**Academic Year/course: 2023/24**

# 30390 - Network and Service Security

## Syllabus Information

**Academic year:** 2023/24
**Subject:** 30390 - Network and Service Security
**Faculty / School:** 110 - Escuela de Ingeniería y Arquitectura
**Degree:** 581 - Bachelor's Degree in Telecommunications Technology and Services Engineering
**ECTS:** 6.0
**Year:** 4
**Semester:** First semester
**Subject type:** Optional
**Module:**

## 1. General information

The main objective of the subject is to provide the student with an overview of the world of cybersecurity both in communication networks and in computer applications and services. Cybersecurity is one of the fundamental pillars for the operation of ICT systems and it is a booming area where a large number of qualified professionals are in demand . The approach is generalist, touching on the most relevant areas of current cybersecurity and deepening in some of them so that the student can experience this exciting topic. To this end, we first present the current cryptographic tools capable of offering the 3 basic pillars of security: confidentiality, integrity and authenticity of origin. We continue with the characteristics of cybersecure networks, services and applications and the tools we have at our disposal to achieve them. In a third step, the most relevant dangers faced by communications systems and services and how they can be dealt with are presented , and finally, in a fourth step, all these pieces are put together in a common framework in order to secure and control a system with a high degree of security (as we will see in the subject, absolute security does not exist).

These approaches and objectives are aligned with some of the Sustainable Development Goals, SDGs, of the Agenda 2030 (https://www.un.org/sustainabledevelopment/es/) and certain specific targets, so that the acquisition of the learning results of the subject provides training and competence to the student to contribute to some extent to the achievement of targets 8.2 of Goal 8, and targets 9.1, 9.5 of Goal 9.

## 2. Learning results

- Know how to classify the different cryptographic operators by different complexity metrics, security, effectiveness, efficiency, versatility, etc.
- Know the complexity of the computational problems underlying these cryptographic operators.
- Know how to characterize the basic cryptographic protocols: confidentiality, authenticity and integrity. Be able to apply them to different distributed applications.
- Know the basic fundamentals of computer security.
- Know the basic tools for the analysis of vulnerabilities in communications networks as well as the techniques and/or tools to mitigate them.
- Know the protocols for securing the different levels of the TCP/IP architecture.

## 3. Syllabus

The distribution in thematic units of the theory of the subject will be as follows:

1. Introduction to cybersecurity

2. Practical cryptography

3. Application, Operating System and Endpoint Security

4. Redundant Systems

5. Botnets: SPAM + Fraud + DDoS

6. Malware

7. TCP/IP architecture security

8. Security protocols and VPNs
9. Anonymity on the Internet: TOR + Proxy
10. Cyberintelligence: Shodan + Foca

Laboratory Practices:
1. External Security Audit
2. Setting up a VPN: OpenVPN tunnel
3. Implementing Perimeter Security: Firewalls
4. Detecting threats: Intrusion Detection Systems
5. Implementing a SIEM: Elasticsearch

## 4. Academic activities

**Participative lectures (30 hours)** Presentation by the teacher of the main contents of the subject, combined with student participation.

**Laboratory practices (30 hours).** Students will conduct 2-hour practice sessions during 15 sessions.

**Supervised practical work (15 hours).** This non face-to-face activity will allow progress in all the proposed learning results. The evolution of the work will be periodically presented to the teacher.

**Assessment (4 hours).** Set of theoretical-practical written tests and presentation of reports or papers used in the evaluation of the student's progress. Details can be found in the section corresponding to the assessment activities.

## 5. Assessment system

The student will be able to pass the subject through continuous assessment. This will consist of class attendance, the completion and delivery of tutored work and the completion of a evaluation test.

A. Problems/exercises represent 40% of the final grade.
B. The practices will represent 20% of the final grade.
C. The assignments will represent 20% of the final grade.
D. The assessment test will represent 20% of the final grade.

To pass the subject by continuous assessment it is necessary that the grade of each of the parts (A, B, C, D) is higher than 3 points out of 10, and that the average of all the parts is higher than 5.

Students who have not passed the subject by continuous assessment will have a global test in each of the exams established throughout the term. The dates and times of the tests will be determined by the School. The grade for this test will be obtained as follows:

E1: Final exam (100%). Scoring from 0 to 10 points. It is a written test that can include both the problem solving, practical tests in the laboratory as well as theoretical and practical questions formulated in test mode or other mode. This test evaluates all the learning results defined for the subject.

A minimum grade of 5 out of 10 is required to pass the subject.