DTC-MIC-523 Cybersecurity

Syllabus

Chapter 1: Introduction to cybersecurity

1.1 Basic concepts and definitions
1.2 History, and real examples in IT & OT environments
1.3 Global approach and Cyber Live Cycle
1.4 Cyberattacks: Cyber Kill Chain
1.5 Defense approach and trends

Chapter 2: Cyberattacks & cyberdefense

2.1 Cyberattacks & cyberthreats classification
2.2 Cyberdefense classification
2.3 SOC/CERT/CSIRT organizations

Chapter 3: Cybersecurity framework

3.1 Best-practices and Cyberframework definitions
3.2 NIST cyberframework approach
3.3 NIST cyberframework tools

Chapter 4: Critical Infrastructures & Essential Services

4.1 European program for CI protection (EPCIP – PEPIC)
4.2 Spanish CI strategy – CNPIC & INCIBE
4.3 NIS directive – Network & Information Security

Chapter 5: OT Cybersecurity Standards

5.1. IT/OT Technological architecture
5.2. Spain: ENSI – National Industrial Security Scheme
5.3. ANSI/ISA – Security for Industrial Automation and Control Systems

Chapter 6: Cybersecurity Protection Measures

6.1.- Data, information and other digital assets classification
6.2.- Logical access control to industrial systems
6.3.- Physical security & access to industrial systems
6.4.- Communication networks protection measures
6.5.- Software protection
6.6.- Cybersecurity technology for OT

Chapter 7: Cryptography & Digital Signature Basics

7.1. Symmetric & asymmetric cryptography
7.2. Cryptographic hash functions
7.3. Digital certificates & digital signature concepts
7.4. HTTPS protocol (SSL/TLS)