polo sistema de avaliación continua, a avaliación da materia consistirá nun único exame final, na data fixada no calendario oficial aprobado pola Comisión Académica do Máster para o curso 2020-2021.
O devandito exame, que comprenderá a totalidade do temario e constitúe o 100% da cualificación da materia, constará de dúas partes, unha teórica e outra práctica, que se cualificarán de 0 a 5 puntos cada unha delas. A parte teórica consistirá en probas tipo test, para cuxa cualificación as respostas correctas suman o dobre que restan as incorrectas, non puntuando as deixadas en branco. A parte práctica consistirá na resolución dun ou varios casos prácticos. A cualificación final do exame será a suma das cualificacións obtidas en cada unha das partes. Para superar a materia é necesario obter un mínimo de 5 puntos na suma da cualificación de ámbalas dúas partes.

2. SEGUNDA OPORTUNIDADE E CONVOCATORIA EXTRAORDINARIA

A avaliación da materia consistirá nun único exame final, na data fixada no calendario oficial aprobado pola Comisión Académica do Máster para o curso 2020-2021.
O devandito exame, que comprenderá a totalidade do temario e constitúe o 100% da cualificación da materia, constará de dúas partes, unha teórica e outra práctica, que se cualificarán de 0 a 5 puntos cada unha delas. A parte teórica consistirá en probas tipo test, para cuxa cualificación as respostas correctas suman o dobre que restan as incorrectas, non puntuando as deixadas en branco. A parte práctica consistirá na resolución dun ou varios casos prácticos. A cualificación final do exame será a suma das cualificacións obtidas en cada unha das partes. Para superar a materia é necesario obter un mínimo de 5 puntos na suma da cualificación de ámbalas dúas partes.

Bibliografía. Fontes de información

Bibliografía Básica

DE LA CUESTA ARZAMANDI, José Luis (dir.), **Derecho penal informático**, 1.ª, Civitas, 2010

LUZÓN PEÑA, Diego-Manuel (dir.), **Código Penal**, 5.ª, Reus, 2017

Bibliografía Complementaria

BARONA VILAR, Silvia, **Justicia civil y penal en la era global**, 1.ª, Tirant lo Blanch, 2017

BARRIO ANDRÉS, Moisés, **Ciberdelitos : amenazas criminales del ciberespacio : adaptado reforma Código Penal 2015**, 1.ª, Reus, 2017

CRESPO SANCHÍS, Carolina (coord.), **Fraude electrónico : panorámica actual y medios jurídicos para combatirlo**, 1.ª, Civitas, 2013

CRUZ DE PABLO, José Antonio, **Derecho penal y nuevas tecnologías : aspectos sustantivos : adaptado a la reforma operada en el Código penal por la Ley orgánica 15-2003 de 25 de noviembre, especial referencia al arículo 286 CP**, 1.ª, Difusión Jurídica y Temas de actualidad, 2006

CUERDA ARNAU, María Luisa (coord.), **Menores y redes sociales : ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia en la red**, 1.ª, Tirant lo Blanch, 2016

DAVARA RODRÍGUEZ, Miguel Ángel, **Manual de derecho informático**, 11.ª, Thomson-Aranzadi, 2015

DE NOVA LABIÁN, Alberto José, **Delitos contra la propiedad intelectual en el ámbito de Internet : especial referencia a los sistemas de intercambio de archivos**, 1.ª, Dykinson, 2010

DE URBANO CASTRILLO, Eduardo et al., **Delincuencia informática : tiempos de cautela y amparo**, 1.ª, Aranzadi, 2012

FARALDO CABANA, Patricia, **Las Nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico**, 1.ª, Tirant lo Blanch, 2009

FERNÁNDEZ TERUELO, Javier Gustavo, **Cibercrimen, los delitos cometidos a través de Internet : estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y ot**, 1.ª, Constitutio Criminalis Carolina, 2017

FLORES PRADA, Ignacio, **Criminalidad informática : (aspectos sustantivos y procesales)**, 1.ª, Tirant lo Blanch, 2012

GALÁN MUÑOZ, Alfonso, **El Fraude y la estafa mediante sistemas informáticos : análisis del artículo 248.2 C.P**, 1.ª, Tirant lo Blanch, 2005

GIANT, Nikki, **Ciberseguridad para la i-generación : usos y riesgos de las redes sociales y sus aplicaciones**, 1.ª, Narcea, 2016

GÓMEZ RIVERO, M.ª del Carmen (dir.), **Nociones fundamentales de Derecho penal. Parte especial. Volumen I**, 2.ª, Tecnos, 2015

GÓMEZ RIVERO, M.ª del Carmen (dir.), **Nociones fundamentales de Derecho penal. Parte especial. Volumen II**, 2.ª, Tecnos, 2015

GÓMEZ TOMILLO, Manuel, **Responsabilidad penal y civil por delitos cometidos a través de Internet : especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces**, 2.ª, Thomson-Aranzadi, 2006

GONZÁLEZ CUSSAC, José Luis (coord.), **Derecho penal. Parte especial**, 5.ª, Tirant lo Blanch, 2016

GONZÁLEZ CUSSAC, José Luis/CUERDA ARNAU, M.ª Luisa (dirs.), **Nuevas amenazas a la seguridad nacional : terrorismo, criminalidad organizada y tecnologías de la información y la comunicación**, 1.ª, Tirant lo Blanch, 2013

GOODMAN, Marc, **Future crimes : inside the digital underground and the battle for our connected world**, 1.ª, Pegasus Books, 2016

HILGENDORF, Eric, **Computer- und Internetstrafrecht : ein Grundriss**, 1.ª, Springer, 2005

Instituto Español de Estudios Estratégicos, Grupo de Trabajo número 03/10, **Ciberseguridad : retos y amenazas a la seguridad nacional en el ciberespacio**, 1.ª, Ministerio de Defensa, Dirección General de Relaci, 2011

LUZÓN PEÑA, Diego-Manuel, **Lecciones de Derecho penal. Parte general**, 3.ª, Tirant lo Blanch, 2016

MARZILLI, Alan, **The Internet and crime**, 1.ª, Chelsea House, 2010

MATA Y MARTÍN, Ricardo M., **Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago : el uso fraudulento de tarjetas y otros instrumentos de pago**, 1.ª, Thomson-Aranzadi, 2007

MORÓN LERMA, Esther, **Internet y derecho penal : "hacking" y otras conductas ilícitas en la red**, 2.ª, Aranzadi, 2002

MUÑOZ CONDE, Francisco/GARCÍA ARÁN, Mercedes, **Derecho penal. Parte general**, 9.ª, Tirant lo Blanch, 2015

ORENES, Eduardo, **Ciberseguridad familiar : cyberbullying, hacking y otros peligros en Internet**, 1.ª, Círculo Rojo, 2013

ORTS BERENGUER, Enrique/ROIG TORRES, Margarita, **Delitos informáticos y delitos comunes cometidos a través de la informática**, 1.ª, Tirant lo Blanch, 2001

QUERALT JIMÉNEZ, Joan Josep, **Derecho penal español. Parte especial**, 7.ª, Tirant lo Blanch, 2015

QUINTERO OLIVARES, Gonzalo (dir.), **Comentarios a la Parte especial del Derecho penal**, 10.ª, Aranzadi, 2016

RALLO LOMBARTE, Artemi, **El derecho al olvido en Internet : Google**, 1.ª, Centro de Estudios Políticos y Constitucionales, 2014

RODRÍGUEZ MESA, M.ª José, **Los delitos de daños**, 1.ª, Tirant lo Blanch, 2017

ROMEO CASABONA, Carlos M.ª (coord.), **El Cibercrimen : nuevos retos jurídico-penales, nuevas respuestas político-criminales**, 1.ª, Comares, 2006

RUEDA MARTÍN, M.ª Ángeles, **Protección penal de la intimidad personal e informática : (los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal)**, 1.ª, Atelier, 2004

SAIN, Gustavo, **Delitos informáticos : investigación criminal, marco legal y peritaje**, 1.ª, B de f, 2017

SÁINZ PEÑA, Rosa M.ª (coord.), **Ciberseguridad, la protección de la información en un mundo digital**, 1.ª, Fundación Telefónica, Ariel, 2016

SEGURA SERRANO, Antonio/GORDO GARCÍA, Fernando (coords.), **Ciberseguridad global : oportunidades y compromisos en el uso del ciberespacio**, 1.ª, Universidad de Granada, 2013

SILVA SÁNCHEZ, Jesús María (dir.)/RAGUÉS I VALLÉS, Ramón (coord.), **Lecciones de Derecho penal: Parte especial**, 5.ª, Atelier, 2018

SINGER, Peter Warren, **Cybersecurity and cyberwar : what everyone needs to know**, 1.ª, Oxford University Press, 2014

TOURIÑO, Alejandro, **El derecho al olvido y a la intimidad en Internet**, 1.ª, Los Libros de la Catarata, 2014

VALLS PRIETO, Javier, **Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial**, 1.ª, Dykinson, 2017

VELASCO NÚÑEZ, Eloy (dir.), **Delitos contra y a través de las nuevas tecnologías : ¿cómo reducir su impunidad?**, 1.ª, Consejo General del Poder Judicial,Centro de Docu, 2006

VELASCOS SAN MARTÍN, Cristos, **La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet**, 1.ª, Tirant lo Blanch, 2012

WALDEN, Ian, **Computer crimes and digital investigations**, 1.ª, Oxford University Press, 2007

Recomendacións

Materias que se recomenda ter cursado previamente

Xestión da seguridade da información/V05M175V01101

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
Non hai cambios. Faranse a través de medios telemáticos (plataforma de teledocencia e aula e despacho virtual).

=== ADAPTACIÓN DA AVALIACIÓN ===
Non hai cambios. Faranse a través de medios telemáticos (plataforma de teledocencia e aula e despacho virtual).

DATOS IDENTIFICATIVOS

Fortificación de sistemas operativos

Materia	Fortificación de sistemas operativos			
Código	V05M175V01202			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	5	OB	1	1c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Lorenzo Veiga, Beatriz			
Profesorado	Lorenzo Veiga, Beatriz Yáñez Izquierdo, Antonio Fermín			
Correo-e	blorenzo@gti.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530007&any_academic=2018_19&idioma_assig=eng			
Descrición xeral	A newly installed Operating system is inherently insecure. It has a certain number of vulnerabilities, depending on such things such as the age of the O.S., the amount of services it provides, the existence of initial backdoors not already patched, and the use of default policies designed without security in mind By Hardening Operating Systems we refer to the act of configuring an operating system with the aim of making it as secure as possible, so thet we minimize the risk of getting it compromised. This usually implies applying patches, changing default O.S. policies, and removing (or disabling) non-essential aplications and/or services. In this course we'll try to identify common O.S. vulnerabilities and how to defend the O.S. against them. Both UNIX (linux) and Windows type O.S. will be considered.			

Competencias

Código

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

	Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS

Tests de intrusión

Materia	Tests de intrusión			
Código	V05M175V01203			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	5	OB	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Costa Montenegro, Enrique			
Profesorado	Carballal Mato, Adrián Costa Montenegro, Enrique			
Correo-e	kike@gti.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530008&any_academic=2018_19&idioma_assig=cast			
Descrición xeral	Non hai mellor forma de probar a forza dun sistema que atacalo. As probas de intrusión serven para reproducir os intentos de acceso dun atacante usando as vulnerabilidades que poden existir nunha infraestrutura dada. Neste curso abordaranse os temas fundamentais orientados ás probas de intrusión (pentesting), que abarcan as diferentes fases dun ataque e explotación (desde o recoñecemento e control do acceso á eliminación de pistas).			

Competencias

Código

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

	Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una

planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS				
Análise de malware				
Materia	Análise de malware			
Código	V05M175V01204			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	5	OB	1	2c
Lingua impartición	Inglés			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos Rivas López, Jose Luis			
Correo-e	jrial@uvigo.es			
Web	http://http://faitic.uvigo.es			
Descrición xeral	O malware utiliza os sistemas e as redes de comunicacións para propagar virus, secuestrar dispositivos ou robar datos confidenciais. O obxectivo desta asignatura é dotar o estudiante da capacidade para analizar, detectar y eliminar malware. Para elo se explorarán y exemplificarán, de forma práctica e con casos reais, as técnicas actuais de ocultación e persistencia de malware, así como as tendencias máis novedosas para a sua detección e eliminación. Esta asignatura impartirase en inglés.			

Competencias	
Código	
CB1	Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación.
CG1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CE11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
CE13	Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Analizar, detectar e eliminar malware en sistemas e redes.	CG1 CE11 CE13 CT5
Conocer, detectar e loitar contra as técnicas de ocultación e persistencia de malware en sistemas e redes.	CB1 CG1 CE8 CE11 CE13 CT5
Estudiar sistemas e redes para detectar e eliminar as vulnerabilidades susceptibles de ser utilizadas polo malware.	CG1 CE8 CE11 CE13 CT5
Conocer as tendencias actuais en malware e as experiencias aprendidas de casos reais.	CB1 CG1 CT4 CT5

Contidos
Tema

Introducción a enxeñaría do malware.	a) Qué é o malware? b) Cómo detectalo e eliminalo? c) En qué consiste a enxeñaría de malware?
Tipos de malware.	a) Estructura. b) Compoñentes. c) Vectores de infección.
Enxeñaría de malware.	a) Técnicas de propagación. b) Procesos de infección. c) Persistencia do malware. d) Técnicas de ocultación.
Enxeñaría inversa de malware.	a) ¿Cómo analizar e inferir o funcionamiento do malware? b) Comprensión do funcionamiento de novos tipos de malware.
Ferramentas de análisis de malware.	a) Ferramentas para a detección de malware. b) Ferramentas para a eliminación de malware.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Actividades introdutorias	2	2	4
Lección maxistral	10	30	40
Prácticas de laboratorio	15	40	55
Foros de discusión	0	2	2
Estudo de casos	5	4	9
Exame de preguntas obxectivas	2	4	6
Resolución de problemas e/ou exercicios	3	6	9

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

Metodoloxía docente

	Descrición
Actividades introdutorias	Faremos unha introdución xenérica aos obxectivos, contidos globais xenerais da materia e resultados esperados. Esta actividade realizarase individualmente.
Lección maxistral	Introduciremos os distintos temas da materia proporcionando o material docente necesario para o seu seguimento. Con esta metodoloxía se traballan as competencias CB1, CG1, CE8, CE11, CE13, CT4 y CT5. Esta actividade realizarase individualmente.
Prácticas de laboratorio	Realizaranse prácticas no laboratorio para comprender mellor os contenidos explicados nas lecciones maxistrais. Con esta metodoloxía trabállanse as competencias CG1, CE8, CE11, CE13 y CT5. Algunhas prácticas realizaranse de forma individual e outras en grupos (dependendo do número de estudiantes).
Foros de discusión	Os estudiantes deben participar no foro dentro da plataforma TEMA en FAITIC. Con esta metodoloxía se traballan as competencias CE8, CE11, CE13 y CT5. Esta actividade realizarase individualmente.
Estudo de casos	Durante as clases maxistrais presentaranse casos de estudio típicos de amenazas, problemas de seguridade coñecidos ou tecnoloxías actuales. Con esta metodoloxía se traballan as competencias CG1, CE11, CE13 y CT5. Esta actividade realizarase en grupo.

Atención personalizada

Metodoloxías	Descrición
Actividades introdutorias	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contenidos e asignaturas do programa de estudios. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de evaluación.

Lección maxistral	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contenidos e asignaturas do programa de estudios. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de evaluación.
Estudo de casos	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contenidos e asignaturas do programa de estudios. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de evaluación.
Prácticas de laboratorio	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contenidos e asignaturas do programa de estudios. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de evaluación.
Foros de discusión	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contenidos e asignaturas do programa de estudios. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de evaluación.

Avaliación

	Descrición	Cualificación	Competencias Avaliadas			
Prácticas de laboratorio	Os alunos realizarán prácticas de laboratorio, onde se traballará cos conceptos estudiados nas clases teóricas.	45	CB1	CG1	CE8 CE11 CE13	CT5
Foros de discusión	Os estudiantes deben participar no foro da plataforma TEMA.	5	CB1	CG1	CE11 CE13	CT4 CT5
Estudo de casos	El alumnado realizará presentacións de casos de estudio, seleccionados por eles, para analizar amenazas actuáis.	15		CG1	CE11 CE13	CT5
Exame de preguntas obxectivas	Dous test de evaluación sucesivos para o contido parcial da materia impartida ata ese momento. Os tests serán individuáis e de tiempo limitado.	30	CB1	CG1	CE11 CE13	CT5
Resolución de problemas e/ou exercicios	Durante as clases maxistrais realizaranse preguntas aos estudiantes para coñecer a súa comprensión do tema baixo estudio.	5	CB1		CE11 CE13	CT5

Outros comentarios sobre a Avaliación

Os elementos que forman parte da avaliación da materia son os seguintes:

- **Cuestionarios**: ao longo do curso realizaranse dous cuestionarios que achegarán un 15% da nota final (cada un).

- **Presentación de casos de estudio**: cada alumno deberá realizar unha presentación orixinal que aportará un 15% da nota final.

- **Prácticas de laboratorio**: cada alumno deberá realizar un conxunto de prácticas propostas no laboratorio que achegarán un 45% da nota final.

- **Participación en clase**: os estudiantes participarán e discutirán sobre as exposiciones realizadas por o profesor e esto contribuirá ata un 5% a nota final.

- **Participación no foro**: os estudiantes deben participar no foro da asignatura, de forma individual, e esto contribuirá ata un 5% a nota final. Para obter dito porcentaxe débense proporcionar, como mínimo, dúas contribucions relevantes.

Así temos:

Nota Final = Cuestionarios (2x15 = 30%) + Presentación de casos de estudio (15%) + Práctica de lab. (45%) + Participación en clase (5%) + Foro (5%) = 100%.

Os estudiantes deben obter o menos 4 puntos sobre 10 na nota dos cuestionarios e a práctica para poder calcular a nota media final. Si calqueira das notas é inferior a 4, entón a notal final non poderá superar 4 puntos sobre 10.

A planificación das diferentes probas de avaliación intermedia aprobarase nunha Comisión Académica de Grado (CAG) e estará dispoñible ao principio do cuatrimestre.

En caso de detección de copia en calquera das probas (probas curtas, exames parciais ou exame final), a cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos.

Seguindo as directrices propias da titulación ofrecerase aos alumnos que cursen esta materia dous sistemas de avaliación: avaliación continua e avaliación final (fin do cuadrimestre).

Avaliación continua: o estudante segue a avaliación continua dende o momento en que se presenta os dous cuestionarios da materia. Un alumno que opta pola avaliación continua considérase que se presentou á materia, independentemente de que se presente ou non ao exame final.

Primeira oportunidade: o alumno deberá realizar un exame teórico que substitúe aos cuestionarios realizados ao longo do curso, ademais de entregar as prácticas e os traballos equivalentes aos que se realizaron como parte da avaliación continua.

Segunda oportunidade: o alumno deberá realizar a parte que non superase. No caso de non superar os cuestionarios deberá realizar un exame equivalente.

Os traballos e tarefas prácticas propostas e realizadas neste curso non son recuperables e só son válidas para o curso actual.

Bibliografía. Fontes de información

Bibliografía Básica

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

Bibliografía Complementaria

Recomendacións

Materias que se recomenda cursar simultáneamente

Análise forense de equipos/V05M175V01207
Fortificación de sistemas operativos/V05M175V01202
Seguridade en dispositivos móbiles/V05M175V01206

Materias que se recomenda ter cursado previamente

Seguridade de aplicacións/V05M175V01104

Plan de Continxencias

Descrición

No caso de que a docencia sexa exclusivamente non presencial, as clases da materia desenvolveranse dun xeito similar, pero empregando as plataformas que proporciona a Universidade.

As clases virtuais impartiranse semanalmente a través do Campus Remoto, tanto nas sesións teóricas (grupos A) como nas sesións prácticas (grupos B). Neste segundo caso, os estudantes realizarán as prácticas empregando os seus ordenadores persoais ou a infraestrutura virtual do laboratorio.

Os medios habilitados para a resolución das dúbidas suscitadas polos estudantes incluirán foros de consulta en liña e titorías na oficina virtual do profesor.

A avaliación non presencial da materia rexerase polas condicións descritas na guía docente para a modalidade de docencia presencial, incluído o mesmo número de probas, idéntica ponderación e notas mínimas. Os exames teóricos e prácticos realizaranse practicamente, empregando as plataformas que proporciona a Universidade.

DATOS IDENTIFICATIVOS				
Seguridade como negocio				
Materia	Seguridade como negocio			
Código	V05M175V01205			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OB	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Fernández Vilas, Ana			
Profesorado	Carneiro Díaz, Victor Manuel Fernández Vilas, Ana			
Correo-e	avilas@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530010&any_academic=2020_21&idioma_assig=cast			
Descrición xeral	Seguridade como negocio aborda as competencias necesarias para comprender o funcionamento dun Security Operation Centre (SOC), desde o punto de vista tecnolóxico, operacional e de intelixencia. Profundarase na infraestrutura, organización, operación e mecanismos de métrica necesarios para a explotación empresarial dos servizos asociados a un SOC. Estudaranse diferentes contornas de especialización como o sector bancario, administración pública ou o ámbito militar.			

Competencias
Código

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

Plan de Continxencias
Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS				
Seguridade en dispositivos móbiles				
Materia	Seguridade en dispositivos móbiles			
Código	V05M175V01206			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OP	1	2c
Lingua impartición	Castelán Galego Inglés			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	López Bravo, Cristina			
Profesorado	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
Correo-e	clbravo@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Nesta materia móstrase unha visión xeral da seguridade en dispositivos móbiles con diferentes características. Partindo do estudo da arquitectura destes dispositivos, descubriremos o seu funcionamento interno e cales son as principais ferramentas de seguridade que inclúen, xunto cos riscos e ameazas que sofren. Estudiaremos como atopar, analizar e mitigar as vulnerabilidades que afectan aos dispositivos móbiles, usando ferramentas de análise forense, de desenvolvemento de aplicacións seguras e de xestión de dispositivos en contornos empresariais. A documentación desta materia estará en inglés.			

Competencias	
Código	
CB2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
CB3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
CB4	Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
CG1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CG2	Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións.
CG5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
CE4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
CE6	Desenvolver e aplicar métodos de investigación forense para o análisis de incidentes ou riscos de ciberseguridade
CE9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
CE15	Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade.
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Coñecer os conceptos fundamentais asociados coa seguridade nos sistemas operativos móbiles e desenvolvemento de apps seguras.	CB2 CG1 CE4 CE15 CT4 CT5

Identificar unha app con comportamento malicioso e vulnerabilidades en sistemas operativos e apps	CB4 CG2 CE4 CT4 CT5
Ser capaz de realizar unha análise forense dun dispositivo móbil	CB3 CG2 CE6 CT5
Coñecer os sistemas de xestión dos dispositivos móbiles	CB2 CG1 CG2 CG5 CE9 CT5

Contidos	
Tema	
Introdución: Ameazas e vulnerabilidades que afectan aos dispositivos móbiles	
Arquitecturas de dispositivos móbiles	
Modelos de seguridade de dispositivos móbiles	
Desenvolvemento de aplicacións seguras	Permisos Xestión de paquetes Xestión de usuarios APIs
Seguridade dos datos	
Seguridade dos dispositivos	
Seguridade da rede	
Vulnerabilidades, exploits e aplicacións maliciosas	
Análise forense de sistemas operativos móbiles	
Sistemas de Xestión de Mobilidade Empresarial (EMM)	

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	9	9	18
Prácticas con apoio das TIC	10	10	20
Exame de preguntas obxectivas	2	14	16
Resolución de problemas e/ou exercicios	0	11	11
Informe de prácticas, prácticum e prácticas externas	0	10	10
*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 profesorado, dos principais contidos teóricos relacionados coa seguridade en dispositivos móbiles. Con esta metodoloxía contribuirase á adquisición das competencias CB3, CG1, CE4, CE15 e CT4.
Prácticas con apoio das TIC	Realización por parte do alumnado de prácticas guiadas e supervisadas. Con esta metodoloxía traballaranse as competencias CG2, CG5, CB2, CB4, CE4, CE6 e CE9.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas con apoio das TIC	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, os profesores orientarán e guiarán aos alumnos durante a realización das tarefas que teñen asignadas nas prácticas con apoio das TIC. As dúbidas atenderanse de forma presencial ou telemática (durante as propias prácticas, durante o horario establecido para as titorías, ou durante o horario acordado cos alumnos para as titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.

Lección maxistral	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial e telemática (durante a propia sesión maxistral, durante o horario establecido para as titorías, ou durante o horario acordado cos alumnos para as titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.

Avaliación

	Descrición	Cualificación	Competencias Avaliadas			
Exame de preguntas obxectivas	Exame de preguntas cortas sobre os contidos teóricos e prácticos revisados ao longo do curso, tanto nas sesións maxistrais, como nas prácticas de laboratorio. Este exame realizarase ao finalizar o bimestre.	50	CB3 CB4		CE4	
Resolución de problemas e/ou exercicios	Resolución de problemas nos que se faga uso dos coñecementos adquiridos tanto nas sesións de teoría como de prácticas. Esta proba realizarase ao longo do bimestre, con entregas parciais nas datas indicadas polo profesorado.	20	CB2 CB4	CG1 CG2	CE4	
Informe de prácticas, prácticum e prácticas externas	O alumnado completará de forma individual cuestionarios e/ou informes de prácticas onde mostrarán a correcta realización e comprensión das prácticas.	30	CB4	CG5	CE4 CE6 CE9 CE15	CT4

Outros comentarios sobre a Avaliación

PRIMEIRA OPORTUNIDADE

Seguindo as directrices propias da titulación ofertaranse a quen curse esta materia dous sistemas de avaliación: avaliación continua e avaliación única.

Antes de que finalice a segunda semana do curso, os estudantes deberán indicar ao profesorado da materia o sistema de avaliación elexido. Quen opte polo sistema de avaliación continua non poderá ser cualificado como "non presentado" se realiza unha entrega ou proba de avaliación con posterioridade á comunicación da súa decisión.

Sistema de avaliación continua

A cualificación global da materia será igual á media aritmética ponderada das probas indicadas previamente. Para superar a materia a cualificación global debe ser maior ou igual que cinco.

Sistema de avaliación única

A cualificación global da materia será igual á media aritmética ponderada das probas indicadas previamante. Neste caso, a proba de resolución de problemas farase nunha única proba ao finalizar o bimestre. Para superar a materia, a cualificación global debe ser maior ou igual que cinco.

SEGUNDA OPORTUNIDADE

A avaliación consistirá en realizar un exame de preguntas obxectivas, un exame de resolución de problemas e entregar os informes de prácticas de todas as prácticas realizadas ao longo do curso.

OUTROS COMENTARIOS

As puntuacións obtidas solo son válidas para o curso académico en vigor.

O uso de calquera material durante a realización dos exames e probas de avaliación deberá ser autorizado explicitamente polo profesorado da materia.

No caso de deteción de plaxio nalgún dos traballos/probas realizadas, a cualificación final da materia será de suspenso (0) e os profesores comunicarán o asunto á dirección da escola para que tome as medidas que considere oportunas.

Bibliografía. Fontes de información

Bibliografía Básica

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

Bibliografía Complementaria

Joshua Drake, **Android hacker's handbook**, 1, John Wiley & Sons, 2014

Charles Miller, **iOS hacker's handbook**, 1, John Wiley & Sons, 2012

Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013

David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016

Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

Recomendacións

Outros comentarios

Recoméndase ter coñecementos básicos sobre o S.O. Linux e coñecementos de programación en Java. Así mesmo, se ben non é imprescindible, recoméndase ter coñecementos de programación de dispositivos móbiles Android.

Plan de Continxencias

Descrición

No caso de que a docencia deba levar a caso de maneira totalmente remota, utilizaranse as mesmas metodoloxías e realizaranse as mesmas probas que se desenvolverían de maneira presencial nas aulas e/ou nos laboratorios da Escola, que pasarán a desenvolverse en liña a través do Campus Remoto e Faitic.

No caso de que a avaliación sexa non presencial, o peso das distintas probas de avaliación pasaría a ser o seguinte:

- Exame de preguntas obxectivas: 30 %
- Resolución de problemas e/ou exercicios: 30 %
- Informes de prácticas: 40 %

BIBLIOGRAFÍA COMPLEMENTARIA

- Platform Architecture - Android Developers: https://developer.android.com/guide/platform/ - Android Secure: https://source.android.com/security
- Android Enterprise: https://www.android.com/enterprise/
- Mobile Threat Catalogue - NIST: https://pages.nist.gov/mobile-threat-catalogue/
- OWASP Mobile Security Project: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- ENISA: Smartphone Secure Development Guidelines: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- Guía de Seguridad de las TIC CCN-STIC 453E. SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID 9.x. Centro Criptográfico Nacional. NIPO: 083-19-015-2: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3588-ccnstic-453g-guia-practica-de-seguridad-en-dispositvos-moviles-android-9/file.html
- Guía de seguridad de las TIC (CCN-STIC-457): Gestión de dispositivos móviles: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-accesopublico-ccn-stic/14-ccn-stic-457-herramienta-de-gestion-dedispositivos-moviles-mdm/file.html

DATOS IDENTIFICATIVOS				
Análise forense de equipos				
Materia	Análise forense de equipos			
Código	V05M175V01207			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OP	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Suárez González, Andrés			
Profesorado	Suárez González, Andrés Vázquez Naya, José Manuel			
Correo-e	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530012&any_academic=2020_21&any_academic=2020_21			
Descrición xeral	A análise forense de equipos consiste na aplicación de técnicas científicas e analíticas para identificar, preservar, analizar e presentar datos que sexan válidos dentro dun proceso legal. A materia "Análise Forense de Equipos" ten unha forte compoñente práctica. Comezarase con unha introdución a este campo, explicando conceptos clave. A continuación, estudiaranse fundamentos e metodoloxías de análise forense dende un punto de vista xenérico e aplicable a novos casos, pero tamén se estudiarán exemplos concretos baseados en casos reais. Paralelamente, nas prácticas de laboratorio o/a alumno/a aprenderá a manexar diferentes ferramentas de análise forense e realizará prácticas simulando problemas reais.			

Competencias
Código

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Nova	

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional

DATOS IDENTIFICATIVOS				
Seguridade ubicua				
Materia	Seguridade ubicua			
Código	V05M175V01208			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OP	1	2c
Lingua impartición	Castelán Galego			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Gil Castiñeira, Felipe José			
Profesorado	Gil Castiñeira, Felipe José Rabuñal Dopico, Juan Ramón			
Correo-e	felipe@uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	Os dispositivos intelixentes estannos proporcionando cada vez máis servizos case sen que sexamos conscientes da súa presenza: o coche deixou de ser unha máquina simplemente mecánica para converterse nun sistema conectado e con un enorme control electrónico; nos hoteis xa non utilizamos unha chave, senón que podemos abrir a nosa habitación con unha tarxeta ou co noso móbil; os termostatos da nosa casa pódense conectar con un servizo de predición meteorolóxica e adecuarse ao tempo das próximas horas. Son todos exemplos das aplicacións que permiten as tecnoloxías "embedded", as redes de comunicacións sen fíos, e en definitiva, a "Internet of Things" (IoT). Esta materia analiza os problemas e as mellores prácticas á hora de facer que este tipo de sistemas sexan seguros.			

Competencias	
Código	
CB2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
CB3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
CB4	Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
CG1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CG2	Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións.
CG5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
CE4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
CE9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias
Coñecer a seguridade nas diferentes capas relacionadas cos sistemas ubicuos e as tecnoloxías que utilizan.	CB2 CB3 CB4 CG1 CG2 CG5 CE4 CE9 CT4 CT5

Entender os problemas de seguridade asociados ao mundo ubicuo.	CB2 CB3 CB4 CG1 CG2 CG5 CE4 CE9 CT4 CT5
Coñecer casos reais de ataques a sistemas ubicuos.	CB2 CB3 CB4 CG5 CE4 CT4 CT5

Contidos	
Tema	
Seguridade física	Elementos de hardware. Compoñentes. - Buses de comunicación. - Interfaces. - Hardware criptográfico. Ataques.
Seguridade no middleware	Seguridade no proceso de arrinque. Seguridade no sistema operativo. Control de acceso. Cifrado. Actualización do firmware.
Seguridade nas comunicacións	Comunicacións sen fíos. Riscos e ameazas nas comunicacións.
Seguridade na percepción do contorno	Ataques nos sistemas de posicionamento. Ataques ás medidas dos sensores. Privacidade.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Aprendizaxe baseado en proxectos	10	35	45
Lección maxistral	10	20	30
*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.			

Metodoloxía docente	
	Descrición
Aprendizaxe baseado en proxectos	Realización en grupo do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. Realización en grupo de ataques á seguridade dos sistemas implementados por outros compañeiros ou de terceiros. Con esta metodoloxía traballaranse as competencias CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 e CT5.
Lección maxistral	Exposición, por parte dos profesores, dos principais contidos teóricos relacionados coa seguridade para sistemas ubicuos (seguridade empotrada, nas comunicacións e nos backends) Con esta metodoloxía contribuirase a adquisición das competencias CB2, CB3, CB4, CG1, CG2, CE4 e CE9.

Atención personalizada	
Metodoloxías	**Descrición**
Lección maxistral	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse durante a propia sesión maxistral, ou durante o horario establecido para as titorias. O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.

Aprendizaxe baseado en proxectos	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, os profesores orientarán e guiarán aos alumnos durante a realización do proxecto. As dúbidas atenderanse durante as sesións de titoría en grupo, ou durante o horario establecido para as titorias. O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.

Avaliación

	Descrición	Cualificación	Competencias Avaliadas
Aprendizaxe baseado en proxectos	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, poñendo especial énfase na seguridade. O mesmo grupo realizará ataques á seguridade dos sistemas implementados por outros compañeiros ou por terceiros. O proxecto realizado, e o informe contendo o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Se os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de ata o 20% da nota. O seguimento será grupal e individual: cada un dos membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	80	CB2 CG1 CE4 CT4 CB3 CG2 CE9 CT5 CB4 CG5
Lección maxistral	Realizaranse un ou varios exames para avaliar a comprensión dos contidos presentados nas sesións maxistrais. De haber máis de un exame, a nota final será a media aritmética das distintas probas.	20	CB2 CG1 CE4 CB3 CG2 CE9 CB4

Outros comentarios sobre a Avaliación

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exames acerca dos contidos expostos na sesión maxistral e proxectos). A nota final será o resultado de aplicar a **media xeométrica ponderada** da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, e a nota do proxecto é NP, a nota final será:

$$\textbf{Nota} = NT^{0.2} \times NP^{0.8}$$

Durante o primeiro mes, os estudantes deberán indicar explicitamente e por escrito o seu desexo de cursar a materia seguindo a avaliación única. Noutro caso considerarase que seguen a avaliación continua. Aqueles que sigan a avaliación continua non se poderán considerar "non presentados" unha vez se realice a entrega do primeiro cuestionario ou tarefa.

Os alumnos que opten pola avaliación única deberán presentar adicionalmente un *dossier* que deberá defender presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto. No caso de seguir a avaliación única, os alumnos deberán realizar o traballo de forma individual, salvo que o profesorado lles comunique explicitamente a autorización para realizalo en grupo.

Segunda oportunidade

Só poderán optar á segunda oportunidade aqueles alumnos que non superaron a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será preciso presentar un *dossier* que deberá ser defendido presencialmente ante os profesores, onde se inclúan tódolos detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Aqueles estudantes que seguisen a avaliación continua poden optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor.

Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, os alumnos deben deixar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, considerarase a súa expulsión do mesmo e/ou poderá ser avaliado de forma individual nesta parte.

O uso de calquera material durante a realización dos exames terá que ser autorizado explicitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a cualificación final da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tome as medidas oportunas.

Bibliografía. Fontes de información

Bibliografía Básica

Brian Russell, Drew Van Duren, **Practical Internet of Things Security**, 1, Packt Publishing, 2016

Bibliografía Complementaria

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 1, Wiley, 2018

Bruce Schneider, **Applied Cryptography: Protocols, Algorithms and Source Code in C**, 2, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security.**, 1, Wiley, 2014

Recomendacións

Materias que se recomenda ter cursado previamente

Fortificación de sistemas operativos/V05M175V01202
Redes Seguras/V05M175V01105
Seguridade de aplicacións/V05M175V01104
Seguridade da información/V05M175V01102
Seguridade en comunicacións/V05M175V01103
Tests de intrusión/V05M175V01203

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===
Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
A metodoloxía de aprendizaxe en proxectos será modificada no caso no que se produza unha situación que impida o traballo en grupo. Se o proxecto en grupo xa estaba iniciado, farase que o sistema IoT deseñado por cada un dos grupos estea accesible a través da Internet para que o proxecto se poda rematar de forma remota. De non se ter iniciado, propoñeráselles aos alumnos a realización dun proxecto alternativo relacionado coa seguridade IoT que podan realizar individualmente (por exemplo, o modelado de ameazas e o ataque dun sistema comercial). De dispoñer do número suficiente de dispositivos, estes faránselles chegar aos alumnos. Noutro caso realizarase un proxecto utilizando simuladores ou limitarase o traballo a unha análise teórica.

DATOS IDENTIFICATIVOS				
Ciberseguridade en contornas industriais				
Materia	Ciberseguridade en contornas industriais			
Código	V05M175V01209			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OP	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría de sistemas e automática			
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel			
Correo-e	mcacho@uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530014&any_academic=2020_21			
Descrición xeral	O concepto da Industria 4.0 deu lugar a que cada vez sexan máis os dispositivos industriais conectados á rede e a procesos físicos. Esta asignatura, además de repasar os sistemas industriais tradicionais (i.e., sistemas de control industrial, control de accesos, sistemas de comunicacións ou de xestión da información), enfocarase na seguridade das tecnoloxías da Industria 4.0: sistemas IoT/IIoT, sistemas robotizados, cloud/edge computing, realidade aumentada, blockchain ou AGVs.			

Competencias
Código

Resultados de aprendizaxe	
Resultados de aprendizaxe	Competencias

Contidos	
Tema	
Introdución	Políticas de seguridade industrial Implicacións da ciberseguridad industrial e de infraestruturas críticas Casos prácticos
Sistemas de control de acceso físico a dependencias industriais	Sistemas de proximidade Sistemas de acceso remoto Sistemas biométricos
Sistemas de control industrial	Arquitecturas de comunicacións Sistemas tradicionais Sistemas ciberfísicos
Sistemas da Industria 4.0	Introdución á Industria 4.0 Sistemas IoT/IIoT Seguridade noutras tecnoloxías 4.0 (p.ex., realidade aumentada, cloud/edge computing, blockchain, AGVs)
Sistemas de xestión de información en contornas industriais	Bases de datos tradicionais ERPs PLMs Sistemas MES

Sistemas de comunicacións industriais	Arquitectura de comunicacións
	Tecnoloxías de comunicación cableadas
	Tecnoloxías de comunicación inalámbricas

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Prácticas con apoio das TIC (Repetida, non usar)	10	10	20
Traballo tutelado	0	20	20
Lección maxistral	9	9	18
Exame de preguntas obxectivas	1	15	16
*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.			

Metodoloxía docente	
	Descrición
Prácticas con apoio das TIC (Repetida, non usar)	Realización por parte do alumnado de prácticas guiadas e supervisadas.
Traballo tutelado	Realización por parte do alumnado de traballos de compoñente tanto teórica como práctica.
Lección maxistral	Exposición por parte do profesorado dos principais contidos teóricos relacionados coa *ciberseguridad en contornos industriais.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas con apoio das TIC (Repetida, non usar)	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, os profesores orientarán e guiarán aos alumnos durante a realización das tarefas que teñan asignadas, tanto nas prácticas como nos distintos traballos tutelados. As dúbidas atenderanse xa sexa durante as propias clases ou durante o horario establecido para *tutorías. Buscarase flexibilizar devandito horario para atender as dúbidas do alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.

Avaliación			
	Descrición	Cualificación	Competencias Avaliadas
Prácticas con apoio das TIC (Repetida, non usar)	Avaliación dos informes de realización de prácticas	30	
Traballo tutelado	Availación da memoria e execución dun traballo tutelado acordado có alumno.	30	
Exame de preguntas obxectivas	Avaliación do resultado dun exame cos contidos teóricos e prácticos da materia	40	

Outros comentarios sobre a Avaliación

PRIMEIRA OPORTUNIDADE

Se ofrecerán dúas alternativas de evaluación: continua e única.

A evaluación contínua implicará a realización das prácticas, dun traballo tutelado e unha proba mixta que serán avaliados nas porcentaxes arriba indicadas (30, 30, 40), sendo necesario obter un cinco sobre dez na evaluación total. Igualmente, será necesario obter un dous sobre catro na proba mixta para poder aprobar a materia. En caso de optar á evaluación continua, o alumnado que realice calquera tipo de entrega (práctica, traballo, proba mixta), non poderá cualificarse como "non presentado".

No caso da evaluación única, toda a puntuación virá dada por unha única proba mixta que incluirá parte teórica e práctica. Dita proba se realizará ao final do bimestre e deberá obterse en total polo menos un cinco sobre dez para poder aprobar a materia.

A selección da alternativa de evaluación deberá indicarse como moi tarde ao final da segunda semana de clase.

Para calquera das dúas alternativas se facilitará flexibilidade horaria para o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.

SEGUNDA OPORTUNIDADE E CONVOCATORIAS EXTRAORDINARIAS

Os alumnos que opten na primeira oportunidade pola evaluación continua terán a opción de conservar as notas de prácticas e traballos tutelados realizados durante o curso académico. Devandito alumnado realizará unha proba mixta, establecéndose a nota nas porcentaxes indicadas arriba (30, 30, 40). O resto de alumnos (incluído o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia) trataranse como alumnos de evaluación única e realizarán unha proba mixta que mesture parte teórica e práctica.

OUTROS COMENTARIOS

Non se conservará ningunha das notas obtidas para os cursos académicos posteriores.

No caso de detección de plaxio durante algunha das entregas, se calificará ao alumno/a con suspenso (0) e se comunicará a situación á dirección do máster e ás autoridades universitarias correspondentes de face a tomar as medidas oportunas.

Bibliografía. Fontes de información

Bibliografía Básica

Eric Knapp, Joel Thomas Langill, **Industrial Network Security.**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, IGI Global, 2012

Tyson Macaulay, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity**, Packt, 2017

Bibliografía Complementaria

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, CRC Press, 2016

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

ESCENARIO 1: DOCENCIA MIXTA

Debido á situación excepcional, ante a imposibilidade de poder impartir a docencia dun modo completamente presencial, utilizaranse medios virtuais para a impartición das clases non presenciais.

Para a parte non presencial utilizaranse os medios proporcionados pola Universidade, actualmente o "Campus Remoto" e FAITIC. No entanto poderase complementar con outros medios.

ESCENARIO 2: DOCENCIA NON PRESENCIAL

Debido á situación excepcional, ante a imposibilidade de poder impartir a docencia dun modo presencial, utilizaranse medios virtuais para a impartición das clases.

Utilizaranse os medios proporcionados pola Universidade, actualmente o "Campus Remoto" e FAITIC. No entanto poderase complementar con outros medios.

=== ADAPTACIÓN DAS METODOLOXÍAS ===

Para as prácticas de laboratorio, substituiranse as prácticas que requiran de equipamento específico por outro simulado ou *virtualizado. Eventualmente proporanse prácticas alternativas que non requiran de devandito equipamento. Estas prácticas poderán ter un formato autónomo en previsión de problemas de conciliación e/ou *conectividad.

As sesións de tutorización (atención ao alumnado) realizaranse por medios telemáticos (Correo electrónico, Foros de FAITIC, Campus Remoto), que se poderán complementar entre si e con outras ferramentas. Nalgunhas delas utilizarase unha modalidade de concertación previa.

=== ADAPTACIÓN DA AVALIACIÓN ===
A avaliación manterá a mesma metodoloxía, sendo o exame unha proba online utilizando Campus Remoto e FAITIC. Non obstante o peso da nota pasará a ser: Prácticas: 40%. Traballo Tutelado: 40%. Exame escrito: 20%

DATOS IDENTIFICATIVOS

Xestión de incidentes

Materia	Xestión de incidentes			
Código	V05M175V01210			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	3	OP	1	2c
Lingua impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Álvarez Sabucedo, Luis Modesto			
Profesorado	Álvarez Sabucedo, Luis Modesto Dafonte Vázquez, José Carlos Gómez García, Ángel			
Correo-e	lsabucedo@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530015&any_academic=2018_19&idioma_assig=cast&idioma_assig=cast			
Descrición xeral	A xestión de incidentes de ciberseguridade céntrase no manexo da proactividade para previr e atenuar posibles consecuencias. Acadarase o coñecemento necesario sobre as ferramentas que poidan facilitar a xestión dos incidentes e as recuperacións, a xustificación dos plans propostos para a recuperación e resiliencia, a identificación e clasificación dos posibles incidentes e a definición das canles para a súa xestión e resolución.			

Competencias

Código

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Competencias Avaliadas

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais 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 DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===
* Metodoloxías docentes que se manteñen

* Metodoloxías docentes que se modifican

* Mecanismo non presencial de atención ao alumnado (titorías)

* Modificacións (se proceder) dos contidos a impartir

* Bibliografía adicional para facilitar a auto-aprendizaxe

* Outras modificacións

=== ADAPTACIÓN DA AVALIACIÓN ===
* Probas xa realizadas
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas pendentes que se manteñen
Proba XX: [Peso anterior 00%] [Peso Proposto 00%]
...

* Probas que se modifican
[Proba anterior] => [Proba nova]

* Novas probas

* Información adicional