

# Ciberseguridad en Ambientes Industriales: Desafíos y Aportes



Jorge Kamlofsky – José Castro Tramontina – Daniel Manrique

Imagen obtenida de: <https://revistaenergia.pe/operacion-de-los-sistemas-electricos-post-covid-19/>

Ekoparty 2025 – Secure OT Village

## En esta presentación

- **Introducción**
- **Los Sistemas de Control Industrial**
- **Desafíos Planteados por Industria 4.0**
- **Gestión de la Ciberseguridad en ICSs**
- **Herramientas para Mejora de la Ciberseguridad en ICSs**
- **Resumen y Conclusiones**

## En esta presentación

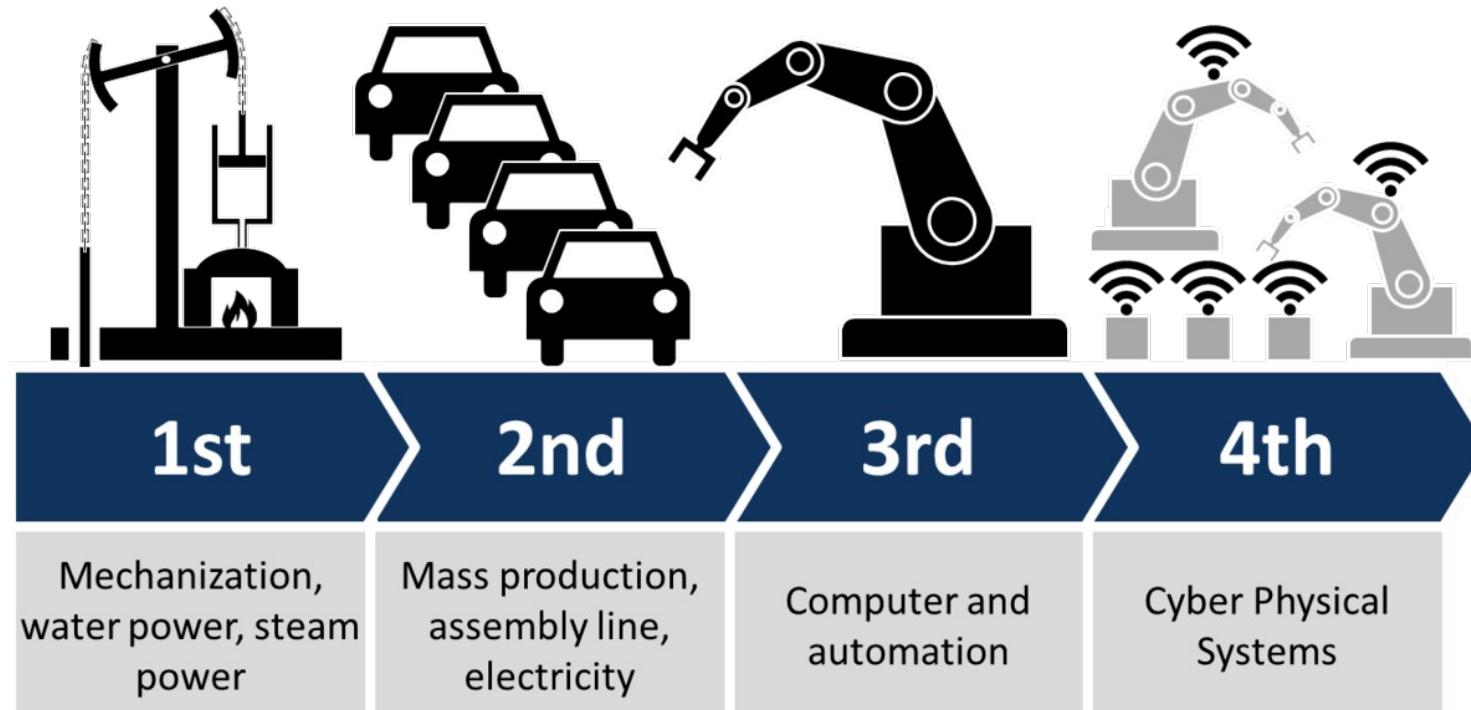
- **Introducción**
- **Los Sistemas de Control Industrial**
- **Desafíos Planteados por Industria 4.0**
- **Gestión de la Ciberseguridad en ICSs**
- **Herramientas para Mejora de la Ciberseguridad en ICSs**
- **Resumen y Conclusiones**

## Introducción:

Desde mediados del siglo XVIII hasta la fecha las **revoluciones industriales** han producido una explosión demográfica: Creció fuertemente la esperanza de vida y se redujo notoriamente la pobreza.

Estos cambios se lograron gracias al incremento de la disponibilidad de bienes y de alimentos, el incremento de la necesidad de mano de obra y mejoras permanentes en las condiciones sanitarias [02].

# Introducción



*Características de cada una de las revoluciones industriales (RI)*

Imagen obtenida de: <https://cadiznoticias.es/la-transicion-demografica-la-revolucion-industrial/>

# Introducción

## Las revoluciones industriales:

- 1) La primera revolución industrial se basó en la mecanización de la producción.
- 2) La segunda (estimada desde 1870 a 1970), se caracterizó por el uso intensivo de energía (eléctrica y petróleo).
- 3) La tercer revolución industrial (1970 - actualidad) se basó en la incorporación de dispositivos electrónicos, informáticos y redes de comunicaciones para la automatización de la producción a través de los **Sistemas de Control Industrial** (ICS) [02].
- 4) **Industria 4.0** es considerada ya como la “Cuarta Revolución Industrial”. Contempla la introducción de las tecnologías digitales en la industria de la fabricación: IoT, cloud, big data, IA, sensores inalámbricos, móviles, sistemas embebidos, entre otros [03].

*Industria 4.0 se propone como una nueva revolución industrial. Sin embargo, la ciberseguridad se considera solo como un asunto de Investigación.*

## En esta presentación

- Introducción
- Los Sistemas de Control Industrial
- Desafíos Planteados por Industria 4.0
- Gestión de la Ciberseguridad en ICSs
- Herramientas para Mejora de la Ciberseguridad en ICSs
- Resumen y Conclusiones

# Los Sistemas de Control Industrial (ICS)

## Presentación

ICS No es ni mejor, ni peor que IT. Es diferente.



Imágenes obtenidas de:

[https://es.wikipedia.org/wiki/Archivo:Tortuga\\_Islands\\_Gal%C3%A1pagos\\_2.jpg](https://es.wikipedia.org/wiki/Archivo:Tortuga_Islands_Gal%C3%A1pagos_2.jpg)  
<https://www.uncruise.com/destinations/galapagos-cruise>

# Los Sistemas de Control Industrial (ICS)

## Presentación



Imagen obtenida de: <https://www.solucoesindustriais.com.br/empresa/quimico-petroleo-plastico/reade-revestimentos-especiais/produtos/petroleo-e-derivados/fabrica-de-pisos-industriais>

# Los Sistemas de Control Industrial (ICS)

## Presentación



Imagen de un Tablero de Control Industrial

Imagen: <https://new.abb.com/low-voltage/products/wire-cable-management/tnb-europe/panel-builder>

# Los Sistemas de Control Industrial (ICS)

## Presentación

Las tecnologías de los sistemas de control Industrial se diseñaron para tener como premisa la alta disponibilidad.

Las bases de la Seguridad de la Información según la ISO27000:

Disponibilidad ✓

Integridad ✗

Confidencialidad ✗

Tecnologías OT

# Los Sistemas de Control Industrial (ICS)

## Presentación

Tienen la capacidad de funcionamiento en ambientes desfavorables (altos rangos de temperatura, vibraciones, ruidos electromagnéticos).

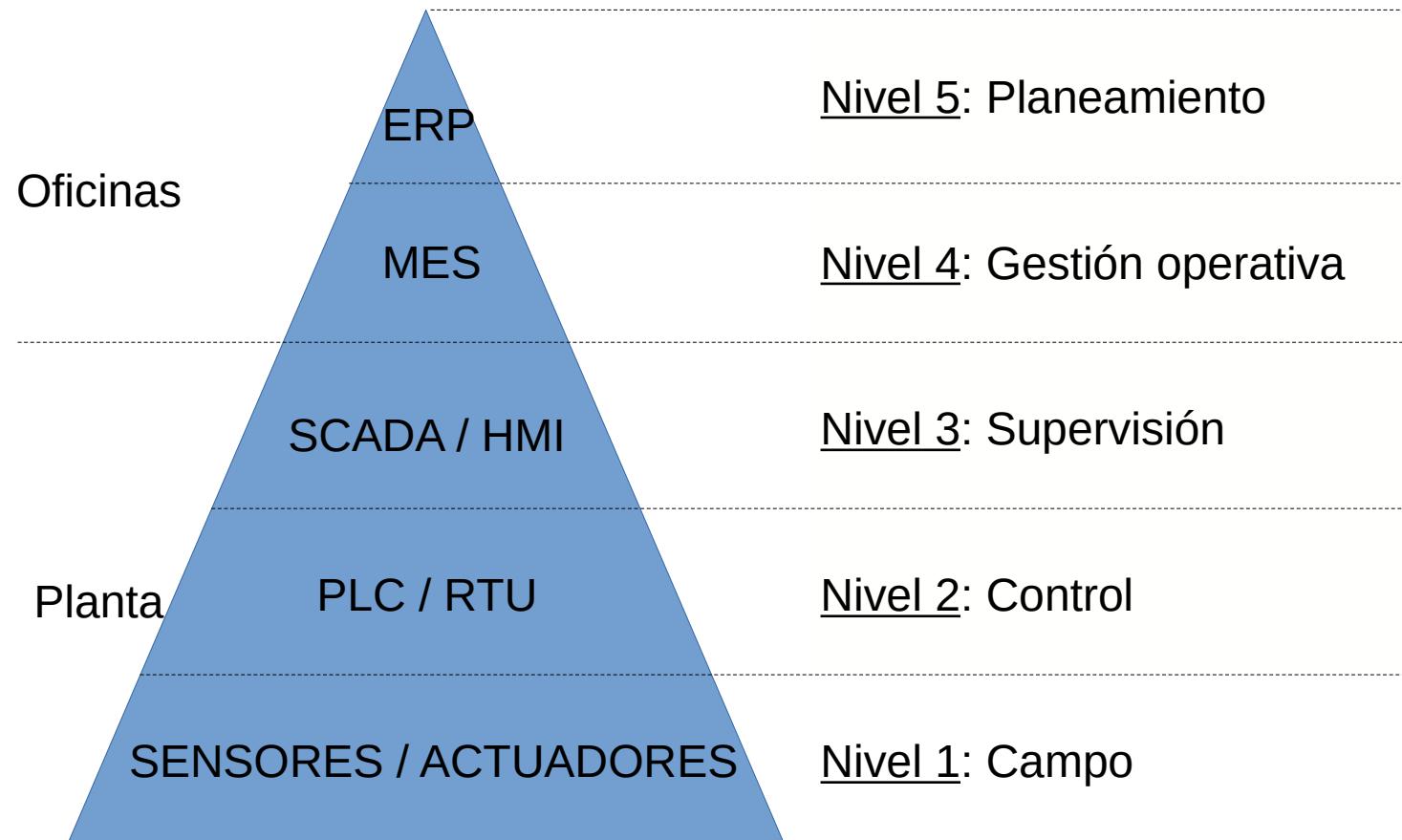
Son sistemas altamente robustos:

- Alto tiempo medio entre fallas (MTBF)
- Alta duración

**¿y la Obsolescencia?**

# Los Sistemas de Control Industrial (ICS)

## Arquitectura Purdue



# Los Sistemas de Control Industrial (ICS)

## Nivel 1: Campo – Entradas / Salidas / Digitales / Analógicas



Imágenes:

Micro-switch; <https://cpi.com.ar/collections/microswitch>

Caudalímetro: [http://www.phelectronica.com.ar/lista\\_productos.php?cat=11&tipo=Caudalimetros](http://www.phelectronica.com.ar/lista_productos.php?cat=11&tipo=Caudalimetros)

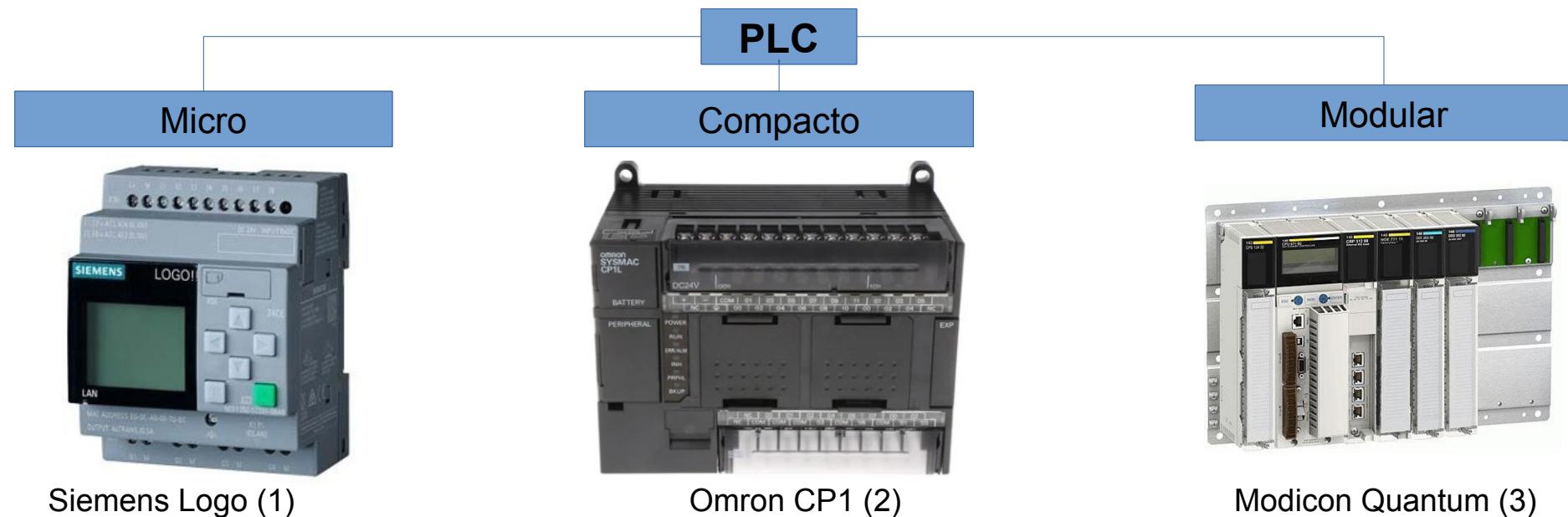
Relé: <https://cpi.com.ar/nuevos-productos/rele-my-omron/>

Variador de velocidad: <https://motores-electricos.com.ar/variadores-de-frecuencia/>

# Los Sistemas de Control Industrial (ICS)

## Nivel 2: Control – Los PLCs / RTUs

Un PLC es una computadora (o autómata) industrial. Es un ordenador industrial para automatizar procesos. Por sus bondades, se convirtieron en herramientas fundamentales para el desarrollo de las industrias.



Siemens Logo (1)

Omron CP1 (2)

Modicon Quantum (3)

Imagenes:

Siemens: <https://listado.mercadolibre.com.ar/plc-logo-8-siemens>

Omron: <https://northpower.co.th/products/plc-omron-cp1l>

Modicon: <https://www.indiamart.com/proddetail/quantum-cpu-modicon-plc-4690961088.html>

Ekoparty 2025 – Secure OT Village

# Los Sistemas de Control Industrial (ICS)

## Nivel 3: Supervisión – Interfaz Hombre / Maquina (HMI)



Imágenes:

Interfaz con switches y lámparas: <http://indpanels.com/spark-conversation-electrical-code-safety-meet-greet-st-joe-missouri/control-panel-with-switches-and-lamps/>

HMI: <http://buffaloadv.com/asa/>

# Los Sistemas de Control Industrial (ICS)

## Nivel 3: Supervisión – SCADA

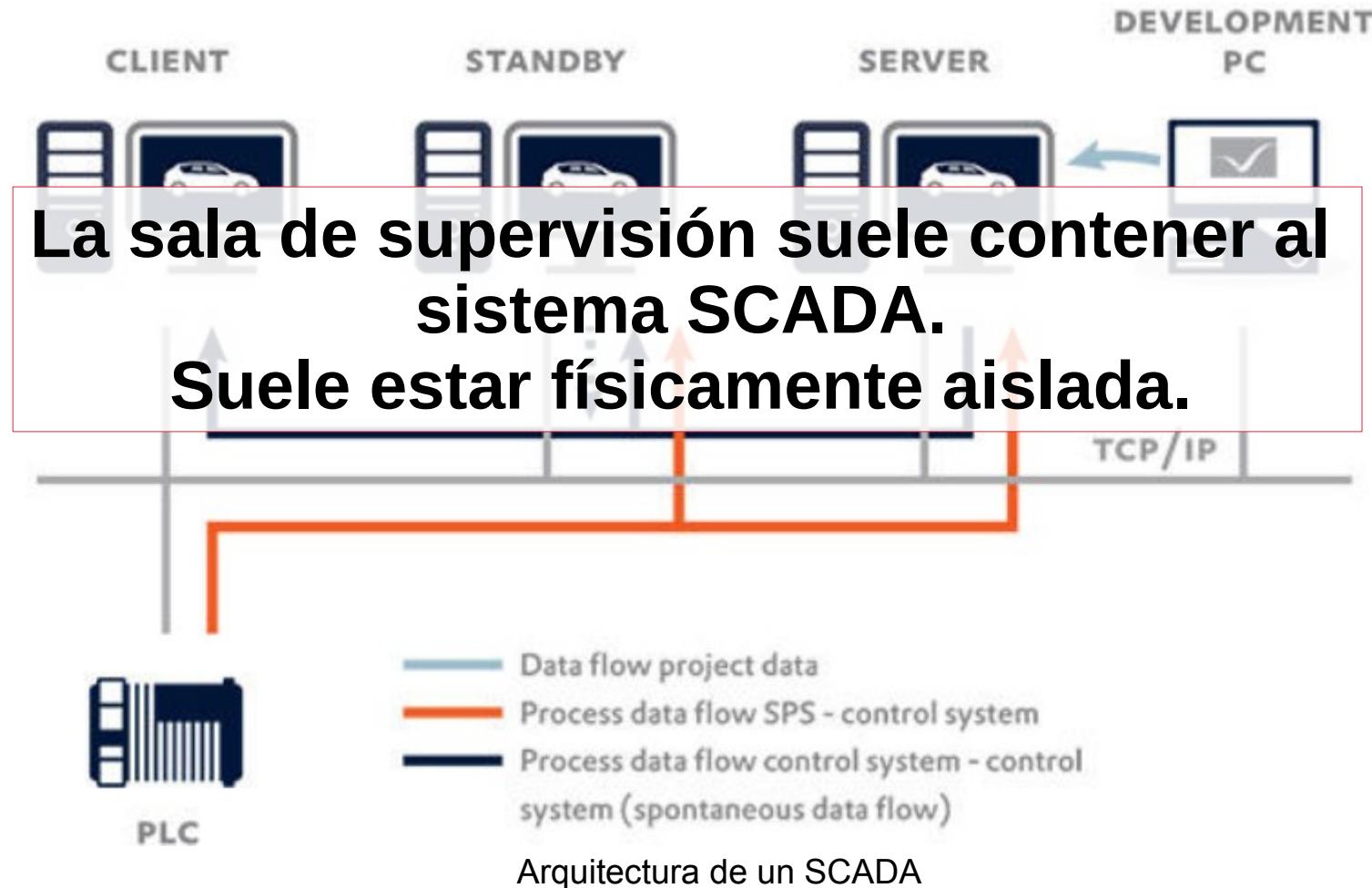


Imagen: <https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/>

# Los Sistemas de Control Industrial (ICS)

## Nivel 3: Supervisión – SCADA

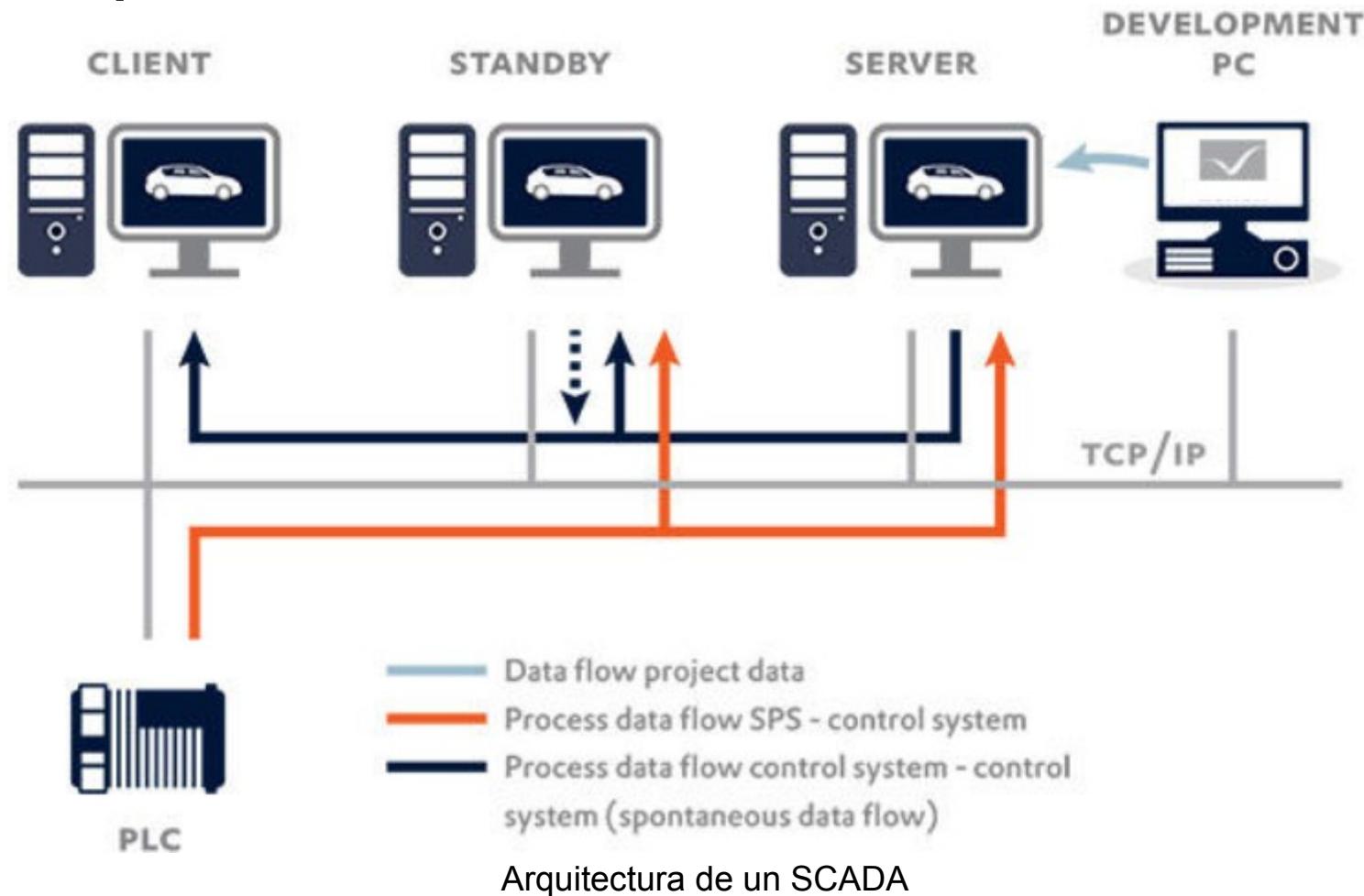


Imagen: <https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/>

# Los Sistemas de Control Industrial (ICS)

## Nivel 3: Supervisión – SCADA



Imagen de una sala de supervisión con un SCADA

Imagen: <https://www.virtualpro.co/noticias/control-de-sistemas--ejemplos-y-aplicaciones>

# Los Sistemas de Control Industrial (ICS)

## Nivel 3: Supervisión – SCADA – Infraestructuras Críticas

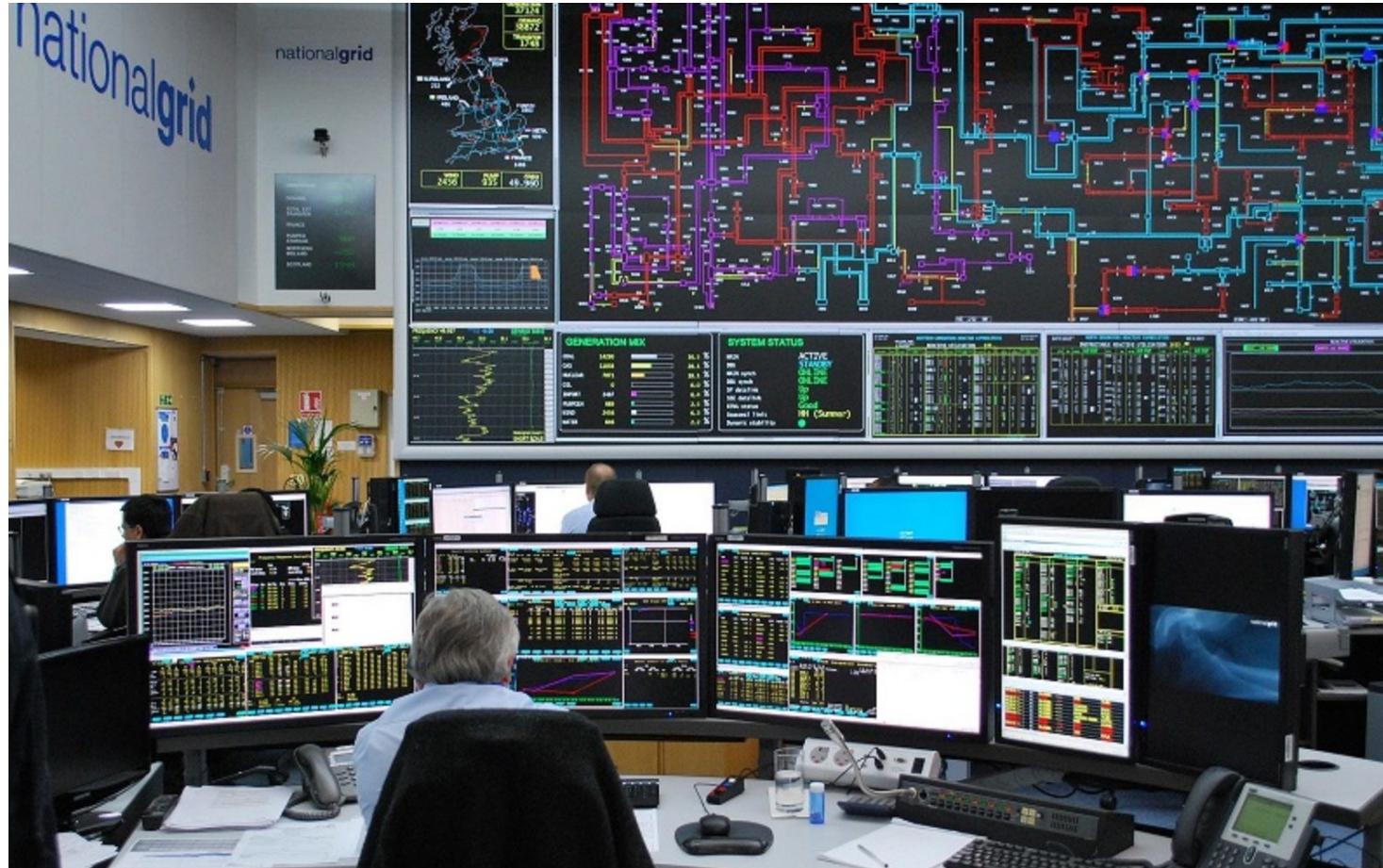


Imagen del SCADA del sistema de distribución de Gas Neoyorquino National Grid

Imagen obtenida de: <https://www.current-news.co.uk/news/cyber-attacks-rise-of-distributed-generation-among-top-risks-to-utilities>

## En esta presentación

- Introducción
- Los Sistemas de Control Industrial
- Desafíos Planteados por Industria 4.0
- Gestión de la Ciberseguridad en ICSs
- Herramientas para Mejora de la Ciberseguridad en ICSs
- Resumen y Conclusiones

# Desafíos planteados por Industria 4.0

## Industria 4.0

Se busca lograr:

- Integración Horizontal: de las redes de toda la cadena de valor de la producción.
- Integración Vertical: de las redes de producción [04].

# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Horizontal

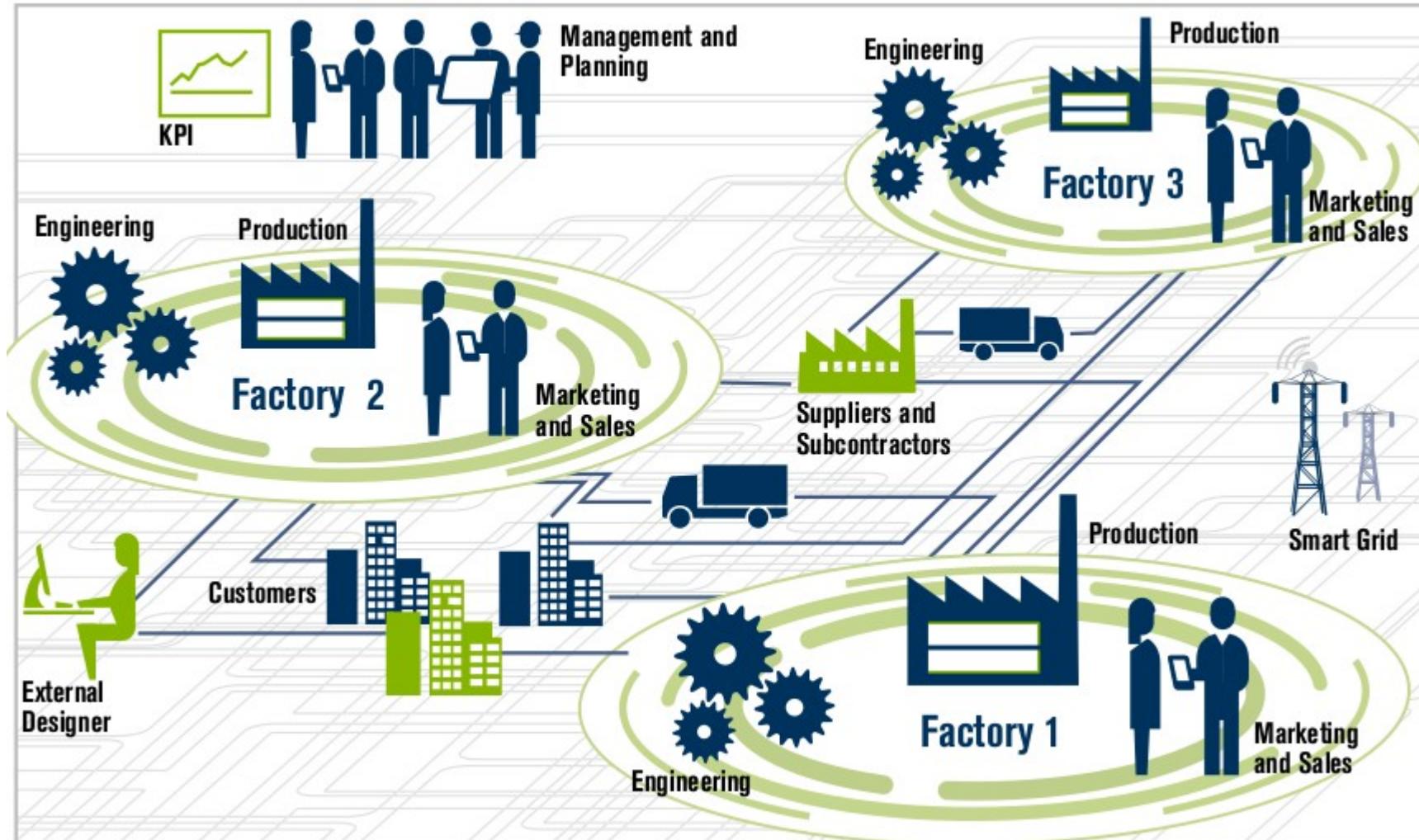


Imagen obtenida de [04].

# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Horizontal

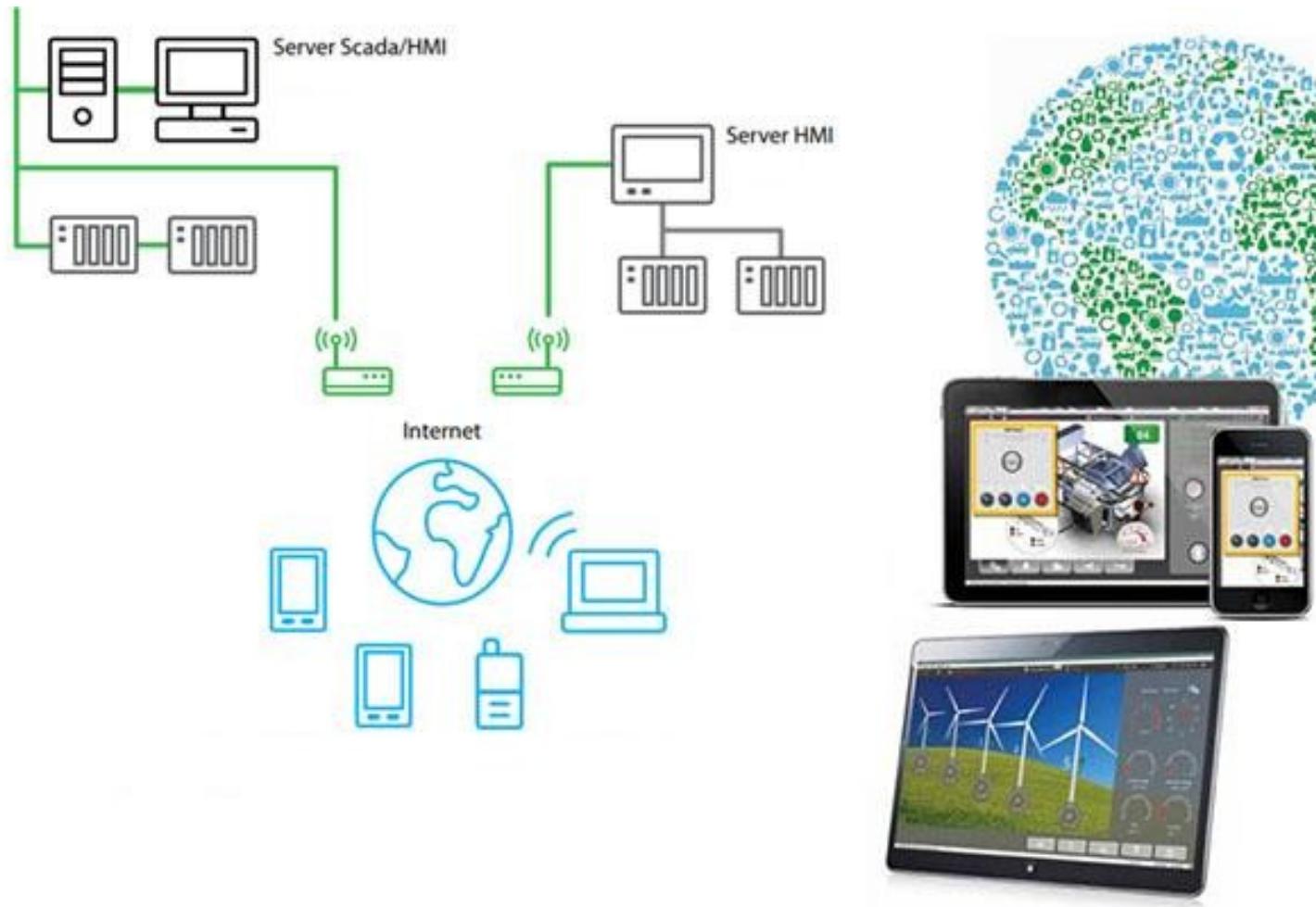


Imagen obtenida de: <https://www.contaval.es/scada-movicon-11-6-con-cliente-web-html5/>

# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Horizontal

Desafío: Existe información pública de sistemas SCADA conectados a internet (shodan.io) y accesibles a un click.

TOTAL RESULTS

75

TOP COUNTRIES

[View Report](#)[View on Map](#)

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**51.148.122.226**

2022-11-27T00:27:03.104991

51-148-122-226.dsl.  
zen.co.ukZen Internet Limited  
United Kingdom, Rochdale

SNMP:

Uptime: 159364482

Description: Siemens, **SIMATIC HMI**, TP900 Comfort, 6AV2 124-0JC01-0AX0, HW: 0, SW: V 13 0 1

Service: 72

Versions:

1

Ordescr: Sample SysOR Description ...

Contact: 1617366602.4284017

Oruptime: 3720

Objectid: 1.3.6.1.4.1.311.1.1.3.3

Orid: 1.3.6.1.2.1

N...



2022-11-27T00:23:51.275385

United States 17

Germany 9

Italy 8

France 7

Spain 6

**103.232.89.148**

HKBN Enterprise

SNMP ·

# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Horizontal

El ICS CERT de USA sugiere el aislamiento de los ICS para la mitigación de la gran mayoría de las Alertas presentadas en su sitio:

### MITIGATION

ICS-CERT is attempting to coordinate with the vendor and security researcher to identify mitigations.

ICS-CERT recommends, as quality assurance, that users test the update in a test development environment that reflects their production environment prior to installation. In addition, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are [not accessible from the Internet](#).
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

*Mientras que Industria 4.0 propone la hiper-conexión, quienes tratan los problemas de ciberseguridad en ICS sugieren su aislamiento físico.*

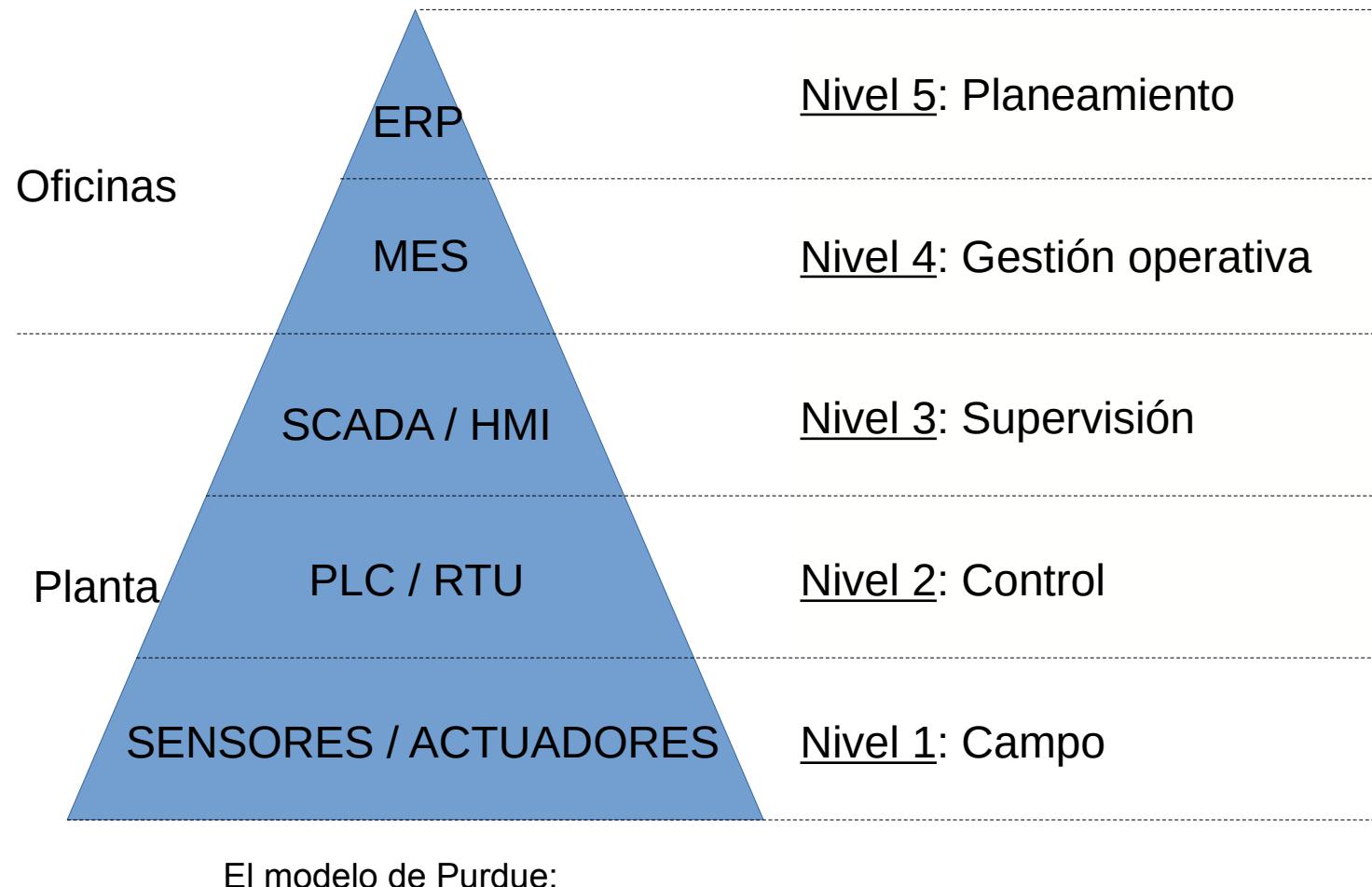
**Este es un problema abierto de gran importancia.**



Fuente: Sitio US-ICS CERT. Link: <https://www.cisa.gov/uscert/ics/alerts>

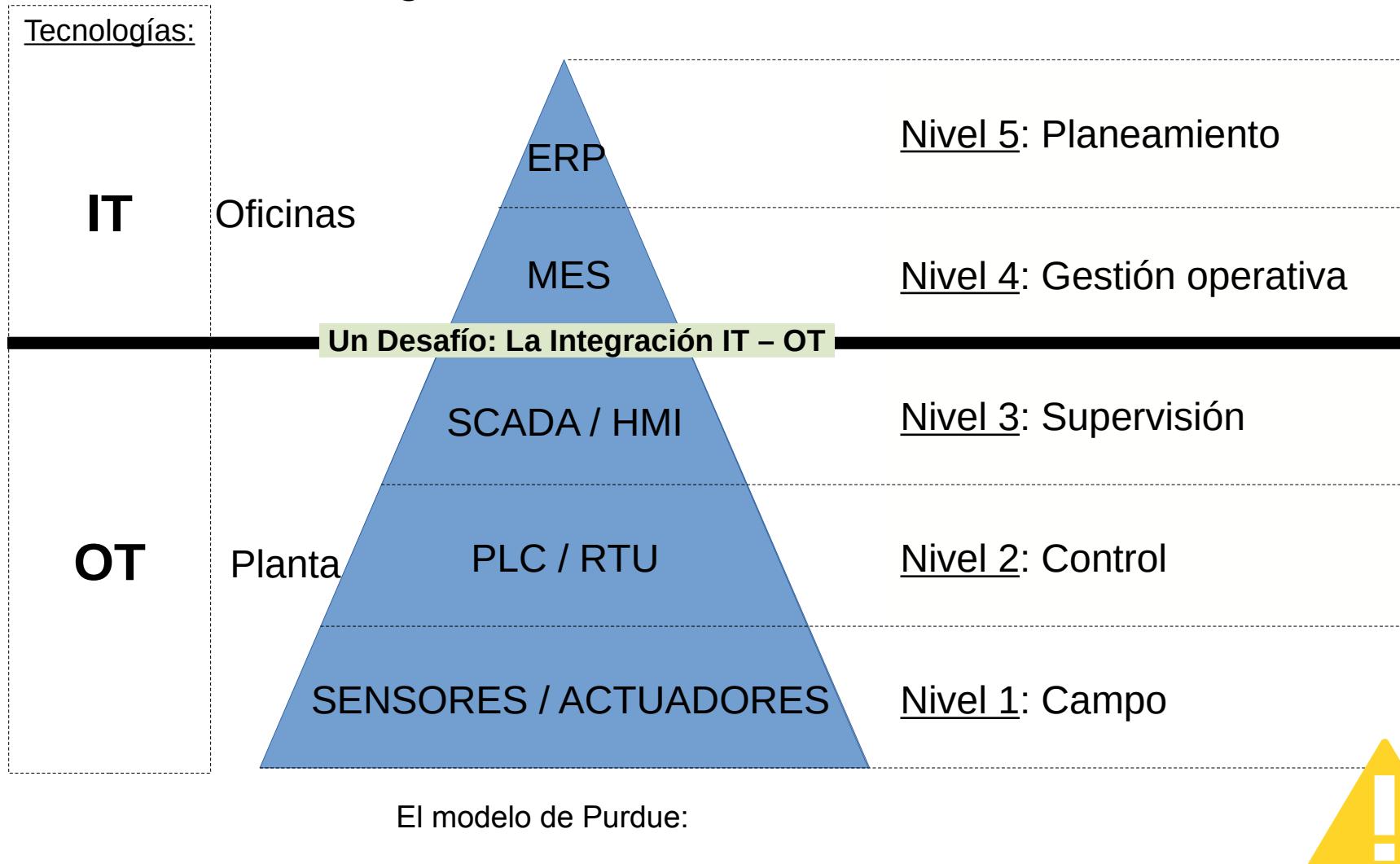
# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Vertical



# Desafíos planteados por Industria 4.0

## Industria 4.0: Integración Vertical



## Desafíos planteados por Industria 4.0

### Industria 4.0: Integración Vertical

La convergencia IT – OT entre las redes corporativas, con gran cantidad de falencias de seguridad y las redes industriales (diseñadas para funcionar aisladamente), han dejado a estas últimas en total vulnerabilidad.

Un análisis hecho sobre la base de datos RISI [06] presenta la hipótesis que ***gran parte de los incidentes en ICS pudo evitarse con la implementación de buenas prácticas.***



## En esta presentación

- **Introducción**
- **Los Sistemas de Control Industrial**
- **Desafíos Planteados por Industria 4.0**
- **Gestión de la Ciberseguridad en ICSs**
- **Herramientas para Mejora de la Ciberseguridad en ICSs**
- **Resumen y Conclusiones**

# Gestión de la Ciberseguridad en ICSs

## Estándares de Seguridad para SCADA

- Informes Técnicos ISA-SP99
- Perfil de protección del sistema NIST
- Estándar de seguridad API-1164
- Documentos AGA-12
- Guía de implementación de firewall NISCC
- Documento NIST SP 800-82
- ISA / IEC 62443

## Gestión de la Ciberseguridad en ICSs

### Incidentes en IIICC vs Incumplimiento de Buenas Prácticas

El trabajo de Mariano Pozzi [07] prueba la correspondencia entre estas variables, insinuada en el trabajo basado en el análisis de la RISI [06].

Algunos Casos estudiados:

- (1) 2011: Ataque a central nuclear Natanz, Iran (Stuxnet).
- (2) 2012: Ataque a petrolera Aramco, Arabia Saudita (Shammon)
- (3) 2017: Ataque Internacional (WannaCry)

Algunos controles que fallaron:

- En (1): SP 800-82 3.3.3 de NIST CIS 7.1-8, subcontroles 8.4 y 8.5 (usb no asegurados), control ISO/IEC 27002 Sección 11 (Seguridad física).
- En (2): ISO 27001 control 9.2 (auditoría), DS7 de COBIT (concientización), gestión de servicios ITIL (seguridad perimetral)
- En (3): DS7 de COBIT (concientización), NIST 800-53 IR7 (respuesta a incidentes), ISO/IEC27010 (intercambio de información)

# Gestión de la Ciberseguridad en ICSs

## CISA: US ICS Cert

### Malas Prácticas:

- Usar software sin soporte
- Usar contraseñas y credenciales conocidas, predeterminadas.
- Usar un solo factor de autenticación.

### Análisis de Alertas e Incidentes: Algunos aspectos

- La mayoría de los subsistemas donde se presentan las alertas son mayormente OT SCADA: componente: “Software”.
- La mayoría de las vulnerabilidades están relacionadas con la Autenticación y con el desbordamiento de pilas o memorias.

*Su explotación puede impactar en la denegación de servicio por desbordamiento y/o el compromiso total de los sistemas por acceso no autorizado [08].*

# Gestión de la Ciberseguridad en ICSs

## Mitre Att&ch: Matriz de técnicas y tácticas de ataques a ICS

### ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Co
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Covert Channels
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Covert Persistence
Exploitation of Remote	Execution	Module Firmware		Indicator Removal on	Remote System	Hardcoded Credentials	Data from Information Repositories	Staged Attacks

Fuente: <https://attack.mitre.org/matrices/ics/>

Ekoparty 2025 – Secure OT Village

## En esta presentación

- **Introducción**
- **Los Sistemas de Control Industrial**
- **Desafíos Planteados por Industria 4.0**
- **Gestión de la Ciberseguridad en ICSs**
- **Herramientas para Mejora de la Ciberseguridad en ICSs**
- **Resumen y Conclusiones**

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Networking: Aislamiento y Segmentación de servicios SCADA

### Segmentación:

- Es necesaria para desacoplar a las Tecnologías IT de OT.
- También dentro del propio entorno OT (separar SCADA, PLC y HMI)

### Aislamiento: Implementación de DMZ entre Servicios IT y SCADA

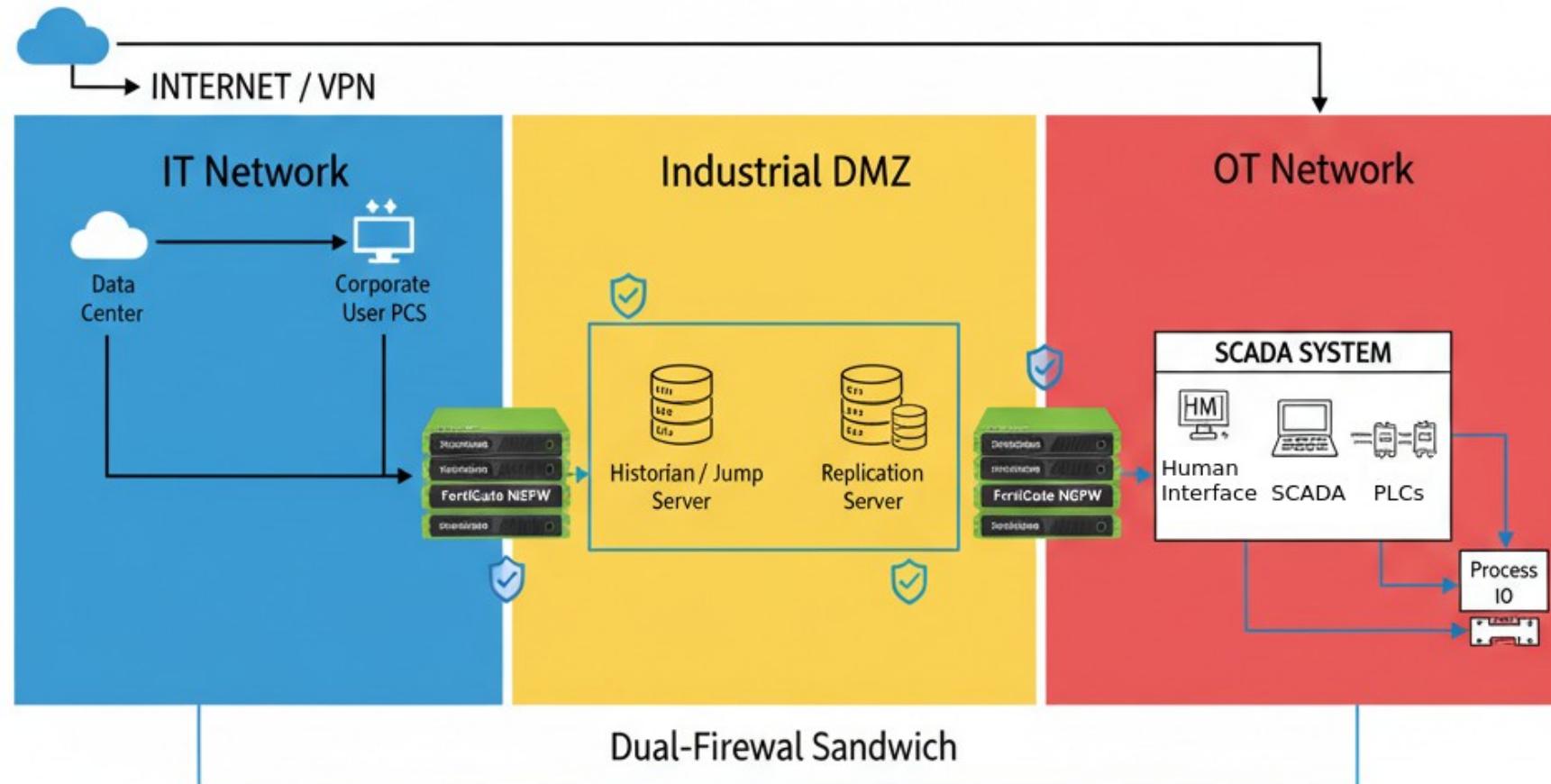
La DMZ actúa como una zona intermedia y neutral entre IT y OT.

Un diseño de firewall doble evitaría que compromisos en IT se trasladen a OT, manteniendo la visibilidad de los protocolos OT.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Networking: Aislamiento y Segmentación de servicios SCADA

### Arquitectura:



**Blue Zone:** Corporate IT

**Yellow :** Industrial DMZ

**Green Devices:** FortiGate Next-Generation Firewalls

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Forensia sobre SCADA:

### Análisis en frío:

En caso de incidentes en un ICS puede obtenerse evidencia de lo sucedido en SCADA, HMI, Sistemas embebidos.

### Inconvenientes:

Los ICS están hechos para funcionar sin parada. Y así suelen operar. Por lo tanto, un análisis en frío del sistema no es posible para la mayoría de los incidentes.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Forensia sobre SCADA:

### Análisis en Vivo:

El análisis forense en vivo se presenta como una herramienta de gran utilidad para conocer la situación del SCADA (servidor, comunicaciones, etc) sin detener el equipo

En [09 – 10] se realizó un análisis sobre un SCADA con Bento.

### Resultados más detallados de:

- Red de comunicaciones (Network Traffic Viewer).
- SO y aplicaciones instaladas en el SCADA (WinAudit)
- Actividades hechas por PLC: Archestra (Log Viewer de InTouch, hoy Aveva)

*Idea: Al obtenerse información en vivo del funcionamiento del ICS, pueden usarse estos resultados para la prevención de ciber-incidentes.*

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Forensia sobre SCADA:

### Análisis en Vivo:

<i>Item</i>	<i>Value</i>
<i>Port Protocol</i>	<i>TCP</i>
<i>Local Address</i>	<i>::1</i>
<i>Local Port</i>	<i>59568</i>
<i>Caption</i>	<i>TCP ::1:59568</i>
<i>Service Name</i>	
<i>Remote Address</i>	<i>::1</i>
<i>Remote Port</i>	<i>49155</i>
<i>Connection State</i>	<i>Connection established (ESTABLISHED)</i>
<i>Process Name</i>	<i>C:\Program Files\Wonderware\DA Server\DA MBTCP\Bin\DA MBTCP.exe</i>
<i>Process ID</i>	<i>2772</i>
<i>Process</i>	<i>ServerExe Module</i>
<i>Description</i>	
<i>Process</i>	<i>Invensys Systems, Inc.</i>
<i>Manufacturer</i>	

*Win Audit puertos abiertos*

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Forensia sobre SCADA:

### Análisis en Vivo:

The screenshot shows a network traffic capture interface from SmartSniff. The main window displays a list of captured packets. A red box highlights the 13th packet, which is an ICMP echo request from 192.168.1.2 to 192.168.1.5. Another red box highlights the 14th packet, which is an ICMP echo reply from 192.168.1.5 to 192.168.1.2. Below the list, a hex dump of the selected packets is shown, revealing ASCII text such as 'abcdefghijklnopqrstuvwxyz' and 'bcdefghijklmnopqrstuvwxyz'. A large red callout box points to the hex dump area with the text: 'Observar que la información viaja En claro' (Observe that the information travels in clear text). A red line connects the highlighted packet in the list to its corresponding hex dump entry.

Paquete de SCADA a PLC

Paquete de Datos en Ascii

Observar que la información viaja  
En claro

Index	Prot..	Local Adr..	Remote ...	Loc... R...	Service ...	Packets	Data Size	Total Size	Data Speed	Capture Time	Last Packet Time	Duration
8	ICMP	192.168.1.2	192.168.1.1			2	156 Bytes	318 Bytes	0.0 KB/Sec	26/09/2020 22:48:4...	26/09/2020 22:50:4...	00:01:59.681
12	ICMP	192.168.1.2	192.168.1.2			504	39.312 Bytes	53.530 Bytes	0.3 KB/Sec	26/09/2020 22:48:4...	26/09/2020 22:50:5...	00:02:07.996
13	ICMP	192.168.1.2	192.168.1.5			8	256 Bytes	540 Bytes	0.1 KB/Sec	26/09/2020 22:49:1...	26/09/2020 22:49:1...	00:00:03.042
14	TCP	192.168.1.2	192.168.1.3	49218	502	11.689	88.977 Bytes	556.589 Bytes	0.1 KB/Sec	26/09/2020 22:49:3...	26/09/2020 23:01:3...	00:11:55.713

12796 Packets Captured

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

Objetivo: Añadir capa adicional de protección criptográfica

15 2.579548 192.168.171.139	192.168.171.182	Modbus/TCP	78 Query: Trans: 64795
16 2.579680 192.168.171.182	192.168.171.139	TCP	66 502-37993 [ACK] Seq=1 ACK=1
17 2.587010 192.168.171.182	192.168.171.139	Modbus/TCP	78 Response: Trans: 64795
18 2.587334 192.168.171.139	192.168.171.182	TCP	66 37993-502 [ACK] Seq=13 ACK=1
19 2.587749 192.168.171.139	192.168.171.182	TCP	66 37993-502 [FIN, ACK] Seq=14 ACK=1
26 2.591935 192.168.171.182	192.168.171.139	TCP	66 502-37993 [FIN, ACK] Seq=15 ACK=1
27 2.592284 192.168.171.139	192.168.171.182	TCP	66 37993-502 [ACK] Seq=14 ACK=1

```

> Frame 17: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: Vmware_c3:29:82 (00:0c:29:c3:29:82), Dst: Vmware_e1:12:81 (00:0c:29:e1:12:81)
> Internet Protocol Version 4, Src: 192.168.171.182 (192.168.171.182), Dst: 192.168.171.139 (192.168.171.139)
> Transmission Control Protocol, Src Port: 502 (502), Dst Port: 37993 (37993), Seq: 1, Ack: 13, Len: 12
> Modbus/TCP

```

Transaction Identifier: 64795

Protocol Identifier: 0

Length: 6

Unit Identifier: 1

Modbus

Function Code: Write Single Register (6)

Reference Number: 8

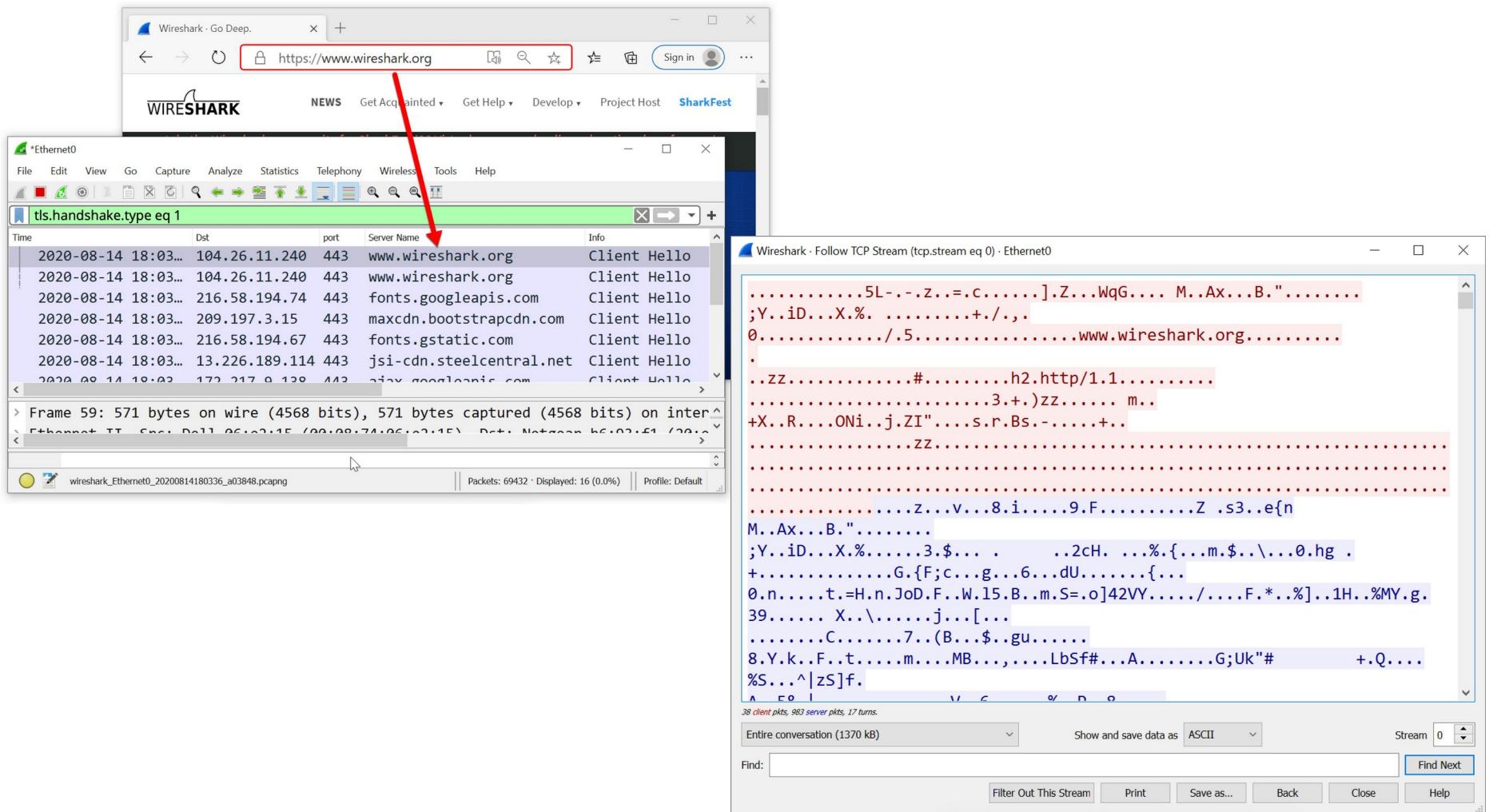
Data: 014d

Code	1/16-bit	Description	I/O Range
01	1-bit	Read coils	00001 – 10000
02	1-bit	Read contacts	10001 – 20000
05	1-bit	Write a single coil	00001 – 10000
15	1-bit	Write multiple coils	00001 – 10000
03	16-bit	Read holding registers	40001 – 50000
04	16-bit	Read input registers	30001 – 40000
06	16-bit	Write single register	40001 – 50000
16	16-bit	Write multiple registers	40001 – 50000
22	16-bit	Mask write register	40001 – 50000
23	16-bit	Read/write multiple registers	40001 – 50000
24	16-bit	Read FIFO queue	40001 – 50000

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

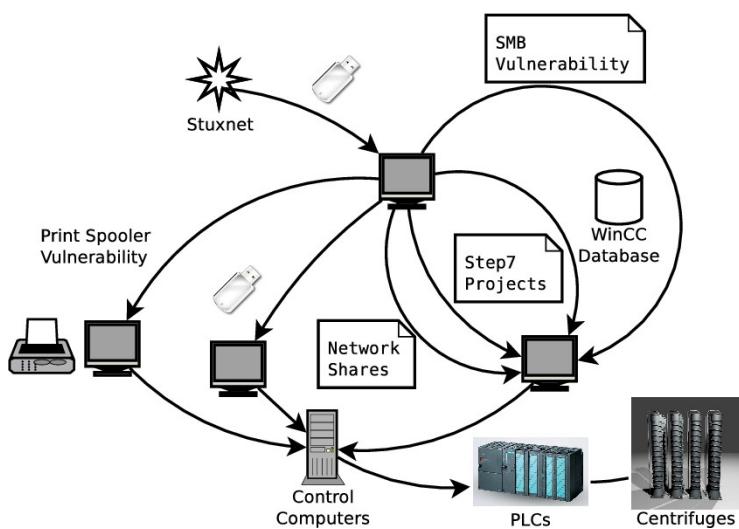
### Escenario Ideal



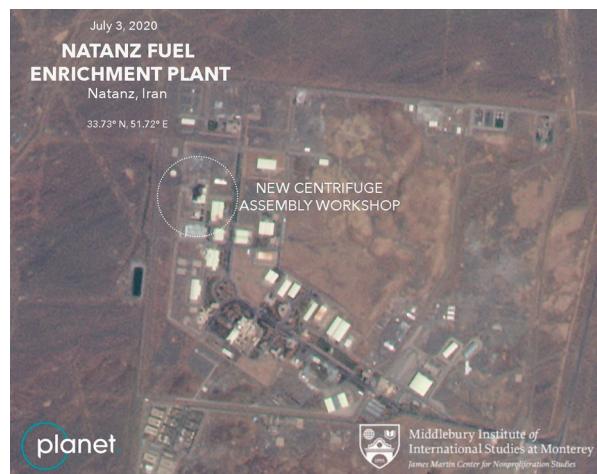
# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

Conclusión: en redes ModbusTCP, un insider o un atacante con acceso a la red industrial, con conocimientos básicos de programación (ej.: librería pymodbus, tal como se demuestra en nuestro stand) PUEDE MODIFICAR UN PROCESO INDUSTRIAL MEDIANTE INYECCIÓN DE TRÁFICO MODBUS EN LA RED



```
from pymodbus.client import ModbusTcpClient
def coilOff(client):
    targetAddress = int(input("\nIngrese bobina (salida) a sobreescibir: "))
    result = client[0].write_coil(targetAddress, False, device_id = client[1])
    if result.isError():
        print("Error al apagar bobina")
    else:
        print("Bobina apagada correctamente")
```



# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

1er paso: determinar punto de partida → MAPEO SIST. LIT.

### Criptografía aplicada en entornos industriales: un mapeo sistemático de la literatura

José Federico Castro Tramontina<sup>1</sup>, Carlos Neil<sup>1</sup>, Jorge Kamlofsky<sup>1</sup>, Pedro Hecht<sup>2</sup>

<sup>1</sup> Universidad Abierta Interamericana – Facultad de Tecnología Informática  
 Centro de Altos Estudios en Tecnología Informática – Buenos Aires, Argentina  
 JoseFederico.CastroTramontina@alumnos.uai.edu.ar

{Carlos.Neil, Jorge.Kamlofsky}@uai.edu.ar

<sup>2</sup> Universidad de Buenos Aires – Facultad de Ciencias Económicas  
 Escuela de Negocios y Administración Pública – Buenos Aires, Argentina  
 phecht@dc.uba.ar

Pregunta de investigación	Motivación
<b>PI1:</b> ¿Qué trabajos abordaron el cifrado de comunicaciones entre autómatas industriales?	Determinar los antecedentes de la aplicación de criptografía para la protección de ICS
<b>PI2:</b> ¿Qué trabajos abordaron la aplicación de protección criptográfica en entornos similares como IoT, IIoT, WSN y en niveles superiores de la Arquitectura de Purdue?	Determinar enfoques actuales aplicados en entornos y dispositivos similares, e implementaciones de criptografía en capas superiores al nivel de control
<b>PI3:</b> ¿Se ha aplicado criptografía sobre ICS (Industrial Control Systems) para su protección?	Identificar las últimas tendencias en cuanto a cifrado de comunicaciones entre autómatas industriales
<b>PI4:</b> ¿Las protecciones criptográficas fueron implementadas sobre el dispositivo o sobre el protocolo de red?	Determinar la capa, zona o sector de la red industrial donde se aplica la protección criptográfica (dispositivo, medio guiado, protocolo de red, etc.)
<b>PI5:</b> ¿Los algoritmos criptográficos implementados son ligeros/livianos o compatibles con dispositivos de poder de cómputo limitado?	Entender las capacidades y limitaciones de los dispositivos de pequeño porte (ej.: PLC) que realizarán el cifrado de la información
<b>PI6:</b> ¿Cuáles son los algoritmos criptográficos, protocolos de red y estándares implementados sobre ICS y similares?	Determinar los protocolos de red, de intercambio de claves, cifradores simétricos y estándares empleados sobre ICS en la actualidad

**NOTA: todos los trabajos relacionados con el proyecto pueden encontrarse en:**  
<https://jorgekamlofsky.github.io/ics-testbench/produccion.html>

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

### 2do paso: determinar limitaciones y dificultades

Criptografía “contemporánea” → principios matemáticos

¿En qué programar un algoritmo criptográfico?

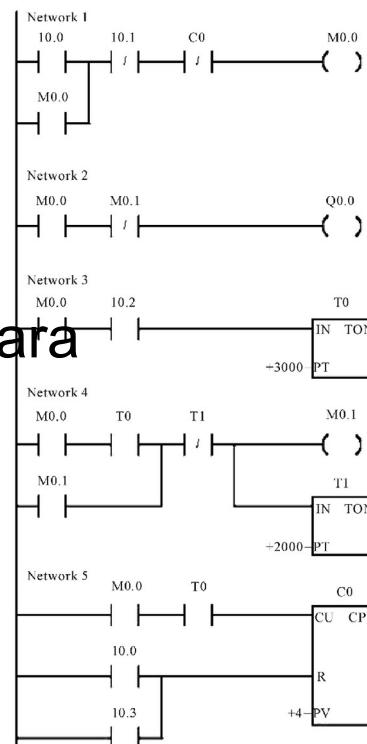
Dos opciones:

- Ladder
- ST (Structured Text)

Sin duda, más “amigable” para

Cripto: **ST**

Pero...



```
1 IF #start = 1 THEN
2   //comment
3   "Max_nr" := #Array[0];
4   FOR #i := 1 TO 10 DO
5     // Statement section FOR
6     IF #Array[#i] > "Max_nr" THEN
7       "Max_nr" := #Array[#i];
8     END_IF;
9   END_FOR;
10 END_IF;
11
```

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

### Comunicaciones

- PLC → PLC
- PLC → SCADA
- SCADA → PLC

*¿Cómo lograr que el emisor (PLC) cifre una trama Modbus?*

*¿Cómo lograr que el receptor (PLC/SCADA) descifre la trama antes de “procesar” la información?*

*¿Será una posible solución cifrar solo la “carga útil” del paquete y dejar en claro el Function Code para facilitar procesamiento?*

*¿Qué sucede con la latencia añadida?*

- *Sist. de tiempo real*
- *Limitado poder de cómputo*
- *Lightweight Cryptography*

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

Una posible solución: **PKI Industrial**

Determinados PLCs modernos soportan certificados

**Modbus TLS** → paquetes se transmiten dentro de un túnel cifrado

¿Está realmente implementado en la industria?



Communication Profile	Modbus.org	IANA Registry	This specification (for brevity)
mbap/TCP	Modbus/TCP	Modbus Application Protocol at System Port 502	Mbap
mbap/TLS/TCP	Modbus/TCP Security	Modbus Security Application Protocol at System Port 802	Mbaps

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Criptografía en ICS

### Modbus TLS

*“Only cipher suites registered with IANA and not known to have current weaknesses should be used in mbaps. This example cipher suite indicates that:*

- RSA will be used for key exchange,
- AES-128 CBC will be used for encryption, and
- SHA256 will be used for message integrity.”

**Nota: RSA y AES-128 no serían inmunes a ataques cuánticos**

**Horizonte temporal “corto”**

**Propuesta → INCLUIR PROTOCOLO DE INTERCAMBIO**

**DE CLAVES POST-CUÁNTICO EN MODBUS TLS**

# Herramientas para Mejora de la Ciberseguridad en ICSs

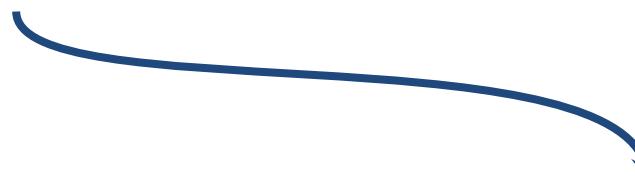
## Criptografía en ICS

**Post-Quantum Cryptography Using Hyper-Complex Numbers**

Jorge Alejandro Kamlofsky<sup>1</sup> – Juan Pedro Hecht<sup>2</sup>

<sup>1</sup> CAETI - Universidad Abierta Interamericana.  
Av. Montes de Oca 725 – Buenos Aires – Argentina.  
Jorge.Kamlofsky@uai.edu.ar

<sup>2</sup> Universidad de Buenos Aires, Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. Maestría en Seguridad Informática, Buenos Aires, Argentina.  
phecht@dc.uba.ar



### Definición formal de la Autoconvolución Discreta Modular Puntual

- Sean  $o_X, o_{Si}$  octoniones en  $Z_p$ ,
- Sea  $q$  un entero en  $Z_p$ ,
- Sea  $g(x)$  una función polinómica definida sobre  $O$ ,
- Se define la operación de *Autoconvolución Discreta Modular Puntual* como:

$$[(g*g)(o_X, o_{Si}, q)] = g(o_X)^q \cdot g(-o_X + o_{Si})^q \pmod{p}. \quad (25)$$

### HK17 → HK17++:

- **Octoniones → álgebra NO asociativa, NO conmutativa (muy útil en Criptografía)**
- **Reformulación del algoritmo que impediría ataques algebraicos de recuperación de claves**
- **Se implementan en forma novedosa conceptos tomados de la Física Matemática (convoluciones discretas "reversionadas")**
- **Se amplía el dominio de búsqueda para el atacante**
- **Pruebas iniciales en Python, SageMath → OK**
- **Inmunidad frente a ataque (Bernstein-Lange) → OK**
- **Otro tipo de ataques → ¿?**

# **Herramientas para Mejora de la Ciberseguridad en ICSs**

## **Ciberdefensa Desplegable**

Una mirada a la doctrina militar

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable

### ¿Qué es la Ciberdefensa Desplegable?

#### Definición Central:

Es la capacidad de desplegar equipos y personal de ciberseguridad fuera de una ubicación fija para llevar a cabo misiones defensivas en entornos remotos, hostiles o sin infraestructura de apoyo.

#### Conceptos Clave:

Movilidad y Autonomía: Los equipos deben ser autosuficientes y capaces de operar con una logística mínima.

Flexibilidad: Adaptables a diversos escenarios, desde operaciones de combate hasta la protección de infraestructuras críticas civiles.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable

### Hitos en su Desarrollo

- Fase Conceptual (2010-2015): El concepto emerge en la literatura militar de EE. UU. y la OTAN.
- Fase de Consolidación (2016-2020): Se formaliza en doctrinas militares y se crean las primeras unidades especializadas, como los Equipos de Ciberprotección (CPTs) en EE. UU.
- Fase de Formalización (2021-2025): El Departamento de Defensa de EE. UU. establece una definición doctrinal oficial, consolidando su importancia estratégica.

### Ejemplos de Aplicación:

- Operaciones Militares: Apoyo a fuerzas desplegadas en el extranjero.
- Defensa Nacional: Protección de redes críticas durante emergencias.
- Cooperación Internacional: Equipos de Respuesta Rápida Cibernética (CRRTs) de la Unión Europea para asistir a países aliados.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable: Estado del Campo

### Estado Actual:

- La ciberdefensa desplegable es un concepto maduro y aceptado en la doctrina de defensa occidental (EE. UU., OTAN, UE).
- La mayor parte de la literatura proviene de fuentes militares y gubernamentales, no académicas.
- Se considera un pilar clave para la resiliencia cibernetica nacional y aliada.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable: Estado del Campo

### Desafíos y Futuro:

- **Vacíos de Investigación:** Faltan estudios públicos sobre la efectividad real, los desafíos logísticos y los marcos legales de estas operaciones. La doctrina actual, aunque madura, presenta vacíos en su aplicación práctica en entornos de Tecnología Operacional (OT).
- **Falta de herramientas especializadas:** Desde la perspectiva de la doctrina no vimos soluciones estandarizadas para el análisis rápido de redes industriales en campo.
- **Dependencia de la conectividad:** Las operaciones a menudo requieren un enlace a un SOC central para el análisis y la inteligencia de vulnerabilidades.
- **Curva de aprendizaje elevada:** Se necesita personal altamente especializado en ciberseguridad industrial para ser efectivo en ventanas de tiempo cortas.
- **Oportunidades:** Desarrollar capacidades más portables, de bajo costo y especializadas que puedan ser operadas por personal de campo con pocos conocimientos técnicos afines.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable

El scanner OT (MVP de software) materializa la doctrina de ciberdefensa desplegable, abordando directamente sus vacíos:

- Autonomía y Operación Offline : Pensado para funcionar sin conexión a Internet y en equipos de cómputo limitado y corriendo sobre multiplataforma, utiliza feeds de vulnerabilidades locales (NVD) para enriquecer los hallazgos en tiempo real, eliminando la dependencia de un SOC remoto.
- Accionabilidad Inmediata: Su interfaz guiada y sus módulos de descubrimiento activo/pasivo permiten a personal no experto (equipos mixtos OT/IT) obtener un inventario y una evaluación de riesgos en tiempos reducidos.
- Seguridad Operacional en Entornos Sensibles : Diseñado con timeouts conservadores y operaciones de solo lectura por defecto, minimiza el riesgo de disruptión en redes industriales activas.
- Inteligencia de Vulnerabilidades en el Borde : Correlaciona los activos descubiertos con CVEs conocidas de forma local, permitiendo priorizar la remediación incluso en escenarios sin conectividad WAN.
- Conectividad a redes públicas: Adicionalmente puede comprobar si la red analizada tiene comunicación hacia redes públicas. Si comprueba la conexión, tiene la capacidad de entregar el footprint de la IP y su superficie de ataque.

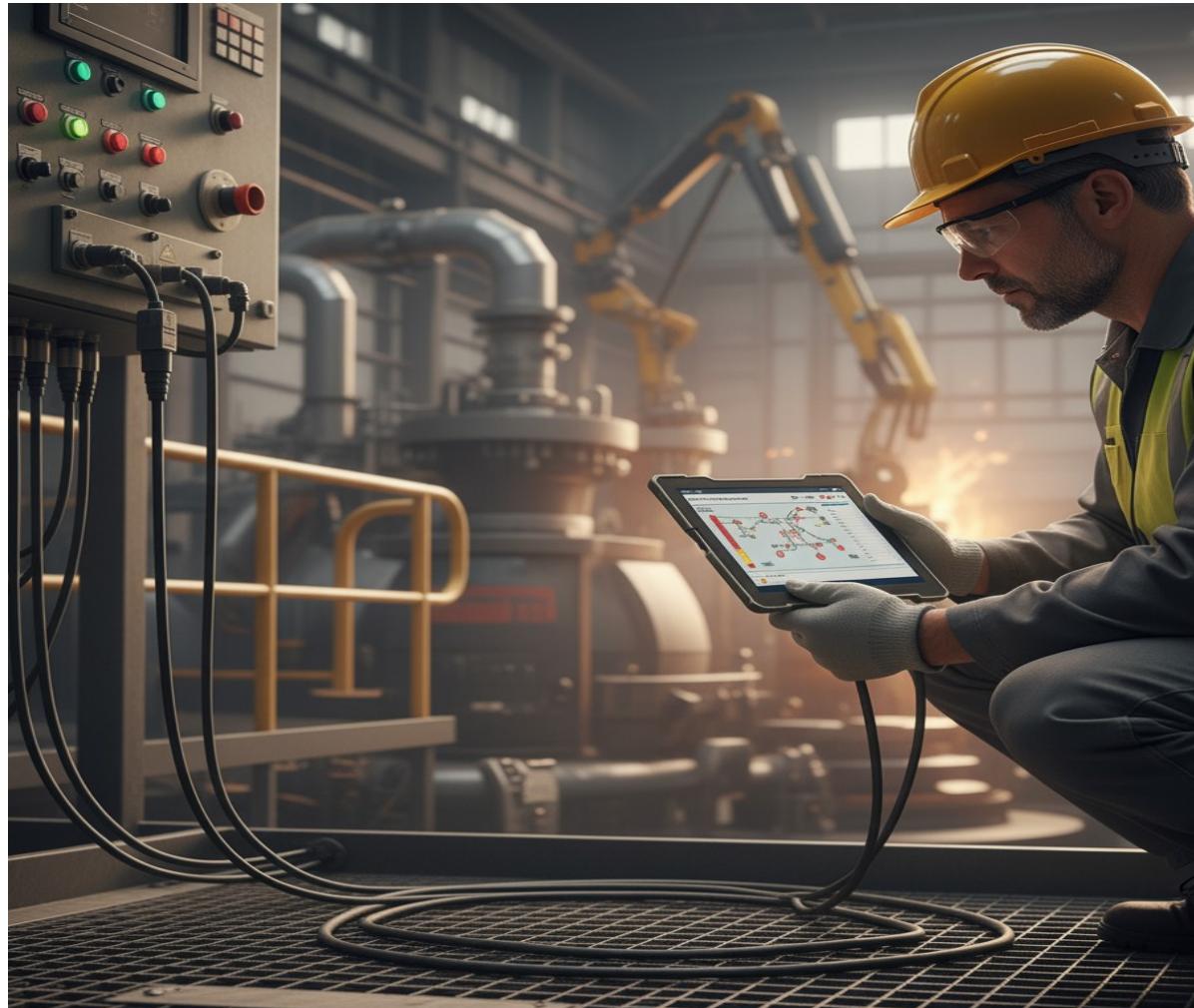
Impacto Final: El scanner acorta el ciclo Descubrir → Entender → Priorizar en el borde, convirtiendo los conceptos doctrinales en una capacidad tangible y desplegable para la protección de infraestructuras críticas. Próximamente montado en un hardware especializado.

Conclusión: La ciberdefensa desplegable ha evolucionado de una idea a una capacidad operativa esencial, y su importancia estratégica seguirá creciendo.

# Herramientas para Mejora de la Ciberseguridad en ICSs

## Ciberdefensa Desplegable

El Scanner OT Desplegable como Herramienta Táctica



## En esta presentación

- **Introducción**
- **Los Sistemas de Control Industrial**
- **Desafíos Planteados por Industria 4.0**
- **Gestión de la Ciberseguridad en ICSs**
- **Herramientas para Mejora de la Ciberseguridad en ICSs**
- **Resumen y Conclusiones**

# Resumen y Conclusiones

## Resumen

Industria 4.0 requiere la integración entre los ICS con la red corporativa, y con Internet, exponiendo a los ICSs a ciberataques.

La implementación de un sistema de gestión de ciberseguridad basado en estándares internacionales, y el uso de equipos y técnicas y equipos adecuados de networking son requerimientos mínimos de ciberseguridad.

Se presentaron los siguientes aportes a la ciberseguridad en ICS:

Uso de Forensia en vivo: Puede hacerse análisis sin detener los sistemas. Incluso, puede usarse sus resultados para prevención.

Criptografía en ICS: Permitiría atender a las dificultades de los SCADA en confidencialidad e integridad (evidando robos de secretos y ciertos hackeos).

Ciberdefensa desplegable: Concepto de origen militar que puede aplicarse a la industria, para prevención de incidentes, y para facilitar la restauración de incidentes.

# Resumen y Conclusiones

## Conclusiones

Es un obstáculo para la ciberseguridad industrial la dificultad de implementar Sistemas de Gestión basados en Buenas Prácticas, así como lograr inversiones en Networking

Los aportes presentados permiten reforzar los perfiles de ciberseguridad en ICS e IIoT: Uso de Forensia en OT, Criptografía y Ciberdefensa Desplegable.

# Resumen y Conclusiones

## Conclusiones

Es un obstáculo para la ciberseguridad industrial la dificultad de implementar Sistemas de Gestión basados en Buenas Prácticas, así como lograr inversiones en Networking

Los aportes presentados permiten reforzar los perfiles de ciberseguridad en ICS e IIoT: Uso de Forensia en OT, Criptografía y Ciberdefensa Desplegable.

Conozca nuestro proyecto =====>

**¡Muchas Gracias!**



## Referencias:

- [01] Wikipedia, "Sistema de Control Distribuido" (2021).  
En línea: [https://es.wikipedia.org/wiki/Sistema\\_de\\_control\\_distribuido](https://es.wikipedia.org/wiki/Sistema_de_control_distribuido)
- [02] Kamlofsky J. "Webinar: Ciberseguridad y análisis forense en entornos industriales" Universidad FASTA. En línea: <https://lnkd.in/dQnWpPxG>(2022).
- [03] Ybzunza Cortes C. y otros. El Entorno de la Industria 4.0: Implicaciones y Perspectivas Futuras. "Conciencia Tecnológica" n°54, 2017.
- [04] Henning, K. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0.
- [05] Brunete A., San Segundo P., Herrero R. "Introducción a la Automatización Industrial". Universidad Politécnica de Madrid. ISBN: 978-84-09-22291-9, (2020). En linea: [https://bookdown.org/alberto\\_brunete/introAutomatica/](https://bookdown.org/alberto_brunete/introAutomatica/)
- [06] Kamlofsky, J., Colombo, H., Sliafertas, M., & Pedernera, J. (2015, November). Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. In III Congreso Nacional de Ingeniería Informática/Sistemas de Información (CONAIISI 2015), ISSN (pp. 2346-9927).
- [07] Pozzi, Mariano. "Evolución del Malware y Defensa ante Ataques Dirigidos a Infraestructuras Críticas". Universidad Abierta Interamericana, 2021
- [08] Alberdi J.I. et al. (2024). GUÍA-ICI : guía para el abordaje de incidentes de ciberseguridad en infraestructuras críticas industriales. - 1a ed - Mar del Plata: Universidad FASTA; Ciudad Autónoma de Buenos Aires : Universidad Abierta Interamericana; Universidad de la Defensa Nacional.
- [09] Romero R.O. (2021). Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas.
- [10] Kamlofsky Jorge, Romero Oscar.(2022) "Live Forensic Analysis on an ICS SCADA". VI Info-Conf,