UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Memoria verificada del título oficial de

MÁSTER UNIVERSITARIO

EN SEGURIDAD INFORMÁTICA

(Aprobado por ANECA el 6 de junio de 2014)

INDICE

1. DESCRIPCIÓN DEL TÍTULO

1.1. Datos básicos

Denominación	**Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja**
Tipo de Enseñanza	a Distancia
Rama de conocimiento	Ingeniería y Arquitectura
ISCED 1	Ciencias de la Computación
ISCED 2	
Profesión regulada	NO
Lengua	**Castellano**

1.2. Distribución de créditos

Materias	Créditos ECTS
Obligatorias	46
Prácticas Externas	6
Trabajo Fin de Máster	8
Créditos totales	**60**

1.3. Universidades y centros

1.3.1. Plazas de nuevo ingreso ofertadas

Año de implantación	
Primer año	200
Segundo año	200

1.3.2. Número de créditos de matrícula por estudiante y período lectivo

	TIEMPO COMPLETO		TIEMPO PARCIAL	
	ECTS Matrícula Min	ECTS Matrícula Max	ECTS Matrícula Min	ECTS Matrícula Max
PRIMER AÑO	60	60	30	42
RESTO AÑOS	42	60	30	36

1.3.3. Normativa de permanencia

http://gestor.unir.net/userFiles/file/documentos/normativa/permanencia.pdf

2. JUSTIFICACIÓN,ADECUACIÓN DE LA PROPUESTA Y PROCEDIMIENTOS

2.1.- Objetivos del título

El objetivo general del máster es preparar al estudiante para el ejercicio de las funciones de experto en seguridad.

Todo el proceso formativo está dirigido a que los alumnos del Máster adquieran las competencias que se recogen en este apartado y estará presidido de manera real y efectiva por los siguientes principios informadores:

a) El respeto y la subordinación de toda actuación a los derechos fundamentales de la persona por su carácter de absolutos axiológicos.

b) La subordinación al principio de igualdad, con especial atención a la no discriminación por razón de sexo, de conformidad con lo previsto en el artículo 14 de la Constitución.

c) El fomento del principio de igualdad de oportunidades en lo que comporta de exigencia de implementación de acciones de discriminación positiva respecto a las personas con diversidad de capacidades.

d) El fomento de la estima de la paz, el pluralismo, el respeto a la diferencia y de los demás valores convivenciales propios de una sociedad democrática avanzada.

Los objetivos generales de nuestra propuesta, de conformidad con el Marco Español Cualificaciones para la Educación Superior (MECES) son:

Conocer y comprender la legislación dirigida a la protección de bienes informáticos, sistemas de información, así como en el despliegue de su actividad, en especial la regulación penal de los comportamientos delictivos asociados.	OB1
Analizar riesgos legales relacionados con la seguridad en todo tipo de sistemas.	OB2
Conocer y saber aplicar procesos de gestión y mejora de la seguridad en las organizaciones.	OB3
Conocer y saber aplicar los principales estándares y buenas prácticas de auditoría de la seguridad.	OB4
Comprender y saber valorar los diferentes algoritmos y técnicas criptográficas, y los mecanismos de protección asociados a ellas.	OB5
Conocer las plataformas hardware especializadas para la seguridad informática.	OB6
Entender el concepto de vulnerabilidad y su tipología y saber analizar vulnerabilidades en sistemas concretos.	OB7
Conocer las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes, el software de aplicación, los sistemas Web y las bases de datos.	OB8
Conocer y saber aplicar correctamente las principales técnicas de análisis forense	OB9

2.2. Interés académico, científico o profesional del título propuesto

La gestión electrónica de la información es una de las tecnologías clave de nuestro tiempo. Cada vez son más los ámbitos de la actividad humana en los que se hace necesario transferir, procesar y almacenar información.
Este hecho se puede comprobar en la siguiente gráfica realizada por la ITU (Unión Internacional de Telecomunicaciones por sus siglas en inglés) titulada "Medición de la Sociedad de la Información 2010"[1].

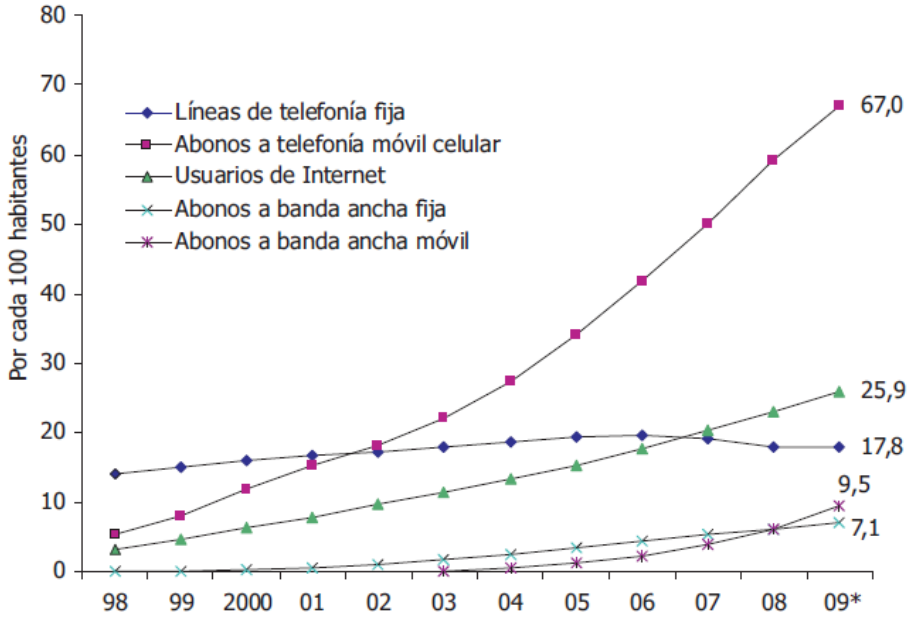


Figura 1. Medición de la Sociedad de la Información 2010.

Fuente: Unión Internacional de Telecomunicaciones 2010.

Sin embargo, los beneficios de la información digital sólo pueden conseguirse cuando se evitan a la vez una serie de posibles amenazas y ataques a su integridad y confidencialidad que van desde el fraude y el robo hasta los ataques a la privacidad. Por otra parte el cumplimiento de la legalidad vigente, en las actividades de gestión electrónica de la información, resulta un aspecto clave en la conformidad legal de la organización así como de su defensa patrimonial. La disciplina de la Seguridad Informática pretende estudiar sistemáticamente esos riesgos y amenazas desde una perspectiva técnica, legal y de gestión para llegar a un diseño de sistemas que ofrecen la máxima seguridad a la comunicación y gestión de la información digital.

Por otro lado, Internet nos brinda nuevas capacidades de comunicación, que también pueden llevar asociadas nuevos peligros, dado que también los delincuentes aprovechan estas nuevas tecnologías y el desconocimiento de sus medidas de seguridad en su propio beneficio.

El Máster en Seguridad Informática proporciona los conocimientos y competencias actualizadas y relevantes para analizar, diseñar y gestionar la seguridad en todo tipo de

1http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_Summary_S.pdf

Sistemas de Información. La triple visión legal, técnica y de gestión proporciona la base para desarrollar carreras profesionales en el ámbito de la Seguridad Informática, desde el diseño de soluciones técnicas hasta la gestión de procesos y auditoría o la consultoría en riesgos legales.

Cada vez más, muchas empresas demandan expertos en seguridad. El aumento de ataques que se realizan a las empresas, queda reflejado en un estudio proporcionado por Symantec en enero del 2010[2]; para cuya realización se han analizado datos de un total de 27 países diferentes y de 2100 encuestas a profesionales de TI (Tecnologías de la Información).

Las conclusiones obtenidas de dicho estudio son las siguientes:

- El 75% de las organizaciones que participaron en el estudio ha sufrido un ataque perdiendo en promedio más de 2 millones de dólares anualmente.
- De los ataques realizados, el 36% fueron calificados como ataques altamente efectivos. Además, el 29% de las empresas informó que los ataques han aumentado en los últimos 12 meses.
- Los principales objetivos de estos ataques fueron el robo de la propiedad intelectual, el robo de información de las tarjetas de crédito de clientes u otra información financiera así como el robo de información de identificación personal de sus clientes.
- El 42% de las organizaciones estudiadas califican la seguridad como su principal prioridad, por encima del crimen tradicional, los desastres naturales y el terrorismo.
- El principal objetivo marcado por dichas empresas para 2010 fue la mejora de la administración de riesgos, siendo calificado por el 84% de ellas como muy importante.
- El 94% de las empresas estudiadas planean aplicar cambios de seguridad en el 2010.

En el siguiente estudio de la empresa de antivirus F-Secure[3] se puede apreciar el crecimiento exponencial en el número de virus informáticos entre 1986 y 2004.

[2] http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf

[3] http://www.f-secure.com/en_EMEA/security/security-threats/threat-summaries/2004.html

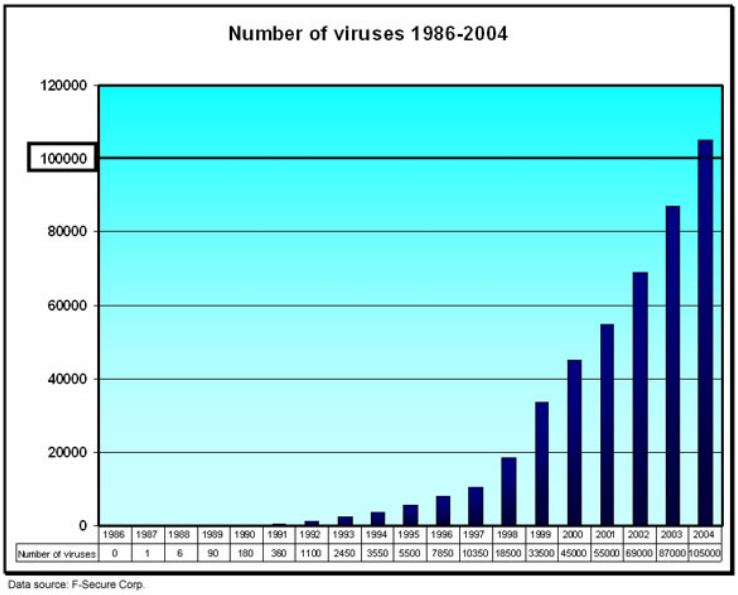


Figura 2. Crecimiento de virus informáticos. Fuente: F-Secure Corp 2004.

Tal y como demuestra un estudio del CERT[4] (Equipo de Respuesta para Emergencias Informáticas, de sus siglas en inglés), el número de vulnerabilidades en el software se ha incrementado notablemente en los últimos años.

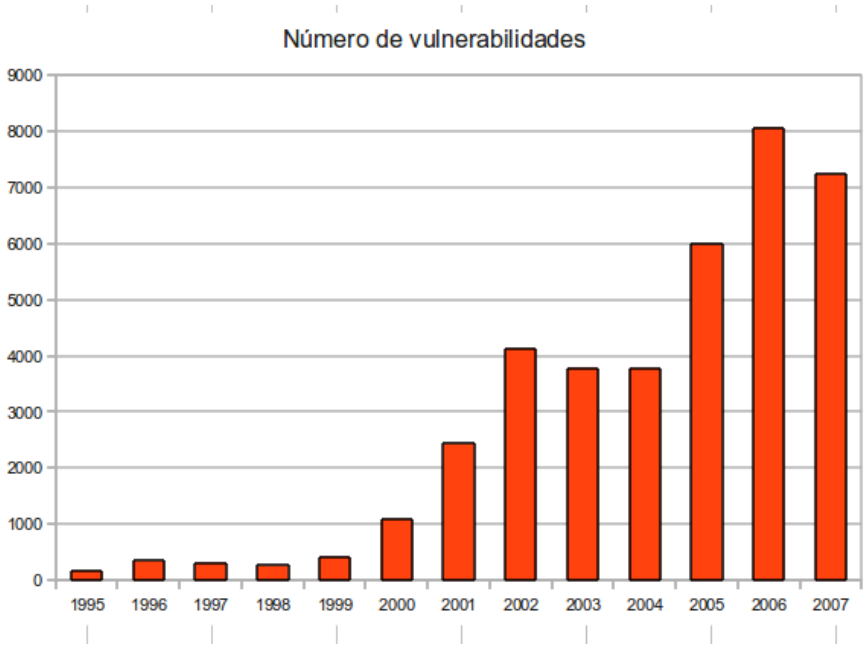


Figura 3. Incremento de vulnerabilidades del software. Fuente: Equipo de Respuesta para Emergencias Informáticas 2008.

En un estudio realizado por el IC3[5] (Centro de Quejas por Delitos en Internet, de sus siglas en

[4] http://www.cert.org/stats/

[5] http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

inglés), organismo subsidiario del Departamento de Justicia de los Estados Unidos de América, se muestra que las pérdidas económicas por ataques informáticos entre 2001 y 2009 han sufrido un crecimiento del 3100%.

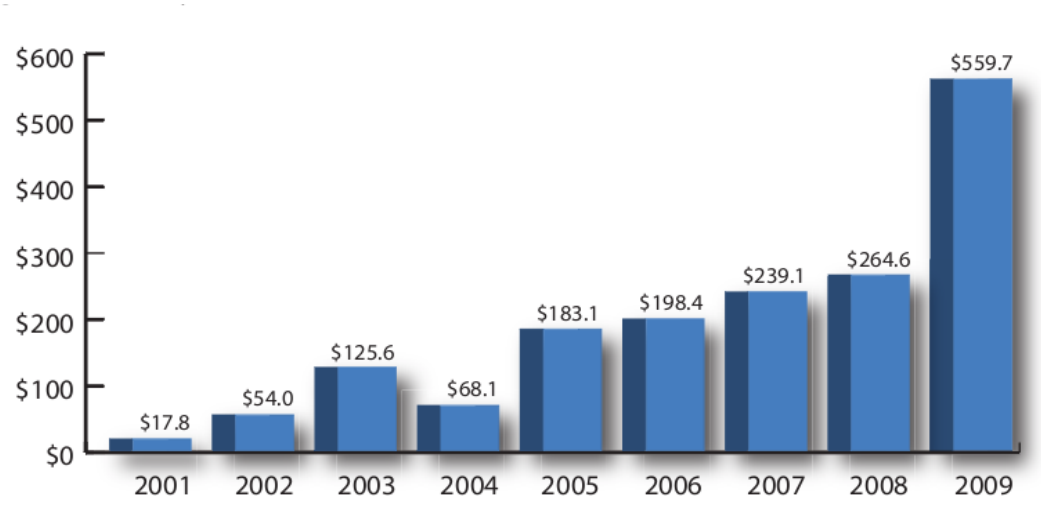


Figura 4. Pérdidas económicas por ataques informáticos. Fuente: Centro de Quejas por Delitos en Internet 2010.

Se pueden consultar más estadísticas sobre seguridad informática en las siguientes referencias, todas ellas muestran la necesidad de profesionales cualificados en la seguridad de la información:

- Informes de US-CERT sobre ataques a USA
  http://www.us-cert.gov/reading_room/#reports
- The Top Cyber Security Risks
  http://www.sans.org/top-cyber-security-risks/
- Network Attacks: Analysis of Department of Justice Prosecutions 1999 - 2006
  http://www.net-security.org/article.php?id=941
- Digital Attacks Report - SIPS Monthly Intelligence Description
  http://www.mi2g.com/cgi/mi2g/sipsgraph.php
- Informe de seguridad de redes informáticas en 2007
  http://esp.sophos.com/pressoffice/news/articles/2007/01/secrep2007.html
- Informes mensuales de amenazas de ESET
  http://www.eset-la.com/company/press.php?year=2010
- Estudios e informes del INTECO
  http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1
- Estadísticas de delitos informáticos en España en el año 2002.
  http://www.delitosinformaticos.com/estafas/estadisticas_2002.shtml
- Usos de internet en los hogares del INE:
  http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t25/p450/e01/&file=pcaxis

- Usos de comercio electrónico en las empresas en la UE por el INE: http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t09/e02/e01/&file=pcaxis

La complejidad en la aplicación efectiva de las medidas de seguridad informática está aumentando cada día más debido a dos factores principales. El primero de ellos es la diversificación de frentes de actuación en seguridad informática, debido al crecimiento del tipo de servicios informáticos profesionales utilizados y ofertados por las empresas. El segundo factor es la falta de personal cualificado en cada uno de dichos campos, debido al rápido crecimiento de las tecnologías y al tiempo necesario para la formación de profesionales.

Las empresas necesitan proteger el valor de sus negocios fortaleciendo la seguridad en todos los niveles de su infraestructura informática. Resultan especialmente sensibles los servicios críticos y aquellos de cuya disponibilidad dependan directamente los beneficios de la empresa. Las empresas deben desarrollar y aplicar las políticas de TI, así como automatizar sus procesos de cumplimiento de normas.

El mantenimiento de las adecuadas medidas administrativas permite no sólo identificar las amenazas de seguridad existentes, sino también diseñar los planes de contingencia proactivos y reactivos.

La no correcta aplicación de estos patrones de seguridad puede derivar en situaciones de peligro como posibles ataques a infraestructuras críticas. Un ejemplo de este tipo de incidentes lo podemos encontrar en las declaraciones del gobierno de los Estados Unidos de abril de 2009[6], en las que admitió que "el control de la infraestructura energética de la nación es vulnerable a los ataques por Internet". En dichas declaraciones, admitieron que sus sistemas de control sufrieron infiltraciones por parte de espías extranjeros.

Los problemas de seguridad informática fuera del ámbito empresarial también pueden afectar a las empresas como se puedo observar con el incidente de la botnet Mariposa[7]. El FBI destacó el trabajo de las autoridades eslovenas y españolas para desmantelar esta red en febrero de 2010 que contaba con más de 12 millones de equipos alrededor del mundo, usurpaba contraseñas bancarias y lanzaba ataques a instituciones financieras.

Otro reciente ejemplo de ataque con grandes consecuencias económicas y políticas fue la infiltración en uno de los servidores del Ministerio de Defensa Británico unas semanas después de que su gobierno anunciara el lanzamiento de un programa de seguridad informática de 650 millones de libras esterlinas (algo más de 754 millones de euros)[8].

El mayor problema de la seguridad informática es que los profesionales del sector no tienen una adecuada formación en dicha materia, como recoge en la noticia titulada "Los

[6] http://news.bbc.co.uk/2/hi/technology/7990997.stm

[7] http://www.elpais.com/articulo/tecnologia/Cae/red/cibercriminal/Mariposa/controlaba/millones/ordenadores/zombis/190/paises/elpeputec/20100302elpeputec_8/Tes

[8] http://www.elmundo.es/elmundo/2010/11/08/navegante/1289231632.html

informáticos no salen preparados de las universidades en materia de seguridad"[9]. En este artículo, el experto en seguridad Sergi Álvarez Capilla asegura que uno de los mayores riesgos de seguridad para una organización es no disponer de informáticos suficientemente concienciados y formados en cuanto a la seguridad informática.

En la actualidad, la figura del auditor externo ha cobrado importancia en el ámbito de la seguridad informática. La certificación de dicho auditor representa una garantía del desarrollo de su labor profesional bajo ciertos estándares que son considerados como mejores prácticas en la materia. Además, el auditor se adhiere a un código de ética que emite la organización certificadora por el que debe cumplir ciertas obligaciones relacionadas con la confidencialidad, formación permanente, cuidado profesional e independencia de criterio.

Si bien hoy la certificación de los auditores de sistemas de seguridad no representa una obligación formal para los profesionales del área, sin embargo, sirven de punto de referencia para el desarrollo de la formación de los profesionales de la seguridad informática. Las certificaciones más relevantes relacionadas con la seguridad informática que se han analizado para el desarrollo del presente currículo son la ISO 27001[10], ISACA[11] y ISO 15408[12]. El profesional TI se desenvolverá con gran soltura en los estándares ISO/IEC desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El mercado laboral demanda constantemente expertos en seguridad informática; ya sea para la administración pública, fuerzas de seguridad del estado o el sector privado. Organismos como la Agencia Española de Protección de Datos[13], el Grupo de Delitos Telemáticos de la Guardia Civil[14], la Brigada de Investigación Tecnología del Cuerpo Nacional de Policía[15] o INTECO (Instituto Nacional de Tecnologías de la Comunicación)[16] son buenos ejemplos que muestran las amplias oportunidades laborales para los expertos en seguridad informática en nuestro país.

2.3. Normas reguladoras del ejercicio profesional

No son de aplicación

2.4. Referentes externos a la universidad proponente que avalen la adecuación de la propuesta a criterios nacionales o internacionales para títulos de similares características académicas

Normativa

La Constitución española establece ciertos principios sobre la seguridad y la privacidad de los

[9] http://www.libertaddigital.com/internet/los-informaticos-no-salen-preparados-de-las-universidades-en-materia-de-seguridad-1276388029/
[10] http://www.iso27000.es/
[11] http://www.isaca.org/
[12] http://www.commoncriteriaportal.org/
[13] https://www.agpd.es/
[14] https://www.gdt.guardiacivil.es
[15] http://www.policia.es/bit/index.htm
[16] http://www.inteco.es/

ciudadanos, tal y como puede verse en estos ejemplos:

- Artículo 18.1: *se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
- Artículo 18.3: *se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
- Artículo 18.4: *la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

Estos principios básicos se plasman en ciertas leyes que, a su vez, suponen el pilar central del marco legislativo sobre seguridad de la información en España.

La Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen establece, en su artículo primero, que dicho derecho *será protegido civilmente frente a todo género de intromisiones ilegítimas*, de acuerdo con lo establecido en dicha ley, implementando el artículo 18.1 de la Constitución.

Por su parte, la normativa europea, estatal y autonómica en materia de protección de datos de carácter personal, en la que ocupa un lugar preeminente la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) y su reglamentación de desarrollo, en especial el Real Decreto 1720/2007, tiene como común objeto la garantía de los derechos que emanan del citado precepto constitucional, especialmente en cuando que tales datos son tratados en el despliegue de la actividad organizacional mediante el uso de la informática.

El hecho de que el corpus legal regulador de la protección de datos de carácter personal defina no sólo derechos y obligaciones, sino también las medidas técnicas y administrativas obligatorias para el tratamiento de los datos personales atendiendo al nivel de clasificación de los mismos (básico, medio y alto); hace que la aplicación de dicha legislación no sólo ataña al asesor legal, sino también a todo profesional de las TI que deba tratar, de una u otra forma, con este tipo de datos.

Así, la formación técnica de los profesionales de las TI se convierte en un imperativo legal, en aplicación de leyes que suponen la implementación práctica de principios básicos de la Constitución, y que sustentan la privacidad e intimidad de todos los ciudadanos.

En una aplicación más práctica, se encuentra la Ley 59/2003 de Firma electrónica, relacionada con la Directiva Europea 1999/93/CE, y que establece un marco europeo común para la firma electrónica. En dicha ley se definen tres tipos de firmas:

- Simple. Datos que puedan ser usados para identificar al firmante (autenticidad).
- Avanzada. Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico). Se emplean técnicas de PKI.
- Reconocida. Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante).

En ocasiones, esta firma se denomina cualificada por traducción del término inglés *qualified* que aparece en la Directiva Europea de Firma Electrónica.

En cuanto a los proveedores de servicios, se encuentra la LSSI o Ley de Servicios de la Sociedad de Información de España, cuyo nombre completo es Ley 34/2002 de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico. En esta ley se regulan las obligaciones de los proveedores de servicios, incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia así como el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

Documentos

Se han consultado los siguientes documentos, indispensables para la elaboración de la propuesta:

- La guía de apoyo para la elaboración de la memoria para la solicitud de verificación de títulos oficiales elaborada por la ANECA.
- El protocolo de evaluación para la verificación de títulos universitarios oficiales elaborado por la ANECA.
- El documento sobre herramientas para el diagnóstico en la implantación de sistemas de garantía interna de calidad de la formación universitaria.

Referentes nacionales

Para la elaboración de esta propuesta, se ha tomado en consideración los siguientes másteres oficiales:

- Universidad Europea de Madrid (UEM): Máster Universitario en Seguridad de Tecnologías de la Información y Comunicaciones http://www.uem.es/postgrado/master-oficial-en-seguridad-de-las-tecnologias-de-la-informacion-y-las-comunicaciones
- Universitat Rovira i Virgil (URV): Máster Universitario en Seguridad Informática y Sistemas Inteligentes http://www.urv.cat/masters_oficials/es_enginyeria_informatica.html
- Universidad de Deusto: Máster Universitario en Seguridad de la Información http://www.postgrado.deusto.es/servlet/Satellite/Postgrados/1240918715667/_cast/%231/0/cx/UniversidadDeusto/comun/render
- Universidad Alfonso X el Sabio (UAX): Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones http://www.uax.es/oferta_docente/titulaciones/mus/
- Universidad Nacional de Educación a Distancia (UNED): Máster Universitario en Comunicación, Redes y Gestión de Contenidos http://portal.uned.es/portal/page?_pageid=93,1339351,93_20541829&_dad=portal&_schema=PORTAL
- Universidad Rey Juan Carlos (URJC): Máster Universitario de Investigación en sistemas

HW y SW avanzados
http://www.urjc.es/estudios/masteres_universitarios/informatica/hardware_software/index.htm

Del mismo modo, se han utilizado como referente los siguientes másteres de título propio:

- Universitat Oberta Catalunya (UOC): Máster en Seguridad Informática
http://www.uoc.edu/masters/esp/web/informatica_multimedia_telecomunicacion/seguridad_informatica_/master/seguridad_informatica/index.html
- Universidad Pontificia de Salamanca (UPSAM): Máster en seguridad informática
http://www.upsam.es/index.php?Mod=Estudios&Section=Mostrar&IdEstudio=137&Lang=es
- Universidad de Almería (UAL): Máster en Administración, Comunicaciones y Seguridad Informática
http://masteracsi.ual.es/index.php
- Universidad del País Vasco (EHU): Diseño y Seguridad en Redes
https://gestion-alumnos.ehu.es/pls/entrada/tprw0270.htm?p_sesion=939c91ac9551a097a49199ab9391a49387a5aa7c9b9b787796898486826e8a75908f6999748193837694
- Universidad de León (UNILEON): Máster profesional en tecnologías de la seguridad
http://masterseguridad.unileon.es/
- Universidad Politécnica de Madrid (UPM) + ALI: Máster en seguridad informática
http://www.fi.upm.es/?id=masterpropios

- Universidad Politécnica de Madrid (UPM) + ALI: Máster en auditoría informática
http://www.fi.upm.es/?id=masterpropios

Referentes internacionales

Se consignan algunos de los principales másteres internacionales sobre esta materia.

Reino Unido

- University of Birmingham: MSc in Computer Security
http://www.cs.bham.ac.uk/admissions/postgraduate-taught/degree_info/msc-csec/
- University of Bedfordshire: MSc Computer Security and Forensics
http://www.beds.ac.uk/courses/bysubject/cominfsys/msc-comforsec
- University of Greenwich: MSc Computer Security Forensics and Risk Management
http://www.gre.ac.uk/courses/pg/com/compsec
- University of Liverpool: MSc in Computer Security
http://www.liverpool.ohecampus.com/index.php?mod=dcp&act=navigationindex&navigationid=2271
- University of Essex: MSc Computer Security
http://www.essex.ac.uk/coursefinder/CourseDetails.aspx?course=MSC+G49312
- University of Bradford: MSc Internet, Computer and System Security
http://computing.brad.ac.uk/courses/pg/mscicss.php

- University of Plymouth: MSc Computer and Information Security http://www.plymouth.ac.uk/courses/postgraduate/taught/3836/MSc+Computer+and+Information+Security
- Royal Hollowat University of London: MSc in Information Security http://www.isg.rhul.ac.uk/msc
- University of Kent: MSc Computer Security http://www.cs.kent.ac.uk/teaching/pg/courses/msc-compsec/index.html
- Newcastle University: MSc Computer Security and Resilience http://www.ncl.ac.uk/postgraduate/taught/subjects/computing/courses/458
- Abertay University: MSc Ethical Hacking & Computer Security http://www.abertay.ac.uk/studying/find/pg/ehcs/
- Kerckhoffs Institute (University of Twente, Eindhoven University of Technology and Radbound University Nijmegen): MSc Computer Security http://www.kerckhoffs-institute.org/index.html
- De Monfort University: MSc Computer Security http://www.dmu.ac.uk/course/computer-security-1003
- University of Manchester: MSc Computer Security http://www.manchester.ac.uk/postgraduate/taughtdegrees/courses/atoz/course/?code=08343
- Queen's University Belfast: MSc in Computer and Electronic Security http://www.qub.ac.uk/schools/eeecs/ProspectiveStudents/PostgraduateStudies/GraduateStudiesTaught/MScinComputerandElectronicSecurity/
- University of Derby: MSc Forensic Computing and Security http://www.derby.ac.uk/computing/msc-forensic
- Liverpool John Moores University: MSc Computer Network Security http://www.ljmu.ac.uk/courses/postgraduate/59566.htm
- Kingston University London: MSc Network and Information Security http://www.kingston.ac.uk/postgraduate-course/network-information-security-msc/
- Staffordshire University: MSc Computer Networks and Security http://www.staffs.ac.uk/courses_and_study/courses/computer-networks-and-security-tcm4220819.jsp
- University of East London: MSc Information Security and Computer Forensics http://www.uel.ac.uk/programmes/cite/postgraduate/iscf.htm
- University of Glamorgan: MSc Computer Systems Security http://courses.glam.ac.uk/courses/254-msc-computer-systems-security
- Dublin City University: MSc in Security and Forensics Computing http://www.dcu.ie/prospective/deginfo.php?classname=MSSF
- University of Westminster: MSc Computer Forensics http://www.westminster.ac.uk/schools/computing/postgraduates/msc-computer-science
- Limerick Institute of Technology: MSc in Computing (stream C - Security and Digital Forensics) http://www.lit.ie/departments/IT/MSC_Computing.html
- University of Bristol: MSc in Advanced Computing - Internet Technologies with Security

http://www.bris.ac.uk/prospectus/postgraduate/2011/prog_details/ENGF/845

- University of Gloucestershire: MSc in Computing with Systems Security Management
  http://www.glos.ac.uk/courses/postgraduate/csm/Pages/default.aspx

Estados Unidos

- Master in Information Security, NOVA Southeastern University, Florida, EEUU
  http://www.scis.nova.edu/masters/msis.html
- Master of Science in Computing Security and Information Assurance, Rochester Institute of Technology (RIT), New York, EEUU
  http://www.nssa.rit.edu/?q=node/29
- Computer Network and Security, Clark Atlanta University, EEUU
  http://www.cau.edu/Academics_Computer_and_Info_Sci.aspx
- Master of Science in Computer Science concentration in Security (Boston University, USA)
  http://www.bu.edu/met/programs/graduate/computer-science/security/

Alemania

- Master in IT-Security, Technische Universität Darmstadt
  http://www.cased.de/en/further_education/master/it_securitymaster.html

Italia

- Master in Sicurezza dei Sistemi e delle Reti Informatiche, Universidad de Roma l'Impresa
  http://mastersicurezza.uniroma1.it/
- Master in Computer Security, University of Trento
  http://mcs.dit.unitn.it/edu/compsciences/s3ad.xml?cds_id=30&aa_ord_id=2004&aa_off_id=2006&pds_id=10002&ad_id=85172

Francia

- Communications and Computer Security, ParisTech, Francia
  http://enseignements.telecom-paristech.fr/programme.php?id=171&langue=EN
- International Masters in Computer Security, EPITA Graduate School in Computer Science
  http://www.epita.fr/masters/masters-computer-security.html

Países nórdicos

- MSc in Security Engineering, Blekinge Institute of Technology
  http://www.bth.se/tek/masters_eng.nsf/pages/4a6eaaeb01210610c1256f5400395fd1!OpenDocument
- MSc in Information Security, Gjøvik University College
  http://english.hig.no/study_programmes/it/master/mis

Otros enlaces y obras editadas.

Seventh Framework Programme for Research (FP7)

http://cordis.europa.eu/fp7/security/home_en.html

La Comisión Europea mantiene una sección completa del FP7 para proyectos de investigación en seguridad. Entre los años 2007 y 2013, la Comisión Europea ha reservado más de 1.4 Billones de euros para proyectos de investigación sobre seguridad. Algunos de estos proyectos están estrictamente enmarcados en el ámbito de la seguridad informática como por ejemplo el proyecto para escribir software más seguro[17].

Agencias y certificaciones

- www.iso27001certificates.com
  Registro internacional de organizaciones certificadas en ISO 27001 y BS 7799-2.
- www.iso.org/iso/en/prods-services/ISOstore/store.html
  Tienda online de ISO (International Organization for Standardization) donde pueden adquirirse todo tipo de normas.
- isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm
  Descarga gratuita de normas ISO relacionadas con las tecnologías de la información. No se encuentra entre ellas ninguna de la serie ISO 27000 o ISO 17799, que son de pago y disponibles en la Tienda Online de ISO.
- www.european-accreditation.org
  European Cooperation for Accreditation Asociación sin ánimo de lucro
- www.ukas.com
  UK Accreditation Service. Organismo de Acreditación del Reino Unido que cuenta con reconocimiento internacional.
- www.irca.org
  International Register of Certificated Auditors. IRCA han sido adoptados como un modelo estándar industrial por otros organismos de certificación de auditores.
- www.isaca.org
  Information Systems Audit and Control Association.
- www.isc2.org
  International Information Systems Security Certification Consortium.
- www.oc.ccn.cni.es
  Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI).
- www.itu.int/ITU-T/studygroups/com17/ict
  Colaboración de ITU, ENISA y NISSG en una base de datos de estándares de seguridad.

17 http://cordis.europa.eu/fetch?CALLER=FP7_SECURITY_NEWS_EN&ACTION=D&DOC=20&CAT=NEWS&QUERY=0126c54beb3a:0c61:661e0428&RCN=32134

Foros y asociaciones

- www.securityforum.org
  Information Security Forum (ISF).
- www.iaf.nu
  International Accreditation Forum.
- www.ismsforum.es
  ISMS Forum Spain. Asociación Española para el Fomento de la Seguridad de la Información.
- www.issa.org
  Information Systems Security Association.
- www.asisonline.org
  ASIS International (antigua American Society for Industrial Security), asociación de profesionales de la seguridad.

Institutos de seguridad y organismo gubernamentales

- www.theiia.org
  The Institute of Internal Auditors.
- buildsecurityin.us-cert.gov
  Web gubernamental de EEUU dirigida a ayudar a los desarrolladores de software a incluir seguridad en sus diseños.
- www.arcert.gov.ar/politica
  Web gubernamental argentina de implantación de políticas de seguridad en la Administración Pública.
- www.iai.es
  Instituto de Auditores Internos de España.
- www.inteco.es
  INTECO. Instituto Nacional de Tecnologías de la Comunicación de España.
- www.ecgi.org
  European Corporate Governance Institute. Instituto europeo
- www.iconsejeros.com
  Instituto de Consejeros-Administradores.
- www.csi.map.es
  Ministerio de Administraciones Públicas – Consejo Superior de Informática.
- www.cni.es
  Centro Nacional de Inteligencia / Centro Criptológico Nacional (España).
- www.ferma-asso.org
  FERMA (Federación de Asociaciones Europeas de Gestión del Riesgo).
- www.sans-ssi.org
  SANS Software Security Institute.

2.5 Descripción de los procedimientos de consulta externos utilizados para la elaboración del plan de estudios

Para los aspectos legales del Máster se ha atendido a la legislación vigente sobre docencia universitaria de Posgrado.
La propuesta que se presenta ha sido fruto de un análisis a fondo de los principales másteres sobre asesoramiento financiero que se imparten en España, resto de Europa y Estados Unidos. De ellos se ha observado ante todo el planteamiento docente, los contenidos y la planificación de las prácticas.

Los puntos de referencia fundamentales desde el punto de vista legal y administrativo han sido la normativa vigente al respecto; así como las experiencias y orientaciones publicadas en la web de la ANECA.

De modo general, la propuesta que se presenta se ha desarrollado de acuerdo con la metodología de las Competencias Profesionales. También se han tenido en cuenta las características que definen la calidad de la formación virtual destinada a personas que desean incorporase al mercado de trabajo y a los trabajadores que desean mejorar su condición laboral, identificadas mediante la aplicación de la Norma UNE 66181:2008.

Los referentes académicos externos que se han empleado han influido en lo que a concepción general del máster se refiere y en la aportación de las asignaturas optativas para poder ofertar contenidos que permitan profundizar en temas específicos.

Pero este enfoque general no agota las aportaciones concretas que se han obtenido de los referentes académicos externos ya señalados. En concreto, y siguiendo el orden y las cuestiones que indica esta propuesta, de los referentes observados se han tomado los siguientes modelos.

Referentes externos que se han aplicado para la redacción de los objetivos y competencias

Para la elaboración de los objetivos del Máster especificados en el apartado 2.1 de esta memoria se ha seguido también los objetivos presentes en diversos programas universitarios nacionales e internacionales.

El Máster en Seguridad busca formar profesionales con conocimientos en la asesoría de la seguridad en las TI, pudiendo gestionar cualquier SGSI(Sistema de Gestión de la Seguridad de la Información) en este sentido sigue la misma línea que la mayoría de los programas antes citados (UEM, UOC, Rey Juan Carlos, EHU, etc).

La titulación propuesta tiene un profundo componente práctico, como medio para satisfacer las necesidades del propio sector de la seguridad informática. En este sentido, el estudio de las principales medidas técnicas y administrativas supone el eje central del plan de estudios.

Referentes externos que se han aplicado para la definición de la estructura del Máster

En el proceso de consulta para la definición del plan de estudios han influido diversos ámbitos:

- En el proceso de diseño y construcción del plan de estudios del presente máster, se ha tenido en cuenta la estructura de los estudios similares ofertados, tanto a nivel nacional como internacional. Durante dicho proceso, se ha asegurado que existe una correspondencia entre las materias del presente diseño docente con respecto a dichos referentes.

- Se ha comprobado que todos los estudios de postgrado sobre seguridad de la información comparten ciertas áreas del conocimiento, como pueden ser el estudio de la criptografía, legislación y marco jurídico, auditoría de sistemas y procesos, estudio de redes avanzadas y sistemas operativos.

- De igual modo en el proceso de consulta se ha tomado en cuenta no sólo el temario sino las necesidades reales de un alumno que se enfrenta a este tipo de formación, tomando en cuenta las posibles necesidades de formación previa. En este sentido, el Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil ha señalado la importancia de contar con una adecuada formación en el mundo de la seguridad informática. Uno de los promotores de este Máster, Juan Salom, es miembro de dicho grupo.

- Dentro del proceso de consulta se han tomado en cuenta experiencias docentes universitarias, como la de la UOC, en cuyos estudios de postgrado participan como consultores varios de los promotores de este máster.

- También se han tenido en cuenta otras experiencias docentes, concretamente en el ámbito legal, dentro de los estudios de postgrado de la Universidad de Alcalá de Henares titulado “Máster en Informática Pluridisciplinar”[18].

- La experiencia docente de varias ediciones en los Cursos de Extensión sobre seguridad informática de la Universidad de Alcalá (“Curso Básico de Seguridad Informática” y “Curso de Auditoría de Seguridad Informática”), ha servido para aportar una evaluación práctica del nivel de los estudiantes de últimos años de carreras técnicas, en el ámbito de la seguridad informática.

Referentes externos aplicados al profesorado

Como criterio general respecto al cuerpo docente, se pretende la colaboración conjunta de académicos universitarios con experiencia en la docencia junto a profesionales de reconocido prestigio en el mundo de la seguridad informática.

Se ha formado el equipo docente de tal manera que se cubran todas las materias propuestas en el máster gracias a sus experiencias profesionales:

- Profesionales de las Fuerzas de Seguridad del Estado, con integrantes del Grupo de Delitos Telemáticos de la Guardia Civil.

- Profesionales de la seguridad informática, con integrantes de equipos de seguridad de

[18] http://www.etsii.uah.es/master_etsii/index.html

empresas como Telefónica y ATOS Origin.

- Profesionales de agencias de certificación como AENOR.
- Profesionales de la auditoría de seguridad.
- Docentes expertos en legislación, con experiencia en docencia de otros másteres oficiales.
- Docentes expertos en seguridad informática, responsables de los cursos de extensión universitaria sobre seguridad en la Universidad de Alcalá de Henares.

2.6. Descripción de los procedimientos de consulta internos utilizados para la elaboración del plan de estudios

Los expertos externos que han sido consultados para la elaboración de la presente propuesta son los siguientes:

- Bernardo Alarcos Alcázar (bernardo.alarcos@uah.es). Doctor Ingeniero de Telecomunicación, experto en redes de computadores y seguridad informática. Imparte en la Universidad de Alcalá de Henares varias asignaturas, tanto de grado como de postgrado, sobre redes de computadores y seguridad de la información.
- Daniel Sanz (dani.dsanz@gmail.com). Ingeniero en Informática, investigador sobre seguridad (DEA en políticas y mecanismos de control de accesos en rbac), responsable técnico en Ándago Soluciones en integración de políticas de seguridad y mecanismos de autenticación, desarrollador en Liferay España.

Las referencias que han influido en el diseño de este Máster son las siguientes:

Medio de Consulta Externo	Aportación al Plan de Estudios
• Planes de estudios de UEM, UOC y EHU.	• Orientación sobre el planteamiento general del Máster, sobre la estructura modular y las asignaturas concretas de la especialidad.
• Planes de estudios de UAX, Deusto, URV y UAL. • Planes de estudios de la universidad de Birmingham y Liverpool.	• Orientación sobre el planteamiento general del Máster, sobre la estructura modular y las asignaturas concretas de la especialidad. • Orientación general sobre el Máster, el plan de estudios y el programa de los distintos módulos que lo componen. • Metodología docente virtual
Medio de Consulta Externo	Aportación al Plan de Estudios

• Planes de estudios y organización docente del Máster de Seguridad de la Universitat Oberta de Catalonya	• Información específica sobre perfil de preferente de ingreso para los alumnos, la planificación de las prácticas y el planteamiento docente.
• Computer Network and Security (Clark Atlanta university, USA). • Máster Universitario en Ingeniería de Seguridad de la Información y las Comunicaciones, Universidad Alfonso X el Sabio	• Sobre los contenidos y competencias de alguna de las asignaturas del Máster. • Información específica sobre la planificación de las prácticas y el planteamiento docente.
DOCUMENTOS	
Libros Blancos del Programa de Convergencia Europea de ANECA (http://www.aneca.es). Informes de colegios profesionales o asociaciones nacionales, europeas, de otros países o internacionales.	• Sobre la estructura general del Máster. • Orientación sobre salidas profesionales de la Titulación • Establecen el marco general del nivel de competencias que deben exigirse para una formación de Máster.
ASESORAMIENTO DE EXPERTOS ACADÉMICOS Y PROFESIONALES	
Bernardo Alarcos Alcázar	Recomendaciones sobre los objetivos del título Recomendaciones sobre el contenido de las materias Recomendaciones sobre la estructura de los módulos del título
Daniel Sanz	Recomendaciones sobre el contenido de las materias. Recomendaciones sobre aspectos técnicos de las materias

Para plasmar la versión definitiva del Máster se han tenido en cuenta las observaciones realizadas por los miembros del comité académico asesor. También ha contado con la

colaboración directa de la coordinadora académica de la UNIR.

Para plasmar la versión definitiva del Máster el redactor del primer documento ha tenido en cuenta las observaciones realizadas por los miembros del comité académico asesor y por los expertos consultados. Este borrador se convirtió en memoria definitiva al ser respaldado de manera unánime por el resto de expertos, tanto académicos como profesionales.

En la elaboración de la Memoria tomaron, así mismo, parte los siguientes expertos:

- Dr. D. José María Vázquez García-Peñuela, Rector de la UNIR, ex Decano de la Facultad de Derecho de la Universidad de Almería y ex Vicerrector en ella de Relaciones Internacionales, y que ha sido nombrado Rector de la UNIR, ha asesorado en materias relativas a movilidad y sistema de garantía de calidad.
- Dª Mónica Pérez Iniesta, Licenciada en Ciencias Empresariales y en Humanidades, y Dª María Gómez Espinosa, Licenciada en Matemáticas, expertas en plataformas de enseñanza virtual, han contribuido en la elaboración de los apartados referentes a la didáctica en entorno virtual.
- D. Juan Bautista Jiménez Herradón, Ingeniero de Telecomunicaciones, ha trabajado en los apartados referentes a recursos materiales y servicios.
- Dª Almudena Castellanos, licenciada en pedagogía, especialista en Nuevas tecnologías aplicadas a la educación y profesora de la Universidad Internacional de La Rioja.

La coordinación del comité académico y de los expertos consultados la llevó a cabo Dª Paloma Puente Ortega.

3. COMPETENCIAS

3.1. Competencias Básicas y Generales

	COMPETENCIAS BÁSICAS
CB6	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
CB7	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.
CB8	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular 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.
CB9	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.
CB10	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.

	COMPETENCIAS GENERALES
CG1	Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.
CG2	Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.
CG3	Mantener una actitud que les permita estudiar de manera autónoma y promover la formación contínua en su futuro desempeño profesional como experto en seguridad informática
CG4	Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.

CG5	Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI.
CG6	Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.
CG7	Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.
CG8	Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.
CG9	Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.

3.2. Competencias Transversales

	COMPETENCIAS TRANSVERSALES
CT1	Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
CT2	Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
CT3	Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
CT4	Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
CT5	Capacidad de investigar y comunicar los resultados de la investigación.

3.3. Competencias Específicas

	COMPETENCIAS ESPECÍFICAS
CE1	Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles

CE2	Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
CE3	Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.
CE4	Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias
CE5	Discernir sobre los distintos entornos de seguridad existentes para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
CE6	Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
CE7	Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
CE8	Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
CE9	Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
CE10	Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
CE11	Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.
CE12	Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
CE13	Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.
CE14	Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
CE15	Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
CE16	Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.
CE17	Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

CE18	Optimizar las políticas de seguridad de la infraestructura de la red de la entidad.
CE19	Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
CE20	Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
CE21	Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas.
CE22	Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante desastres.
CE23	Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
CE24	Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.
CE25	Conocer e interpretar la normativa de centros de respuesta a incidentes de seguridad, seguridad en centros financieros, seguridad en infraestructuras de defensa y principales conceptos de auditoría de sistemas.
CE26	Implantar procesos de análisis forense de cualquier sistema informático.
CE27	Diseñar, implantar e institucionalizar un proceso de gestión de riesgos legales en cualquier organización.

4. ACCESO Y ADMISIÓN DE ESTUDIANTES

4.1. Sistema de información previa a los alumnos de nuevo ingreso

La UNIR cuenta con un Departamento de admisiones (Contact center) que centraliza y contesta todas las solicitudes de información (llamadas y correos electrónicos) que gestiona y soluciona todas las pregunta y posibles dudas de los futuros estudiantes de la UNIR. Desde el punto de vista procedimental los pasos a seguir serán:

-Registrarse como usuario de la UNIR.

-La web muestra un formulario que el usuario tiene que completar y enviar. Cuando envía el formulario se realiza la validación automática de los campos.

-Este formulario llega a la secretaría y se realiza la validación manual de la información.

-Se le comunica al alumno el resultado y se le pide la documentación necesaria.

-Entregar la documentación justificativa del cumplimiento de los requisitos legales necesarios para la admisión; en la actualidad la normativa reguladora es:

- Ley Orgánica de Universidades 6/2001, de 19 de diciembre, modificada por la Ley Orgánica 4/2007, de 12 de abril.
- Real Decreto 1393/2007, de 29 de octubre.
- Real Decreto 1892/2008, de 14 de noviembre.

A partir de ese momento un asesor personal contacta con el alumno para verificar que cumple los requisitos exigidos para la titulación que quiere cursar y le ayuda en la elaboración de un plan de estudios personalizado así como en la resolución de dudas de los futuros estudiantes de Unir, referidas a :

- Descripción de la metodología de la UNIR. Para ello, los alumnos tendrán acceso a una demo donde se explica paso por paso.
- Niveles de dificultad y horas de estudio estimadas para poder llevar a cabo un itinerario formativo ajustado a las posibilidades reales del estudiante para poder planificar adecuadamente su matrícula.
- Descripción delos estudios.
- Reconocimiento de créditos de sus estudios previos (si los tuvieran).
- Preguntas sobre el Espacio Europeo de Educación Superior.

Una vez que la Secretaría académica comprueba toda la documentación, se procede a la formalización de la matrícula y aceptación por parte de la Universidad. El alumno recibe un Correo electrónico de confirmación.

A partir de este momento, el estudiante recibe todo el apoyo administrativo necesario para realizar de manera óptima todo el proceso de admisión y matriculación por medio de atención telefónica, por correo electrónico, con información guiada en la web para la realización de la matrícula on-line.

Por último, el alumno recibe un correo electrónico confirmando su inscripción y con las claves de acceso al CAMPUS VIRTUAL.

4.2. Requisitos de acceso y criterios de admisión

4.2.1. Requisitos de acceso con carácter general

Las enseñanzas de los diversos Másteres de la UNIR se ofrecen a cualquier persona que reuniendo las condiciones de acceso que expresa la ley desea tener una enseñanza a distancia ofrecida en un entorno virtual.

Los motivos que suelen llevar a esa elección están relacionados con algún tipo de dificultad para cursar estudios presenciales. Entre estos destacan los de aquellos que ya desempeñan una ocupación laboral o que ya tienen trabajo, que quieren iniciar o reanudar estudios universitarios.

4.2.2. Perfil recomendado de ingreso para estudiantes del Máster Universitario de Seguridad Informática

Se recomienda que el estudiante que pretenda realizar el Máster Universitario de Seguridad Informática además de los requisitos de acceso que señala la ley reúna el siguiente perfil:

· Actitud abierta y capacidad de análisis

· Capacidad de comunicación, relación social y trabajo en equipo.

· Autodisciplina.

4.2.3. Requisitos de acceso con carácter específico:

Ingenieros o ingenieros técnicos en Informática, Telecomunicaciones o Telemática fundamentalmente, así como en cualquier otra ingeniería relacionada con las TICs. También profesionales con grado de diplomados, ingenieros técnicos, licenciados o ingenieros con amplia y constatable experiencia laboral en TICs.

4.2.4. Criterios de admisión

Para poder acceder al Máster Universitario de Seguridad Informática, es necesario contar con Titulación Universitaria, según el artículo 7 del RD 39/1997. Este requisito se corresponde con los criterios de acceso establecidos en el artículo 16 del RD 1393/2007:

· Estar en posesión de un título universitario oficial español u otro expedido por una institución de educación superior del Espacio Europeo de Educación Superior que facultan en el país expedidor del título para el acceso de enseñanzas de Máster.

· Titulados conforme a sistemas educativos ajenos al Espacio Europeo de Educación Superior sin necesidad de homologar sus Títulos, previa comprobación por la Universidad de que aquellos acreditan un nivel de formación equivalente a los correspondientes Títulos universitarios oficiales españoles y que facultan en el país expedidor del Título para el acceso a enseñanzas de postgrado. El acceso por esta vía no implicará en ningún caso, la homologación del Título previo de que esté en posesión el interesado, ni su reconocimiento a otros efectos que el cursar las enseñanzas del Máster.

4.3. Apoyo a estudiantes

Sistemas de apoyo y orientación de los estudiantes una vez matriculados

1. Una vez matriculado en la UNIR, cada alumno tiene *un tutor* personal que le ayudará en:

· Su integración en los estudios, en la Universidad y en su orientación al empleo.

· La adquisición y dominio de las técnicas de trabajo intelectual y en el desarrollo de las capacidades

· Todas las cuestiones profesionales que necesite para aprovechar al máximo los servicios que le puede prestar la universidad.

2. Para explicar con detalle todos los recursos de que dispone la UNIR, así como la metodología, los alumnos cuentan con un curso especial de una semana con toda la información que necesitan antes de empezar.

El alumno entra en Aula virtual y durante la primera semana realiza el curso denominado: Lo que necesitas saber antes de empezar.

Este curso incluye los siguientes apartados:

I. ¿Qué es la universidad?:

1.1. Bienvenida del Rector, D. José Mª Vázquez García Peñuela así como comentarios de diferentes profesores de la UNIR y de otras universidades españolas.

1.2. Breve explicación del Espacio Europeo de Educación Superior.

II.Guía docente de la asignatura: En este apartado se explica mediante diferentes videos algunos aspectos relacionados con:

2.1. Metodología.

2.2. Planificación del trabajo personal y evaluación.

2.3 .Profesorado y funciones.

2.4. Orientación para el estudio.

2.5. Pack de bienvenida, libros y exámenes

III. Aula virtual:

3.1. Campus UNIR: el aula virtual.

3.2. Clases presenciales virtual

3.3. ¿Cómo participar en el foro?

3.4. El correo electrónico del campus

3.5. ¿Cómo enviar actividades?

IV. Actividades

4.1. Cuestionario de 10 preguntas para conocer mejor algunos aspectos relacionados con la disponibilidad y el tiempo de dedicación a los estudios, el manejo de las tecnologías y el conocimiento de las web 2.0 así como las características del equipo informático.

4.2. Participa en el foro de debate: primera toma de contacto de los alumnos con sus compañeros.

4.3. Participa en una clase virtual.

V. *Test*: autoevaluación de 12 preguntas de selección múltiple para comprobar si ha entendido correctamente toda la información previa al comienzo del curso.

De cada alumno se abrirá un completo dossier acumulativo que, implementando el expediente académico, registre los datos profesionales relevantes que puedan facilitar el oportuno asesoramiento personal y profesional. En todo momento se respetará la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de carácter personal así como su normativa de desarrollo.

Canales de difusión para informar a los potenciales estudiantes

Para informar a los potenciales estudiantes sobre la Titulación y sobre el proceso de matriculación se emplearán los siguientes canales de difusión:

- Página web oficial de la Universidad Internacional de La Rioja.

- Sesiones informativas en diversas ciudades de España y en algunos puntos del extranjero.

- Participación en ferias y workshops tanto en España como en el exterior, organizados por Eduespaña en colaboración con el Instituto de Comercio Exterior (ICEX).

- Sesiones informativas virtuales en directo, a través de la plataforma de UNIR a usuarios que han solicitado información o su preinscripción.

- Acciones de marketing directo (mailing, email, repartos de materiales publicitarios) sobre bases de datos segmentadas.

- Acciones comerciales e informativas a colectivos, instituciones, empresas, asociaciones, etc.

- Portales educativos como emagister, aprendemas, etc.

- Presencia en Redes Sociales.

- Presencia en buscadores, tanto en SEO (Búsquedas naturales) como SEM (Enlaces patrocinados).

- Inserciones en los medios de comunicación convencionales y digitales, nacionales e internacionales, tanto generalistas como especializados, incluidos los distintos canales de comunicación en Internet:

§ Google Adwords

§ Emagister

§ Ofertaformativa

§ Infocursos

§ Universia

§ Procenet

§ Portal Formativo

§ Hispavista

§ Aprendemas y Mastermas

§ Tu Curso y Canal Cursos.

4.4. Sistemas de transferencia y reconocimiento de créditos

http://gestor.unir.net/userFiles/file/documentos/normativa/reconocimiento_tranferencia_creditos.pdf

Reconocimiento de Créditos Cursados en Enseñanzas Superiores No Universitarias	
MÍNIMO	**MÁXIMO**
0	**9**

Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	**9**

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	**9**

5. PLANIFICACIÓN DE LAS ENSEÑANZAS

5.1. Estructura de las Enseñanzas

5.1.1. Distribución del Plan de estudios en créditos ECTS, por tipo de Asignatura para el Titulo del Máster

TIPO DE ASIGNATURAS	CRÉDITOS
Obligatorias	46
Prácticas externas	6
Trabajo fin de Máster	8
CRÉDITOS TOTALES	60

Tabla 1. Resumen de las materias y distribución en créditos ECTS

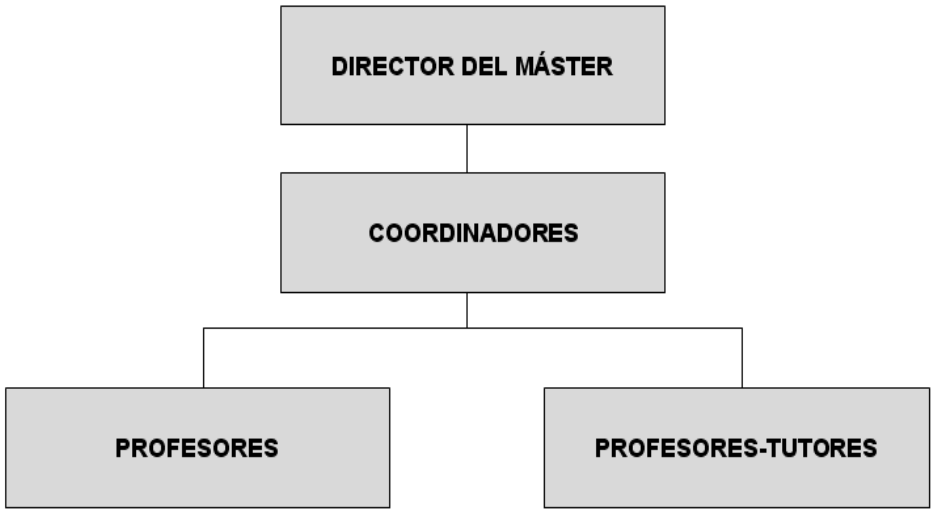
Las Prácticas externas proporcionarán la posibilidad a los estudiantes de desarrollar las competencias profesionales necesarias para enfrentarse al ámbito laboral de la empresa.

Se realizarán de manera obligatoria, por tratarse de un Máster con orientación profesional, en empresas de diversos sectores, estableciendo los convenios oportunos para la realización de las mismas.

Fundamentalmente los alumnos de este postgrado podrán acceder a prácticas en empresas dedicadas a seguridad de la información. Los centros con los que se tiene convenio de colaboración para la realización de prácticas se detallan en el criterio siete.

Mecanismos de coordinación

Estructura Docente del Máster



Directores del	Organizan a los Coordinadores de los Módulos que constan en el Plan

Máster	de Estudios del Máster. Aprueban los materiales de aprendizaje para los estudiantes. Atienden y valoran las sugerencias e iniciativas de los coordinadores referidos a ellos y resuelven en última instancia los problemas que puedan afectar a las tareas de los coordinadores.
Coordinadores	Coordinan los Módulos de que consta el Plan de Estudios en función de su especialización y a los Profesores y tutores personales de cada Asignatura. Aseguran de manera práctica que los materiales generados por los profesores y aprobados por el director del Máster son adecuados. Igualmente verifican que no se producen solapamientos ni hay lagunas en los contenidos previstos. Proponen al director del Máster las mejoras referidas tanto a los materiales como a la planificación. Resuelven en primera instancia, las incidencias en el desarrollo del Máster.
Profesores	Generan los materiales de aprendizaje de los estudiantes y realizan la revisión y adaptación de los mismos que les indiquen los coordinadores. Desarrollan las clases virtuales presenciales y dirigen los debates. Diseñan casos prácticos y ejercicios de autoevaluación y evaluación para los estudiantes bajo la supervisión de los coordinadores.
Profesores–Tutores	Llevan a cabo el proceso de tutoría-seguimiento y la evaluación continua de los estudiantes. Actúan como Tutores de Prácticas y Tutores de Proyecto para los estudiantes.

Igualdad entre hombres y mujeres, fomento de la educación y cultura de la paz y de la no discriminación

La Escuela de Ingeniería de la Universidad Internacional de La Rioja, de la que depende el Máster Universitario en Seguridad Informática, se compromete a impulsar la divulgación de los contenidos que señala la legalidad vigente a este respecto para procurar que se difundan en la actividad profesional de los ahora estudiantes; en concreto a lo que indican las siguientes leyes:

- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. BOE núm. 71, de viernes 23 marzo 2007.
- Ley 27/2005, de 30 de noviembre, de fomento de la educación y la cultura de la paz. BOE núm. 287, de jueves 1 diciembre 2005.
- Ley 51/2003, de 2 de diciembre de 2003, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. BOE núm. 289, de miércoles 3 diciembre 2003.

5.1.2. Explicación general de la planificación del plan de estudios

El plan de estudios del Máster en Seguridad Informática por la Universidad Internacional de La Rioja se estructura en cuatro módulos de asignaturas: Aspectos legales y marco jurídico, Auditoría y gestión de la seguridad, Técnicas avanzadas de seguridad y Seguridad en aplicaciones y análisis forense. Cada uno de estos módulos es de tipo teórico-práctico y engloba asignaturas de carácter obligatorio.

Además de estos cuatro módulos de asignaturas, y como un quinto módulo especial, se encuentra la práctica profesional y la preparación de un trabajo final.

5.1.3. Esquemática y temporalmente, la Planificación del Máster queda de la siguiente manera:

El Máster plantea su desarrollo en un año académico.

Atendiendo a los distintos perfiles de estudiantes que pueden estar interesados en cursar el Máster, se ha diseñado un Plan de estudios, que contempla la realización del Máster en uno o en dos años, en función del tiempo que pueda dedicarle cada estudiante. Se trata por tanto de un Máster pensado para ser cursado, bien a tiempo completo, en un año, bien a tiempo parcial, en dos años.

En todo caso el estudiante deberá escoger la temporalidad antes del inicio del Máster, no pudiendo cambiar una vez iniciado.

CARÁCTER ANUAL (dedicación a tiempo completo)

1er Cuatrimestre (27 ECTS)		
Asignaturas	***ECTS***	***Carácter***
Aspectos legales y regulatorios	3	Obligatorio
Gestión de la seguridad	3	Obligatorio
Seguridad en redes	5	Obligatorio
Seguridad en sistemas operativos	5	Obligatorio
Análisis forense	3	Obligatorio
Criptografía y mecanismos de seguridad	5	Obligatorio
Análisis de vulnerabilidades	3	Obligatorio
2º Cuatrimestre (33 ECTS)		
Asignaturas	***ECTS***	***Carácter***
Análisis de riesgos legales	3	Obligatorio
Auditoría de la seguridad	3	Obligatorio

Seguridad en aplicaciones online y bases de datos	5	Obligatorio
Seguridad en el software	5	Obligatorio
Delitos informáticos	3	Obligatorio
Prácticas externas en empresa	6	PE
Trabajo Fin de Máster	8	TFM

CARÁCTER BIANUAL (dedicación a tiempo parcial)

1 año 1er Cuatrimestre (16 ECTS)		
Asignaturas	***ECTS***	***Carácter***
Aspectos legales y regulatorios	3	Obligatorio
Seguridad en redes	5	Obligatorio
Criptografía y mecanismos de seguridad	5	Obligatorio
Análisis de vulnerabilidades	3	Obligatorio
1 año 2º Cuatrimestre (14 ECTS)		
Asignaturas	***ECTS***	***Carácter***
Análisis de riesgos legales	3	Obligatorio
Auditoría de la seguridad	3	Obligatorio
Seguridad en aplicaciones online y bases de datos	5	Obligatorio
Delitos informáticos	3	Obligatorio
2º año 1er Cuatrimestre (11 ECTS)		
Asignaturas	***ECTS***	***Carácter***
Gestión de la seguridad	3	Obligatorio
Seguridad en sistemas operativos	5	Obligatorio
Análisis forense	3	Obligatorio
2º año 2º Cuatrimestre (19 ECTS)		
Asignaturas	***ECTS***	***Carácter***

Seguridad en el software	5	Obligatorio
Prácticas externas en empresa	6	PE
Trabajo Fin de Máster	8	TFM

5.1.4. Metodología de la Universidad Internacional de la Rioja

La Universidad Internacional de La Rioja basa su enfoque pedagógico en los siguientes puntos:

- Participación de los alumnos y trabajo colaborativo que favorece la creación de redes sociales y la construcción del conocimiento. Las posibilidades técnicas que ofrece el campus virtual permiten crear entornos de aprendizaje participativos (con el uso de foros, chats, correo web, etc.) y facilitar y fomentar la creación colaborativa de contenidos (blogs, videoblogs, etc.).
- A partir de aquí, los procedimientos y estrategias cognitivas llevan al alumno, mediante su actividad directa y personal, a la construcción del propio conocimiento y elaboración de significados. Los docentes son mediadores en el proceso. Además de programar y organizar el proceso, el docente anima la dinámica y la interacción del grupo, facilita recursos. Se destaca el aprendizaje significativo, la colaboración para el logro de objetivos, la flexibilidad, etc.
- Organización de los contenidos y variedad de recursos de aprendizaje.

Los puntos clave de nuestra metodología son:

- Formular los objetivos de aprendizaje.
- Facilitar la adquisición de las competencias básicas para el ejercicio de la profesión.
- Elaborar los contenidos que el profesor desea transmitir.
- Organizar los contenidos divididos en básicos, específicos y complementarios.
- Elaborar las herramientas de evaluación necesarias que garanticen el aprovechamiento de su formación.
- Evaluación continua de las respuestas de los alumnos
- Control del ritmo de progreso de los alumnos.
- Crear aportaciones para que los alumnos se enfrenten a situaciones que entren en contraste con sus experiencias anteriores.
- Sugerir actividades que les ayuden a reestructurar su conocimiento.
- Proponer actividades de resolución de problemas.
- Fomentar actividades que requieran interacción y colaboración con otros alumnos.
- Crear contextos “reales”. El formador puede diseñar simulaciones de la realidad que ayuden al alumno a comprender la validez de lo que aprende para resolver problemas

concretos y reales.

- Utilizar casos prácticos que muestren al alumno experiencias reales.
- Aprovechar las posibilidades del hipertexto para permitir a los alumnos que construyan sus propios caminos de aprendizaje (un camino adecuado a su estilo de aprendizaje).

Aula virtual

Descripción general del aula virtual

El aula virtual es un espacio donde los alumnos tienen acceso a la totalidad del material didáctico asociado a la asignatura (unidades didácticas, documentación de interés complementaria, diccionario digital de términos asociados a las asignaturas del programa de formación, etc.).

Este recurso se encuentra en el campus virtual, una plataforma de formación donde además del aula, el alumno encuentra otra información de interés. Se hace a continuación una descripción general sobre las diferentes secciones de campus virtual con una descripción más detallada del aula.

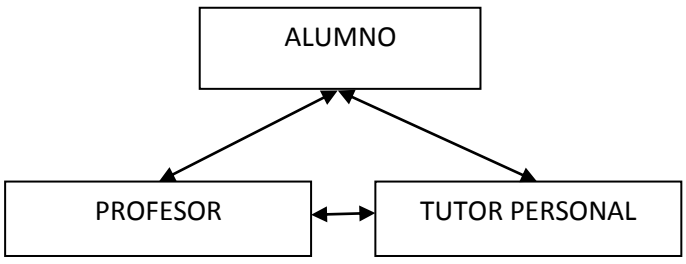
CAMPUS VIRTUAL	
AGENDA	Permite al estudiante consultar los principales eventos (exámenes, actividades culturales, clases presenciales). La agenda puede estar sincronizada con dispositivos móviles.
CLAUSTRO	En este apartado se encuentran los nombres de todo el personal docente de UNIR y el nivel de estudios que poseen.
NOTICIAS	Información común a todos los estudios que puede resultar interesante.
FAQ	Respuestas a preguntas frecuentes.
DESCARGAS	Apartado desde donde se pueden descargar exploradores, programas, formularios, normativa de la Universidad, etc.
LIBRERÍA/BIBLIOTECA	Acceso a libros y manuales para las diferentes asignaturas, existen también herramientas donde se pueden comprar o leer libros online.
EXÁMENES	Cuestionario a rellenar por el alumno para escoger sede de examen y una fecha de entre las que la Universidad le ofrece.
ENLACES DE INTERÉS	UNIR propone enlaces tales como blogs, voluntariado, actividades culturales destacadas, etc.
AULA VIRTUAL	El alumno tendrá activadas tantas aulas virtuales como asignaturas

	esté cursando. Contiene el material necesario para la impartición de la asignatura, que se organiza en las **SECCIONES que se describen a continuación:**
RECURSOS	**Temas:** Cada uno de los temas incluye varias secciones que serán básicas en el desarrollo de la adquisición de las competencias de la titulación: - **Ideas claves:** Material didáctico básico para la adquisición de competencias. - **Lo más recomendado:** lecturas complementarias, videos y enlaces de interés, etc. - **+ Información:** pueden ser textos del propio autor, opiniones de expertos sobre el tema, artículos, páginas web, Bibliografía, etc. - **Actividades:** diferentes tipos de ejercicios, actividades y casos prácticos. - **Test:** al final de cada uno de los temas se incluye un test de autoevaluación para controlar los resultados de aprendizaje de los alumnos.
	Programación semanal: Al comienzo de cada asignatura, el alumno conoce el reparto de trabajo de todas las semanas del curso. Tanto los temas que se imparten en cada semanas como los trabajos, eventos, lecturas. Esto le permite una mejor organización del trabajo.
	Documentación: A través de esta sección el profesor de la asignatura puede compartir documentos con los alumnos. Desde las presentaciones que emplean los profesores hasta publicaciones relacionadas con la asignatura, normativa que regule el campo a tratar, etc.
TV DIGITAL	**Presenciales virtuales:** permite la retransmisión en directo de clases a través de Internet, donde profesores y estudiantes pueden interactuar.
	Clases magistrales: En esta sección se pueden ver sesiones grabadas en la que los profesores dan una clase sobre un tema determinado sin la presencia del estudiante.
	UNIRTV: Desde esta sección, los alumnos pueden subir vídeos y ver los que hayan subido sus compañeros.

COMUNICACIONES	**Última hora:** Se trata de un tablón de anuncios dedicado a la publicación de noticias e información de última hora interesantes para los alumnos.
	Correo: Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente.
	Foros: Este es el lugar donde profesores y alumnos debaten y tratan sobre los temas planteados.
	Chat: Espacio que permite a los distintos usuarios comunicarse de manera instantánea.
ACTIVIDADES	**Envío de actividades:** Para realizar el envío de una actividad hay que acceder a la sección *Envío de actividades*. En este apartado el alumno ve las actividades que el profesor ha programado y la fecha límite de entrega. Dentro de cada actividad, el alumno descarga el archivo con el enunciado de la tarea para realizarla. Una vez completado, el alumno adjunta el documento de la actividad. En caso de necesitar enviarla de nuevo, solo hace falta repetir el proceso. La plataforma, automáticamente, sustituirá el archivo anterior por el nuevo. Una vez completado el proceso, solo queda conocer el resultado. Para ello hay que ir a *Resultado de actividades.*
	Resultado de actividades: El alumno puede consultar los datos relacionados con su evaluación de la asignatura hasta el momento: calificación de las actividades y suma de las puntuaciones obtenidas hasta el momento, comentarios del profesor y del tutor personal, etc. y descargarse las correcciones.

Comunicación a través del aula virtual

El aula virtual dispone de sistemas de comunicación tanto síncrona como asíncrona que facilitan la interacción en tiempo real o diferido para sus usuarios: profesor, estudiante y tutor personal:



La comunicación entre los usuarios es un elemento fundamental que permite al alumnado la adquisición de competencias y resultados de aprendizaje de las diferentes materias y se realiza a través de las siguientes herramientas del aula virtual:

HERRAMIENTA	UTILIDAD
CLASES PRESENCIALES VIRTUALES	Permite a los alumnos ver y escuchar al docente a la vez que pueden interactuar con él y el resto de alumnos mediante chat y/o audio. El profesor dispone de una pizarra electrónica que los alumnos visualizan en tiempo real. También se permite al alumno **acceder a las grabaciones** de las sesiones presenciales virtuales de las asignaturas, de manera que puede ver la clase en diferido.
FORO	Son los profesores quiénes inician los foros. Existen diferentes tipos: - Foro *"Consúltale al profesor de la asignatura":* trata los aspectos generales de la asignatura. Los profesores y tutores personales lo consultan a diario. - Foros programados: tratan sobre un tema específico y son puntuables. Los profesores actuarán de moderadores, marcando las pautas de la discusión. - Foros no programados: se trata de foros no puntuables cuyo objetivo es centrar un aspecto de la asignatura que considere importante el profesor. En la programación semanal de la asignatura se especifica la fecha de inicio y fin de los foros, el tema sobre el que se va a debatir y la puntación máxima que se puede obtener por participar. Las intervenciones se pueden filtrar por título, leídas/no leídas, participante, ponente y fecha y pueden descargar los foros en formato EXCEL para guardarlos en su ordenador.
CORREO ELECTRÓNICO	A través del correo electrónico el estudiante se pone en contacto con el tutor personal, quien contesta todas las consultas de índole técnico o deriva el correo al profesor si se trata de una cuestión académica.
CHAT	Permite una comunicación instantánea entre los usuarios conectados ya sea de manera colectiva o privada. Fomenta el debate y consultas entre estudiantes. Además, a través de esta herramienta el profesor realiza tutorías en grupos reducidos u otras actividades.
ÚLTIMA HORA	Desde este medio el tutor personal pone en conocimiento del alumnado eventos de interés como pueden ser: foros, sesiones, documentación, festividades etc.

Además de las herramientas del aula virtual, también existe comunicación vía telefónica. Asiduamente el tutor personal se pone en contacto con los estudiantes y si es necesario y/o el estudiante lo solicita el profesor llamará al estudiante para resolverle cualquier cuestión.

Toda esta información se resume de manera esquemática en la tabla que a continuación se presenta:

Herramientas / Usuarios	Clase	Foro	Correo	Chat	Última hora	Vía telefónica
Profesor-tutor personal			X			X
Profesor-estudiante	X	X		X		X
Tutor personal -estudiante		X	X	X	X	X

Sesiones presenciales virtuales

En este apartado se explica, con mayor detalle el funcionamiento de las sesiones presenciales virtuales, que se considera el elemento pionero y diferenciador de esta Universidad. El aula virtual, permite a través de la televisión digital, crear un espacio donde profesor y estudiantes pueden interactuar del mismo modo que lo harían en un aula física. Además, el uso de chat en las sesiones virtuales fomenta la participación de los estudiantes.

Las características de estas aulas es que permiten realizar las siguientes acciones:

- El alumno ve y escucha al profesor a tiempo real.
- El alumno puede participar en cualquier momento a través de un chat integrado en la sesión virtual.
- Si para la adquisición de competencias lo requiere, el aula ofrece una gran variedad de posibilidades, entre las más utilizadas están:
    - Intervención de los estudiantes a través de audio y video, ya sea de manera grupal o individual.
    - Realización de talleres de informática.
    - Construcción de laboratorios virtuales.

Sistema de seguimiento y procedimientos para evitar abandonos

Primer contacto con el campus virtual

Cuando los estudiantes se enfrentan por primera vez a una herramienta como es una plataforma de formación en Internet pueden surgir muchas dudas de funcionamiento.

¿Cómo superamos este primer problema? A través de un periodo de adaptación previo al comienzo del curso denominado semana cero, en el que el alumno dispone de un aula de información general que le permite familiarizarse con el campus virtual.

En esta aula se explica mediante vídeos y textos el concepto de UNIR como universidad en Internet. Incluye la metodología empleada, orientación para el estudio y la planificación del trabajo personal y sistemas de evaluación. El estudiante tiene un primer contacto con el uso de foros y envío de tareas a través del aula virtual.

Además los alumnos reciben en su domicilio una guía de funcionamiento del aula virtual.

Seguimiento diario del alumnado

UNIR aplica un Plan de Acción Tutorial, que consiste en el acompañamiento y seguimiento del alumnado a lo largo del proceso educativo. Con ello se pretende lograr los siguientes objetivos:

- Favorecer la educación integral de los alumnos.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada alumno y recurrir a los apoyos o actividades adecuadas.
- Promover el esfuerzo individual y el trabajo en equipo.

Para llevar a cabo el plan de acción tutorial, UNIR cuenta con un grupo de tutores personales. **Es personal no docente** que tiene como función la guía y asesoramiento del estudiante durante el curso. Todos ellos están en posesión de títulos superiores en el ámbito de la pedagogía. Se trata de un sistema muy bien valorado por el alumnado, lo que se deduce de los resultados de las encuestas realizadas a los estudiantes.

A cada tutor personal se le asigna un grupo de alumnos para que realice su seguimiento. Para ello cuenta con la siguiente información:

- El acceso de cada usuario a los contenidos teóricos del curso además del tiempo de acceso.
- La utilización de las herramientas de comunicación del campus (chats, foros, grupos de discusión, etc.).
- Los resultados de los test y actividades enviadas a través del campus.

Estos datos le permiten conocer el nivel de asimilación de conocimientos y detectar las necesidades de cada estudiante para ofrecer la orientación adecuada.

Proceso para evitar abandonos

Cuando se detecta poca o nula participación de un estudiante en las actividades del curso, el tutor personal se pone en contacto con el estudiante. El objetivo es que se sienta «arropado» y motivado, y facilitar su integración y participación. De esta manera, se evitan buena parte de abandonos causados por desmotivación, sensación de aislamiento, pérdida de interés, etc.

5.1.5. Sistema de Evaluación de la Adquisición de las Competencias

La evaluación del Máster Universitario de Seguridad informática sigue estrictamente los criterios del RD 1125/2003.

Módulos teóricos
Las asignaturas de los módulos teóricos se evaluarán basándose en los siguientes criterios:

- **Evaluación continua** a través de las **actividades formativas** de la plataforma de e-learning de la UNIR.
- Una **prueba final** presencial de cada materia.

Evaluación Continua
La evaluación continua engloba la nota media de las asignaturas que componen el Módulo.

La calificación de cada una de las asignaturas se obtiene teniendo en cuenta:

- Estudio de material básico y lecturas complementarias.
- Realización de trabajos, proyectos, ejercicios y resolución de casos.
- Participación/implicación en Foros, Debates y otros medios colaborativos.
- Nota Media de los Test de Evaluación que componen las Unidades Didácticas de cada Asignatura.

El porcentaje variará en función del tipo de materia y de las actividades formativas previstas en cada una de ellas.

Examen presencial
Una vez concluido el estudio de cada asignatura de tipo teórico, se plantea una evaluación final para cada asignatura, certificada mediante la documentación fehaciente de identidad, que consiste en realizar un examen presencial.

La superación de las pruebas presenciales es imprescindible para que compute la nota de la evaluación continua.

Prácticas en empresas

La calificación de las Prácticas supone un 10 % sobre la nota global del Máster. Se llevará a cabo una evaluación continua durante la realización de las mismas tanto por el Tutor asignado

por la empresa como por el Profesor designado para orientar y asesorar al estudiante durante el desarrollo de las mismas.

El Tutor de Prácticas Externas en Empresa refleja por medio de un "Cuestionario de Evaluación", el desempeño logrado por el estudiante durante su periodo de prácticas atendiendo a una serie de criterios.

Criterios de Evaluación
• Grado de cumplimiento de los objetivos previstos. • Competencia técnica. • Responsabilidad e interés del estudiante. • Capacidad de aprendizaje. • Organización y planificación del trabajo. • Espíritu de colaboración y trabajo en equipo. • Habilidades sociales: relaciones con superiores, compañeros y clientes. • Asistencia y puntualidad. • Adaptabilidad, motivación, iniciativa y creatividad.

La puntuación máxima a obtener en el cuestionario son 100 puntos. El Profesor evalúa el cumplimiento de los objetivos de las Prácticas en base a la valoración obtenida en el "Cuestionario de Evaluación", pudiendo incrementar la calificación final en 5 puntos a tenor de la participación e implicación del estudiante en las distintas acciones formativas: uso del servicio de Tutorías, Foro y Chat.

Trabajo Fin de Máster

La evaluación del Trabajo Fin de Máster se realiza atendiendo a tres aspectos:

Criterios de Evaluación	
Organización	Atender a la estructura y organización del Trabajo Fin de Máster.
Exposición	Valorar la claridad en la exposición, así como la redacción y la capacidad de síntesis, análisis y respuesta.
Contenido	Se tomará como referencia la memoria del Trabajo y todo el resto de la documentación técnica de apoyo para comprobar la validez de la exposición. Se valorará la capacidad de síntesis y la fácil lectura del mismo. También se valorará la corrección y claridad de la expresión, tanto escrita como gráfica

Sistema de Calificaciones

La nota final del Máster engloba los resultados obtenidos por el estudiante en cada una de las Asignaturas y las Prácticas y el Trabajo Fin de Máster.

La calificación final se establece en el artículo 5 del Real Decreto 1125/2003, de 5 de septiembre, en función de una escala numérica de 0 a 10:

0 - 4,9: Suspenso (SS).

5,0 - 6,9: Aprobado (AP).

7,0 - 8,9: Notable (NT).

9,0 - 10: Sobresaliente (SB).

5.1.5. Descripción detallada de las actividades formativas

Sesiones presenciales virtuales

Para cada asignatura, la UNIR podrá realizar tantas clases presenciales virtuales se necesiten, según necesidades de la materia y el contexto. Las clases se prevén de 45 minutos y los alumnos podrán interaccionar con el profesor a través del chat. En cada sesión el profesor titular contará con el apoyo de un profesor ayudante. La UNIR dispone de un Servicio técnico para solventar cualquier incidencia que pueda surgir durante la sesión. La programación de los horarios de las clases está a disposición de los alumnos en el Aula virtual de cada asignatura con la suficiente antelación.

La propia aplicación que se utiliza para estas sesiones genera un informe de asistencia de los participantes, donde queda registrada la hora de entrada y de salida. Este informe se envía por correo electrónico a tutores y profesores que lo incluyen en la ficha del alumno.

Estudio de material básico y lectura de material complementario

Muestra el contenido teórico que se precisa para el aprovechamiento de la clase. La formación que impartimos es eminentemente práctica, por tanto las lecturas deben estar bien enfocadas, han de ir al núcleo del tema, eliminando todo lo accesorio. Aportan lo fundamental para que el alumno se enfrente al caso sin necesidad de consultar manuales, etc. Esto no obsta para que se ofrezca, cuando sea conveniente, bibliografía de consulta.

Realización de trabajos, ejercicios y resolución de casos prácticos

En el máster universitario de seguridad informática de la UNIR, está prevista la realización por parte de los alumnos de diferentes tipos de ejercicios y actividades para facilitar la adquisición de las competencias.

Está comprobado (por la experiencia de numerosas universidades) que el estudio de casos es una herramienta efectiva para formar a estudiantes en la seguridad informática.

Un caso es la descripción de una situación real acontecida en un sistema concreto (sea informático o no), en un momento determinado del tiempo o en una sucesión de ellos. Como tal descripción, contiene una información (estructural, técnica, administrativa, humana, circunstancial...) que se transmite a lo largo del texto.

Dicha información puede ser o no relevante, a efectos que el caso plantea, y, al igual que sucede en la vida real, limitada. Hay que observar, que la cualidad pedagógica del caso no reside en la información que contiene.

Un caso puede contener más de un problema y es tarea del alumno tanto detectarlos como priorizarlos.

En un entorno virtual, los casos se discuten a través de la herramienta Foro incorporada en el aula virtual. El caso es presentado a todos los alumnos en el programa de temas, y el alumno a través de un ejercicio realiza una reflexión para encontrar la solución que, posteriormente, se debatirá en el foro. Después del trabajo individual, el foro permite debatir, ampliar y contrastar la posición personal con la de otros participantes del curso.

El tutor personal evalúa la implicación del estudiante teniendo en cuenta por un lado, el uso de los sistemas de comunicación bidireccional de la Plataforma, y por el otro, la resolución de los Casos Prácticos que engloban las distintas Asignaturas.

	Criterios de Evaluación
Sistemas de Comunicación Bidireccional	Medios Colaborativos: Se pone a disposición de los estudiantes las siguientes herramientas de comunicación: ○ Chat. ○ Foro. ○ Debate. Se plantea como mínimo un debate por Módulo. Así mismo, por cada Asignatura se establecerá en el foro un tema relacionado con la misma. Los criterios de evaluación se basan en comprobar la intervención en los mismos de forma activa exponiendo sus opiniones, consultas, conclusiones, etc. Tutorías: Se basan en constatar el uso de este servicio por parte del estudiante, teniendo en cuenta el apoyo tutorial continuo que se le ofrece.
Elaboración de Casos Prácticos	Se basan en evidenciar la aplicación de los conocimientos teóricos adquiridos a lo largo del temario, aportando y fundamentando soluciones adecuadas a las cuestiones

	planteadas en los mismos.

Test de autoevaluación

Cada Asignatura se estructura en Unidades. Cada Unidad contiene un Test de Evaluación compuesto de cinco preguntas de respuesta múltiple. Una vez realizado el Test, queda grabado automáticamente en la base de datos de la Plataforma. La Plataforma eLearning informa de manera automática de la nota media global de los Test, por Asignatura.

La realización de los Test es obligatoria. Para superarlos, se debe obtener como mínimo, una media global del 60% de preguntas acertadas.

5.1.6. Sistemas de evaluación de la adquisición de competencias

La naturaleza virtual de las enseñanzas de la UNIR, hace necesaria la realización de una prueba presencial (certificada mediante documentación fehaciente de identidad) que supone un 60% de la evaluación final. Esta tiene un carácter básico y solo cuando se supera la nota establecida para el aprobado, puede completarse la calificación con los procedimientos específicos de evaluación continua que establezca cada materia. Por tanto el peso de las pruebas que constituyen la evaluación continua (evaluación progresiva) no podrá ser superior a un 40%.

Los instrumentos de evaluación en un entorno on-line permiten la realización de pruebas variadas. En términos generales puede considerarse que las señaladas en el Cuadro siguiente son las más importantes y significativas. Indudablemente en función de la naturaleza de cada materia, tendrán un peso específico diverso cada una de ellas. Los ejercicios serán corregidos posteriormente por los correspondientes profesores de cada materia

Actividades formativas y su relación con ECTS

La distribución de estas actividades formativas responde a un criterio de dedicación del alumno a cada una de las actividades que le permitirán aprobar satisfactoriamente las asignaturas del Máster. En este sentido, el mayor porcentaje se agrupa en el estudio del material básico y complementario que el alumno debe llevar a cabo para la evaluación final y por supuesto, para el correcto desarrollo de otras actividades contempladas en la evaluación continua. El resto de las actividades formativas tienen un porcentaje de dedicación adecuado para la superación de las tareas que se plantearán en cada una de las materias.

En el caso de las asignaturas de contenido eminentemente práctico, se dará más importancia a las tareas que impliquen realización de ejercicios, trabajos individuales, resolución de casos, actividades colaborativas, etc.

Es importante destacar que dada la modalidad virtual de las presentes enseñanzas, para que los estudiantes adquieran las competencias establecidas en el Máster, a lo largo del Módulo se programan varias actividades formativas que son comunes a todas ellas ya que se realizan en la misma plataforma virtual de la UNIR. No obstante sí se incluyen algunas variaciones tal como se especifica en la descripción detallada de los módulos.

El porcentaje de cada una de las actividades varía en función de la naturaleza específica de la materia que establece las horas de dedicación del alumno a cada una de las actividades. Las materias más teóricas tendrán más horas de estudio de material básico que alguna de las materias que requiere más ejercicios prácticos y clases presenciales virtuales. (**5.4, Contenido específico de cada módulo**).

En la Universidad Internacional de La Rioja, se han considerado 30 horas por ECTS, siguiendo la normativa del RD 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional. (BOE 18/09/2003).

A continuación se presenta la distribución porcentual de las actividades formativas en función del número de ECTS de las asignaturas en un modelo general de tres créditos.

Cada clase se compone de un conjunto de elementos y actividades que aseguran la reflexión y el progreso medible semana a semana. A continuación se muestra **un ejemplo** de cómo podría ser la composición de una asignatura de 3 créditos ECTS, extrapolable a cualquier otra situación:

Actividades formativas	ECTS	Porcentaje	Horas
Sesiones presenciales virtuales	0,10	3,33%	3,00
Estudio de material básico	1,20	40,00%	36,00
Lectura de material complementario	0,75	25,00%	22,50
Realización de casos prácticos	0,28	9,20%	8,28
Realización de test y exámenes	0,17	5,80%	5,22
Trabajo colaborativo (foros, chats…)	0,25	8,33%	7,50
Tutorías individuales y grupales	0,25	8,33%	7,50
	3,00	100,00%	90,00

5.2. Planificación y gestión de la movilidad de los estudiantes propios y de acogida

El perfil del estudiante de UNIR –persona adulta que, por lo general, desarrolla un trabajo profesional– pensamos que no impide la realización de acciones de movilidad, aunque se encaucen o se realicen de manera adecuada a las peculiares circunstancias de los estudiantes.

Una posibilidad es la realización de intercambios con presencia física en universidades nacionales o del extranjero de manera presencial en conformidad con los programas Erasmus y Leonardo (enfocado a la realización de prácticas en el extranjero).

En cualquier caso el programa de movilidad que mejor se adaptará al perfil de nuestros alumnos y también al propio carácter de la UNIR es el programa Gundtvig para la educación de adultos.

En segundo lugar se iniciarán las gestiones de adhesión a los programas de intercambio cultural, en concreto entre los que ISEP o ANUIES, sin descartar posteriormente otros.

Aunque la universidad ha comenzado a gestionar acuerdos para la puesta en marcha de los programas de movilidad más difundidos (Erasmus, Séneca) el previsible carácter de nuestros estudiantes pensamos que no utilizará mayoritariamente estos recursos.

Entendemos que la movilidad interuniversitaria constituye un factor relevante en la formación de nuestros estudiantes (modo práctico de apertura a otras culturas a otros modos de vida, a otras formas de entender la educación y el ejercicio profesional, etc), por lo tanto se potenciará la movilidad virtual entre universidades on-line ya que ofrece un gran número de posibilidades para acceder a cursos y programas que permiten la comunicación entre docentes y estudiantes a través de las TIC.

El objetivo a corto plazo es establecer acuerdos con otras universidades de manera que nuestros alumnos podrán cursar determinadas materias en universidades extranjeras con oferta de enseñanza virtual.

A este respecto, suscribimos la experiencia del proyecto NetACTVE (AISAD-EADTU: Credit Transfer in Virtual and Distance Education) enmarcado en el programa Erasmus Mundus de la Unión Europea. La Universidad Nacional de Educación a Distancia es quien coordina este proyecto a través de la Cátedra UNESCO de Educación a distancia (CUED), http://www.uned.es/cued

Asimismo, la Universitat Oberta de Cataluña ha sido pionera en este sentido con la puesta en marcha de un programa de movilidad virtual en colaboración con la universidad de Guadalajara (México) para estudiantes de postgrado en tecnologías de aprendizaje. (www.uoc.es).

5.2.1. Gestión de la movilidad

La información y gestión sobre (y de) los programas de movilidad e intercambio, la realizará, de manera centralizada para toda la Universidad, la Unidad de Relaciones Internacionales.

La UNIR centraliza la movilidad de estudiantes y profesores en el departamento de Relaciones Institucionales, que se encargará de la confección y tramitación de los learning agreements de manera que se garantice no sólo el reconocimiento de los ECTS realizados en la universidad de acogida de nuestros estudiantes, sino también su congruencia desde el punto de vista formativo.

La web de la UNIR en materia de movilidad e intercambio será una herramienta fundamental, no sólo por la información y los contactos con las universidades asociadas, sino también para su gestión (solicitud de las becas, propuesta de “asignaturas en movilidad”, validación del learning agreement y reconocimiento académico).

En cuanto al sistema de reconocimiento de créditos ECTS nos remitimos a lo expuesto en elapartado 4.4. (Transferencia y reconocimiento de créditos) explicitando que la Facultad dispondrá de todos los elementos de gestión necesarios para garantizar que en el expediente académico de cada alumno figure la descripción cuantitativa y cualitativa de todos los créditos ECTS cursados en otra universidad a través de un programa de movilidad.

5.3 Descripción detallada de los módulos.

MÓDULO I

ASPECTOS LEGALES Y MARCO JURÍDICO
Número de créditos ECTS: 9 ECTS
Unidad temporal: Tres asignaturas cuatrimestrales obligatorias
Carácter: Obligatorio

Descripción de las materias o asignaturas			
Denominación de la asignatura	**ECTS**	**Carácter**	**Cuatrimestre**
Aspectos Legales y Regulatorios	3	Obligatoria	1
Análisis de Riesgos Legales	3	Obligatoria	2
Delitos Informáticos	3	Obligatoria	2

Resultados de aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta comprensión de los aspectos relacionados con la legislación reguladora y su ámbito de aplicación, la protección de datos, los delitos informáticos y los análisis de riesgos legales.

Contenido de módulo/materia.
Aspectos Legales y Regulatorios. Estudio genérico del marco legal vigente en materia de bienes y servicios informáticos, centrado en aspectos clave tales como propiedad industrial e intelectual, protección de datos o regulación de mercados. **Análisis de Riesgos Legales**. Metodología para una gestión proactiva de los riesgos legales inherentes al desarrollo, implantación y despliegue de actividad informática, con especial atención a la industria del software, especialmente relevante en esta materia. **Delitos Informáticos**. Estudio de la legislación penal en materia de infracciones cuyo medio de comisión u objeto de la misma sean bienes o servicios informáticos, de tal manera que se

permita su identificación, su denuncia y correspondiente seguimiento procesal.

El módulo da una visión de conjunto sobre los aspectos legales y el marco jurídico institucional en relación a la seguridad informática. También se estudia cómo analizar y recomendar diversas estrategias en dicho ámbito.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE1, CE2, CE4, CE7, CE15, CE16, CE19, CE27,

Actividades formativas	HORAS
Clases, conferencias, técnicas expositivas	95
Tutoría individual (atención personal del profesor o dinamizador)	9
Realización de pruebas de seguimiento	9
Participación en foros y otros medios colaborativos	22
Elaboración de trabajos	38
Lecturas complementarias dirigidas	16
Estudio personal	81

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	10
Realización de trabajos, proyectos y casos	0	20
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

MÓDULO II

AUDITORÍA Y GESTIÓN DE SEGURIDAD
Número de créditos ECTS: 9 ECTS
Unidad temporal: Tres asignaturas cuatrimestrales obligatorias.
Carácter Obligatorio

Descripción de las materias o asignaturas			
Denominación de la asignatura	**ECTS**	**Carácter**	**Cuatrimestre**
Gestión de la Seguridad	3	Obligatoria	1
Análisis de Vulnerabilidades	3	Obligatoria	1
Auditoría de la Seguridad	3	Obligatoria	2

Resultados de aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta comprensión de los aspectos relacionados con el análisis de riesgos de seguridad, los mecanismos de protección, el diseño de planes de seguridad, los SGSI, y la auditoría de sistemas en entornos sensibles.

Contenido de módulo/materia. Observaciones
Gestión de la Seguridad. Identificación de los problemas relacionados con la gestión de sistemas informáticos de seguridad, diseño de planes de auditoría, implantación de SGSI, grado de implantación de las normativas de seguridad, diseño de planes de seguridad proactivos, desarrollo de políticas de seguridad,despliegue de políticas de seguridad, seguimiento de políticas de seguridad, autenticación, control de accesos, pruebas de conocimiento nulo. **Análisis de Vulnerabilidades.** Estudio de los fallos de seguridad, gestión de memoria, mecanismos de protección de memoria, espacio de usuario y de sistema, exploits locales, exploits remotos, alteraciones básicas, explotaciones de memoria, shellcodes, escalada de privilegios, integer overflow, buffer overflow, heap overflow, inyección de código, protección de ejecutables. **Auditoría de la Seguridad**. Planes de auditoría, auditoría técnica y de certificación, tipos de auditorías, auditorías de SGSI, aspectos documentales, metodologías de auditoría, ejecución de auditorías, herramientas de auditoría, ISO 27000, estudio comparativo de auditorías.

Este módulo se centra en el estudio de los Sistemas de Gestión de la Seguridad que permitirán diseñar e implementar medidas y planes para mejorar la seguridad informática en una organización. Del mismo modo, se estudiarán las vulnerabilidades más utilizadas para desestabilizar sistemas informáticos permitiendo interrumpir su funcionamiento e incluso tomar control sobre ellos de forma no autorizada. El estudio de estos dos temas se complementará con la auditoría de seguridad, que servirá para comprender los procesos más avanzados utilizados en dicha disciplina.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE1, CE2, CE3, CE8, CE9, CE10, CE11, CE12, CE21, CE24, CE25

Actividades Formativas	Horas
Clases, conferencias, técnicas expositivas	81
Tutoría individual (atención personal del profesor)	9
Realización de pruebas de seguimiento	9
Participación en foros y otros medios colaborativos	22
Elaboración de trabajos	51
Lecturas complementarias dirigidas	16
Estudio personal	82

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	10
Realización de trabajos, proyectos y casos	0	20
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

MÓDULO III

TÉCNICAS AVANZADAS DE SEGURIDAD
Número de créditos ECTS: 15 ECTS
Unidad temporal: Tres asignaturas cuatrimestrales obligatorias.
Carácter: Obligatorio

Descripción de las materias o asignaturas			
Denominación de la asignatura	**ECTS**	**Carácter**	**Cuatrimestre**
Seguridad en Redes	5	Obligatoria	1
Seguridad en Sistemas Operativos	5	Obligatoria	1
Criptografía y Mecanismos de Seguridad	5	Obligatoria	1

Resultados de Aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta comprensión de los aspectos relacionados con las distintas herramientas de seguridad, los mecanismos de seguridad, los informes técnicos de seguridad, los mecanismos criptográficos y los elementos involucrados en un entorno de seguridad.

Contenido de módulo/materia. Observaciones
Seguridad en Redes. Aspectos avanzados sobre redes TCP/IP, seguridad en redes, ataques contra redes, denegaciones de servicio, analizadores de tráfico, zonas desmilitarizadas, características avanzadas de los sistemas de cortafuegos, redes privadas virtuales, sistemas remotos seguros, TLS/SSL, IPSec, sistemas de detección de intrusos, detección de ataques distribuidos, medidas de protección proactivas, escaneo de vulnerabilidades en redes. **Seguridad en Sistemas Operativos.** Administración de servidores, estudio avanzado de servicios, estudio avanzado de sistemas de memoria, mecanismos de protección de memoria, sistemas de protección del espacio de núcleo, monitorización de procesos, sistemas de detección de intrusiones en sistemas de ficheros, cuotas de disco, monitorización de usuarios, gestión de permisos, políticas de sistemas operativos en organizaciones, administración de discos, denegaciones de servicio. **Criptografía y Mecanismos de Seguridad.** Fundamentos matemáticos avanzados sobre sistemas criptográficos, criptografía clásica, criptografía de clave secreta, criptografía de clave

pública, sistemas criptográficos híbridos, funciones de resumen criptográfico hash, funciones de resumen criptográfico HMAC, autenticación de mensajes, firma digital, protocolos criptográficos seguros, transmisión segura de información, criptoanálisis, ataques de diccionario, ataques de fuerza bruta.

El módulo da una visión de conjunto sobre los aspectos más avanzados de la seguridad en redes, tratando temas que resultarán decisivos a la hora de proteger correctamente una red desde el punto de vista de la seguridad informática. Igualmente, se aprenderán las técnicas más avanzadas de seguridad en los distintos sistemas operativos y los sistemas criptográficos más modernos y seguros,_que sustentan la arquitectura de seguridad de todos los sistemas críticos en Internet.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE5, CE6, CE9, CE10, CE13, CE15, CE17, CE18, CE21, CE22, CE23

Actividades Formativas	Horas
Clases, conferencias, técnicas expositivas	121
Tutoría individual (atención personal del profesor)	16
Realización de pruebas de seguimiento	16
Participación en foros y otros medios colaborativos	36
Elaboración de trabajos	99
Lecturas complementarias dirigidas	40
Estudio personal	122

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	10
Realización de trabajos, proyectos y casos	0	20
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

MÓDULO IV

SEGURIDAD EN LAS APLIACIONES Y ANÁLISIS FORENSE
Número de créditos ECTS:13 ECTS
Unidad temporal: Tres asignaturas cuatrimestrales obligatorias.
Carácter Obligatorio

Descripción de las materias o asignaturas			
Denominación de la asignatura	**ECTS**	**Carácter**	**Cuatrimestre**
Análisis Forense	3	Obligatoria	1
Seguridad en Aplicaciones online y Bases de Datos	5	Obligatoria	2
Seguridad en el Software	5	Obligatoria	2

Resultados de Aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta comprensión de los aspectos relacionados con el análisis de entornos atacados, la determinación y reproducción de vectores de ataque, la confidencialidad en bases de datos, la reducción del impacto de ataques en sistemas y la recuperación ante desastres y ataques.

Contenido de módulo/materia. Observaciones
Análisis Forense. Recuperación de información, adquisición de datos, metodología de análisis forense, investigación de datos, documentación de procesos, herramientas de recuperación de información, medidas reactivas, protección ante desastres, redundancia de sistemas de ficheros, sistemas de ficheros avanzados. **Seguridad en Aplicaciones online y Bases de Datos.** Principales arquitecturas de bases de datos, inyección SQL, inyección SQL a ciegas, desbordamiento de memoria en bases de datos, Cross-site scripting, Cross-site request forgery, form tampering, clickjacking, remote file inclusión, escalada de directorios, escalada transversal de directorios, ataques a ciegas, acceso remoto a sistemas, protección de servidores web, medidas de seguridad en servidores, ataques a sistemas desplegados sobre infraestructuras de red, autenticación, control de acceso. **Seguridad en el Software.** Sistemas de memoria, tipos de vulnerabilidades, fortificación de aplicaciones, shellcodes, explotación de vulnerabilidades, prevención de desbordamientos de

memoria, prevención de ataques basados en cadenas, condiciones de carrera, inducción de fallos, política de mínimos privilegios, puertas traseras, rootkits, malware, autenticación, control de acceso.

Este módulo trata otro de los pilares de la seguridad informática. La seguridad de las aplicaciones que se están ejecutando en una infraestructura informática. Los errores en las aplicaciones online son un punto de entrada muy atractivo para los posibles atacantes y es necesario saber cuáles son las técnicas más avanzadas para su protección. Por otra parte, el análisis forense permite recuperar la información que se ha producido durante un acceso no autorizado o durante un fallo total del sistema para descubrir las causas que lo propiciaron, y el responsable de dicho incidente.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE5, CE8, CE9, CE14, CE19, CE20, CE22, CE24, CE26, CE27

Tipo de actividad del estudiante	Horas
Clases, conferencias, técnicas expositivas	117
Tutoría individual (atención personal del profesor)	14
Realización de pruebas de seguimiento	14
Participación en foros y otros medios colaborativos	30
Elaboración de trabajos	86
Lecturas complementarias dirigidas	20
Estudio personal	109

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	10
Realización de trabajos, proyectos y casos	0	20
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

MÓDULO IV

PRÁCTICAS EN EMPRESA
Número de créditos ECTS: 6 ECTS
Unidad temporal: Una materia semestral obligatoria
Carácter: Obligatorio

Descripción de las materias			
Denominación de la materia	**Créditos ECTS**	**Carácter**	**Cuatrimestre**
Prácticas en empresas	6	obligatoria	2

Resultados de Aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de módulos del plan de estudios.

Contenidos de módulo/materia y observaciones
Realización labores básicas de seguridad informática, tuteladas por un profesional que supervisa el correcto desarrollo de las tareas que se le asignen y mantiene las relaciones pertinentes con el tutor designado por la UNIR quienes, en régimen de colaboración, velan por la óptima formación del alumno. Los detalles de las tareas a desarrollar por el alumno durante la estancia en la empresa serán fijadas por el Tutor de Prácticas Externas y se adaptarán a las peculiaridades propias de cada centro.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE1-CE27

Tipo de actividad del estudiante	HORAS	PRESENCIALIDAD
Tutoría individual	2	100%
Prácticas en empresa	150	100%
Elaboración del trabajo	28	0%
TOTAL	180	

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	15
Realización de trabajos, proyectos y casos	0	15
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

EVALUACIÓN PRÁCTICAS EN EMPRESA	(%)
Cuestionario de Valoración	
Grado de cumplimiento de los objetivos previstos	10
Competencia técnica.	10
Responsabilidad e interés del estudiante.	10
Capacidad de aprendizaje.	10
Organización y planificación del trabajo.	10
Espíritu de colaboración y trabajo en equipo.	10
Habilidades sociales: relaciones con superiores, compañeros y clientes.	10
Asistencia y puntualidad.	10
Adaptabilidad, motivación, iniciativa y creatividad.	10
Total	**90**
Participación/implicación en Foros, Debates y otros medios colaborativos.	5
Realización de consultas a Través de las Tutorías al Profesor Tutor	5
TOTAL	**100**

MÓDULO VI

TRABAJO FIN DE MÁSTER
Número de créditos ECTS: 8 ECTS
Unidad temporal: Una materia~~s~~ semestral~~es~~ obligatoria~~s~~
Carácter: Obligatorio

Descripción de las materias			
Denominación de la materia	**Créditos ECTS**	**Carácter**	**Cuatrimestre**
Trabajo Fin de Máster	8	Obligatoria	2

Resultados de Aprendizaje
Los resultados del aprendizaje esperados para este módulo pasan por la correcta aplicación de los conocimientos adquiridos durante el estudio del resto de módulos del plan de estudios.

Contenidos de módulo/materia y observaciones

Trabajo Fin de Máster

Se realiza individualmente bajo del asesoramiento y orientación del Profesor-Tutor para la elaboración del mismo.

Elaboración, diseño y defensa de un caso teórico o práctico sobre seguridad informática, donde el estudiante deberá demostrar sus habilidades y conocimientos en relación a uno o varios de los siguientes aspectos:

- Análisis exhaustivo de sistemas informáticos complejos, en los que la seguridad resulte un elemento crítico para su correcto funcionamiento.
- Identificación de las potenciales amenazas, debilidades y elementos inseguros, tanto externos como internos. Estos pueden pertenecer tanto al plano técnico, como administrativo, legal, o una combinación de los mismos.
- Realización de un análisis detallado de las amenazas, debilidades y elementos inseguros; para la posterior realización de un informe con posibles soluciones, así como con recomendaciones para mejorar el sistema desde el punto de vista de la seguridad informática.
- Presentación del plan de implantación para las soluciones anteriormente descritas.

Competencias Básicas y Generales	Competencias Transversales	Competencias Específicas
CB6 – CB10 CG1 – CG9	CT1-CT5	CE1-CE27

Tipo de actividad del estudiante	HORAS
Sesión inicial de presentación	2
Lectura del material complementario	10
Seminarios	10
Tutoría individual	8
Sesiones grupales	5
Elaboración del TFM	203
Defensa del TFM	2
TOTAL	240

Sistemas de evaluación y calificación	Ponderación Mínima	Ponderación Máxima
Participación en foros y otros medios participativos	0	15
Realización de trabajos, proyectos y casos	0	15
Lecturas Complementarias	0	10
Prueba de evaluación final	0	60

Evaluación	(%)
Organización	
Estructura.	20
Redacción de cada uno de los capítulos del Trabajo.	20
Total	40
Exposición	
Claridad en la exposición.	15

Forma de expresión, capacidad de síntesis, análisis y respuesta.	15
Total	**30**
Contenido	
Capacidad de síntesis y fácil lectura del mismo.	20
Corrección y claridad de la expresión, tanto escrita como gráfica.	20
Total	**40**
TOTAL	**100**

6. PERSONAL ACADÉMICO

6.1. Profesorado

Como establece el RD 1393/2007, el equipo docente es experto en los contenidos del Máster y tiene experiencia académica, profesional o en ambos campos.

La UNIR cuenta con los recursos humanos necesarios para llevar a cabo el plan de estudios propuesto y cumplir así los requisitos definidos en el Anexo I del RD 1393/2007 en cuanto a personal académico disponible. Asimismo, en cuanto a descripción y funciones del profesorado la UNIR sigue lo establecido en el V Convenio colectivo nacional de Universidades Privadas *(Resolución de 27 de diciembre de 2005).*

6.1.1 Proceso de selección del profesorado

En la selección de profesorado se respetará lo dispuesto en las siguientes leyes:

- LEY ORGÁNICA 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. BOE núm. 71 Viernes 23 marzo 2007.
- LEY 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. BOE núm. 289 Miércoles 3 diciembre 2003

En la formulación serán criterios determinantes los de:

a) el mérito y capacidad de los candidatos en las respectivas asignaturas;

b) la experiencia personal de los candidatos en la enseñanza a distancia.

6.1.2. Previsión Profesorado

El Personal docente e investigador, está compuesto por profesores doctores y licenciados en Ingeniería Informática con amplia experiencia docente. En algunos casos se contará con expertos con amplia experiencia en temas de seguridad e integridad de sistemas informáticos.

El equipo docente está formado por: 19 profesores doctores con amplia experiencia profesional en el ámbito de la docencia, 3 profesores con experiencia en empresas tecnológicas relacionadas con la seguridad, 2 profesores que trabajan en empresas de normalización y certificación (AENOR) y 1 miembro de las fuerzas de seguridad del estado dedicado a la detección de delitos informáticos. Todos profesores, además de los doctores, son licenciados universitarios o ingenieros.

La estructura docente del Máster está constituida por un equipo con las competencias necesarias para llevar a cabo la organización y desarrollo del Máster.

Composición del Equipo Docente, en Función de su Categoría Académica	
% Profesores Doctores	75%

% Profesores no Doctores	25%
% Profesor agregado	60%
% Profesor adjunto	15%
% Profesor asociado	25%

El conjunto de profesores, por su formación y experiencia, cubre todas las competencias necesarias para llevar a cabo la organización e impartición del Máster, representando uno o varios de los aspectos definidos en los perfiles del profesorado.

Título	Experiencia docente, profesional e investigadora	Líneas de Investigación y realizaciones	Acreditado	Materias en los que imparte docencia	Dedicación al Máster
Doctor Ingeniero en Informático	Experto en asesoría jurídica especialistas y en Derecho de las TIC. Miembro del Grupo de Asesores Legales en Tecnologías de la Información	Derecho Informático. Informática para Juristas	SI	Aspectos Legales y Regulatorios TFM	40 %
Ingeniero en Informática	Más de 15 años de experiencia en el área del Peritaje informático y la auditoria forense. Miembro de AENOR	Gobierno de la Seguridad de la Información	No procede	Análisis Forense	40%

Ingeniero en Informática	Experto en el área de delitos informáticos a nivel internacional. Miembro proactivo de diversas organizaciones que velan por la seguridad nacional.	Seguridad en los Sistemas de Información	No Procede	Delitos Informáticos Practicas Externas	40%
Ingeniero en Informática	Más de 30 años de experiencia en el área del gobierno informático y la auditoria informática. Subdirector de AENOR. CISA, CISM, ITIL Experto. Más de 30 años de experiencia en enseñanza universitaria.	Gobierno de las Tecnologías de la Información. Auditoría Informática.	No Procede	Auditoria de Seguridad Practicas Externas	40%

Doctor Ingeniero en Informático	Profesor de Universidad en departamento de informática. Amplia experiencia profesional en consultoría y asesoría de Seguridad de la información y las comunicaciones	Seguridad en las Tecnologías de la Información y las Comunicaciones Gestión de protocolos de seguridad en Internet, el Análisis y Gestión de los Riesgos Informáticos y la protección de sistemas de información distribuidos.	No	Criptografía y Mecanismos de Seguridad TFM	50%
Doctor en Ingeniería Informática	Profesor en programas de Máster del Departamento de Ciencias de la Computación en diversas universidades. Experiencia profesional de 9 años en el sector de las TIC. Publicación de artículos en revistas internacionales y participación en congresos.	Ingeniería del Software y en especial en gestión de riesgos legales y planificación y gestión de proyectos	No	Análisis de Riesgos Legales Practicas Externas TFM	60%

Doctorando Ingeniero en Informática Máster sobre Redes Comunicación.	Amplia experiencia docente. Carrera profesional en el ámbito del Ministerio de Defensa. Jefe del área de Comunicaciones e Informática del Grupo Central de Mando y Control del Ejército del Aire.	Análisis de Seguridad Automática en Aplicaciones Web	No procede	Seguridad en Aplicaciones Online TFM	60%
Doctor Ingeniero en Informática.	Amplia experiencia docente en el ámbito universitario. Amplia experiencia en la investigación de fraudes relacionados con la informática.	Experto en análisis forense	SI	Gestión de la Seguridad TFM	60%
Doctor Ingeniero en Informática	Experto en gestión de los protocolos de seguridad en Internet, la seguridad del protocolo IPv6 y la validación de protocolos de seguridad.	Seguridad en Tecnologías de la Información	SI	Seguridad en Redes. TFM	60%

Ingeniero Técnico en Informática de Gestión	Profesor desde el año 2006 en cursos sobre Seguridad y Auditoría Informática. Experiencia profesional en administración de sistemas gestión de riesgos de sistemas de información. Gestiona proyectos relacionados con la Auditoría de seguridad y de Vulnerabilidades.	Seguridad Digital e Internet del Futuro	No procede	Seguridad en Sistemas Operativos Análisis de Vulnerabilidades	100%
Ingeniero en Electrónica, Armamento y Técnico de Telecomunicaciones, Licenciado en Físicas. **Máster en Sistemas de Comunicación e Información para la Seguridad y Defensa**	Ha realizado labores de enseñanza como profesor asociado. Ha sido oficial responsable de seguridad TIC de la Unidad Militar de Emergencias, Es representante español en el grupo de trabajo "IA/Cyber Defence Research Framework" de la Agencia de Investigación de la OTAN (STO).	Análisis de malware. Director Técnico de los Programas de Telecomunicaciones y Sistemas de Información de la UME eI+D Guerra Electrónica Táctica.	No procede	Seguridad en el Software	40%

Doctor Ingeniero en Informática	Con diez años de experiencia docente universitaria y con tres años de experiencia investigadora Postdoctoral, y múltiples publicaciones JCR	Simulación, Inteligencia Artificial y Dirección de Proyectos	SI	Atención TFM	30%
Doctor Ingeniero en Informática	Con veinte años de experiencia docente universitaria y con tres años de experiencia investigadora Postdoctoral, y múltiples publicaciones JCR	Seguridad de la información.	SI	Atención TFM	30%
Doctor Ingeniero en Informática	Experto en gestión universitaria con más de 100 TFM dirigidos hasta la fecha. Dirección de múltiples tesis doctorales y trabajos en proyectos de investigación	Usabilidad y Experiencia de Usuario en entornos web seguros	SI	Atención TFM	30%
Doctor Ingeniero en Informática	Director de proyectos de investigación competitivos y vinculados a la empresa en líneas de seguridad informática.	Sistemas de Gestión de Seguridad Perimetral	NO	Atención TFM	30%

Doctor Ingeniero en Informática	Director de programas académicos con 10 tesis doctorales dirigidas y más de 60 TFM.	Dirección de Proyectos TIC y Gobierno de TI	SI	Atención TFM	30%
Doctor Ingeniero en Informática	Con siete años de experiencia docente universitaria y con tres años de experiencia investigadora Postdoctoral, y múltiples publicaciones JCR	Sistemas Industriales y Gestión de la Seguridad	SI	Atención TFM	30%
Doctor Ingeniero en Informática	Director de proyectos de investigación competitivos y vinculados a la empresa en líneas de seguridad informática y GIS. Miembro de la Academia militar.	Seguridad en Sistemas de Información Geográfica	SI	Atención TFM	20%
Doctor Ingeniero en Informática	Experto en gestión universitaria con más de 50 TFM dirigidos hasta la fecha. Dirección de múltiples tesis doctorales y trabajos en proyectos de investigación	Seguridad en redes sociales.	SI	Atención TFM	30%

Doctor Ingeniero en Informática	Director de la Revista IJIMAI. Doctor en AI. Director habitual de TFM y TD.	Algoritmos de Inteligencia Artificial para garantizar la Seguridad en SI	SI	Atención TFM	20%
Doctor Ingeniero en Informática	Experto en la Dirección de Proyectos Informáticos. PMP. Director de Tesis de Fin de Máster en varias Universidades.	Director de Proyectos Informáticos.	NO	Atención TFM	20%
Doctor Ingeniero en Informática	Con cuatro años de experiencia docente universitaria y con tres años de experiencia investigadora. Varias publicaciones JCR.	Seguridad en Portales Web. Seguridad en el menor.	SI	Atención TFM	20%
Doctor Ingeniero en Informática	Director de programas académicos con 10 tesis doctorales dirigidas y más de 60 TFM.	Director de Proyectos Informáticos	SI	Atención TFM	20%

Doctor Ingeniero en Informática	Experto en gestión universitaria con más de 35 TFM dirigidos hasta la fecha. Dirección de múltiples tesis doctorales y trabajos en proyectos de	Seguridad Informática	SI	Atención TFM	20%
Doctor Ingeniero en Informática	Experto en la coordinación de bolsas de trabajo universitarias. Contacto con multitud de empresas en el área de la seguridad de la información	Seguridad Informática	SI	Practicas Externas	40%

6.1.3. Formación prevista para el profesorado

La Universidad Internacional de la Rioja dispone de un programa de formación específica para el profesorado de la titulación. Ésta se realiza a través de las acciones siguientes:

- Perfeccionamiento continuado en el contenido de las respectivas asignaturas a través de la participación de los profesores en congresos, foros, jornadas, reuniones, cursos y seminarios especializados. Como complemento la Universidad Internacional de la Rioja tiene la previsión de celebrar convenios de colaboración y cooperación con otras universidades a través de los programas de movilidad virtual y presencial para su profesorado.

- Actualización permanente en las tecnologías de información y comunicación (TIC), con preferente atención a la enseñanza de *e-learning* de la Universidad Internacional de la Rioja. Esta formación, impartida por personal técnico especializado, pretende perfeccionar el conocimiento integral de las innovaciones que permitan el mejor desarrollo de la docencia virtual.

- Formación pedagógica de los profesores a través de un programa específico sobre estrategias de enseñanza – aprendizaje incluido necesariamente en el Plan General de Calidad que el Servicio de Calidad habrá de presentar anualmente.

6.1.4. Funciones del profesorado de la UNIR

La UNIR precisa de un tipo de docente con una formación y funciones específicas que se concretan en:

- Profesores Titulares. Son los directores de la asignatura y pueden ser o no profesores de la asignatura, dependiendo del número de alumnos y disponibilidad horaria. Son doctores con dilatada experiencia en la impartición de la asignatura.
- Profesores Ayudantes. Cuando el titular no puede atender a todos los estudiantes personalmente, se introducen profesores ayudantes que son dirigidos por el titular en la impartición de la asignatura. Tienen la formación académica necesaria. Sus funciones básicas son:
  - Impartir las clases presenciales virtuales y algunas clases magistrales.
  - Coordinar la asignatura y ser responsable de todos los aspectos académicos.
  - Intervenir y moderar los foros de debate programados.
  - Atender las dudas individuales y del grupo a través de los Foros.
  - Corregir las actividades formativas programadas.
  - Corregir el examen final de la asignatura.
  - Calificar la asignatura.

- Tutor personal:

UNIR asigna un tutor personal por cada grupo de estudiantes. Son todos licenciados con experiencia en formación *on line*.

Sus funciones básicas son:

Orientar y asesorar a los estudiantes durante el desarrollo de las Asignaturas:
- Facilitar instrucciones de uso del aula virtual.
- Orientar sobre el acceso a los contenidos de la Asignatura.
- Ayuda en la planificación de los tiempos de dedicación a las asignaturas.
- Informar del comienzo y finalización de las actividades individuales y colaborativas programadas. Existen actividades y fechas de obligado cumplimiento.

Fomentar la participación de los estudiantes
- Abrir espacios de interacción, a través de los foros y debates.
- Facilitar la interactividad entre los estudiantes.
- Animar y supervisar el uso de los foros.
- Moderar los debates.
- Fomentar el uso de las herramientas de trabajo que ofrece el aula virtual.

Resolver las dudas de los estudiantes
- Resolver las dudas planteadas por los estudiantes, facilitándoles una respuesta en un plazo máximo de 48 horas (los profesores de la asignatura resolverán las relacionadas con la temática de la asignatura, y el tutor otras dudas de índole académico).

- Extrapolar a través de los foros, siempre que se considere de interés para el grupo, consultas que los estudiantes realicen a nivel particular.

Realizar un seguimiento continuo de las tareas individuales y colaborativas de los estudiantes que forman parte de la evaluación continua.

- Tutores de Prácticas Externas. El Itinerario profesional del Máster comporta la realización de prácticas profesionales. Para garantizar el adecuado desarrollo de estas prácticas, cada estudiante tiene asignado un Tutor, un profesional de reconocido prestigio. El tutor es responsable de:
  - Orientar el trabajo profesional del alumno.
  - Realizar sugerencias y correcciones.
  - Proporcionar al estudiante la información necesaria para el desarrollo de los trabajos asignados.
  - Evaluar su trabajo.
- Profesor y Tribunal Evaluador del Proyecto Fin de Máster. La elaboración del Proyecto fin de máster está dirigida por un profesor doctor, integrante del equipo docente que se asigna a cada estudiante. Los Proyectos fin de máster son evaluados por un tribunal, formado por dos componentes del equipo docente y un profesor de universidad ajeno a la UNIR y del área de Empresa, que decide la calificación correspondiente tras la defensa de los proyectos.

6.2. Otros recursos humanos disponibles

6.2.1 Dotación del Personal de Administración y Servicios

Departamentos y Servicios

La UNIR es una universidad que imparte sus enseñanzas en modalidad totalmente virtual por lo que el personal de apoyo para cada una de las titulaciones son, en su mayoría personal titulado, no docente, con una formación específica tal y como se detalla a continuación. Hemos elaborado un cuadro donde relacionamos el perfil de este personal con los diferentes departamentos y servicios de la Universidad.

La UNIR cuenta ya con el apoyo de los siguientes departamentos y servicios para que sea posible la implantación y desarrollo de las distintas titulaciones de la UNIR.

Departamentos y Servicios	Apoyo a las Titulaciones	Perfil de PAS
Oficina de atención al alumno	Información sobre las diferentes titulaciones	6 Auxiliares administrativos con experiencia en el campo de la Formación.

Servicio Técnico de Orientación	Orientación a futuros alumnos	30 Licenciados superiores en diferentes titulaciones (Pedagogía, Psicología y Sociología).
Servicio de Admisiones	Acceso, admisión y matrícula	22 Auxiliares administrativos con experiencia en el campo de la Formación.
Servicio Técnico Informático	Mantenimiento, desarrollo e innovación del campus virtual	15 Titulados superiores (ingeniería, técnicos de informática y especialistas en e-learning); uno de ellos responsable del mantenimiento.
Servicio de Publicaciones, Recursos Docentes y Documentación	Diseño y desarrollo de los materiales y Recursos docentes para su aplicación on line	24 Titulados superiores, uno de ellos responsable del diseño y edición de los contenidos.
Comunicación y Expansión Académica	Plan de Comunicación y desarrollo de proyectos nacionales e internacionales.	12 Licenciados en diferentes áreas relacionadas. Marketing, ADE y Relaciones Públicas.
TV y Producción Audiovisual	Grabación, edición y producción de material didáctico audiovisual.	10 Licenciados en diferentes Titulaciones (Comunicación y Periodismo).

6.2.2. Selección, formación y perfil del Personal de Administración y Servicios

Selección

En la selección del PAS se respetará lo dispuesto en las siguientes leyes:

- LEY ORGÁNICA 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres. BOE núm. 71 Viernes 23 marzo 2007.
- LEY 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. BOE núm. 289 Miércoles 3 diciembre 2003

Los criterios de selección del PAS, fijados con carácter general para atender las necesidades administrativas y de apoyo a la docencia, son los siguientes:

- Conocimientos exigidos para el desarrollo de su categoría, atendiendo a los estudios

de enseñanzas oficiales o complementarias que se acrediten por el candidato y su adecuación a las tareas requeridas.
- Conocimientos de inglés, tanto a nivel hablado y escrito.
- Experiencia profesional acreditada en puestos con alto requerimiento en el manejo de las nuevas tecnologías, así como en tareas de apoyo docente.

Formación

El plan de formación para el PAS de la Universidad Internacional de la Rioja se ha diseñado con el objetivo de disponer de un instrumento eficaz que gestione y desarrolle las estrategias de la organización, en materia de capacitación y desarrollo, permitiendo la adaptación de las personas a los puestos de trabajo (nuevas tecnologías y actualización de conocimiento), facilitando su promoción profesional y asegurando el éxito de la implantación de nuevos modelos organizativos.

En este sentido, las acciones formativas se gestionarán con un el objetivo de alcanzar la metas que la Universidad se ha trazado y que incluye el necesario desarrollo de la carrera profesional de cada trabajador.

Dicho plan contará con un sistema de evaluación de los resultados obtenidos. Partiendo de un análisis de necesidades "normativas y formativas" del personal, se propondrán un plan formativo, que posteriormente, permitirá ir ajustando la definición de las nuevas acciones formativas a realizar en períodos posteriores.

6.2.3. Funciones del tutor personal

UNIR aplica un Plan de Acción Tutorial, que consiste en el acompañamiento y seguimiento del alumnado a lo largo del proceso educativo. Con ello se pretende lograr los siguientes objetivos:

- Favorecer la educación integral de los alumnos.
- Potenciar una educación lo más personalizada posible y que tenga en cuenta las necesidades de cada alumno y recurrir a los apoyos o actividades adecuadas.
- Promover el esfuerzo individual y el trabajo en equipo.

Para llevar a cabo el plan de acción tutorial, UNIR cuenta con un grupo de tutores personales. **Es personal no docente** que tiene como función la guía y asesoramiento del estudiante durante el curso. Todos ellos están en posesión de títulos superiores. Se trata de un sistema muy bien valorado por el alumnado, lo que se deduce de los resultados de las encuestas realizadas a los estudiantes.

A cada tutor personal se le asigna un grupo de alumnos para que realice su seguimiento. Para ello cuenta con la siguiente información:

- El acceso de cada usuario a los contenidos teóricos del curso además del tiempo de acceso.

- La utilización de las herramientas de comunicación del campus (chats, foros, grupos de discusión, etc.).
- Los resultados de los test y actividades enviadas a través del campus.

Estos datos le permiten conocer el nivel de asimilación de conocimientos y detectar las necesidades de cada estudiante para ofrecer la orientación adecuada.

7. RECURSOS MATERIALES Y SERVICIOS

7.1. Justificación de la adecuación de los materiales y servicios disponibles

En el desarrollo de la actividad propia de la universidad siempre se dispone de la infraestructura necesaria para desarrollar sus actividades de enseñanza, investigación, extensión y gestión.

La infraestructura fundamental para el desarrollo del título es el campus virtual, que se ha descrito en el criterio cinco desde un punto de vista académico, abarcando en este criterio los aspectos técnicos.

Además, para el desarrollo de las funciones de UNIR, se dispone de:

- Rectorado.
- Secretaría General.
- Recepción e información.
- Una biblioteca.
- Un salón de actos para 100 personas.
- Cinco salas de reuniones.
- Tres aulas de trabajo.
- Tres aulas polivalentes.
- Dos aulas totalmente informatizadas de 50 m^2 cada una, con la incorporación de 50 equipos informáticos de última generación.
- Dos salas de sistemas, para albergar los sistemas informáticos y tecnológicos.
- Siete salas de impartición de sesiones presenciales virtuales.
- Un aula-plató con los recursos necesarios para grabar las sesiones magistrales.

7.2. Instituciones colaboradoras para la realización de prácticas externas optativas

UNIR tiene firmados convenios de colaboración para la realización de prácticas externas con los siguientes centros:

CENTRO DE PRÁCTICAS
ATOS
VISION MUNDIAL COLOMBIA
SEGURIDAD ATLAS LTDA
EXCIN SA
FUNDACIÓN AMIGOS DE LA SALUD
INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE COMFACAUCA
JIG INTERNET CONSULTING
INSTITUCIÓN UNIVERSITARIA ITA (INSTITUTO TÉCNICO AGRÍCOLA)
CGB INFORMÁTICA S.L.
EQUINORTE S.A.
NAVANTIA
SOLINIX LTDA
PODRAVSKA BANKA
INFOSTOCK EUROPA DE EXTREMADURA S.A.U.

INFORMÁTICA FORENSE S.L.
A2SECURE SL
ELEVEN PATHS
ASOCIACIÓN PROFESIONAL DE PERITOS INFORMÁTICOS
NORTHGATE ARINSO SAU
DISEÑOS WEB LTDA
INTECO
RED.ES
PROVIDE HCM PEOPLE
UTE NOVASOFT SADIEL DIASOFT
AYTO DE TORREVIEJA - DPTO DE INFORMÁTICA

7.3. Dotación de infraestructuras docentes

7.3.1. Software de gestión académica

La Universidad Internacional de La Rioja dispone de herramientas de gestión que permiten desarrollar de forma eficiente los procesos académico-administrativos requeridos por el título que son los de acceso, admisión, expediente, reconocimientos y transferencias, gestión de actas, expedición de títulos, convocatorias) y los procesos auxiliares de gestión de la universidad como son la gestión de exámenes, gestión de defensas de Trabajo Fin de Grado/Máster, gestión de prácticas, etc.

Dichas herramientas se han desarrollado sobre la base de la gestión por procesos, la gestión de calidad y la satisfacción de las necesidades y expectativas de los usuarios; y todo ello, al tratarse de una universidad en internet, previendo que las solicitudes y trámites puedan desarrollarse íntegramente a distancia.

7.3.2. Campus virtual

UNIR cuenta con una plataforma de formación propia preparada para la realización de los títulos (eLMSCepal) diseñada sobre la base de la experiencia formativa de una de las empresas promotoras de UNIR, que cuenta con más de 13 años en gestión y formación y por la que han pasado más de 30.000 alumnos.

Esta plataforma pertenece a Entornos de Aprendizaje Virtuales (VLE, Virtual Learning Managements), un subgrupo de los Gestores de Contenidos Educativos (LMS, Learning Management Systems).

Se trata de aplicaciones para crear espacios donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por unos docentes y organiza el acceso a esos recursos por los estudiantes y, además, permiten la comunicación entre todos los implicados (alumnado y profesorado). Entre sus características cabe destacar:

- Es fácil de utilizar y no requiere conocimientos específicos por lo que el estudiante puede dedicar todos sus esfuerzos al aprendizaje de la materia que le interesa.
- Todo el sistema opera a través de la Web por lo que no es necesario que los alumnos aprendan a utilizar ningún otro programa adicional.
- Es un sistema flexible que permite adaptarse a todo tipo de necesidades formativas.

Dentro del campus virtual el estudiante encuentra tantas aulas virtuales como asignaturas tenga matriculadas. Desde el aula puede acceder a las sesiones presenciales virtuales a través de la televisión en Internet, que está basado en Adobe Flash Player, una aplicación que ya está instalada en más del 98% de los equipos de escritorio conectados a Internet.

La difusión se realiza mediante el streaming, es decir, el usuario no descarga nada en su ordenador, el visionado se realiza almacenando una mínima cantidad de información (buffering) para el visionado de los contenidos.

Los requisitos técnicos para participar en las sesiones virtuales se resumen en la siguiente tabla:

REQUISITOS TÉCNICOS	
Sistema operativo	Windows 98 SE, 2000, XP, Vista, Mac OS
Navegadores	▪ Internet Explorer 6.0 o superior ▪ Mozilla firefox 1.5 ▪ Netscape Navigator 7.1 ▪ Safari 2.x ▪ AOL 9
Resolución pantalla	Resolución Mínima de 800x600 (se recomienda 1024x768 o superior).
Ancho de banda	56 ADSL/ Cable (conexión alámbrica recomendada).
Red	Acceso externo a Internet, sin restricción de puertos o URL no corporativas.
Audio	Tarjeta de audio integrada, con altavoces o toma de auriculares.
Video	WebCam compatible con los sistemas operativos mencionados.
Equipos PC	RAM: mínimo recomendado 512 Mb. Procesador: mínimo Pentium IV o superior

7.3.3. Biblioteca virtual

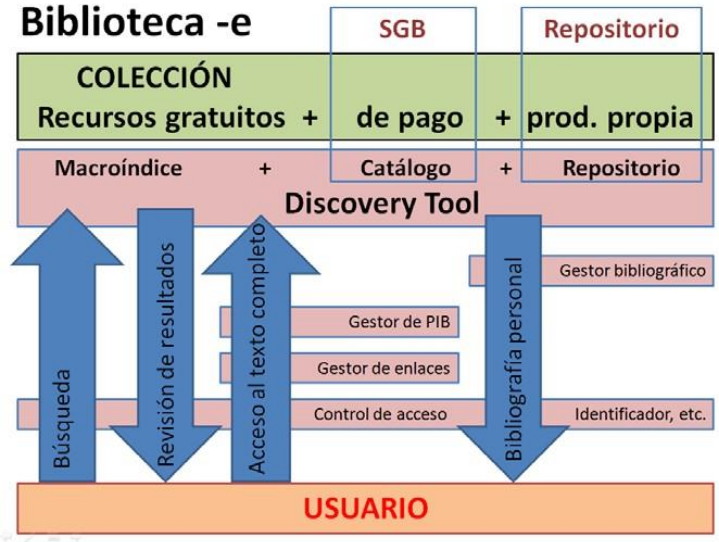
El material bibliográfico y documental, se gestiona a través de una biblioteca virtual. Esta cubre las necesidades de información de sus profesores, investigadores, alumnos y PAS, para la realización de sus tareas de docencia, investigación y gestión.

La política de adquisiciones de la biblioteca de UNIR bascula fundamentalmente sobre recursos en soporte digital. La aún imprescindible adquisición de bibliografía en soporte de papel, se enfocará prioritariamente sobre aquellas áreas de conocimiento en las que se incardinen las líneas de investigación estratégicas de la universidad.

La adscripción de UNIR a la CRUE ha implicado la pertenencia a la red REBIUN, con los derechos y obligaciones que prevé su Reglamento. El servicio de préstamo interbibliotecario de REBIUN es un instrumento fundamental para la investigación de los profesores.

La constitución de la biblioteca virtual se ha iniciado con la adquisición de un sistema de gestión de biblioteca y una herramienta de descubrimiento propiedad de PROQUEST, las cuales son la base para futuras extensiones.

La visión de biblioteca virtual sigue el modelo mostrado en la siguiente figura:



7.4. Dotación de infraestructuras investigadoras

El profesorado está integrado en cuatro ejes académicos fundamentales: Educación, Comunicación, Ciencias Sociales y Tecnología. Estos cuatro ejes vertebran la estructura investigadora.

Ha sido creado, además, la Oficina de Consultoría y Apoyo a Proyectos de Investigación (OCAPI) con carácter interdisciplinar para coordinar todas las actividades investigadoras de UNIR y proporcionar apoyo al personal docente-investigador (PDI) adscrito a la Universidad. Su finalidad es estimular y facilitar la participación efectiva de la comunidad académica UNIR en iniciativas de investigación, tanto propias como europeas, nacionales y regionales.

UNIR desarrolla un plan bienal de investigación (Plan Propio de Investigación) que define las líneas maestras para el presente bienio, y aprueban seis líneas iniciales de I+D, que son

desarrolladas por grupos de Investigación formados en torno a las líneas básicas de I+D. Los grupos están dirigidos por catedráticos y académicos de prestigio en sus áreas. Los grupos son flexibles e incorporan candidatos durante el bienio. Así, se parte de una estructura de 7 grupos con 15 miembros, aunque se espera duplicar en el plazo de 18 meses.

Al mismo tiempo, todo profesor recibe orientación y apoyo para mantener una carrera investigadora (publicación científica, dirección de trabajos de grado, tesinas de máster y tesis doctorales, estancias de investigación, etc.) que dependerá tanto de su implicación en Unir como del plan individual de carrera elaborado para cada uno.

De esta manera, articulamos el personal investigador alrededor de Grupos y Líneas de trabajo, sin olvidar la atención individual según parámetros personales.

7.5. Recursos de telecomunicaciones

Los recursos disponibles en UNIR son los siguientes:

- 90 líneas de teléfono a través de tres primarios de telefonía en Madrid.
- 30 líneas de teléfono a través de un primario de telefonía en Logroño.
- Número de teléfono de red inteligente para llamadas entrantes: 902 02 00 03.
- Centralita de telefónica administrativa Panasonic TDA 600. 16 canales voIP + analógicos.
- Nueve enlaces móviles con conexión digital a la central.
- Cuatro líneas de banda ancha redundantes y balanceadas utilizando tecnología Cisco para dar acceso a: Internet, Conectividad con Universitas XXI y al Campo Moodle que tiene UNIR externalizado.
- Telefonía basada en VoIP sobre servidores Cisco Call Manager 5.1 redundados.
- 100 por 100 de los puestos de trabajo con acceso a la red local mediante cable.
- Cobertura WIFI en todas las dependencias universitarias.
- Sistemas de alimentación eléctrica ininterrumpida mediante baterías y un generador diesel que garantiza el servicio necesario para las comunicaciones y el normal funcionamiento de todos los equipos informáticos en caso de fallo eléctrico con autonomía de ocho horas.

7.6. Mecanismos para garantizar el servicio basado en las TIC

El modelo de enseñanza de UNIR hace un uso intensivo de las TIC para garantizar el proceso de enseñanza-aprendizaje. Las infraestructuras tecnológicas que sirven de apoyo a la educación a distancia en UNIR garantizan la accesibilidad a los servicios en todo momento.

UNIR tiene contratado un proveedor europeo de servicios de Presencia en Internet, Hosting Gestionado, Cloud Computing y Soluciones de Infraestructura TIC (Arsys).Que nos permite:

- Optimizar la velocidad de conexión con todos los usuarios de Internet, de esta manera nuestros servidores pueden ser vistos con gran rapidez y sin cuellos de botella por usuarios de conexiones RTB, RDSI, ADSL, cable, etc, así como por internautas extranjeros.
- Redundancia física. Si una línea sufre un corte, las restantes mantendrán la conectividad con Internet.
- Velocidad de descarga hacia cualquier destino. Los paquetes de datos escogerán la ruta más adecuada para llegar al usuario que está viendo las páginas por el camino más corto.

Desde el punto de vista técnico, UNIR dispone de las más avanzadas instalaciones en materia de seguridad física, control de temperatura y humedad, seguridad contra incendios y alta disponibilidad de energía eléctrica. Se detalla a continuación:

INSTALACIONES DE SEGURIDAD
Seguridad física
- Sensores para el control de la temperatura y humedad ambiente. - Filtrado de aire para evitar la entrada de partículas. - Sistema automático balanceado y redundante de aire acondicionado. - Sistema de detección de incendios que dispara, en caso de necesidad, un dispositivo de expulsión de gas inerte que extingue el fuego en pocos segundos.
Seguridad en el suministro eléctrico
- Sistema de Alimentación Ininterrumpida (SAI) para garantizar la estabilidad y continuidad de los equipos. - Grupo electrógeno autónomo que suministraría, en caso de corte prolongado, la energía necesaria para que no haya pérdida de alimentación, de modo que los servicios a clientes no sufran ninguna alteración.
Seguridad perimetral
- Acceso restringido por control de tarjeta magnética y contraseña. - Sistema generalizado de alarmas. - Tele vigilancia.

7.7. Detalle del servicio de alojamiento

7.7.1. Recursos software

La infraestructura lógica necesaria para el funcionamiento del campus virtual se describe en la siguiente tabla:

RECURSOS SOFTWARE	
Acceso Remote Desktop	Servidor de base de datos MySQL
Express Edition Soporte ASP y ASP.NET	Servidor de base de datos PostgreSQL
Extensiones FrontPage	Servidor de base de datos SQL Server 2000/2005
Filtro antivirus / antispam avanzado	Servidor de correo (POP3/SMTP/listas)
Gestor de Base de datos: Microsoft SQL Server 2005/2008	Servidor de estadísticas AWStats
Indexador de ficheros Microsoft Index Server	Servidor FTP
Intérpretes VBScript, JScript, Active Perl, PHP y Python	Servidor Multimedia Windows Media Server
Lenguaje de programación ASP y ASP.NET	Servidor web IIS
Mailenable	Sistema Operativo: Windows 2000/2003/2008 Server
Microsoft oBind	Tecnología Microsoft
Microsoft Servidor DNS	Webmail Horde

7.7.2. Recursos hardware

La infraestructura física necesaria para el funcionamiento del campus virtual se describe en tres puntos: Características técnicas del servidor, Características del hosting y Sistema de copias de seguridad. Tal como se describen a continuación en la tabla:

<table>
<tr><th colspan="2">RECURSOS HARDWARE</th></tr>
<tr><th colspan="2">Características técnicas del servidor</th></tr>
<tr><th>Detalle de la máquina</th><th>Gestión del producto</th></tr>
<tr><td rowspan="7">Fabricante: IBM
Modelo Xeon E5-2630 0
Tipo CPU: Intel Xeon Quad-Core
Número de núcleos: 24
Velocidad de cada núcleo: 2.30 GHz
Memoria RAM: 32 GB ECC
Tamaño de discos 2x300 GB
HDD Discos: 136 GB RAID 1
HDD cabina FC: 2 TB
SAS RAID: RAID 1 Hot Swap –
Transferencia: 18 Mbps</td><td>Panel de control
Reinicios y reseteos
Avisos automáticos (email/SMS)
Gráficos de ancho de banda y transferencia
Direcciones IP extra</td></tr>
<tr><td>Seguridad</td></tr>
<tr><td>Alojamiento IDC Protección firewall
Monitorización avanzada</td></tr>
<tr><td>Garantías y Soporte</td></tr>
<tr><td>Garantía hardware ilimitada Soporte 24x7</td></tr>
<tr><td colspan="2">Características del hosting</td></tr>
<tr><td colspan="2">Disponibilidad 24x7 del portal y la plataforma de formación con un porcentaje de disponibilidad del 99%.</td></tr>
<tr><td colspan="2">Servicio de backup y recovery de los datos almacenados en los servidores.</td></tr>
<tr><td colspan="2">Servicios de retenciones: Retención de la imágenes de los backup realizados por el tiempo que se acuerde.</td></tr>
<tr><td colspan="2">Servicios de sistemas de seguridad: Física (Control de Accesos, Extensión de Incendios, Alimentación ininterrumpida eléctrica, etc.,..) y Lógica (Firewalls, Antivirus, Securización Web, etc.).</td></tr>
<tr><td colspan="2">Servicio de Monitorización, Informes y estadísticas de Ancho de Banda, disponibilidad de URL, rendimiento, etc.</td></tr>
</table>

<table>
<tr><th>Sistema de copias seguridad</th></tr>
<tr><th>Compresión de datos de alto nivel</th></tr>
</table>

El proceso de copia se realiza a través de una tecnología puntera de copias de seguridad incrementales y completas, FastBit, que le garantiza: - Altos niveles de compresión (un 50% de media), lo que nos permite almacenar en el servidor 2 veces el espacio contratado. - Menor transferencia de datos, por lo que podrá realizar sus copias desde cualquier tipo de acceso a Internet, incluso desde una conexión RTB por línea analógica.
Proceso sencillo y automático
Pues no se ha de recurrir a los métodos manuales en los que tiene que dedicar mucho tiempo y esfuerzo. Con el sistema de Backup Online se realizan las copias de seguridad con gran facilidad, lo que permite despreocuparse del proceso.
Copia segura
El proceso de copia se realiza a través de una clave de cifrado y previa autentificación del usuario de acceso al servicio. Se utiliza un algoritmo de cifrado de 448 bits (superior a los que se utilizan en certificados de seguridad web), a través de una clave privada, lo que garantiza que la información se almacena de forma segura y no es accesible más que por el usuario del servicio. Además, al efectuar la copia en un servidor de Internet, sus datos se encuentran a salvo de cualquier incidente y fuera de sus instalaciones, lo que le protege ante catástrofes como incendios, errores humanos, fallos hardware o software, etc.

7.8. Previsión de adquisición de recursos materiales y servicios necesarios

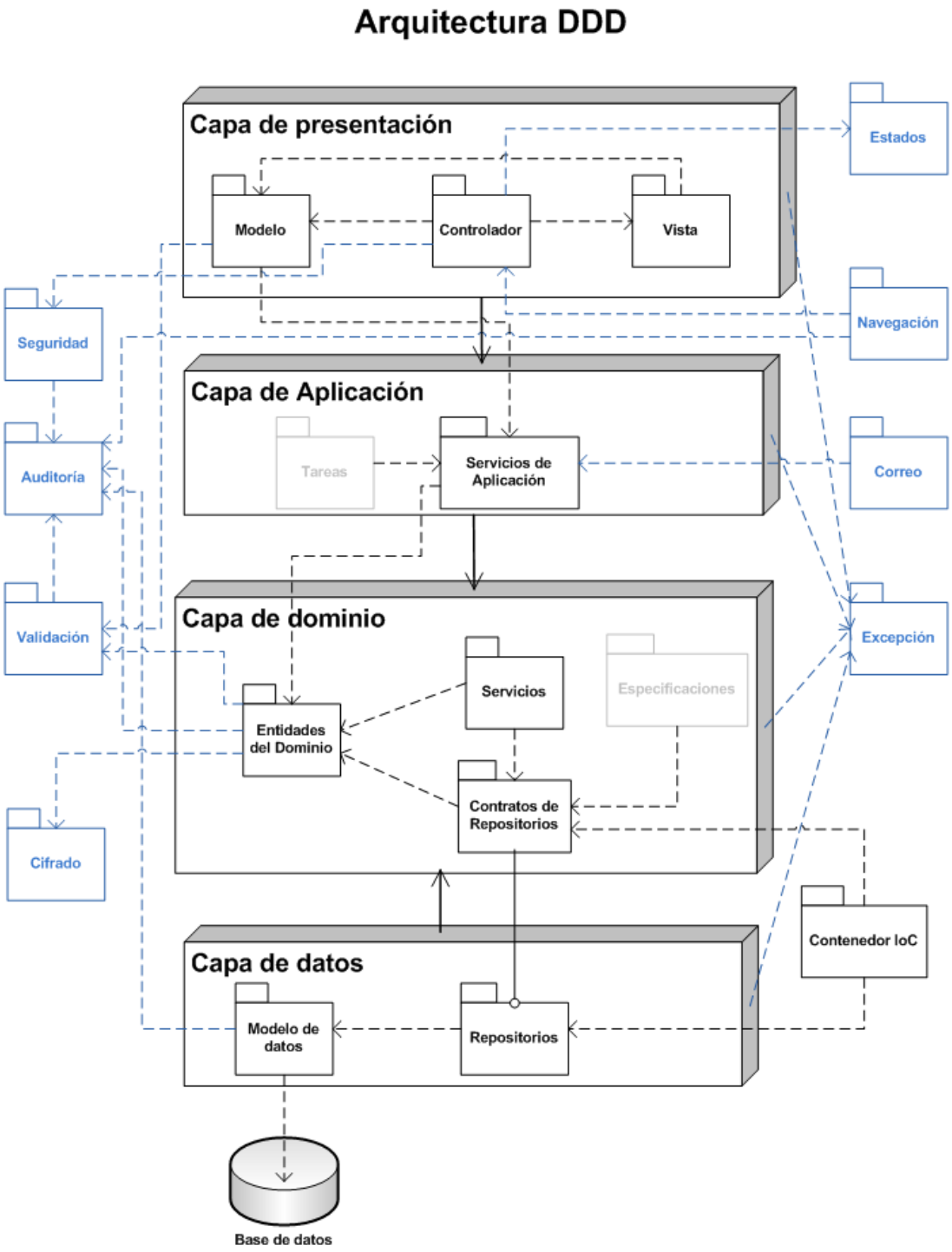
Este cuadro resume la planificación sistemática de infraestructuras, materiales y servicios de los que la Universidad se dotará en los próximos años de acuerdo a la previsión anual de incorporación de personal.

RECURSOS	2013-14	2014-15	2015-16
Capacidad máxima de acceso a Internet	600 Mb	700 Mb	560 Mb
Líneas de acceso a internet redundadas	9	10	8
Capacidad de almacenamiento en servidores centrales en TeraBytes	24	30	24
Impresoras departamentales (con fax y escáner)	32	32	32

Impresoras escritorio	8	10	12
Potencia de SAI	30Kwa	40Kwa	40Kwa
Potencia generadores diésel	50Kw	60Kw	60Kw
Líneas telefónicas	160	190	130
Puntos de acceso *wireless*	14	16	18
Ordenadores sobremesa	460	500	412
Ordenadores portátiles	17	20	25
Teléfonos VoIP sobremesa	20	24	28
Teléfonos VoIP softphone	20	24	28

7.9. Arquitectura de software

Para el desarrollo de las aplicaciones informáticas desarrolladas a partir del 2012. UNIR ha implantado una arquitectura de software orientada a Dominio DDD. Esta arquitectura dispone de componentes horizontales y transversales que se muestran en la siguiente figura:



7.9.1. Componentes horizontales

Componentes horizontales.	
Capa de presentación	Basada en la definición del modelo vista controlador. Implementa las pantallas de usuario y los controladores de estas.
Capa de	Coordina actividades propias de la aplicación pero no incluye lógica de

aplicación	negocio siguiendo el Principio de "Separation of Concerns".
Capa de dominio	Basada en la definición del patrón "Entity" e implementada a través de las "IPOCO Entities". Esta capa está completamente desacoplada de la capa de datos para lo cual se aplica el patrón "Inversion of Control".
Capa de datos	Basada en la definición del patrón "Repository" y es la encargada de acceder a la base de datos de la aplicación.

7.9.2. Componentes transversales

1.1.1. **Componentes transversales**	
Componente de seguridad	Gestiona la seguridad en el acceso a la aplicación, y se divide en dos: 1. Autenticación: Permite validar la identidad de los usuarios e incluye el inicio y fin de sesión, el recordatorio y cambio de contraseña y la activación de cuenta de los usuarios. 2. Autorización: Permite gestionar los permisos de los usuarios en la aplicación a partir de los roles que les hubiesen sido asignados e incluye: Permisos de acceso a las páginas Permisos de acceso a las opciones de menú Permisos de lectura, escritura, eliminación y consulta Permisos de ejecución de acciones
Componente de estados	Implementado en base al patrón "Memento" y permite recuperar el estado anterior de una página durante el proceso de navegación del usuario para mantener los valores introducidos en los filtros, listados, asistentes, etc. Deberá estar preparado para escenarios con granja de servidores.
Componente de navegación	Permite establecer la relación de flujos entre las páginas de la aplicación para mantener la coherencia en la navegación del usuario.
Componente de validación	Permite realizar las validaciones de los valores de entrada y salida de la aplicación. Incluye lo siguiente: 1. Validación de definición de campos: Permite validar la definición de los campos en base a la longitud, tipo de dato, rango de valores, etc. 2. Validación de formatos: Permite validar los formatos de texto conocidos como son: NSS, NIE, NIF, CIF, CCC, EMAIL, MOVIL, etc. 3. Filtrado de textos: Permite filtrar los textos de entrada (usuarios) y salida (base de datos) en base a una lista negra de palabras con el fin

	de evitar inyecciones de SQL y de XSS.
Componente de auditoría	Permite registrar una bitácora de las acciones realizadas por los usuarios en la aplicación almacenando: la naturaleza de la acción, el momento en que se realizó, desde donde y el usuario que la ejecutó. Incluye 5 niveles de auditoría: 1. Auditoría de acceso: Encargado de registrar los inicios, cierres de sesión, intentos fallidos en la aplicación, solicitudes de recordatorio y cambios de contraseña. 2. Auditoría de navegación: Encargado de registrar las páginas visitadas por los usuarios en la aplicación recogiendo la mayor cantidad de parámetros posibles (tiempo, navegador, etc.). 3. Auditoría de acciones: Encargado de registrar todas las acciones realizadas por el usuario en el sistema recogiendo la mayor cantidad de parámetros posibles (contexto, registro, etc.). 4. Auditoría de datos: Encargado de registrar los cambios que un usuario realiza sobre los datos de la aplicación recogiendo la mayor cantidad de parámetros posibles. Incluye operaciones de alta, edición, eliminación y consulta de registros (contexto, registro, filtro, etc.). 5. Auditoría de validación: Encargado de registrar las validaciones incorrectas y filtros aplicados que eliminaron cadenas de inyección SQL y XSS.
Componente de excepciones	Encargado de interceptar, registrar, categorizar y comunicar los errores encontrados en la aplicación en producción. Estas excepciones deberán estar dentro de un contexto para identificar como han ido subiendo por las diferentes capas e incluirán información relativa al espacio de nombres, clase, método y cualquier información adicional como ser el usuario.
Componente de cifrado	Encargado de realizar el cifrado y descifrado de información sensible como la contraseña o datos sensibles según la L.O.P.D.
Componente de correo	Encargado de realizar el envío de los correos electrónicos de la aplicación.

7.10. Criterios de accesibilidad universal y diseño para todos

Se está trabajando para que el campus virtual alcance el nivel AA de las Pautas de Accesibilidad para el Contenido en la Web 2.0 del W3C, cuyos requisitos se recogen en la norma española sobre accesibilidad web (UNE 139803:2012).

Para garantizar la integración de las personas con discapacidad en el aula, se presta especial atención a la accesibilidad de aquellas funcionalidades que promueven la interacción entre estudiantes y de éstos con los profesores: foro, videoconferencia, etc.

El objetivo es que los contenidos formativos y las actividades sean igualmente accesibles, tanto a nivel técnico (aplicación de las citadas Pautas de Accesibilidad para el Contenido en la Web 2.0) como pedagógico (objetivos formativos alcanzables por los distintos perfiles de discapacidad).

Para que la producción de contenidos por parte del equipo docente se ajuste a los requerimientos de accesibilidad establecidos, éstos se desarrollarán mediante plantillas en Word con estilos cerrados. Además, una vez producidos, se exportarán a distintos formatos para facilitar a los estudiantes el acceso multidispositivo: HTML y PDF accesible.

Por último, con el fin de asegurar que tanto el campus virtual como los contenidos se ajustan a los requerimientos del W3C y de la norma española, UNIR está negociando con FundosaTechnosite, empresa especializada en tecnología y accesibilidad de la Fundación ONCE, la certificación del grado de adecuación a los estándares de accesibilidad, y contempla un plan de mantenimiento mediante revisiones periódicas para asegurar que la accesibilidad se mantiene en el tiempo.

8. RESULTADOS PREVISTOS.JUSTIFICACIÓN DE LOS INDICADORES PROPUESTOS

8.1. Estimación de valores cuantitativos

Una previsión de los resultados que obtendrán los estudiantes del Máster se enfrenta con los siguientes factores de dificultad.

- Primero.- Se trata de una titulación que se impartirá en una universidad de reciente creación y carece de precedentes sobre los que basarse.

- Segundo.- El carácter de universidad no presencial (que está, en estrecha relación con el perfil del estudiante que la elegirá) comporta que los periodos para la finalización con éxito de la enseñanza han de estimarse, a priori, más dilatados que en las presenciales.

  A este factor apunta directamente la indicación que se recoge en la *Guía de apoyo para la elaboración de la Memoria de solicitud de verificación de Titulaciones oficiales Máster*, en su versión de 18.02.2008, cuando señala que "el grado de dedicación a los estudiantes a la carrera" es un aspecto cuya consideración "será especialmente importante en el caso de enseñanzas a distancia, donde el planteamiento de cara a los indicadores habrá de ser substancialmente diferente de las enseñanzas a tiempo completo" (p. 29, nota 1).

- Tercero.- No es posible acudir a los datos de las universidades que en este apartado podrían actuar como referentes, la UNED y la UOC. La publicación de la CRUE "La universidad española en cifras", no contiene datos ni de una ni de otra.

Para la UNIR, definir una previsión de tasa de graduación, abandono y eficiencia es extremadamente difícil debido a varias razones:

1. La UNIR es una Universidad de reciente creación, por lo que no dispone de datos previos.
2. Su sistema de enseñanza a distancia por lo que la comparación de datos con universidades tradicionales debe hacerse con especial cautela.

Sí podemos afirmar que el perfil de alumnos que realizarán este Máster son estudiantes muy motivados y que son conscientes de la mejora profesional que puede suponer la especialización que se obtiene con esta titulación ya que las necesidades sociales en este ámbito son cada vez mayores.

Por todo ello, y en base a datos obtenidos de alguna universidad presencial que hemos podido obtener, se pueden prever las siguientes tasas:

Tasa de graduación	80%
Tasa de abandono	10%
Tasa de eficiencia	75%

8.2. Procedimiento general para valorar el progreso y los resultados

La Universidad Internacional de La Rioja evalúa el rendimiento general de los estudiantes de sus titulaciones oficiales principalmente a través del estudio de:

- Tasa de rendimiento: porcentaje de créditos superados respecto de los matriculados.
- Tasa de éxito: porcentaje de créditos superados respecto de los presentados.
- Tasa de eficiencia: relación entre el número de créditos superados y el número de créditos de que se tuvieron que matricular, a lo largo de los estudios, para superarlos.
- Tasa de abandono: porcentaje de estudiantes que no se matricularon en los dos últimos cursos.
- Duración media de los estudios: media de los años empleados en obtener el título de Máster.
- Tasa de graduación: porcentaje de estudiantes que acaban la titulación en el tiempo establecido en el plan.

También está previsto el estudio de las series de resultados en función de los perfiles de los estudiantes. El número de créditos matriculados, la edad, la vía de acceso al Máster, la nacionalidad e idioma, los lapsos de tiempo de conexión a la plataforma y la intensidad en la participación de los medios colaborativos serán factores que se pondrán en relación con las calificaciones obtenidas en los exámenes finales.

9. SISTEMA DE GARANTÍA DE CALIDAD

http://gestor.unir.net/userFiles/file/documentos/planes_calidad/garantia_calidad_grado_master.pdf

10.CALENDARIO DE IMPLANTACIÓN

10.1. Cronograma de implantación

La implantación se hará de forma progresiva, de acuerdo con la temporalidad prevista en el plan de estudios.

Máster previsto para un año

CURSO 2011-2012	
Primer cuatrimestre	**Segundo cuatrimestre**
M I:Aspectos Legales y Marco Jurídico	M I:Aspectos Legales y Marco Jurídico
M. II: Auditoría y Gestión de Seguridad	M. II: Auditoría y Gestión de Seguridad
M. III: Técnicas Avanzadas de Seguridad	M. IV: Seguridad en las Aplicaciones y Análisis Forense
M. IV: Seguridad en las Aplicaciones y Análisis Forense	M V: Prácticas en Empresa y Trabajo Fin de Máster

Máster previsto para dos años

CURSO 2011-2012		CURSO 2012-2013	
Primer cuatrimestre	**Segundo cuatrimestre**	**Primer cuatrimestre**	**Segundo cuatrimestre**
M I:Aspectos Legales y Marco Jurídico	M I:Aspectos Legales y Marco Jurídico	M. II: Auditoría y Gestión de Seguridad	M. IV: Seguridad en las Aplicaciones y Análisis Forense
M. II: Auditoría y Gestión de Seguridad	M. II: Auditoría y Gestión de Seguridad	M. III: Técnicas Avanzadas de Seguridad	M V: Prácticas en Empresa y Trabajo Fin de Máster
M. III: Técnicas Avanzadas de Seguridad	M. IV: Seguridad en las Aplicaciones y Análisis Forense	M. IV: Seguridad en las Aplicaciones y Análisis Forense	

10.2. Procedimiento de adaptación

No aplicable.

10.3. Enseñanzas que se extinguen por la implantacñon del correspondiente Máster propuesto.

No aplicable.

10.4. Extinción de las enseñanzas

UNIR podrá decidir, a través de los órganos previstos en sus normas de organización y funcionamiento con competencia en la implantación y extinción de titulaciones, que el presente Máster se extinga si, tras tres cursos consecutivos, el número de alumnos de nuevo ingreso no supera la cifra de 15.

La salvaguardia de los derechos de los estudiantes queda asegurada, tal como se indica en la disposición primera de las Normas de Permanencia: “Se garantiza a todo estudiante el derecho a terminar su titulación siempre que cumpla las normas que se indican en el punto 2. En el supuesto de que el Consejo de Administración, debido a causas graves, se plantease la posible extinción de la titulación, esta sólo podría ejecutarse mediante el procedimiento de no ofertar plazas para nuevos estudiantes en el curso siguiente definiendo un plan de extinción que, de acuerdo con la legislación vigente, garantice la finalización de los estudios a quienes lo hubieran comenzado”.