

17. Cybersecurity Awareness

Functional Area: IT (60h)

Pre-Requisites:

Assessment criteria

Knowledge

LO17.1. Applies cybersecurity strategies in the phases of Mechatronics projects to minimize the impact of any possible incident.

- Resolve the cybersecurity elements to be included in the design, establishes the cybersecurity measures in the execution and implementation of an industrial project.
- Implements the cybersecurity activities of the operation and maintenance phase of an industrial project documenting the activities carried out.
- Plans purchase management determining the cybersecurity requirements to be met by suppliers
- Dismantles the facilities complying with the requirements established in destruction and / or conservation of the systems in a safe way.

- Cybersecurity activities in the design of an industrial project.
- Cybersecurity equipment in the purchasing management process.
- Measures cybersecurity in the execution and implementation of the industrial project
- Cybersecurity activities in the operation and maintenance phase of an industrial project.
- Cybersecurity activities in the dismantling of facilities.

Skills

- Evaluates the design of the industrial project:
- Identifies the actors and managers involved in the project, as well as their functions, competences and liabilities in cybersecurity.
- Maps the threats, risks and attack scenarios.
- Executes and implements the project after analysing cybersecurity functions and responsibilities.
- Establishes a detailed plan of cybersecurity measures.
- Take into account the principles of circular economy.
- Incorporates in factory acceptance tests (FAT) cybersecurity and safety criteria.
- Establishes quality control plans and audits.

	<ul style="list-style-type: none"> • Identifies and implements cybersecurity improvements on the installation. • Implements and documents operation and maintenance cybersecurity activities. • Implements cybersecurity awareness and training plans. • Establishes the acquiring management process for suppliers. • Execute analysis and manage the risks associated with the supply chain. • Defines cybersecurity activities in the dismantling, decontamination, declassification, demolition and replacement of project facilities. • Implements and verifies systems destruction measures documenting incidents. • Implements and verifies systems conservation measures documenting incidents.
	<p>Transferable skills</p>
	<ul style="list-style-type: none"> • Understand descriptions, specifications, manuals and other info typical of the profession in English and prepare them for the next phase of project/Customer in understandable manner. • Ability to communicate effectively, orally and in writing with “engineering” community and with “society”, extrapolating concepts for “non-experts) through an abstraction approach.