BASIC DETAILS:

Subject:	SEGURIDAD EN REDES Y SISTEMAS		
Id.:	33444		
Programme:	DOBLE GRADO EN INGENIERÍA INFORMÁTICA Y BIOINFORMÁTICA		
Module:	COMUNICACIONES		
Subject type:	OBLIGATORIA		
Year:	4	**Teaching period:**	Segundo Cuatrimestre
Credits:	6	**Total hours:**	150
Classroom activities:	59	**Individual study:**	91
Main teaching language:	Inglés	**Secondary teaching language:**	Castellano
Lecturer:	TORNOS MARTINEZ, JOSE LUIS (T)	**Email:**	jltornos@usj.es

PRESENTATION:

Currently, Information Systems Security (Infosec) has passed to be an area attached to others, as applications development or network management, to become an area by itself. In the same way, several years ago security was managed by very specificall applications related with cryptography and mathematic models or security experts but today, terms such as digital certificate, digital signature or secure protocols are managed or at least known by network managers and end users.

We must value that new models on security services must be part of the Information Society and, therefore, the professionals involved in the design of solutions in this field must guarantee the properties of the security.

In this context, it is intended that the subject "Seguridad en Redes y Sistemas" allows the student to address the main processes of designing secure systems, including the techniques, methodologies and services.

PROFESSIONAL COMPETENCES ACQUIRED IN THE SUBJECT:

General programme competences	G02	Innovative capacity to propose and find new and efficient ways to undertake any task and/ or function within the professional environment - highly motivated by quality.
	G03	Capacity to work in multidisciplinary teams to achieve common objectives, placing group interests before personal ones.
	G04	Capacity to always commit to working responsibly - creating a strong sense of duty and fulfilment of obligations.
	G06	Capacity to analyse and find a solution to complex problems or unforeseen situations which may arise while working in any type of socio-economic organisation.
	G10	Critical and analytical capacity when assessing information, data and courses of action.
	G12	Capacity to undertake professional activities with integrity, respecting social, organisational and ethical norms.
	G13	Capacity to use individual learning strategies aimed at continuous improvement in professional life and to begin further studies independently.
	G14	Capacity for abstraction to handle various complex knowledge models and apply them to examining and solving problems.
	G15	Capacity to structure reality by means of linking objects, situations and concepts through logical mathematical reasoning.
Specific programme competences	E01	Capacity to understand the engineering profession and commitment to serve society under the corresponding professional code of conduct.
	E02	Capacity to apply the intrinsic engineering principles based on mathematics and a combination of scientific disciplines.
	E03	Capacity to recognise the technical principles and apply the appropriate practical methods satisfactorily to analyse and solve engineering problems.
	E08	Capacity to communicate productively with clients, users and colleagues both orally and in writing, so as to pass on ideas, solve conflicts and achieve agreements.
	E10	Capacity to understand and assess the impact of technology on individuals, organisations, society and the environment, including ethical, legal and political factors, recognising and applying the pertinent standards and regulations.s éticos, legales y políticos, reconociendo y aplicando los estándares y regulaciones oportunos

	E11	Capacity to remain up-to-date in the technological and business worlds in the area of information and communication technologies.
	E13	Capacity to identify, assess and use current and emerging technologies, considering how they apply in terms of individual or organisational needs.
	E17	Capacity to identify and analyse user needs with the intention of designing effective, usable IT solutions which can be incorporated into the user's operating environment.
	E18	Capacity to identify and define the requirements to be satisfied by IT systems to cover the stated needs of organisations or individuals.
	E19	Capacity to design and define the architecture of IT systems (software, hardware and communications) under the requirements agreed upon by the parties involved.

PRE-REQUISITES:

"Sistemas operativos"; "Administración de sistemas operativos"; "Administración de servidores"

SUBJECT PROGRAMME:

Subject contents:

1 - Introduction to Information Security Systems
1.1 - Introduction
1.2 - Definitions and different views
1.3 - Properties and services
1.4 - Network and OS security
2 - Secure systems design
2.1 - Introduction
2.2 - PKI: Public Key Infrastructure
2.3 - IBS and PGP
3 - Attacks and viruses
3.1 - Attacks
3.2 - Viruses

Subject planning could be modified due unforeseen circumstances (group performance, availability of resources, changes to academic calendar etc.) and should not, therefore, be considered to be definitive.

TEACHING AND LEARNING METHODOLOGIES AND ACTIVITIES:

Teaching and learning methodologies and activities applied:

Lectures will be used to present the content of the different topics of the subject. Also several readings will be used to promote the debate of the different parts of the subject.

Practical work sessions are not carried out in strict order. They will be organized according to the themes presented and the evolution of the proposed works. Each type of sessions are designed for the development of the competences that the student must acquire in the subject.

Student work load:

Teaching mode	Teaching methods	Estimated hours
Classroom activities	Master classes	28
	Practical exercises	25
	Debates	2
	Assessment activities	4
Individual study	Tutorials	8
	Individual study	15
	Individual coursework preparation	12
	Group cousework preparation	13

	Research work	8
	Compulsory reading	18
	Recommended reading	17
	Total hours:	150

ASSESSMENT SCHEME:

Calculation of final mark:

Written tests:	20	%
Individual coursework:	60	%
Group coursework:	20	%
TOTAL	100	%

*Las observaciones específicas sobre el sistema de evaluación serán comunicadas por escrito a los alumnos al inicio de la materia.

BIBLIOGRAPHY AND DOCUMENTATION:

Basic bibliography:

Reference material (subject slides and notes) will be upload to pdu.usj.es

Recommended bibliography:

Adams, C, and S Farrell. “RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols,” 1999.http:/ / tools.ietf.org/ html/ rfc2510.

Aguirre, Jorge Ramió. Libro Electrónico De Seguridad Informática y Criptografía. UPM, 2006.http:/ / www.criptored.upm.es/ guiateoria/ gt_m001a.htm.

Gómez, J; Villar, E y Alcayde, A.: Seguridad en Sistemas Operativos Windows y GNU/ Linux\\; 2ª Edición,2011

IBM Redbooks. Implementing PKI Services on z/ OS, 2004. http:/ / www.redbooks.ibm.com/ abstracts/ SG246968.html?Open.

OpenCA Team. The Open–source PKI Book, 2000. http:/ / sourceforge.net/ projects/ ospkibook/ files/

PKIX Working Group. “Public-key Infrastructure (X.509) (pkix),” 2004. http:/ / www.ietf.org/ html.charters/ pkix-charter.html.

Zurawski, R. "The Industrial Information Technology Handbook" 2004

Recommended websites:

Kali Linux Revealed	https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf