

GRADO EN INGENIERÍA DE LA SEGURIDAD

Information security management

1. The administration and organization of cybersecurity in AA PP. The National Cybersecurity strategy
2. Standardization, homologation, evaluation, certification and accreditation. Legal framework.
 - 2.1. International (ISO, IEC, ITU), European (CEN, CENELEC, ETSI) and national (UNE) organizations. UNE standards-
 - 2.2. Military normalization.
3. The Information Security Management System. ISO 27XXX family.
 - 4.1. Certifiable standards.
 - 4.2. Standards 27000, 27001 and 27002.
4. The comprehensive security plan for information systems.
 - 5.1. Security policy.
 - 5.2. Security Department. CERT, CSIRT, SOC
 - 5.3. Security program.
5. Risk analysis and management. The MAGERIT method. The PILAR tool
6. Training and awareness plans.
 - 6.1. The security manual.
7. Information classification.
 - 7.1. Classification levels. HPS, HSEM, HSES
 - 7.2. ICT security policy that handle classified information.
8. Security assessment and certification
 - 8.1. Criteria and standards for evaluation and certification
 - 8.2. The national certification and evaluation scheme
9. Legal aspects related to security management.
 - 9.1. Regulation (EU) 2014/910. Electronic identification and trust services (eIDAS Regulation). Law 6/2020. Trusted electronic services
 - 9.2. Directive 2016/1148. Security of networks and information systems (NIS Directive). Royal Decree Law 12/2018.
 - 9.3. Management aspects in the (EU) 2016/679 General Data Protection Regulation (GDPR). Law 3/2018. Protection of personal data and guarantee of digital rights.
 - 9.4. Royal Decree 3/2010. National Security Scheme in the field of electronic Administration.
10. Security management and personal data audit.