Information Systems, which may include computer equipment, networks and data carriers, are responsible for working with the sensitive information of any organization. These Information Systems are threatened by risks and threats that may have different origins. We may encounter physical risks such as damage caused by a natural disaster, or by unauthorized access to information; and logical risks generated by a computer attack such as a virus, denial-of-service attacks, etc.

In this subject, the different risks to which the information and the systems that contain it can be subjected will be studied, in order to know them in depth and thus be able to control them and minimize their impact.

By the end of the course, the student will have acquired the following skills:

- Ability to integrate information and communications technology solutions and business processes to meet the information needs of organizations, allowing them to achieve their objectives effectively and efficiently, thus giving them competitive advantages.
- Ability to determine the requirements of the information and communication systems of an organization attending to aspects of security and compliance with regulations and current legislation.
- Ability to actively participate in the specification, design, implementation and maintenance of information and communication systems.
- Ability to understand and apply the principles of risk assessment and apply them correctly in the development and implementation of action plans.

Recommended reading:

- The governance of privacy. C.J. Bennett y C.D. Raab, Massachussets Institute of Technology Press 2006
- Beyond Fear. B. Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World; 2006; Springer
- Vigilancia permanente. Edward Snowden. Planeta, 2019
- Social Engineering: The Science of Human Hacking. Christopher Hadnagy, Wiley 2018
- El pequeño libro rojo del activista en la red. Marta Peirano, Roca 2015
- Grokking Bitcoin. Kalle Rosenbaum, Manning 2019