MANAGEMENT AND ADMINISTRATION OF SECURITY
DETAILED SCHEDULE

1. Introduction and Basic Concepts. Standardization, evaluation, certification and accreditation. Standardizing bodies. Legal framework
   1.1. Introduction and Basic Concepts
   1.2. Standardization, certification, accreditation, etc. Legal framework
   1.3. International and european Standardization
   1.4. National standardization. UNE. technical standardization committees
   1.5. Standards of iure and standard of fact. Examples
2. management systems information security. ISO / IEC standards. 27XXX series
   2.1. UNE-ISO / IEC 27000: 2014
   2.2. UNE-ISO / IEC 27001: 2017
   2.3. UNE-ISO / IEC 27002: 2017
   2.4. Certifiable Standards Series
3. Information classification
4. Business Continuity Plans
   4.1. UNE-EN-ISO 22301: 2015. Management System Business Continuity (BCMS). Specifications
   4.2. UNE-ISO 22313 5.2: 2013. Management System Business Continuity (BCMS). Guidelines
5. Strategies and Legal Framework cybersecurity
   5.1. National Cybersecurity Strategy
   5.2. Law 11/2007 and RD 3/2010 National Security Scheme
   5.3. Electronic Signature Law 53/2002. Regulation (UE) 910/2014 eIDAS
   5.4. Computer crime and the Penal Code
   5.5. Directive (UE) 2016/1148 NIS y Real Decreto Ley 12/2018
6. Safety Audit. Frameworks and standards for the audit. Audit of personal data. Evidences. Analysis. The audit report
   6.1. Objectives of control. Internal control system
   6.2. Marcos and standards for the audit.
   6.3. Audit security of personal data
   6.4. Objectives, scope, phases, techniques and tools of the audit
   6.5. Aspects to be reviewed. Sources to consider
   6.6. Analysis. Evidences. The audit report

June 2020