CYBER SECURITY MANAGEMENT AND ADMINISTRATION

DETAILED PROGRAM

1. Cybersecurity in the State.
   - 1.1 National cybersecurity strategy.
   - 1.2 Main actors of cybersecurity in Spain and their competences: CCN / CNI; INCIBE; MCCD; CNPIC, etc.
   - 1.3 Cybercrime in Spain
2. Standardization, evaluation, certification and accreditation in information security.
   - 2.1 Introduction, legal framework and definitions.
   - 2.2 International and European standardization institutions.
   - 2.3 National standardization entity, UNE. Committees, subcommittees and working groups.
   - 2.4 De jure and de facto standards. Examples.
3. Information security management systems. ISO / IEC standards. 27XXX Series
   - 3.1 UNE-ISO / IEC 27000: 2019
   - 3.2 UNE-EN ISO / IEC 27001: 2017
   - 3.3 UNE-EN ISO / IEC 27002: 2017
   - 3.4 Certifiable standards of the series.
4. Evaluation and certification of the safety of systems and products.
   - 4.1 Safety evaluation criteria. TCSEC; ITSEC and Common Criteria. ISO / IEC 15408 standard.
   - 4.2 Evaluation methodologies: ITSEM and Common evaluation methodology. ISO / IEC 18045 standard.
   - 4.3 National scheme for the evaluation and certification of ICT security.
5. Legal framework of cybersecurity.
   - 5.1 EU Regulation 2014/910. Electronic identification and trust services (eIDAS). Law 6/2020. Trusted electronic services.
   - 5.2 Directive 2016/1148. Network and information systems security (NIS). RD Law 12/2018. Security in networks and information systems.
   - 5.3 Regulation 2019/881 relative to ENISA and the certification of ICT cybersecurity.
   - 5.4 The "computer crime" and the Penal Code.
6. Security audit.
   - 6.1 Control objectives. Internal control system.
   - 6.2 Frameworks and standards for auditing.
   - 6.3 Security audit of personal data.
   - 6.4 Objectives, scope, phases, techniques and tools of the audit.
   - 6.5 Aspects to review. Sources to consider.
   - 6.6 Analysis. Evidence. The audit report