CÓDIGO VIGÍA · GUÍA DE CONCEPTOS

Ciberataques en entornos industriales

Y los riesgos de usar IA en pruebas de seguridad. Todo lo que vimos en la conferencia, explicado desde cero: IT y OT, PLC y HMI, ARP, Modbus, el ataque de hombre en el medio, cómo prevenirlo y qué cambia cuando una IA hace el pentest.

01 Lo esencial en una página
02 IT y OT
03 PLC, HMI, SCADA y el modelo Purdue
04 Redes: IP, MAC, subred y puerta de enlace
05 ARP: cómo funciona y por qué es débil
06 El ataque de hombre en el medio
07 Modbus TCP
08 Otros protocolos industriales
09 La demo: lo que viste
10 Cómo se detecta y cómo se previene
11 IA en pruebas de seguridad
12 Casos reales
13 Glosario
14 Para seguir aprendiendo

Material de la conferencia · Asociación Sinaloense de Ciberseguridad · 5 de noviembre de 2026
Código Vigía · Servicios de ciberseguridad y formación

01 Lo esencial en una página

Si solo lees una página, que sea esta.

Concepto	En una frase
IT	Tecnología que crea, guarda y mueve **datos**. Su prioridad es la confidencialidad.
OT	Tecnología que **monitorea y controla procesos físicos**. Su prioridad es que el proceso siga funcionando y que nadie salga lastimado.
PLC	Computadora industrial que lee sensores, ejecuta una lógica y mueve actuadores, en un ciclo de milisegundos.
HMI	*Human-Machine Interface*: la pantalla del operador. Lee del PLC y le manda órdenes.
SCADA	Tipo de sistema que supervisa muchos PLC, guarda históricos y maneja alarmas.
ARP	Traduce una IP a una MAC dentro de la red local. No tiene autenticación: cualquiera puede responder.
ARP spoofing	Enviar respuestas ARP falsas para que otros equipos asocien una IP ajena a **la MAC del atacante**.
Hombre en el medio	El atacante se coloca entre dos equipos que creen hablar directo: puede escuchar, alterar o cortar la conversación.
Modbus TCP	Protocolo industrial de 1979, puerto 502, **sin cifrado ni autenticación**.
Agente de IA	Una IA que no solo sugiere: ejecuta herramientas por su cuenta. En OT, «probar» un fallo es actuar sobre equipos físicos.

> **Tres ideas para llevarte**
>
> 1. En IT un error borra un archivo; en OT puede abrir una válvula.
> 2. La HMI no ve la planta: ve lo que la red le dice.
> 3. Una IA sin límites no es un pentester más rápido: es un accidente más rápido.

02 IT y OT

IT (Information Technology, Tecnología de la Información): hardware, software y redes para crear, guardar, procesar e intercambiar datos. Correo, ERP, bases de datos, servidores, nube.

OT (Operational Technology, Tecnología de Operación): hardware y software que monitorea y controla equipos y procesos físicos. Bombas, válvulas, motores, hornos, subestaciones, plantas de agua. Ejemplos cercanos: ingenios azucareros, plantas de tratamiento de agua, empacadoras, sistemas de riego, subestaciones eléctricas.

Términos relacionados: **ICS** (Industrial Control Systems, el conjunto de sistemas de control industrial) y **DCS** (Distributed Control System, típico de plantas químicas y refinerías).

Aspecto	IT	OT
Prioridad	Confidencialidad → integridad → disponibilidad	Disponibilidad y seguridad física primero
Vida útil	3 a 5 años	15 a 30 años o más
Parches	Frecuentes y automáticos	Raros: hay que detener la planta, probar y certificar
Si falla	Pérdida de datos, dinero, reputación	Daño físico, ambiental o a personas
Protocolos	El cifrado ya es normal: HTTPS, SSH, VPN	Modbus, DNP3, Profinet: muchos nacieron sin cifrado ni autenticación
Tiempo	Tolera retrasos	Respuestas en milisegundos
Escaneos	Rutina	Un escaneo agresivo puede colgar un PLC antiguo

Convergencia IT/OT: conectar la planta con la red corporativa para tener datos en tiempo real. Trae eficiencia y mantenimiento predictivo, pero también abre un camino desde la red de oficina, o desde internet, hasta la planta.

> **¿Por qué no se protegen igual?**
> En IT, si hay duda, se apaga el servidor y se investiga. En OT, apagar puede ser justo lo peligroso: un reactor, una caldera o una línea de producción no se detienen con un clic. Por eso en OT la disponibilidad va primero.

03 PLC, HMI, SCADA y el modelo Purdue

PLC: Controlador Lógico Programable

Computadora industrial robusta (aguanta calor, polvo y vibración) que repite sin parar su **ciclo de escaneo**:

1. **Leer entradas:** sensores de nivel, presión, temperatura.
2. **Ejecutar la lógica:** el programa. Ejemplo: «si el nivel supera 80 %, cierra la válvula de entrada».
3. **Escribir salidas:** abrir o cerrar válvulas, arrancar bombas o motores.

Se programa con los lenguajes de la norma **IEC 61131-3**, sobre todo **Ladder** (diagrama de escalera). Marcas comunes: Siemens, Allen-Bradley, Schneider, Mitsubishi, Omron. **OpenPLC** es un PLC de código abierto, ideal para practicar.

Dato importante: el PLC también es un **servidor en la red**. Responde a quien le pregunta y, con muchos protocolos, obedece a quien le escribe.

HMI: Interfaz Humano-Máquina

La pantalla del operador. Hace dos cosas: **lee** (pide al PLC valores cada segundo para dibujar tanques, niveles y alarmas) y **escribe** (cada botón que el operador presiona es una orden al PLC). Un ejemplo de código abierto es **Scada-LTS**.

> **La idea clave**
>
> La HMI no ve la planta: ve lo que el PLC le dice por la red. Si alguien se mete en medio, puede ver lo mismo que el operador... o mostrarle algo falso.

SCADA y otras piezas

- **SCADA** (Supervisory Control and Data Acquisition): tipo de sistema que supervisa muchos PLC o RTU, a veces en sitios lejanos (ductos, redes eléctricas, agua). Incluye HMI, servidores, históricos y alarmas.
- **RTU** (Remote Terminal Unit): parecido a un PLC, pensado para sitios remotos.
- **Historiador:** base de datos que guarda los valores del proceso en el tiempo.
- **Estación de ingeniería:** donde se programa el PLC y se configura la HMI. Es un blanco muy valioso.
- **SIS** (Safety Instrumented System): sistema de seguridad independiente que detiene la planta si algo se sale de control.

El modelo Purdue: la planta por niveles

Nivel	Nombre	Qué vive ahí
4 – 5	Empresa (IT)	ERP, correo, internet
3.5	DMZ industrial	Frontera controlada entre IT y OT
3	Operaciones del sitio	Historiadores, servidores SCADA
2	Supervisión	HMI, estación de ingeniería
1	Control básico	PLC, RTU
0	Proceso físico	Sensores, actuadores, la planta

La idea de seguridad: cada nivel habla solo con sus vecinos, y entre IT y OT hay una zona intermedia (DMZ). Si un atacante llega al nivel 2, ya comparte red con la HMI. La norma de referencia para segmentar es **IEC 62443** (zonas y conductos).

04 Redes: lo mínimo para entender el ataque

Término	Explicación sencilla
Dirección IP	Capa 3, lógica. Dice *a quién* va el mensaje. Se configura. Ej.: 192.168.90.107.
Dirección MAC	Capa 2, física. Identifica la tarjeta de red. Ej.: `fe:bf:36:b4:57:9e`. El switch entrega los paquetes por MAC.
Subred	Qué direcciones están «en mi misma red». Con máscara 255.255.255.0, todo 192.168.90.x es local.
Puerta de enlace	El router: a él se manda todo lo que va a otra subred.
Broadcast	Mensaje a todos los equipos del segmento (MAC destino `ff:ff:ff:ff:ff:ff`).
Switch	Conecta equipos de la misma red local y reenvía según la MAC.
Puerto TCP	La «puerta» de un servicio dentro de un equipo. Modbus = 502, web = 80/443.

> **Una analogía**
>
> La IP es el nombre y el departamento del destinatario; la MAC es el número de la puerta en el pasillo. Para entregar dentro del edificio (red local) necesitas la puerta. Para mandar a otro edificio (otra subred), se lo das al mensajero de la entrada (el router).

05 ARP: cómo funciona y por qué es débil

ARP (Address Resolution Protocol, RFC 826, 1982) resuelve la pregunta «¿qué MAC tiene esta IP?» dentro de la red local.

1. **Petición, a todos:** «¿Quién tiene 192.168.90.1? Avísale a 192.168.90.107».
2. **Respuesta, directa:** «192.168.90.1 está en 1a:e1:48:7b:6b:9e».
3. **Caché ARP:** el equipo guarda el par IP → MAC unos segundos o minutos y lo usa para enviar directo.

ARP gratuito: un equipo anuncia su propio par IP → MAC sin que nadie pregunte (por ejemplo, al arrancar). Es legítimo, y por eso los equipos aceptan respuestas que no pidieron.

Por qué es tan fácil de engañar

- No tiene **autenticación**: nada prueba quién responde.
- Los equipos aceptan **respuestas que nunca pidieron**.
- La **última respuesta gana**: sobrescribe la entrada anterior.
- Se diseñó en los años 80 para redes pequeñas y de confianza.

Mira tu propia tabla ARP

```
# Windows o Linux
arp -a
# Linux moderno
ip neigh
```

Señal de alerta: **dos IP distintas con la misma MAC**, o la MAC de tu puerta de enlace que cambia de repente.

06 El ataque de hombre en el medio

Hombre en el medio (MITM, Man-in-the-Middle; también AitM, Adversary-in-the-Middle): el atacante se coloca entre dos equipos que creen hablar directamente. Puede **escuchar** (confidencialidad), **alterar** (integridad) o **cortar** (disponibilidad). Hay muchas formas de lograrlo: Wi-Fi falso, DNS, proxies. En redes industriales planas, la más clásica es el **envenenamiento ARP** (ARP spoofing).

El envenenamiento ARP en cuatro pasos

1. **Estar en la red:** el atacante necesita estar en el mismo segmento que la víctima (mismo switch o VLAN). Esta es la barrera real.
2. **Mentir con ARP:** envía respuestas falsas («la IP de la HMI está en mi MAC»), una y otra vez para que la mentira no caduque.
3. **Reenviar:** pasa cada paquete a su destino real. Si no lo hiciera, la comunicación se cortaría y el ataque se notaría.
4. **Observar o modificar** todo el tráfico que ahora pasa por él.

> **Ojo con un error común**
>
> El atacante **no se roba la IP** de nadie. Lo que hace es convencer a otros equipos de que esa IP está en *su* tarjeta de red.

Un sentido o los dos

El engaño puede hacerse en un solo sentido (por ejemplo, convencer al router de que el atacante es la HMI: así ve lo que llega a la HMI) o en los dos (engañar también a la HMI: así ve lo que entra y lo que sale). En el video de la conferencia se engañó un solo sentido, por eso se veían las respuestas del PLC hacia la HMI.

Herramientas conocidas para laboratorio: `arpspoof` (paquete dsniff), Ettercap y Bettercap; para analizar tráfico, **Wireshark**.

> **Solo en laboratorio**
>
> Interceptar tráfico en una red sin autorización es ilegal. Practica únicamente en entornos propios o con permiso por escrito.

07 Modbus TCP

Modbus lo creó Modicon (hoy Schneider Electric) en **1979** para comunicar PLC por cable serial. **Modbus TCP** lo lleva a Ethernet en el **puerto 502**. Es abierto y simple, por eso está en todas partes. Funciona como **cliente/servidor**: la HMI pregunta y ordena; el PLC responde.

Los cuatro tipos de dato

Tipo	Tamaño	Acceso	Ejemplo en planta
Coils	1 bit	Lectura y escritura	Encender o apagar una bomba; un botón START
Discrete Inputs	1 bit	Solo lectura	Un interruptor de nivel alto
Input Registers	16 bits	Solo lectura	Nivel, presión, flujo medidos
Holding Registers	16 bits	Lectura y escritura	Puntos de ajuste (setpoints)

Códigos de función más comunes

Código	Nombre	Qué hace
01	Read Coils	Lee bits de encendido/apagado
02	Read Discrete Inputs	Lee entradas digitales
03	Read Holding Registers	Lee registros de lectura/escritura
04	Read Input Registers	Lee mediciones
05	Write Single Coil	Escribe un bit: `FF00` = encender, `0000` = apagar
06	Write Single Register	Escribe un registro (por ejemplo, cambiar un setpoint)
15 / 16	Write Multiple Coils / Registers	Escribe varios a la vez

Cada mensaje lleva un encabezado **MBAP** de 7 bytes (identificador de transacción, protocolo, longitud y unidad) seguido del código de función y los datos. Si el PLC no puede cumplir una petición, responde con una **excepción** (el código de función + 0x80).

Por qué es inseguro

- **Sin cifrado:** todo viaja en texto claro; cualquiera en medio lee los valores.
- **Sin autenticación:** el PLC obedece a cualquiera que le escriba.
- **Sin integridad:** nada impide modificar un paquete en el camino.

Existe una versión segura, **Modbus/TCP Security** (con TLS, puerto 802), pero pocos equipos la soportan.

Filtros de Wireshark para practicar

```
modbus                          # todo el tráfico Modbus
tcp.port == 502                 # por puerto
modbus.func_code == 5           # solo escrituras de un coil
arp                             # tráfico ARP
arp.duplicate-address-detected # IP duplicadas: señal de spoofing
```

08 Otros protocolos industriales

Protocolo	Puerto	Dónde se usa
Modbus TCP	TCP 502	En todas partes; el más común y el más simple
DNP3	TCP 20000	Sector eléctrico y agua; tiene una extensión de autenticación
IEC 60870-5-104	TCP 2404	Redes eléctricas
IEC 61850	Varios	Automatización de subestaciones
EtherNet/IP (CIP)	TCP 44818	Equipos Rockwell / Allen-Bradley
PROFINET	Mayormente capa 2	Equipos Siemens, tiempo real
S7comm	TCP 102	PLC Siemens S7
BACnet	UDP 47808	Edificios: aire acondicionado, accesos
OPC UA	TCP 4840	Moderno: sí soporta cifrado y autenticación

09 La demo: lo que viste

La demostración usó **GRFICSv3** de Fortiphyd Logic, un laboratorio abierto que simula una planta química en contenedores Docker. El proceso se basa en el **Tennessee Eastman**, un proceso químico clásico que se usa en investigación de control.

Equipo	IP	Rol
Atacante (Kali Linux)	192.168.90.6	Hace el envenenamiento ARP y captura el tráfico
HMI (Scada-LTS)	192.168.90.107	Pantalla del operador, en el puerto 8080
PLC (OpenPLC)	192.168.95.2	Controla la planta; habla Modbus en el puerto 502
Router / firewall	Ambas redes	Une la red de la HMI con la del PLC

#	Lo que pasó	Lo que significa
1	El atacante revisa su IP	Ya está dentro de la red de la HMI
2	Lanza `arpspoof` con la IP de la HMI	Anuncia a la red que la IP de la HMI está en su MAC
3	Abre Wireshark, filtro `arp`	Se ven las respuestas falsas repetidas sin parar
4	Filtro `modbus`	Respuestas del PLC: lecturas de coils (función 1) y de registros (función 4)
5	Detalle de los registros	Los valores del proceso viajan en texto claro
6	El operador hace clic en la HMI	El proceso pasa de RUNNING a STOPPED y viceversa
7	`Write Single Coil`, coil 40, `FF00`	El clic del operador, visible para el atacante. Lo que se puede leer, se puede modificar

> **¿Y cómo entra un atacante a la red de planta?**
>
> El video asume que ya está dentro. En la vida real los caminos más comunes son: phishing a alguien de IT que luego salta a OT, accesos remotos de proveedores mal protegidos, una laptop de mantenimiento infectada, un puerto de red libre en planta o equipos industriales expuestos a internet.

10 Cómo se detecta y cómo se previene

Cómo se detecta

- Dos IP con la misma MAC en `arp -a`.
- La MAC de la puerta de enlace que cambia.
- Muchísimas respuestas ARP no solicitadas.
- Wireshark avisa «duplicate use of IP detected».
- Herramientas como **arpwatch**.
- Sensores pasivos de red: **Zeek**, Suricata, Snort o plataformas especializadas en OT.
- Alertas de **escrituras Modbus inesperadas** (funciones 05, 06, 15, 16 desde un equipo que no es la HMI).

Cómo se previene

- **Segmentar** la red (IEC 62443) y separar IT de OT con una DMZ.
- **Inspección dinámica de ARP** (DAI) en los switches: valida cada mensaje ARP contra una tabla confiable.
- **Entradas ARP estáticas** en equipos críticos.
- **Seguridad de puerto y 802.1X:** solo equipos conocidos se conectan.
- **Cifrar y autenticar** donde se pueda: Modbus/TCP Security, OPC UA, VPN entre zonas.
- **Seguridad física:** gabinetes cerrados y puertos deshabilitados.
- **Firewalls industriales** que solo permitan escribir al PLC desde la HMI.

Ninguna medida basta sola: se combinan en capas. En OT muchas veces no se puede cifrar porque los equipos son antiguos, así que la segmentación y el monitoreo pesan más.

11 IA en pruebas de seguridad

Chatbot o agente: un chatbot te sugiere un comando y tú decides si lo ejecutas. Un **agente de IA** tiene herramientas reales (terminal, escáneres, scripts) y trabaja en ciclo: observa, decide, actúa y evalúa, sin pausa. Para un pentester es muy poderoso, y por eso mismo es peligroso sin límites.

Seis riesgos de dejar que una IA hackee libremente en OT

1. **Escaneos que tumban equipos:** un barrido agresivo puede colgar un PLC antiguo y detener la línea.
2. **«Probar» es actuar:** validar un fallo de Modbus es escribir un coil; una bomba real se apaga.
3. **No entiende la física:** no sabe que una válvula alimenta un reactor ni qué pasa si se cierra.
4. **Se sale del alcance:** si encuentra un camino hacia producción, lo sigue para cumplir su objetivo.
5. **Alucina y exagera:** puede reportar fallos o credenciales que no existen y actuar sobre datos falsos.
6. **Velocidad sin freno:** cientos de acciones por minuto; cuando un humano lo nota, el daño ya ocurrió.

Dos casos reales (ninguno en OT, pero ilustran el riesgo)

Caso	Qué pasó	Lección
Replit, julio 2025	Un agente de programación borró la base de datos en producción de una empresa durante un congelamiento de código, pese a instrucciones explícitas de no tocar nada, y generó datos falsos.	Una instrucción no es un control
Reporte de Anthropic, noviembre 2025	Atacantes usaron un agente de IA contra unas 30 organizaciones, entre ellas empresas químicas. La IA realizó entre 80 y 90 % del trabajo táctico, y también exageró hallazgos e inventó credenciales que no funcionaban.	La IA ya encadena ataques casi sola, y se equivoca

Ocho reglas para usar IA en un pentest

1. **Alcance escrito** y lista blanca de IP: lo que no está en la lista, no se toca.
2. **Humano en el ciclo:** toda acción que escriba o explote requiere aprobación.
3. **Solo lectura en OT:** sin funciones de escritura (05, 06, 15, 16).
4. **Laboratorio o gemelo digital** primero, nunca producción.
5. **Herramientas y velocidad limitadas:** nada de escaneos masivos.
6. **Botón de paro** y operador de planta presente durante las pruebas.
7. **Registro completo** de cada acción del agente.
8. **Verificar cada hallazgo** antes de reportarlo.

Los límites se ponen en la herramienta (permisos, firewall, bloqueo de funciones de escritura), no solo en las instrucciones. La responsabilidad legal y ética siempre es del pentester.

Lo que recomiendan las agencias

En diciembre de 2025, CISA y agencias de Australia, Reino Unido, Canadá, Alemania, Países Bajos y Nueva Zelanda publicaron *Principles for the Secure Integration of AI in OT*, con cuatro principios: **1)**

entender la IA y sus riesgos, **2)** justificar su uso, **3)** gobernanza y pruebas, **4)** supervisión humana y mecanismos a prueba de fallas.

12 Casos reales de ciberataques industriales

Caso	Qué pasó	Qué enseña
Stuxnet (descubierto en 2010)	Malware contra la planta de enriquecimiento de Natanz, Irán. Alteraba PLC Siemens que controlaban centrífugas mientras mostraba a los operadores lecturas normales.	La pantalla del operador puede mentir
Ucrania (diciembre 2015)	Ataque a tres distribuidoras eléctricas: unos 225,000 clientes sin luz durante horas. Los atacantes entraron por phishing y operaron las HMI a distancia.	De la red de oficina a la planta
Industroyer (2016)	Apagón en Kiev con malware que hablaba directamente protocolos eléctricos.	Protocolos industriales sin autenticación
Triton (2017)	Ataque al sistema de seguridad (SIS) de una petroquímica en Arabia Saudita; buscaba desactivar la protección que evita accidentes.	En OT el riesgo es físico y humano
Colonial Pipeline (mayo 2021)	Ransomware en la red de IT. La empresa detuvo el oleoducto por precaución durante varios días y hubo desabasto de combustible en el este de EE. UU.	Un incidente de IT puede detener la operación

13 Glosario

Término	Significado
ARP	Address Resolution Protocol: traduce IP a MAC en la red local
Coil	En Modbus, un bit de encendido/apagado
DAI	Dynamic ARP Inspection: el switch valida cada mensaje ARP
DCS	Distributed Control System: control distribuido en plantas de proceso
DMZ industrial	Zona intermedia entre la red de IT y la de OT
Estación de ingeniería	Computadora donde se programa el PLC
Gemelo digital	Réplica virtual de una planta para probar sin riesgo
HMI	Human-Machine Interface: la pantalla del operador
ICS	Industrial Control Systems: sistemas de control industrial
IEC 62443	Familia de normas de ciberseguridad industrial
MITM	Man-in-the-Middle: ataque de hombre en el medio
Modbus	Protocolo industrial de 1979, sin cifrado ni autenticación
OT	Operational Technology: tecnología que controla procesos físicos
PLC	Programmable Logic Controller: controlador lógico programable
Registro	En Modbus, un número de 16 bits (nivel, presión, setpoint)
RTU	Remote Terminal Unit: controlador para sitios remotos
SCADA	Supervisory Control and Data Acquisition: sistema de supervisión
Setpoint	Punto de ajuste: el valor objetivo de una variable
SIS	Safety Instrumented System: sistema que detiene la planta ante un peligro
Spoofing	Suplantación: hacerse pasar por otro equipo

14 Para seguir aprendiendo

Recurso	Para qué sirve
GRFICSv3 (Fortiphyd Logic)	El laboratorio de la demo. Gratis, con Docker: planta simulada, PLC, HMI y atacante
«How ARP Spoofing Exposes OT Traffic»	El video original de la demostración
OpenPLC	PLC de código abierto para aprender a programar y atacar en laboratorio
Wireshark	Analizar tráfico de red, incluidos ARP y Modbus
MITRE ATT&CK for ICS	Catálogo de técnicas de ataque contra sistemas industriales
NIST SP 800-82 Rev. 3	Guía de seguridad para OT
CISA: sistemas de control industrial	Alertas y guías sobre vulnerabilidades en ICS
Principles for the Secure Integration of AI in OT	La guía de CISA y aliados sobre IA en OT (diciembre 2025)

Practica con ética

Todo lo de esta guía es para aprender y defender. Usa laboratorios propios como GRFICS. Interceptar tráfico, escanear o explotar sistemas sin autorización por escrito es ilegal, y en entornos industriales puede poner vidas en riesgo.

Código Vigía

Servicios de ciberseguridad y formación.
[Sitio web] · [Correo de contacto] · [Redes sociales]

Fuentes de los casos de IA: OECD.AI, incidente Replit · The Register, reporte de Anthropic. Los datos técnicos de Modbus, ARP, el modelo Purdue y los casos históricos son conocimiento técnico general; los datos de la demo provienen del video de Fortiphyd Logic.