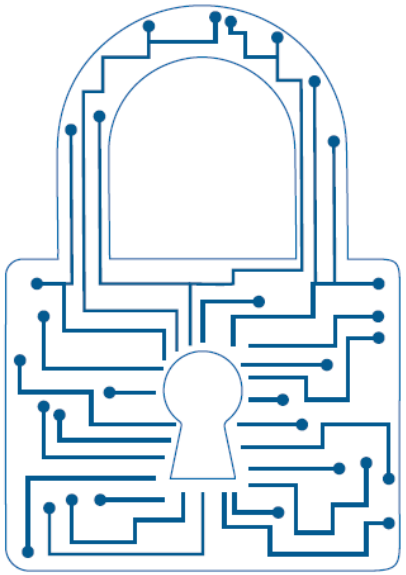
Cyber-IN en el aula

Cómo introducir la ciberseguridad industrial en FP paso a paso en especialidades relacionadas con la industria: informática, robótica…



Proyecto Erasmus+ Cyber-In
https://cyber-in.eu/

HETEL

maristak
Maristak Durango
Maristak Euskadi Fundazioa

Idea clave del proyecto

El proyecto NO busca formar especialistas en ciberseguridad industrial.

El objetivo es que el alumnado de automatización, informática, redes o robótica adquiera conocimientos básicos de ciberseguridad aplicados a su propia especialidad y comprenda los riesgos presentes en entornos industriales reales.

La ciberseguridad industrial debe entenderse como una competencia transversal dentro de los perfiles técnicos actuales.

Objetivo de la jornada

Integrar la ciberseguridad industrial de forma práctica y progresiva.

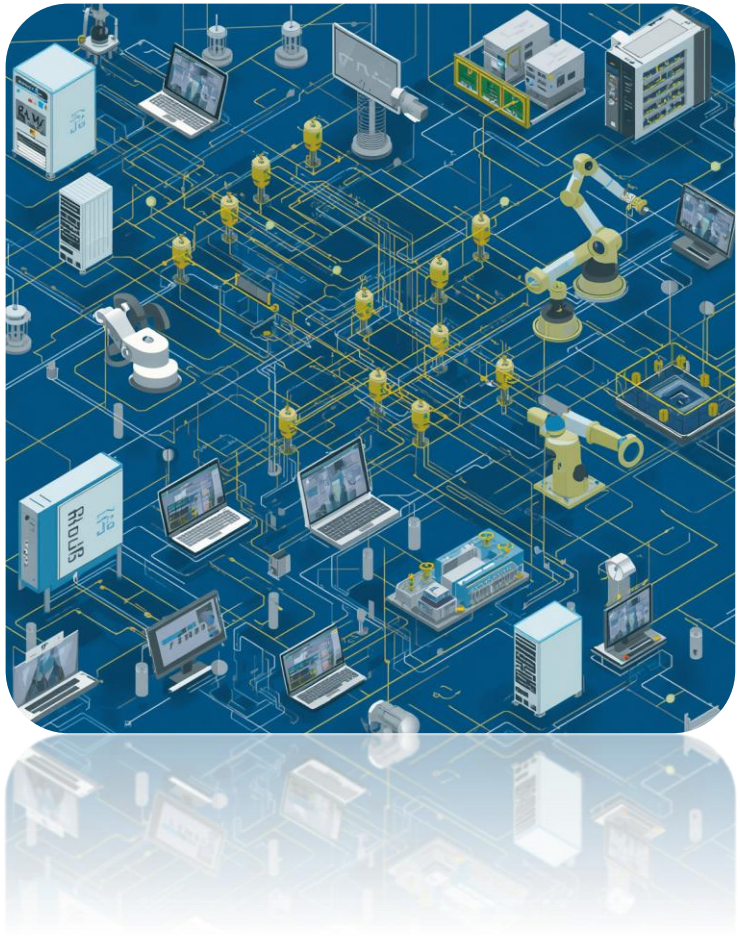
- Entender qué necesita saber un docente para empezar
- Diferenciar entre IT y OT
- Reconocer riesgos básicos en entornos industriales
- Identificar actividades fáciles de integrar en el aula
- Ver ejemplos reales para usar
- Entender cómo montar un laboratorio sencillo
- Descubrir recursos reutilizables

No hace falta ser experto en ciberseguridad industrial para empezar.

¿Por qué hablar de ciberseguridad industrial?

La industria ya está conectada:

- PLCs
- Robots
- Sensores
- HMIs
- SCADAs
- Redes industriales
- Monitorización remota
- …



Más conectividad = más superficie de ataque.

Casos reales

Un ataque en entornos industriales no solo afecta a dispositivos: puede generar consecuencias operativas y físicas críticas.

- **Stuxnet**: Sabotaje físico de centrifugadoras mediante manipulación de PLC.
- **Industroyer**: Interrupción de redes eléctricas usando protocolos industriales.
- **Colonial Pipeline**: Ransomware que paralizó un oleoducto crítico en EEUU.
- **Triton / Trisis**: Ataque a sistemas de seguridad (SIS) con riesgo de daño físico.
- **BlackEnergy**: Apagones reales en Ucrania tras comprometer SCADA.

Un ataque OT afecta al mundo físico.

¿Qué es OT?

OPERATIONAL TECHNOLOGY

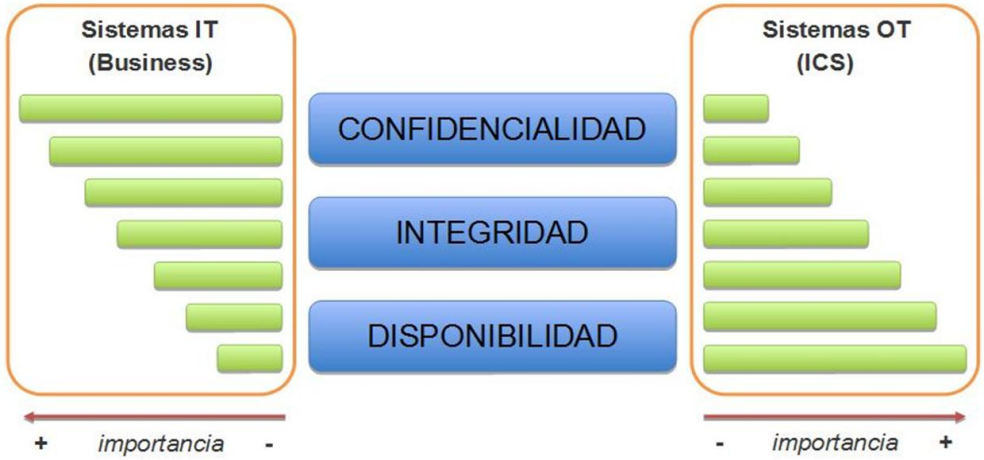
Sistemas y equipos que monitorizan y controlan procesos físicos industriales.

- PLCs, SCADA, RTUs, HMIs
- Robots, sensores, motores, válvulas
- Protocolos industriales: Modbus, OPC-UA, DNP3…
- Prioridad: **disponibilidad** y seguridad física

OT controla máquinas y procesos reales.

IT vs OT

Disponibilidad frente a confidencialidad.



En OT no siempre se puede parar y actualizar.

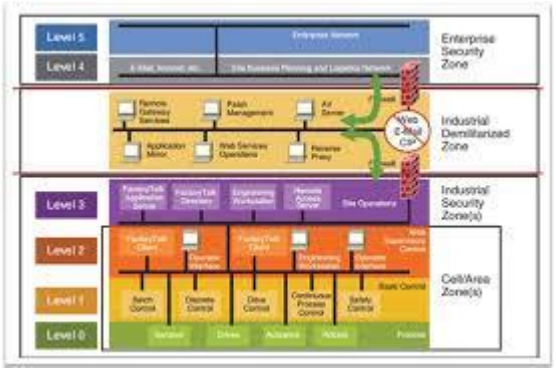
IT	OT
Servidores	PLCs
Datos	Procesos físicos
Confidencialidad	Disponibilidad
Reinicios frecuentes	Sistemas 24/7
Windows/Linux	Sistemas embebidos
Antivirus tradicional	Segmentación

Arquitectura

La arquitectura **Purdue** divide los sistemas industriales en niveles:

- Nivel 0: Sensores y actuadores
- Nivel 1: PLCs
- Nivel 2: HMI / SCADA
- Nivel 3: Supervisión OT
- Nivel 4: Sistemas IT

Flujo típico: Sensores → PLC → HMI/SCADA → MES/Historian → ERP(IT)



La segmentación entre niveles ayuda a proteger la red OT

Protocolos industriales

Protocolos OT comunes

- Modbus TCP
- Profinet
- Profibus
- OPC-UA
- DNP3

Riesgos habituales

Muchos protocolos industriales antiguos:

- NO cifran comunicaciones
- NO autentican usuarios
- NO validan identidad

Algunos PLCs pueden ejecutar comandos sin validar su origen.

Ejemplo: Modbus TCP

Uno de los protocolos OT más extendidos

- Utiliza el puerto 502
- Muy presente en PLCs y sistemas industriales
- Diseñado para comunicación rápida y sencilla

Problema principal. Muchos dispositivos Modbus TCP:

- NO cifran comunicaciones
- NO autentican usuarios
- Aceptan comandos directamente

Riesgo. Un acceso no autorizado puede:

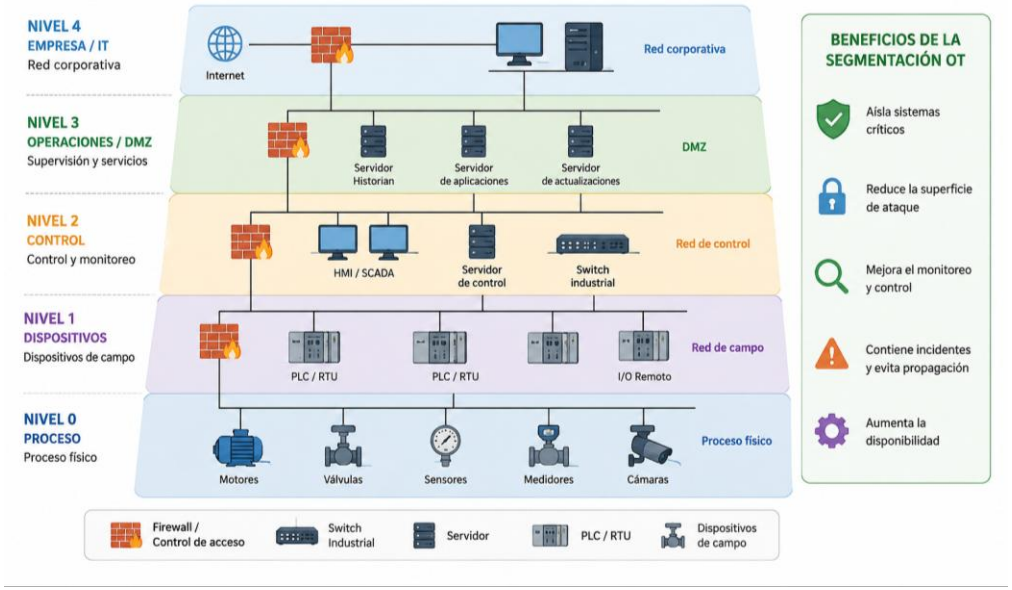
- Modificar variables de proceso
- Alterar la producción
- Afectar el funcionamiento del PLC

Diseñado para automatización, no para ciberseguridad.

¿Qué riesgos existen en OT?

Amenazas frecuentes

- Credenciales comprometidas
- PLCs expuestos a internet
- Malware y ransomware
- Accesos remotos inseguros
- Redes sin segmentación
- Errores humanos y malas configuraciones



La falta de segmentación aumenta significativamente el riesgo en entornos OT.

Regulación y normativa

Obligatorias (según sector y organización)

- Directiva NIS2: operadores esenciales y entidades críticas en la UE
- ENS: sector público y proveedores de ESP
- Cyber Resilience Act (CRA): fabricantes y productos conectados

Estándares de referencia

- IEC 62443: Referencia clave en seguridad industrial
- ISO 27001: Buenas prácticas en gestión de seguridad

Exigencias habituales

Gestión de riesgos, segmentación OT, control de accesos, monitorización y respuesta a incidentes, formación y concienciación.

La ciberseguridad OT es obligatoria.

Proyecto Cyber-IN

Objetivo: Integrar la ciberseguridad industrial en especialidades técnicas como: automatización, informática, redes, robótica…

Problema detectado:

- La ciberseguridad suele enseñarse principalmente desde el enfoque IT
- Existe poca formación específica en entornos OT
- Las empresas industriales demandan competencias básicas en ciberseguridad industrial

Propuesta Cyber-In:

- Aprendizaje basado en escenarios prácticos (retos)
- Actividades alineadas con entornos industriales reales

La ciberseguridad industrial debe enseñarse de forma transversal y conectada con el entorno técnico real.

Trabajo interdisciplinar

La ciberseguridad industrial requiere colaboración.
Los entornos industriales necesitan combinar conocimientos de:

- Informática y redes
- Automatización y control industrial

Problema habitual

- El alumnado de informática desconoce los sistemas OT
- Automatización y robótica suelen tener poca formación en IT y ciberseguridad

Objetivo
Fomentar el trabajo conjunto entre perfiles IT y OT mediante actividades y escenarios reales.

La seguridad industrial depende de la colaboración entre ambas disciplinas.

Metodología Cyber-IN

Aprendizaje basado en retos.

Los escenarios Cyber-IN plantean situaciones similares a las que pueden encontrarse en una industria real.

El alumnado trabaja mediante:

- Análisis e investigación
- Resolución de incidentes
- Identificación de riesgos
- Toma de decisiones
- Trabajo colaborativo entre perfiles técnicos

Aprender haciendo y resolviendo problemas reales.

Qué necesita saber el profesorado

NO es necesario ser especialista en ciberseguridad industrial.
Lo importante es entender:

- Cómo funciona una red OT
- Qué hacen los componentes OT (PLCs, HMIs, SCADA)
- Cómo se comunican los sistemas industriales
- Qué riesgos y amenazas existen
- Cómo detectar situaciones inseguras o anómalas

Competencias básicas recomendadas

- Informática y redes: IPs, puertos, Wireshark, firewalls y monitorización básica..
- Automatización y robótica: PLCs, sensores, variables, procesos, HMIs y SCADA.

Objetivo

Introducir la ciberseguridad industrial de forma práctica dentro de los módulos técnicos.

Entender los riesgos y enseñar buenas prácticas es suficiente para empezar.

Cómo empezar en el aula

Empieza utilizando elementos que el alumnado pueda identificar fácilmente en una arquitectura OT: PLC, HMI, SCADA, sensores, switch industrial, firewall…

Plantea preguntas sencillas:

- ¿Cómo se comunican?
- ¿Qué ocurriría si alguien accede al PLC?
- ¿Dónde debería existir segmentación?

Dinámica recomendada

1. Observar la arquitectura
2. Identificar equipos y comunicaciones
3. Detectar riesgos visibles
4. Aplicar medidas básicas de protección

Recurso práctico: Escenario interactivo Cyber-IN

Escenario 1: Chlorine Problems

Manipulación de variables de un PLC en una planta de tratamiento de agua.

Herramientas que pueden ser utilizadas

- Nmap: detección de puertos y servicios OT
- Wireshark: análisis de tráfico Modbus TCP
- Zabbix / Grafana: monitorización y alarmas
- QModMaster: lectura y modificación de variables Modbus
- OpenPLC: simulación de PLC industrial
- Vmware: virtualización del entorno

Qué aprende el alumnado

- Detectar puertos y servicios expuestos
- Analizar tráfico industrial
- Identificar manipulaciones en PLCs
- Monitorizar procesos industriales
- Aplicar segmentación y protección básica OT

Requisitos previos

- **redes y direcciones IP**
- **máquinas virtuales**
- **conceptos básicos de PLC y redes OT**
- **monitorización y análisis básico de red**

Escenario 2: Fake Operator

Uso no autorizado de una cuenta de operador en un entorno HMI/SCADA.

Herramientas que pueden ser utilizadas

- Nmap: detección de puertos y servicios OT
- Wireshark: análisis de tráfico Modbus TCP
- Zabbix / Grafana: monitorización y alarmas
- Cisco Packet Tracer: simulación de red y análisis de accesos
- HMI / SCADA virtual: análisis de accesos y registros
- Vmware: virtualización del entorno

Qué aprende el alumnado

- Analizar logs de acceso
- Detectar comportamientos sospechosos
- Identificar uso indebido de credenciales
- Configurar alarmas de seguridad
- Aplicar medidas como RBAC y MFA

Requisitos previos

- **redes y direcciones IP**
- **máquinas virtuales**
- **conceptos básicos de HMI/SCADA**
- **monitorización y análisis básico de red**

Escenario 3: Silent Virus

Tráfico anómalo y comportamiento similar a malware dentro de una red OT.

Herramientas que pueden ser utilizadas

- Nmap: detección de puertos y servicios OT
- Wireshark: análisis de tráfico Modbus TCP
- Zabbix / Grafana: monitorización y alarmas
- QModMaster: análisis de variables Modbus
- Cisco Packet Tracer: diseño y segmentación de red
- OpenPLC: simulación de PLC industrial
- Vmware: virtualización del entorno

Qué aprende el alumnado

- Detectar tráfico anómalo en OT
- Identificar sistemas comprometidos
- Configurar alarmas de monitorización
- Analizar comportamiento similar a malware
- Aplicar segmentación y aislamiento en redes OT

Requisitos previos

- **redes y direcciones IP**
- **máquinas virtuales**
- **conceptos básicos de PLC y redes OT**
- **monitorización y análisis básico de red**

¿Cómo introducirlo progresivamente?

1 NIVEL 1 SENSIBILIZACIÓN

OBJETIVO

Que el alumnado descubra que un PLC también puede ser vulnerable.

ACTIVIDADES

- Recursos interactivos
- Vídeos
- Casos reales
- Debate
- Identificación de riesgos

DURACIÓN
1 hora

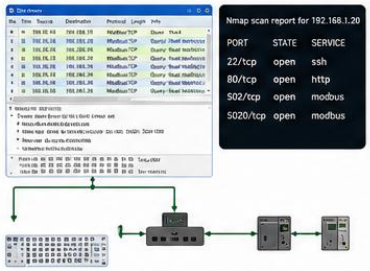
2 NIVEL 2 REDES Y ANÁLISIS BÁSICO

ACTIVIDADES SENCILLAS

- Detectar IPs
- Analizar tráfico
- Ver puertos abiertos
- Identificar dispositivos OT
- Capturar tráfico Modbus

HERRAMIENTAS

Wireshark · Nmap



3 NIVEL 3 PRIMER LABORATORIO OT

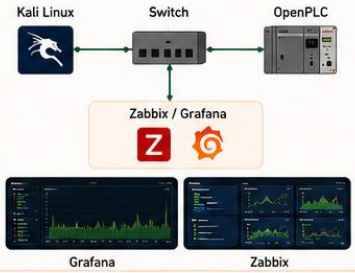
EL MOMENTO DONDE TODO COBRA SENTIDO

Con un pequeño laboratorio virtual el alumnado ya puede:

- ✓ Analizar tráfico real
- ✓ Detectar anomalías
- ✓ Comunicarse con un PLC
- ✓ Entender cómo funciona una red industrial

HERRAMIENTAS

OpenPLC · VMware · Kali Linux · Wireshark



4 NIVEL 4 ESCENARIOS COMPLETOS

ESCENARIOS CYBER-IN

- Investigación
- Monitorización
- Alarmas
- Firewall
- Segmentación
- Análisis de incidentes

RESULTADO
Simulación muy cercana a una empresa real.

SECUENCIA DIDÁCTICA PROPUESTA

1. **PRIMERA SESIÓN** — Sensibilización y escape room
2. **SEGUNDA SESIÓN** — Introducción a PLCs y tráfico industrial
3. **TERCERA SESIÓN** — Captura Wireshark y análisis de tráfico
4. **CUARTA SESIÓN** — Investigación del incidente
5. **QUINTA SESIÓN** — Medidas de protección y presentación final

OBJETIVO FINAL: Trabajar como si el alumnado fuese un equipo técnico real.

NO HACE FALTA EMPEZAR COMPLEJO

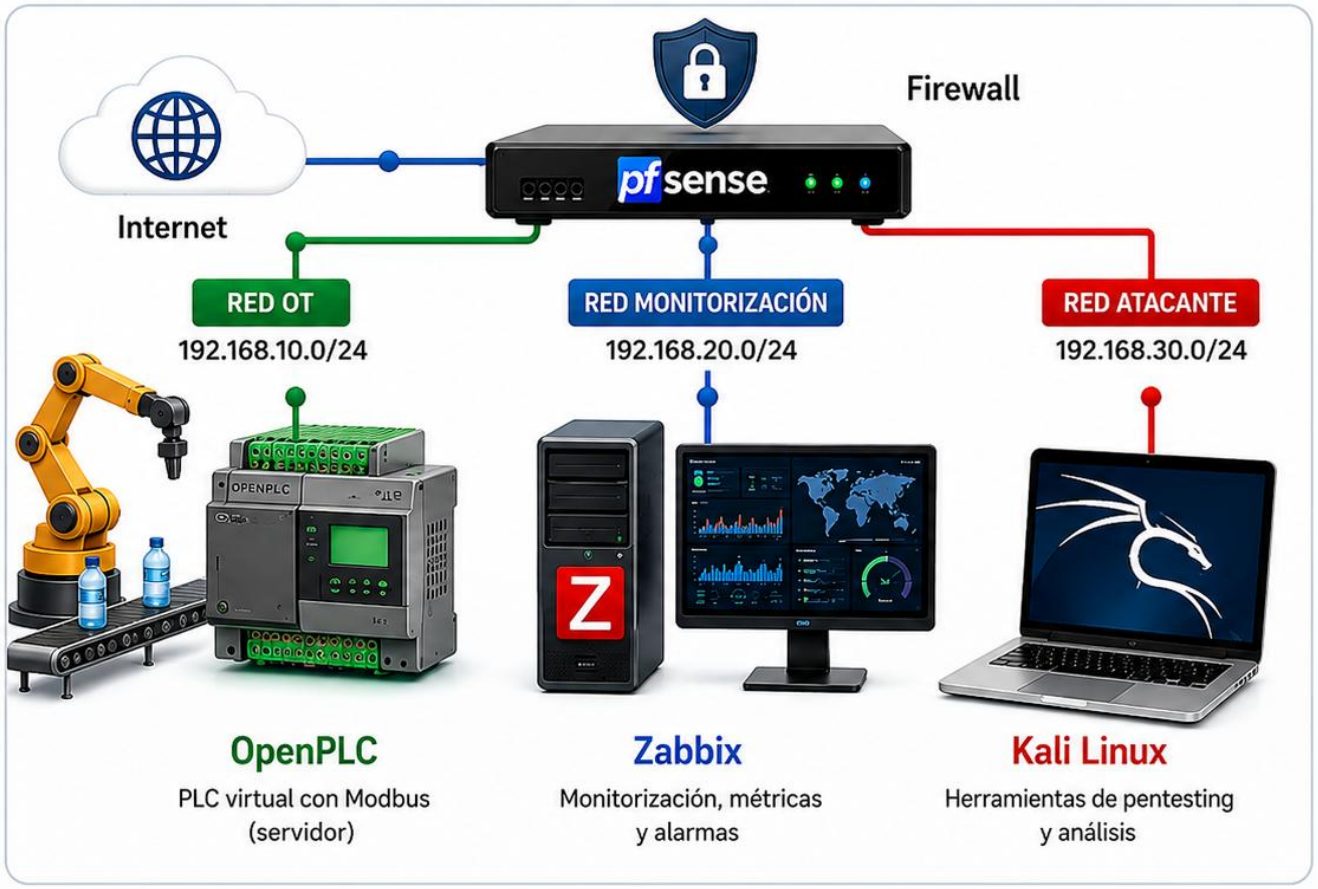
NIVEL INICIAL
- Wireshark básico
- Puertos
- IPs
- Logs

NIVEL MEDIO
- Modbus
- PLCs
- Alarmas

NIVEL AVANZADO
- Segmentación
- Respuesta a incidentes
- Diseño OT

Más conocimiento • Más herramientas • Más seguridad

Laboratorio OT sencillo



pfSense
Firewall y enrutamiento entre redes

OpenPLC
PLC virtual con Modbus (servidor)

Zabbix
Monitorización, métricas y alarmas

Kali Linux
Herramientas de pentesting y análisis

VMware
Plataforma de virtualización (todo el laboratorio)

Ejemplo de actividad práctica

Investigación guiada de un incidente OT.
El alumnado trabaja sobre un escenario industrial donde debe analizar y responder ante comportamientos anómalos en una red OT.

Actividades prácticas

- Escaneo del PLC mediante Nmap
- Identificación del puerto industrial 502 (Modbus TCP)
- Captura y análisis de tráfico Modbus
- Modificación controlada de variables del PLC
- Bloqueo de accesos mediante firewall

Entorno de trabajo

La práctica se realiza inicialmente en un entorno virtualizado, pero el objetivo ideal sería evolucionar posteriormente hacia laboratorios físicos con dispositivos reales.

Actividad basada en análisis, investigación y resolución de incidentes OT.

¿Qué necesita un centro?

Infraestructura mínima recomendada:

Hardware:

- PCs/portátiles convencionales
- Capacidad de virtualización

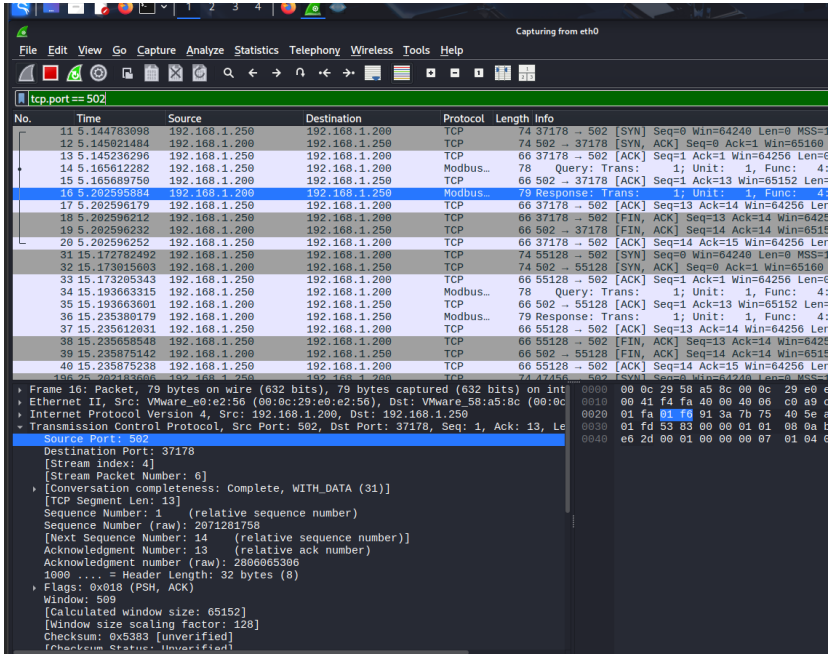
Software gratuito:

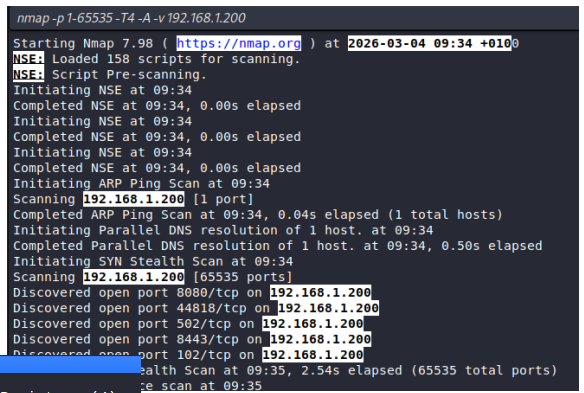
- OpenPLC
- Wireshark
- Nmap (Kali Linux)
- Zabbix
- QModMaster
- VMware
- pfSense

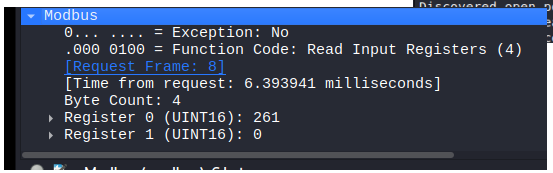
No es necesario disponer de un laboratorio industrial real para comenzar.
Los primeros escenarios y prácticas pueden realizarse completamente virtualizados.

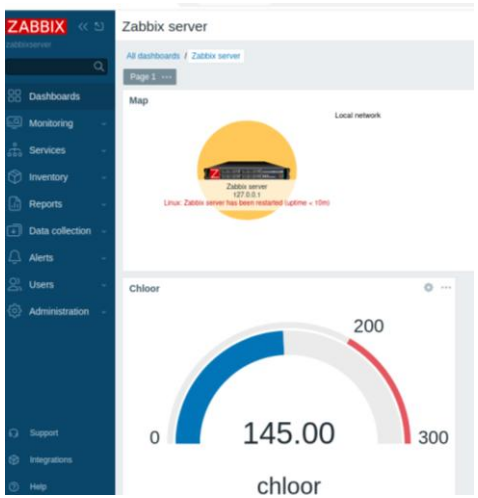
Resultado del alumnado (Escenario 1)

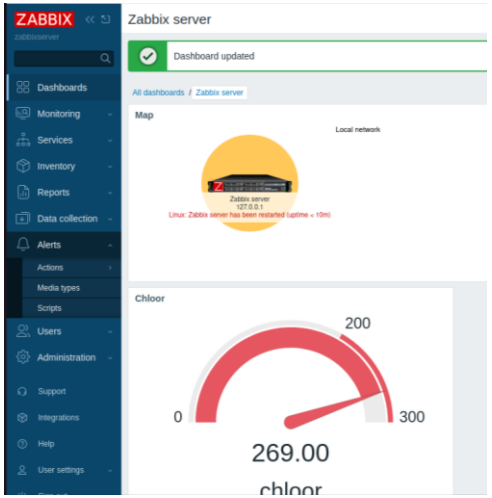
- Detección de puertos abiertos
- Análisis de tráfico industrial
- Comparación de datos reales y monitorizados
- Investigación de comportamiento anómalo
- Creación de alarmas y medidas de protección











Resultado del alumnado (Escenario 2)

- Análisis de logs de acceso HMI
- Identificación de IPs sospechosas
- Detección de patrones de login anómalos
- Investigación de posible robo de credenciales
- Propuesta de mejora mediante MFA y control de accesos

IP-adresses
Good:
- 192.168.1.210
- 192.168.1.211

Bad:
- 192.168.50.200
- 172.16.99.50
- 10.66.6.6

Timestamp	Local time	Value
2026-03-03 14:12:17		2026-03-03T15:12:17+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:15		2026-03-03T15:12:15+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:13		2026-03-03T15:12:13+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:12:11		2026-03-03T15:12:11+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:09		2026-03-03T15:12:09+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:07		2026-03-03T15:12:07+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:12:05		2026-03-03T15:12:05+01:00 user=operator1 src_ip=10.66.6.66 action=login_success
2026-03-03 14:12:03		2026-03-03T15:12:03+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:01		2026-03-03T15:12:01+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:11:59		2026-03-03T15:11:59+01:00 user=operator1 src_ip=172.16.99.50 action=hmi_change_setpoint
2026-03-03 14:11:59		2026-03-03T15:11:59+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:11:57		2026-03-03T15:11:57+01:00 user=operator1 src_ip=10.66.6.66 action=hmi_change_setpoint
2026-03-03 14:11:57		2026-03-03T15:11:56+01:00 user=operator1 src_ip=10.66.6.66 action=login_success
2026-03-03 14:11:55		2026-03-03T15:11:54+01:00 user=operator1 src_ip=192.168.50.200 action=hmi_change_setpoint
2026-03-03 14:11:55		2026-03-03T15:11:54+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:11:53		2026-03-03T15:11:52+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:11:51		2026-03-03T15:11:50+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:11:49		2026-03-03T15:11:48+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:11:46		2026-03-03T15:11:46+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:11:44		2026-03-03T15:11:44+01:00 user=operator1 src_ip=192.168.50.200 action=login_success

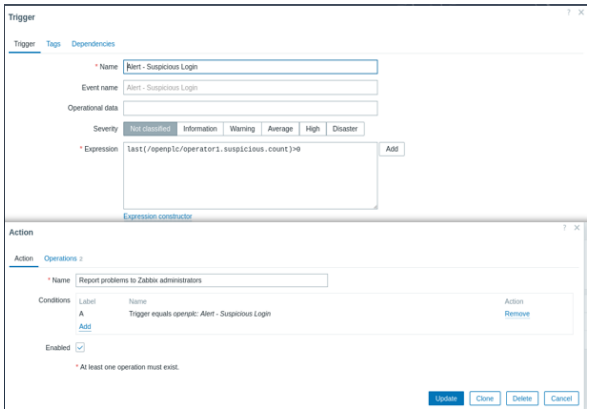
- Same account logging
- Distinct IP addresses
- Rapid succession

→

- Impossible travel
- Evade brute-force

2026-03-03 14:12:15	2026-03-03T15:12:15+01:00 user=operator1 src_ip=172.16.99.50 action=login_success
2026-03-03 14:12:13	2026-03-03T15:12:13+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:12:11	2026-03-03T15:12:11+01:00 user=operator1 src_ip=172.16.99.50 action=login_success

2026-03-03 14:12:07	2026-03-03T15:12:07+01:00 user=operator1 src_ip=192.168.50.200 action=login_success
2026-03-03 14:12:05	2026-03-03T15:12:05+01:00 user=operator1 src_ip=10.66.6.66 action=login_success
2026-03-03 14:12:03	2026-03-03T15:12:03+01:00 user=operator1 src_ip=172.16.99.50 action=login_success



¿Cómo encaja en informática?

Contenidos IT habituales	Aplicación en OT
Redes y direccionamiento	Redes industriales
Análisis de tráfico	Tráfico Modbus y protocolos OT
Monitorización	Supervisión de PLCs y procesos
Logs y eventos	Detección de anomalías OT
Firewalls y segmentación	Protección de redes industriales
Seguridad de sistemas	Protección de HMIs y SCADA
Hardware y dispositivos	PLCs, switches industriales y sensores

La base técnica es similar, pero aplicada a entornos industriales reales.

¿Cómo encaja en automatización y robótica?

Contenidos de automatización	Enfoque de ciberseguridad OT
PLCs y control industrial	Protección de PLCs
HMIs y SCADA	Accesos seguros y usuarios
Redes industriales	Segmentación y comunicaciones OT
Sensores y procesos	Detección de anomalías
Monitorización industrial	Alarmas y supervisión
Mantenimiento y operación	Buenas prácticas de seguridad
Contenidos de automatización	Enfoque de ciberseguridad OT

El objetivo no es enseñar hacking, sino incorporar la ciberseguridad dentro del entorno industrial real.

¿Cómo hacer proyectos interdisciplinares?

Informática / Redes	Automatización / Robótica
Monitorización de red	Programación de PLC
Análisis de tráfico	Supervisión del proceso
Segmentación y firewall	Configuración de variables
Detección de accesos	Detección de anomalías
Gestión de alertas	Validación del proceso industrial
Informática / Redes	Automatización / Robótica
Monitorización de red	Programación de PLC

Trabajo colaborativo IT + OT mediante escenarios industriales realistas.

Recursos Cyber-IN

Recursos online: https://cyber-in.eu/learningresources/

Cursos Online

Incluyen:

- Formación técnica
- Materiales docentes
- Recursos reutilizables
- Apoyo para profesorado

Recursos reutilizables

- Escenarios
- Máquinas virtuales (VMs)
- Guías
- Laboratorios
- Materiales de apoyo
- Cursos online

Objetivo: reducir las barreras de entrada a la formación en ciberseguridad industrial y facilitar la adopción de recursos educativos prácticos.

Recomendaciones

Recomendación	Aplicación en el aula
Empezar poco a poco	No intentar montar un SOC industrial completo
Usar pocos elementos	OpenPLC, Wireshark, una VM y un escenario sencillo
Priorizar actividades visuales	Tráfico real, capturas y comportamiento del PLC
Trabajar en equipo	Colaboración entre informática y automatización

La ciberseguridad industrial es necesaria.
No es solo para especialistas.
Puede integrarse progresivamente en el aula.
IT y OT deben colaborar.

Debate

¿Dónde veis oportunidades para introducir la ciberseguridad OT en vuestro centro?

¿Qué barreras o dificultades pueden aparecer?

¿Qué actividades prácticas serían más fáciles de implementar?

¿Cómo podría trabajarse la colaboración entre IT y OT?

El objetivo es identificar primeros pasos realistas para empezar en el aula.

La ciberseguridad industrial forma parte de la realidad de las empresas y, por tanto, también debe formar parte de la formación de nuestro alumnado.

Cyber-In propone una forma práctica, progresiva y accesible de introducir estos conocimientos en el aula, fomentando la colaboración entre informática y automatización y ayudando al alumnado a entender los riesgos reales de los entornos industriales actuales.

Eskerrik asko!