



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 Ulteira 2020 da Xunta de Galicia).

O Grao en Enxeñaría de Tecnoloxías de Telecomunicación habilita para o exercicio das profesións reguladas de enxeñaría 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 Ulteira 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 Ciberseguridad

Materias

Curso 2

Código	Nome	Cuadrimestre	Cr.totais
--------	------	--------------	-----------

V05M175V01106	Prácticas en empresa	1c	15
V05M175V01107	Trabajo Fin de Máster	1c	15

DATOS IDENTIFICATIVOS**Prácticas en empresa**

Materia	Prácticas en empresa			
Código	V05M175V01106			
Titulación	Máster Universitario en Ciberseguridad			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	15	OB	2	1c
Lingua de impartición	Castelán			
Departamento	Tecnoloxía electrónica			
Coordinador/a	Marcos Acevedo, Jorge			
Profesorado	Marcos Acevedo, Jorge			
Correo-e	acevedo@uvigo.es			
Web	http://www.munics.es/			
Descrición xeral	(*)La misión del máster es formar profesionales de alta cualificación en todos los procesos técnicos, organizativos, operativos y forenses relativos a la seguridad digital. El profesorado pertenece a las áreas de Ingeniería Telemática, Teoría de la Señal y Comunicaciones, Ciencias de la Computación e Inteligencia Artificial, Ingeniería de Sistemas y Derecho Penal de las dos universidades, y se complementa con la contribución de destacados profesionales de empresas del sector en Galicia y el compromiso de éstas en apoyar las prácticas de los estudiantes.			

Competencias

Código	
A1	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.
A2	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 máis amplos (ou multidisciplinares) relacionados coa súa área de estudo
A3	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.
A4	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
A5	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
B1	Ter capacidade de análise 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
B2	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.
B3	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
B4	Compromiso ético. Capacidade para diseñar e implantar solucións técnicas e de xestión con criterios éticos de responsabilidade e deontoloxía profesional no ámbito da seguridade da información, as redes e/ou os sistemas de comunicacións
B5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestructuras, equipamientos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
B6	Destreza para investigar. Capacidade para innovar e contribuir ao avance dos principios, as técnicas e os procesos referidos o seu ámbito profesional, deseñando novos algoritmos, dispositivos, técnicas ou modelos útiles para a protección dos activos dixitais públicos, privados ou comerciais
C1	Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras.
C2	Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
C3	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
C4	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
C5	Diseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
C6	Desenvolver e aplicar métodos de investigación forense para o análise de incidentes ou riscos de ciberseguridade
C7	Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análise de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
C8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
C9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados

C10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.
C11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
C12	Coñecer o papel da ciberseguridade no deseño das novas industrias, así como as particularidades, restricións e limitacións que teñen que acometerse para obter unha infraestrutura industrial segura.
C13	Ter capacidade de análise, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
C14	Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia.
C15	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.
C16	Ter capacidade para albiscar e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable.
C17	Ter capacidade de planificar no tempo os períodos de detección de incidentes ou desastres, e a súa recuperación
C18	Interpretar dunha forma axeitada as fontes de información no ámbito do dereito penal informático (leis, xurisprudencia e doutrina) de ámbito nacional e internacional.
C19	Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector
C20	Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna.
D1	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.
D2	Ter capacidade para comunicarse oralmente e por escrito en lingua galega
D3	Incorporar no exercicio profesional criterios de sustentabilidade e compromiso ambiental. Incorporar aos proxectos o uso equitativo, responsable e eficiente dos recursos
D4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Experiencia no desempeño da profesión e das súas funcións máis habituais nunha contorna real de empresa.	A1
	A2
	A3
	A4
	A5
	B1
	B2
	B3
	B4
	B5
	B6
	C1
	C2
	C3
	C4
	C5
	C6
	C7
	C8
	C9
	C10
	C11
	C12
	C13
	C14
	C15
	C16
	C17
	C18
	C19
	C20
	D1
	D2
	D3
	D4
	D5

Contidos			
Tema			
Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Prácticum, Practicas externas e clínicas	375	0	375
*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.			
Metodoloxía docente			
	Descrición		
Prácticum, Practicas externas e clínicas	Estancia en empresas desenvolvendo funcións propias dun Master en Ciberseguridad		
Atención personalizada			
Metodoloxías		Descrición	
Prácticum, Practicas externas e clínicas		Os alumnos terán un titor na empresa e un titor na Universidade, a quen os alumnos poderán consultar dúbidas sobre a actividade a desenvolver e a quen terán que presentar os resultados do traballo realizado.	
Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticum, Practicas externas e clínicas	A avaliación realizaraa o titor na Universidade en función da memoria do traballo realizado na empresa e da avaliación do alumno por parte do titor na empresa.	100	
Outros comentarios sobre a Avaliación			
Bibliografía. Fontes de información			
Bibliografía Básica			
Bibliografía Complementaria			
Recomendacións			
Plan de Continxencias			
Descrición			
=== ADAPTACIÓN DAS METODOLOXÍAS ===			
* Metodoloxías docentes que se manteñen			
Ningunha porque a materia consiste na permanencia nunha empresa desenvolvendo actividades adaptadas á titulación.			
* Metodoloxías docentes que se modifican			
Todas. A materia cosisted na estancia na empresa do alumno durante un tempo. No caso de que a docencia sexa exclusivamente non presencial, a práctica na empresa só poderase realizar si faise en remoto.			
* Modificacións (si proceden) dos contidos a impartir			
Non hai cambios			
* Bibliografía adicional para facilitar o auto-aprendizaxe			
Non hai			
* Outras modificacións			
Non hai máis modificacións			
=== ADAPTACIÓN DA AVALIACIÓN ===			
Sen cambios			

DATOS IDENTIFICATIVOS**Traballo Fin de Máster**

Materia	Traballo Fin de Máster			
Código	V05M175V01107			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	15	OB	2	1c
Lingua de impartición	Castelán Galego Inglés			
Departamento	Enxeñaría telemática			
Coordinador/a	Gil Castiñeira, Felipe José			
Profesorado	Gil Castiñeira, Felipe José			
Correo-e	felipe@uvigo.es			
Web	http://munics.es			
Descrición xeral	O Traballo Fin de Máster (TFM) é un traballo académico, persoal e orixinal que se debe presentar en público e que é avaliado por un tribunal.			

Trátase dun proxecto no que o estudante ten que mostrar os coñecementos adquiridos durante o mestrado. Debe concluír coa redacción por escrito dun conxunto de explicacións, teorías, ideas, razoamentos, descrición de desenvolvementos ou deseños, etc. sobre unha temática elixida polo alumno, e supervisada por un titor ou tutores, que velarán pola súa progresión e polo nivel de calidade. Non obstante, o Traballo Fin de Máster é responsabilidade única do aspirante ao título de máster.

Competencias

Código	
A1	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.
A2	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 máis amplos (ou multidisciplinares) relacionados coa súa área de estudo
A3	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.
A4	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
A5	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
B1	Ter capacidade de análise 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
B2	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.
B3	Capacidade para o razonamiento crítico e a avaliación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
B4	Compromiso ético. Capacidade para diseñar e implantar solucións técnicas e de xestión con criterios éticos de responsabilidade e deontoloxía profesional no ámbito da seguridade da información, as redes e/ou os sistemas de comunicacións
B5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestruturas, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
B6	Destreza para investigar. Capacidade para innovar e contribuír ao avance dos principios, as técnicas e os procesos referidos o seu ámbito profesional, deseñando novos algoritmos, dispositivos, técnicas ou modelos útiles para a protección dos activos dixitais públicos, privados ou comerciais
C1	Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras.
C2	Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
C3	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
C4	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
C5	Diseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
C6	Desenvolver e aplicar métodos de investigación forense para o análise de incidentes ou riscos de ciberseguridade

C7	Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análise de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
C8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
C9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
C10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.
C11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
C12	Coñecer o papel da ciberseguridade no deseño das novas industrias, así como as particularidades, restricións e limitacións que teñen que acometerse para obter unha infraestrutura industrial segura.
C13	Ter capacidade de análise, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
C14	Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia.
C15	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.
C16	Ter capacidade para albiscar e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable.
C17	Ter capacidade de planificar no tempo os períodos de detección de incidentes ou desastres, e a súa recuperación
C18	Interpretar dunha forma axeitada as fontes de información no ámbito do dereito penal informático (leis, xurisprudencia e doutrina) de ámbito nacional e internacional.
C19	Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector
C20	Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna.
D1	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.
D3	Incorporar no exercicio profesional criterios de sostenibilidade e compromiso ambiental. Incorporar aos proxectos o uso equitativo, responsable e eficiente dos recursos
D4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Capacidade de planificación e execución dun traballo orixinal no ámbito da ciberseguridade.	A1 A2 A3 A4 A5
Capacidade para a busca de información no ámbito da ciberseguridade, do seu estudo e análise, de cara á extracción de resultados relevantes.	B1 B3 B5 B6 D1 D3 D4 D5

Resolución de problemas orixinais e con implicacións reais no ámbito da ciberseguridade.

A1
A2
A3
B1
B2
B3
B4
B5
B6
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
C15
C16
C17
C18
C19
C20
D1
D3
D4
D5

Elaboración dunha memoria de proxecto que recolla a situación actual, a problemática analizada, os obxectivos, o traballo completado, as conclusións e as liñas futuras.

A1
A3
A4
B1
B2
B6

Presentación dun resumo dos principais resultados ante un tribunal e o público.

A4
D1
D4

Contidos

Tema

O Traballo Fin de Máster é un traballo académico, persoal e orixinal no que o estudante ten que mostrar os coñecementos adquiridos durante o mestrado.

Polo tanto, o contido de cada traballo debe ser único, aínda que deberá mostrar a capacidade do alumno para analizar un problema dunha forma metódica, propoñer solucións, analizar os resultados obtidos e expoñelos de forma clara.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Traballo tutelado	0	350	350
Presentación	1	24	25

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

Metodoloxía docente

Descrición

Traballo tutelado	O estudante realizará un traballo académico, persoal e orixinal no que deberá mostrar os coñecementos adquiridos durante o mestrado. Debe concluír coa redacción por escrito dun conxunto de explicacións, teorías, ideas, razoamentos, descrición de desenvolvementos ou deseños, etc. sobre unha temática elixida polo alumno, e supervisada por un titor ou titores, que velarán pola súa progresión e polo nivel de calidade.
-------------------	---

Atención personalizada

Metodoloxías	Descrición
Traballo tutelado	Durante a realización do TFM realizaranse reunións periódicas entre o estudante e os titores para definir, orientar, supervisar e delimitar o traballo, así como para orientar a escritura da memoria do mesmo.
Probas	Descrición
Presentación	Os directores do traballo orientarán ao estudante na preparación da presentación e defensa do traballo fin de máster.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Traballo tutelado	O traballo será avaliado por un tribunal. O alumno poñerá á súa disposición a memoria do traballo, e realizará unha presentación pública. O tribunal utilizará unha rúbrica que estará dispoñible publicamente.	100	

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Manuel Ruiz-de-Luzuriaga-Peña, **Guía para citar y referenciar. Estilo IEEE**, Universidad Pública de Navarra, 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 ===

A presentación pública realizarase mediante ferramentas de videoconferencia.

Non existirán outros cambios na materia.