ID	TITLE	LEVEL	LENGTH (h)	PREREQUISITES
	ICT STRATEGY			
101	**Cyber Security Awareness for non-technical Decision Makers** This course explains the basic concepts of IT security. The aim of the course is to provide the basic tools for the understanding and analysing the risks and threats of cyber space.	Basic	8	-
102	**Cyber Security Awareness for non-technical Decision Makers** The course exposes the concepts related to the culture of IT security. The aim of the course is to develop the knowledge and tools useful for understanding and analysing the risks and threats of cyber space and to improve defenses through prevention and post-incident actions.	Advanced	16 (*)	101
103	**Social Media security** The course introduces the basic principles of social media security. The aim of the course is to provide the basic tools for the understanding and analysing the risks and threats associated with the use of social networks.	Basic	8	101
104	**Cloud and Mobile security** The course introduces the basic principles related to the security of the data stored on the cloud and the use of mobile devices. The aim of the course is to provide the basic tools for the understanding and analysing the risks and threats associated with the personal and corporate use of smartphones, tablets and cloud.	Basic	8	101
105	**Critical Infrastructures and Industrial Systems Security** The course introduces the basic principles related to critical infrastructure and industrial systems security. The aim of the course is to provide the basic tools for the understanding and analysing the risks and threats in the industrial field.	Basic	8	101
106	**Cyber Crime, Cyber Espionage and Information Warfare** The course introduces the concepts of cyber crime, cyber espionage and information warfare. The aim of the course is to provide the basic tools for the understanding and analysing the risks and threats of cyber crime, cyber espionage and information warfare.	Basic	8	101
107	**Digital Self Defence for non-technical Personnel** This course will teach those basic concepts of Digital Self Defense. The aim of the course is to provide a key knowledge of the main instruments for encryption, files secure erasing, anonymized browsing, files encryption on hard drives and USB sticks, etc. The topics covered in this course will be useful both at work and in everyday life, for example in order to recover deleted data from USB sticks and external hard drives.	Basic	8	101

201	**Introduction to Information Security** Through the analysis of the family ISO/IEC 27000 standards, the course outlines the criteria for the implementation of the most widespread organizational model for the Information Security management. During the two days course, the foundations for a thorough understanding of the new ISO/IEC 27001:13 standard and the operational principles that are the basis for an efficient and sustainable business approach to Information Security (InfoSec) are laid.	Basic	16	-
202	**Introduction to IT Service Management** Through the analysis of ISO/IEC 20000 norms family and the main differences with the ITIL model, the course describes the criteria for an IT Service Management System implementation, based on the recent ISO/IEC 20000-1:11. During the two-days course, foundations for a thorough understanding of the norm and operational principles underlying an effective management of IT services.	Basic	16	-
203	**Risk Management for Information Security** Through the analysis of the most recent standards for Risks Management (ISO 31000:09), as related to Security Information (ISO/IEC 27005:11), the foundations for the definition of an efficient and pragmatic process of assessment and management of risks for the Information Security in the field of ICT are laid.	Basic	16	201
204	**Incident Handling for Information Security** Through the analysis of the most recent standards for the incidents management related to information security (ISO/IEC 27035:11), basis for the definition of an effective and pragmatic process of incidents management will be set, taking into account the correlations with Crisis Management processes and current legislation.	Basic	16	201
205	**Business Continuity for Information Security** Through the analysis of the most recent standards for the Business Continuity (ISO 22301:12) and the specific aspects of the Information Security (ISO/IEC 27031:11), the foundations for the definition of an efficient and pragmatic process of Business Continuity Management will be laid.	Basic	16	201
206	**Disaster Recovery for Information Security** Through the analysis of the disaster recovery management norm (ISO/IEC 24762:08), the basis for the definition of an effective and pragmatic process to restore the information security will be laid, also taking into account legislative and contractual issues typical of the ICT sector.	Basic	16	201

(*) = The lenght of the course can be further extended, according to the needs of the Client.

ID	TITLE	LEVEL	LENGTH (h)	PREREQUISITES
207	**Auditor/Lead auditor of Management Systems for Information Security (ISO/IEC 27001:13) – RICEC Qualified training** The ISO/IEC 27001:13 standard and the family of the ISO/IEC 27000 will be re-examined from the auditor point of view, understanding which elements are needed to be taken into account to assess the efficiency and the conformity of an Information Security Management System. Exercises and simulations will allow the understanding of techniques to manage and lead e audits for the Information Security Management Systems.	Advanced	40	201
208	**Auditor/Lead auditor of Management Systems for IT Services (ISO/IEC 20000-1:11) – RICEC Qualified training** The ISO/IEC 20000-1:11 standard and the correlated ISO/IEC 20000 norms will be revisited from the auditor perspective, including which elements should be taken into account in assessing the effectiveness and compliance of an IT services management system. Exercises and simulations will enable the learning of managing techniques and conducting audits for IT services management systems.	Advanced	40	201
209	**Auditor/Lead auditor of Management Systems for IT Services (ISO/IEC 20000-1:11) and of Management Systems for Information Security (ISO/IEC 27001:13) –** The ISO/IEC 20000-1:11 and ISO/IEC 27001:13 standards will be re-examined from the auditor perspective, understanding which elements are needed to be taken into account to assess the efficiency and the conformity of an integrated Management System (information security and IT services). Exercises and simulations will allow the understanding of techniques to manage and lead e audits for integrated Management Systems.	Advanced	56	201 / 202
210	**Information Security Manager – RICEC Qualified training** The whole family of ISO/IEC 27000 allows to acquire the skills needed to certify the competencies of an Information Security Manager, compared to the worldwide reference model. A detailed analysis will lead participants from the introductory issues to the operational activities able to effectively manage the organizational information security.	Advanced	40	201 / 202
211	**Auditor/Lead Auditor of Management Systems for Business Continuity (ISO 22301:2012) – RICEC Qualified training** The ISO 22301:12 standard will be analyzed from the auditor's perspective, understanding which elements are needed to be taken into account to assess the efficiency and the conformity of a Business Continuity Management System. Exercises and simulations will allow the comprehension of techniques to manage and lead business continuity management systems.	Advanced	40	201

(*) = The lenght of the course can be further extended, according to the needs of the Client.

ID	TITLE	LEVEL	LENGTH (h)	PREREQUISITES
212	**Auditor/Lead Auditor of Management Systems for Quality (ISO 9001:2008) – RICEC Qualified training** The standard ISO 9001:2008, basis of all ISO standards, will be analyzed from the auditor's perspective, understanding what elements should be taken into account in assessing the effectiveness and compliance of a quality management system. Exercises and simulations allow the participants to learn the management techniques and the conduction of audits for quality management systems.	Advanced	40	201
213	**Auditor/Lead Auditor of Management Systems for Business Continuity (ISO 22301:2012) – RICEC Qualified training** This course, specifically engineered for auditors/lead auditors already qualified in other schemes of certification, analyzes the ISO 22301:12 standard and the techniques that are needed to assess the efficiency and the conformity of a Business Continuity Management System. The course includes exercises which are essential to lead audits in this scheme and to take the qualification exam at the end of the course.	Advanced	24	201