|  |  | |
| --- | --- | --- |
| ***ELECTRICIDAD Y ELECTRÓNICA - INSTALACIÓN Y MANTENIMIENTO*** | | |
| ***AUTOMATIZACIÓN Y ROBÓTICA INDUSTRIAL, SISTEMAS ELECTROTÉCNICOS Y AUTOMATIZADOS, MECATRÓNICA.*** | | |
| ***CIBERSEGURIDAD INDUSTRIAL (TRANSVERSAL)*** | | |
| ***Duración: n Sesiones x h*** | | ***Organización: Grupos n personas*** |

| ***Reto n***  ***Implementar actividades de programación segura en PLC.Ciberseguridad industrial en sistemas automatizados*** |
| --- |
| ***Breve descripción***  Implementa diferentes actividades de programación segura en el/los PLC que controlan la instalación automatizada sobre la que has realizado el reto del ciclo. |

| **El Reto** |
| --- |

La **Industria 4.0** se caracteriza por la fabricación inteligente y los dispositivos interconectados. Pero como cualquier otro sistema interconectado son objetivos potenciales para los ciberataques. Las intrusiones en las instalaciones pueden tener consecuencias de gran alcance para las organizaciones industriales.El ámbito de la ciberseguridad industrial está cada vez más presente en estos procesos y eso lleva a bordar medidas de seguridad en cuanto a la arquitectura de la red aplicando medidas de segmentación ,cortafuegos…

En el ámbito informático IT están más concienciados de programar de forma segura, pero en mundo industrial del PLC prima la operativa y que el sistema funcione de manera correcta.

En este caso nos vamos a centrar en las medidas que se pueden aplicar en el propio PLC desde el punto de vista de la programación para que dicha programación ya presente elementos de seguridad.Para ello vamos a utilizar el estudio realizado por [ISA Global Cybersecurity Alliance](https://isaautomation.isa.org/cybersecurity-alliance/?__hstc=16245038.eea9d694906b1b53d21c498b66594e22.1635937421002.1637133996604.1637741466758.3&__hssc=16245038.1.1637741466758&__hsfp=4274510458) en el que ha trabajado un grupo de expertos y el cual ha dado como resultado una **PLC Security Top 20 list** en la que se propone medidas de seguridad en la programación de PLC.Puedes encontrar dicha lista en <https://plc-security.com/index.html>

**En este reto tendrás que incorporar actividades de programación segura a la instalación automatizada en la cual estás trabajando actualmente dentro de tu ciclo formativo**.Incorporando dichas actividades generarás en el entorno del aula una concienciación sobre la necesidad de proteger las instalaciones industriales, te familiarizaras con terminología del mundo de la ciberseguridad y adquirirás conocimientos técnicos sobre cómo llevar a cabo dichas actividades.

 

| **Objetivos / Resultados de Aprendizaje** |
| --- |

TÉCNICOS

**-Ciclo Grado superior en Sistemas electrotécnicos y automatizados.**

Módulo profesional 0521 Técnicas y procesos en instalaciones domóticas y automáticas.

RA4. Implementa sistemas automáticos industriales, elaborando programas de control y configurando los parámetros de funcionamiento.

**-Ciclo Grado superior en Automatización y robótica industrial.**

Módulo profesional 0965 Sistemas programables avanzados.

RA3. Programa controladores lógicos, identificando la tipología de los datos del proceso y utilizando técnicas avanzadas de programación y parametrización.

RA4. Verifica el funcionamiento de los sistemas de control analógico programado, ajustando los dispositivos y aplicando normas de seguridad.

**-Ciclo Grado superior en Mecatrónica industrial.**

Módulo profesional 0943 Integración de sistemas.

RA2. Integra el PLC en el montaje de sistemas mecatrónicos de procesos discretos y continuos, conexionándolo, programándolo, comprobando y manteniendo su funcionamiento.Implementa sistemas automáticos industriales, elaborando programas de control y configurando los parámetros de funcionamiento.

**-Curso de especialización en Ciberseguridad en entornos de las tecnologías de operación.**

Módulo Profesional 2: Sistemas de control industrial seguros

RA2: Reconoce los dispositivos programables que intervienen en el control de sistemas dinámicos, sistemas de control de movimiento, identificando los componentes que los forman, identificando su funcionalidad y determinando sus aplicaciones en entornos industriales automatizados.

TRANSVERSALES ([Rúbricas](https://drive.google.com/file/d/1_Zt2z45TvpSIETja-Lstk92v75cg96ks/view?usp=sharing))

* Personal:
  + Autonomía
  + Implicación
  + Iniciativa emprendedora
* Comunicación:
  + Comunicación oral
  + Comunicación escrita
* Digital:
  + Alfabetización en información y datos
  + Comunicación y colaboración
  + Creación de contenidos digitales
  + Seguridad
  + Resolución de problemas
* Colaborativo:
  + Trabajo en equipo
  + Resolución de problemas
  + Toma de decisiones
  + 

| 1. **Tareas a realizar** |
| --- |

Incorpora estas actividades de programación segura al reto de automatización sobre el que estás trabajando:

* Identifica porqué están en peligro las instalaciones industriales y cuales son las situaciones de riesgo.
* Localiza y analiza artículos en los que se justifique la necesidad de realizar una programación segura en PLC
* Analiza las lista **PLC Security Top 20 list** y selecciona de la lista las 10 medidas que consideres más viables para aplicar en tu proyecto.
* De las 10 medidas seleccionadas implementa las que de una manera real y efectiva puedan ser integradas en tu programa de PLC.

| 1. **Criterios de evaluación** |
| --- |

* Competencias Técnicas 70 %
* Competencias Transversales 30 %

**Propuesta de evaluación**. Utilizar la hoja de evaluación para proyectos/retos que utilizas habitualmente incorporando los items relacionados con las actividades de ciberseguridad realizadas.

| **PROYECTO NªX** | **Curso: AR32** |  |
| --- | --- | --- |
| **CRITERIOS DE CORRECCIÓN DE PROYECTOS** | **Año : 202X/2X** |  |
| **Alumno :** | **Proyecto Nº :** |  |
| **VALORACIÓN DE COMPETENCIAS TÉCNICAS: ( 7 puntos )** | |  |
| Identifica porqué están en peligro las instalaciones industriales y cuales son las situaciones de riesgo. | |  |
| Localiza y analiza artículos en los que se justifique la necesidad de realizar una programación segura en PLC | |  |
| Analiza las lista PLC Security Top 20 list y selecciona de la lista las 10 medidas que consideres más viables para aplicar en tu proyecto | |  |
| Implementa las que de una manera real y efectiva las prácticas que puedan ser integradas en tu programa de PLC | |  |
| * Medida1 | |  |
| * Medida2 | |  |
| * Medida3 | |  |
|  | |  |
| **VALORACIÓN DE COMPETENCIAS TRANSVERSALES (3 puntos)** | |  |
| Personal: Autonomía ,Implicación , Iniciativa emprendedora . | |  |
| Comunicación: Comunicación oral, Comunicación escrita. | |  |
| Digital:Alfabetización en información y datos, Comunicación y colaboración, Creación de contenidos digitales, Seguridad y Resolución de problemas | |  |
| Colaborativo:Trabajo en equipo, Resolución de problemas, Toma de decisiones | |  |
| **Comp. Técnicas (7)** | |  |
| **Comp. Transversales (3)** | |  |
| **NOTA** | |  |

| 1. **Recursos** |
| --- |

* Centro Vasco de Ciberseguridad <https://www.basquecybersecurity.eus/es/>
* Centro de Ciberseguridad Industrial de Gipuzkoa <https://www.ziur.eus/es/>
* Industrias de Ciberseguridad del País Vasco. <https://www.cybasque.eus/>
* INCIBE Instituto nacional de Ciberseguridad <https://www.incibe.es/>
* CCI Centro de Ciberseguridad Industrial <https://www.cci-es.org/>
* Global Cybersecurity alliance
  + <https://isaautomation.isa.org/cybersecurity-alliance/>
  + <https://gca.isa.org/blog/the-top-20-secure-plc-coding-practices-project>
  + <https://plc-security.com/index.html>
* Bibliografía: <https://infolibros.org/libros-de-seguridad-informatica-gratis-pdf/>

| 1. **Temporalización** |
| --- |

| **Lunes** | **Martes** | **Miércoles** | **Jueves** | **Viernes** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |