



## Escuela de Ingeniería de Telecomunicación

### (\*)Páxina web

(\*)

[www.teleco.uvigo.es](http://www.teleco.uvigo.es)

### (\*)Presentación

(\*)

A Escola Enxeñaría de Telecomunicación oferta para o curso académico 2017-18 un grao e dous másteres totalmente adaptados ao Espacio Europeo de Educación Superior, verificados pola ANECA axustándose á Orde Ministerial CIN/352/2009. A continuación indicanse os enlaces de acceso aos dípticos informativos dos tres títulos.

#### **Grao en Enxeñaría de Tecnoloxías de Telecomunicación**

<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**

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

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

#### **Máster Interuniversitario en Matemática Industrial**

[http://teleco.uvigo.es/images/stories/documentos/promocion/M2i\\_Presentacion.pdf](http://teleco.uvigo.es/images/stories/documentos/promocion/M2i_Presentacion.pdf)

www: <http://m2i.es>

### (\*)Equipo directivo

(\*)

#### EQUIPO DIRECTIVO DEL CENTRO

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

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

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

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

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

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

#### COORDINACIÓN DEL GRADO

Coordinadora General: Rebeca Díaz Redondo ([teleco.grao@uvigo.es](mailto:teleco.grao@uvigo.es))

Coordinadora do Módulo de Formación Básica: Inés García-Tuñón Blanca (inesgt@com.uvigo.es )

Coordinadora do Módulo de Telecomunicación: Yolanda Blanco Fernández (Yolanda.Blanco@det.uvigo.es)

Coordinadora do Módulo de Sistemas Electrónicos: Lucía Costas Pérez (lcostas@uvigo.es)

Coordinador do Módulo de Sistemas de Telecomunicación: Marcos Curty Alonso (mcurty@com.uvigo.es)

Coordinador do Módulo de Sone Imaxe: Manuel Sobreira Seoane (msobre@gts.uvigo.es)

Coordinador do Módulo de Telemática : Raúl Rodríguez Rubio (rrubio@det.uvigo.es)

Coordinadora do Módulo de Optatividad: Ana Vázquez Alejos (analejos@uvigo.es)

Coordinador de Proxectos: Manuel Caeiro Seoane (manuel.caeiro@det.uvigo.es)

Coordinador de Mobilidade: Enrique Costa Montenegro (teleco.subdir.internacional@uvigo.es)

Coordinador de Prácticas Externas: Jorge Marcos Acevedo (teleco.practicas@uvigo.es )

Coordinador do TFG : Manuel Fernández Veiga (teleco.subdir.academica@uvigo.es)

Coordinador do Plan de Acción Titorial: Artemio Mojón Ojea (teleco.pat@uvigo.es)

#### COORDINACIÓN DO MESTRADO EN ENXEÑARÍA DE TELECOMUNICACIÓN

Coordinadora Xeral: María José Moure Rodríguez (teleco.master@uvigo.es)

#### COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN MATEMÁTICA INDUSTRIAL

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

---

## Máster Universitario en Ciberseguridad

---

### Asignaturas

#### Curso 2

Código	Nombre	Cuatrimestre	Cr.totales
V05M175V01106	Prácticas en empresa	1c	15
V05M175V01107	Traballo Fin de Máster	1c	15

**DATOS IDENTIFICATIVOS****Prácticas en empresa**

Asignatura	Prácticas en empresa			
Código	V05M175V01106			
Titulación	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Carácter	Curso	Cuatrimestre
	15	OB	2	1c
Lengua Impartición	Castellano			
Departamento	Tecnología 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>			
Descripción general	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		Tipología
CB1	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación.	• Saber estar /ser
CB2	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio	• Saber estar /ser
CB3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.	• Saber estar /ser
CB4	Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades	• Saber estar /ser
CB5	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo	• Saber estar /ser
CG1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación	• Saber estar /ser
CG2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.	• Saber estar /ser
CG3	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones	• Saber estar /ser
CG4	Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones	• Saber estar /ser
CG5	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos	• Saber estar /ser
CG6	Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales	• Saber estar /ser
CE1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras	• Saber estar /ser
CE2	Conocer en profundidad las técnicas de ciberataque y ciberdefensa	• Saber estar /ser
CE3	Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información	• Saber estar /ser

CE4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información	• Saber estar /ser
CE5	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia	• Saber estar /ser
CE6	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad	• Saber estar /ser
CE7	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros	• Saber estar /ser
CE8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad	• Saber estar /ser
CE9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados	• Saber estar /ser
CE10	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras.	• Saber estar /ser
CE11	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones.	• Saber estar /ser
CE12	Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura.	• Saber estar /ser
CE13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes	• Saber estar /ser
CE14	Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia.	• Saber estar /ser
CE15	Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad.	• Saber estar /ser
CE16	Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable.	• Saber estar /ser
CE17	Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación	• Saber estar /ser
CE18	Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional.	• Saber estar /ser
CE19	Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector	• Saber estar /ser
CE20	Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno.	• Saber estar /ser
CT1	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.	• Saber estar /ser
CT2	Tener capacidad para comunicarse oralmente y por escrito en lengua gallega	• Saber estar /ser
CT3	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos	• Saber estar /ser
CT4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad	• Saber estar /ser
CT5	Tener capacidad para comunicarse oralmente y por escrito en inglés.	• Saber estar /ser

## Resultados de aprendizaje

Resultados de aprendizaje	Competencias
---------------------------	--------------

Experiencia en el desempeño de la profesión y de sus funciones mas habituales en un entorno 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

### Contenidos

Tema

El alumno realizará una estancia en la empresa desarrollando funciones propias de un Master en Ciberseguridad

### Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Prácticas externas	375	0	375

\*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

### Metodologías

	Descripción
Prácticas externas	Estancia en empresas desarrollando funciones propias de un Master en Ciberseguridad

### Atención personalizada

Metodologías	Descripción
Prácticas externas	Los alumnos tendrán un tutor en la empresa y un tutor en la Universidad, a quienes los alumnos podrán consultar dudas sobre la actividad a desarrollar y a quines tendrán que presentar los resultados del trabajo realizado.

### Evaluación

	Descripción	Calificación	Competencias Evaluadas
Prácticas externas	La evaluación la realizará el tutor en la Universidad en función de la memoria del trabajo realizado en la empresa y de la evaluación del alumno por parte del tutor en la empresa.	0	

---

**Otros comentarios sobre la Evaluación**

---

---

**Fuentes de información**

---

**Bibliografía Básica**

---

**Bibliografía Complementaria**

---

---

**Recomendaciones**

---

**DATOS IDENTIFICATIVOS****Trabajo Fin de Máster**

Asignatura	Trabajo Fin de Máster			
Código	V05M175V01107			
Titulación	Máster Universitario en Ciberseguridad			
Descriptor	Creditos ECTS	Carácter	Curso	Cuatrimestre
	15	OB	2	1c
Lengua Impartición				
Departamento	Ingeniería telemática			
Coordinador/a	Gil Castiñeira, Felipe José			
Profesorado	Gil Castiñeira, Felipe José			
Correo-e	felipe@uvigo.es			
Web	http://munics.es			
Descripción general	El Trabajo Fin de Máster (TFM) es un trabajo académico, personal y original que se debe presentar en público y que es evaluado por un tribunal.			
	Se trata de un proyecto en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Debe finalizar con la redacción por escrito de un conjunto de explicaciones, teorías, ideas, razonamientos, descripción de desarrollos o diseños, etc. sobre una temática elegida por el alumno, y supervisada por un tutor o tutores, que velarán por su progresión y por el nivel de calidad. No obstante, el Trabajo Fin de Máster es responsabilidad única del aspirante al título de máster.			

**Competencias**

Código		Tipología
CB1	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación.	• saber
CB2	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio	• saber hacer
CB3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.	• saber hacer
CB4	Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades	• saber hacer
CB5	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo	• saber • saber hacer
CG1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación	• saber • saber hacer
CG2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.	• saber • saber hacer
CG3	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones	• saber • saber hacer
CG4	Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones	• saber • saber hacer
CG5	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos	• saber • saber hacer
CG6	Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales	• saber • saber hacer
CE1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras	• saber
CE2	Conocer en profundidad las técnicas de ciberataque y ciberdefensa	• saber
CE3	Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información	• saber
CE4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información	• saber • saber hacer

CE5	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia	• saber hacer
CE6	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad	• saber hacer
CE7	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros	• saber hacer
CE8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad	• saber hacer
CE9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados	• saber hacer
CE10	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras.	• saber
CE11	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones.	• saber hacer
CE12	Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura.	• saber
CE13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes	• saber hacer
CE14	Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia.	• saber hacer
CE15	Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad.	• saber hacer
CE16	Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable.	• saber hacer
CE17	Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación	• saber hacer
CE18	Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional.	• saber hacer
CE19	Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector	• saber
CE20	Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno.	• saber
CT1	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.	• saber • saber hacer
CT3	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos	• saber • saber hacer
CT4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad	• saber
CT5	Tener capacidad para comunicarse oralmente y por escrito en inglés.	• saber hacer

### Resultados de aprendizaje

Resultados de aprendizaje	Competencias
Capacidad de planificación y ejecución de un trabajo original en el ámbito de la ciberseguridad.	CB1 CB2 CB3 CB4 CB5
Capacidad para la busca de información en el ámbito de la ciberseguridad, de su estudio y análisis, de cara a la obtención de resultados relevantes.	CG1 CG3 CG5 CG6 CT1 CT3 CT4 CT5



Resolución de problemas originales y con implicaciones reales en el ámbito de la ciberseguridad.

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 de una memoria de proyecto que recoja la situación actual, la problemática analizada, los objetivos, el trabajo completado, las conclusiones y las líneas futuras.

CB1  
CB3  
CB4  
CG1  
CG2  
CG6

Presentación de un resumen de los principales resultados ante un tribunal y el público.

CB4  
CT1  
CT4

## Contenidos

### Tema

El Trabajo Fin de Máster es un trabajo académico, personal y original en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster.

Por lo tanto, el contenido de cada trabajo debe ser único, aunque deberá mostrar la capacidad del alumno para analizar un problema de una forma sistemática, proponer soluciones, analizar los resultados obtenidos y exponerlos de forma clara.

## Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Trabajo tutelado	0	350	350
Presentación	1	24	25

\*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

## Metodologías

Descripción

Trabajo tutelado	El estudiante realizará un trabajo académico, personal y original en el que deberá mostrar los conocimientos adquiridos durante el máster. Debe concluir con la redacción por escrito de un conjunto de explicaciones, teorías, ideas, razonamientos, descripción de desarrollos o diseños, etc. sobre una temática elegida por el alumno, y supervisada por un tutor o tutores, que velarán por su progresión y por el nivel de calidad.
------------------	---

### Atención personalizada

Metodologías	Descripción
Trabajo tutelado	Durante la realización del TFM se realizarán reuniones periódicas entre el estudiante y los tutores para definir, orientar, supervisar y delimitar el trabajo, así como para orientar la escritura de la memoria del mismo.
<b>Pruebas</b>	Descripción
Presentación	Los directores del trabajo orientarán al estudiante en la preparación de la presentación y defensa del trabajo fin de máster.

### Evaluación

	Descripción	Calificación	Competencias Evaluadas
Trabajo tutelado	El trabajo será evaluado por un tribunal. El alumno pondrá a su disposición a memoria del trabajo, y realizará una presentación pública. El tribunal utilizará una rúbrica que estará disponible públicamente.	100	

### Otros comentarios sobre la Evaluación

### Fuentes de información

#### Bibliografía Básica

#### Bibliografía Complementaria

Manuel Ruiz-de-Luzuriaga-Peña, Guía para citar y referenciar. Estilo IEEE, Universidad Pública de Navarra, 2016, [http://www2.unavarra.es/gesadj/servicioBiblioteca/tutoriales/Citar\\_referenciar\\_\(IEEE\).pdf](http://www2.unavarra.es/gesadj/servicioBiblioteca/tutoriales/Citar_referenciar_(IEEE).pdf)

### Recomendaciones