



## Escola de Enxeñaría de Telecomunicación

### Páxina web

[www.teleco.uvigo.es](http://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 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 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 Infraestructuras: 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](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](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](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 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 Ciberseguridade			
Descritores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	15	OB	2	1c
Lingua impartición	Castelán			
Departamento	Tecnoloxía electrónica			
Coordinador/a	Marcos Acevedo, Jorge			
Profesorado	Marcos Acevedo, Jorge			
Correo-e	acevedo@uvigo.es			
Web	<a href="http://www.munics.es/">http://www.munics.es/</a>			
Descrición xeral	A misión do máster é formar profesionais de alta cualificación en todos os procesos técnicos, organizativos, operativos e forenses relativos á seguridade dixital. O profesorado pertence ás áreas de Enxeñaría Telemática, Teoría do Sinal e Comunicacións, Ciencias da Computación e Intelixencia Artificial, Enxeñaría de Sistemas e Dereito Penal das dúas universidades, e complementábase coa contribución de destacados profesionais de empresas do sector en Galicia e o compromiso destas en apoiar as prácticas dos estudantes.			

**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.
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 máis 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
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 análise e síntesis. Ter capacidade para proxectar, modelar, calcular e deseñar 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.
CG3	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
CG4	Compromiso ético. Capacidade para deseñar 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
CG5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestruturas, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
CG6	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
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
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
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
CE5	Deseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
CE6	Desenvolver e aplicar métodos de investigación forense para o análise de incidentes ou riscos de ciberseguridade
CE7	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
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CE9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
CE10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.

CE11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
CE12	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.
CE13	Ter capacidade de análise, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
CE14	Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia.
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.
CE16	Ter capacidade para albiscar e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable.
CE17	Ter capacidade de planificar no tempo os períodos de detección de incidentes ou desastres, e a súa recuperación
CE18	Interpretar dunha forma axeitada as fontes de información no ámbito do dereito penal informático (leis, xurisprudencia e doutrina) de ámbito nacional e internacional.
CE19	Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector
CE20	Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna.
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.
CT2	Ter capacidade para comunicarse oralmente e por escrito en lingua galega
CT3	Incorporar no exercicio profesional criterios de sustentabilidade e compromiso ambiental. Incorporar aos proxectos o uso equitativo, responsable e eficiente dos recursos
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
Experiencia no desempeño da profesión e das súas funcións máis habituais nunha contorna real de empresa.	CB1
	CB2
	CB3
	CB4
	CB5
	CG1
	CG2
	CG3
	CG4
	CG5
	CG6
	CE1
	CE2
	CE3
	CE4
	CE5
	CE6
	CE7
	CE8
	CE9
CE10	
CE11	
CE12	
CE13	
CE14	
CE15	
CE16	
CE17	
CE18	
CE19	
CE20	
CT1	
CT2	
CT3	
CT4	
CT5	

## Contidos

Tema	
Contido xeral	A definir polo titor na empresa e o titor académico.

Integración na empresa e na súa contorna de traballo	Durante a súa estancia o alumno integrarase na organización da empresa e deberase coordinar co resto de integrantes do equipo de traballo ao que sexa asignado.
Desenvolvemento da súa actividade profesional	O alumno realizará as tarefas encomendadas, de acordo cos seus coñecementos e competencias.

### Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Prácticum, Practicas externas e clínicas	370	5	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 nunha empresa desenvolvendo funcións propias dun titulado de Master en Ciberseguridade para que poida pór en práctica os coñecementos e competencias adquiridas, para completar a súa formación académica.

### Atención personalizada

Metodoloxías	Descrición
Prácticum, Practicas externas e clínicas	O alumno terá un titor dentro da empresa que lle guiará e supervisará nas tarefas específicas que terá que desenvolver dentro da mesma; e un titor académico -profesor da E.E.T. da UVIGO o da FIC da UDC- que definirá xunto co titor da empresa, o marco xeral da actividade do alumno, comprobando que se axusta ao perfil/mención estudado polo estudante.

### Avaliación

	Descrición	Cualificación	Competencias Avaliadas
Prácticum, Practicas externas e clínicas	A avaliación realizarase en función de: 1) A memoria de actividades 2) A avaliación do titor na empresa	100	CB1 CG1 CE1 CT1 CB2 CG2 CE2 CT2 CB3 CG3 CE3 CT3 CB4 CG4 CE4 CT4 CB5 CG5 CE5 CT5 CG6 CE6 CE7 CE8 CE9 CE10 CE11 CE12 CE13 CE14 CE15 CE16 CE17 CE18 CE19 CE20

### Outros comentarios sobre a Avaliación

**MEMORIA DE ACTIVIDADES:** O alumno/a deberá entregar unha memoria explicativa das actividades realizadas durante as prácticas, especificando a súa duración, as unidades ou departamentos da empresa en que se realizaron, a formación recibida (cursos, programas informáticos, etc.), o nivel de integración dentro da empresa e as relacións co persoal.

A memoria debe incluír tamén un apartado de conclusións, que conterá unha reflexión sobre a adecuación dos ensinados recibidos durante a carreira para o desempeño da práctica (aspectos positivos e negativos máis significativos relacionados co desenvolvemento das prácticas). Valorarase, ademais, a inclusión de información sobre a experiencia profesional e persoal obtida coas prácticas (valoración persoal da aprendizaxe conseguida ao longo das prácticas e suxestións ou achegas propias sobre a estrutura e funcionamento da empresa visitada).

A valoración da memoria será o 60% da nota final.

**AVALIACIÓN DO TITOR NA EMPRESA:** O titor da empresa entregará un informe valorando aspectos relacionados coas prácticas realizadas polo alumno: puntualidade, asistencia, responsabilidade, capacidade de traballo en equipo e integración na empresa, calidade do traballo realizado, etc.

A valoración do titor na empresa será o 40% da nota final.

---

---

### **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 consistiu 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 se fai 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	Carácter	Curso	Cuadrimestre
	15	OB	2	1c
Lingua impartición	Castelán Galego Inglés			
Departamento	Enxeñaría telemática			
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel			
Correo-e	mcaeiro@det.uvigo.es			
Web	<a href="http://moovi.uvigo.es">http://moovi.uvigo.es</a>			
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 concluir 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. Non obstante, o Traballo Fin de Máster é responsabilidade única do aspirante ao título de máster.

**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.
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 máis 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
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 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
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.
CG3	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
CG4	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
CG5	Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestruturas, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
CG6	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
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
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
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
CE5	Diseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
CE6	Desenvolver e aplicar métodos de investigación forense para o análise de incidentes ou riscos de ciberseguridade



CE7	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
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CE9	Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
CE10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.
CE11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
CE12	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.
CE13	Ter capacidade de análise, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
CE14	Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia.
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.
CE16	Ter capacidade para albiscar e enfocar o esforzo de negocio en temáticas relacionadas coa ciberseguridade, e cunha monetización viable.
CE17	Ter capacidade de planificar no tempo os periodos de detección de incidentes ou desastres, e a súa recuperación
CE18	Interpretar dunha forma axeitada as fontes de información no ámbito do dereito penal informático (leis, xurisprudencia e doutrina) de ámbito nacional e internacional.
CE19	Saber identificar os perfís de persoal necesarios para unha institución en función das súas características e o seu sector
CE20	Coñecemento das empresas orientadas especificamente ao sector de seguridade da nosa contorna.
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.
CT3	Incorporar no exercicio profesional criterios de sostenibilidade e compromiso ambiental. Incorporar aos proxectos o uso equitativo, responsable e eficiente dos recursos
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
Capacidade de planificación e execución dun traballo orixinal no ámbito da ciberseguridade.	CB1
	CB2
	CB3
	CB4
	CB5
Capacidade para a busca de información no ámbito da ciberseguridade, do seu estudo e análise, de cara á extracción de resultados relevantes.	CG1
	CG3
	CG5
	CG6
	CT1
	CT3
	CT4
	CT5

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

CB1  
CB2  
CB3  
CG1  
CG2  
CG3  
CG4  
CG5  
CG6  
CE1  
CE2  
CE3  
CE4  
CE5  
CE6  
CE7  
CE8  
CE9  
CE10  
CE11  
CE12  
CE13  
CE14  
CE15  
CE16  
CE17  
CE18  
CE19  
CE20  
CT1  
CT3  
CT4  
CT5

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

CB1  
CB3  
CB4  
CG1  
CG2  
CG6

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

CB4  
CT1  
CT4

### 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 mestrado.

### Avaliación

	Descrición	Cualificación	Competencias Avaliadas
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.