

2025 - Día 3/3



INGELEARN

# MASTERCLASS

Python • Ciberseguridad • Inteligencia Artificial

4.0

## CUADERNO DE TRABAJO DÍA 3

### CIBERSEGURIDAD INDUSTRIAL

DA TUS PRIMEROS PASOS PARA CONVERTIRTE EN  
UN ESPECIALISTA

[INGELEARN.COM](https://ingelearn.com)

INGELEARN

# LO QUE APRENDERÁS HOY

En esta última jornada, nos adentraremos en un tema clave para la industria moderna: la **ciberseguridad**.

Descubriremos qué es realmente un **hacker** y qué tipos existen, además de entender por qué la seguridad industrial es hoy más importante que nunca.

Analizaremos los ciberataques más comunes en **entornos industriales**, conoceremos normativas específicas y revisaremos casos reales de ataques a sistemas.

Por último, veremos qué estrategias y técnicas podemos implementar para **proteger nuestras instalaciones** y procesos de amenazas cada vez más sofisticadas.

¿Todo listo? ¡Comencemos!

INGELEARN

# INSTRUCTOR



**IGNACIO LAVAGGI**  
Especialista en Automatización

Soy programador industrial hace más de 10 años, y me especializo en sistemas de control basados en PLCs, además de contar con experiencia en múltiples áreas de la industria convencional

Siempre me mantengo aprendiendo, y últimamente estoy enfocado en el desarrollo de soluciones de Industria 4.0, ML, e IA

Tengo además mucha experiencia como docente e instructor, así que:  
Acá estoy para darles una mano ¡Un placer conocerlos!

# TOP SECRET



## PALABRAS CLAVE

¡ANOTA AQUÍ LA PALABRA CLAVE DE HOY!

### **Nota sobre las palabras clave:**

Las palabras clave pueden aparecer en cualquier momento de la clase. No las diremos en voz alta, pero te aseguramos que las verás. Es una clave por día, así que ¡Presta atención!

No spamees el chat pidiendo por la palabra clave o el certificado. Recuerda que estamos aquí para aprender.

Si te perdiste el momento donde está la palabra clave, podrás ver la repetición cargada en YouTube para buscarla allí.

Obtendrás tu certificado **AL INGRESAR LAS TRES PALABRAS CLAVE EN SU LUGAR DESIGNADO EN LA PLATAFORMA.**

De no recibir tu certificado en ese período, escribe a [certificaciones@ingelearn](mailto:certificaciones@ingelearn), con nombre, apellido y las tres palabras clave.

# CONTENIDO

PARTÉ

1

## CIBERSEGURIDAD

¿En qué consiste?

PARTÉ

2

## TIPOS DE HACKER

No todo es como en las películas.

PARTÉ

3

## PUNTOS VULNERABLES

Áreas donde debemos prestar especial atención.

PARTÉ

4

## VULNERABILIDADES CONOCIDAS

Un repaso de las piezas de software más infames de la historia

PARTÉ

5

## OPEN SOURCE INTELLIGENCE

El que busca, encuentra.

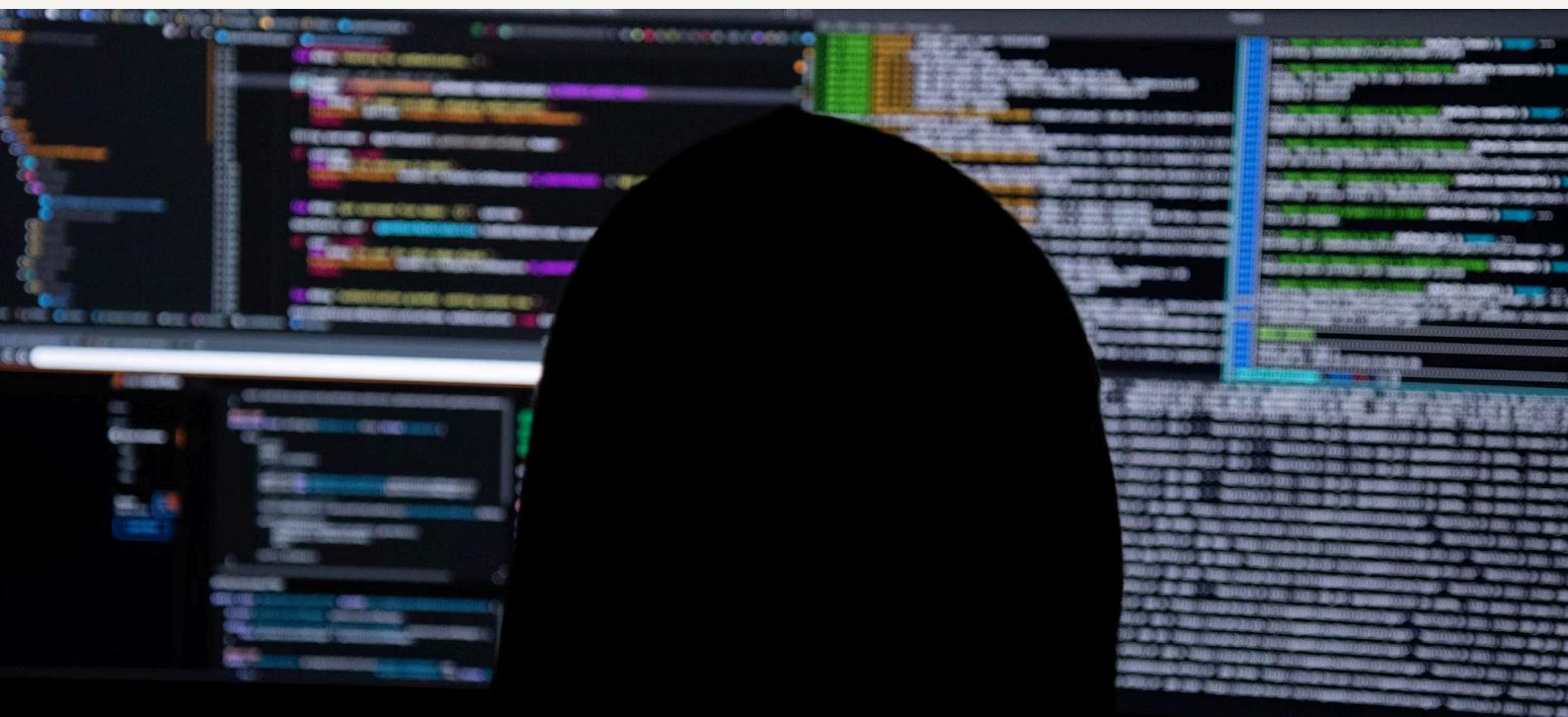
# CIBERSEGURIDAD

En la actualidad, la **ciberseguridad** se percibe, en muchos casos, como un campo reservado solo para expertos o grandes corporaciones. Sin embargo, la realidad es que este tema nos involucra a todos.

Tanto personas como empresas, sin importar su tamaño o sector, están expuestas a amenazas cada vez más frecuentes y sofisticadas.

Hoy, vamos a ver qué es un **hacker**, los tipos de ataques más comunes y qué medidas podemos tomar para proteger nuestros sistemas y procesos.

Entender cómo proteger la información y los sistemas no es solo una ventaja, sino una necesidad para el mundo moderno. Aunque parezca algo lejano, la ciberseguridad es una **necesidad en todos los entornos**.



# TIPOS DE HACKER

Los tipos de hacker se clasifican por “colores”, en función de su propósito y motivación. Éste área es para que puedas describirlos



1.



2.



3.



4.



5.



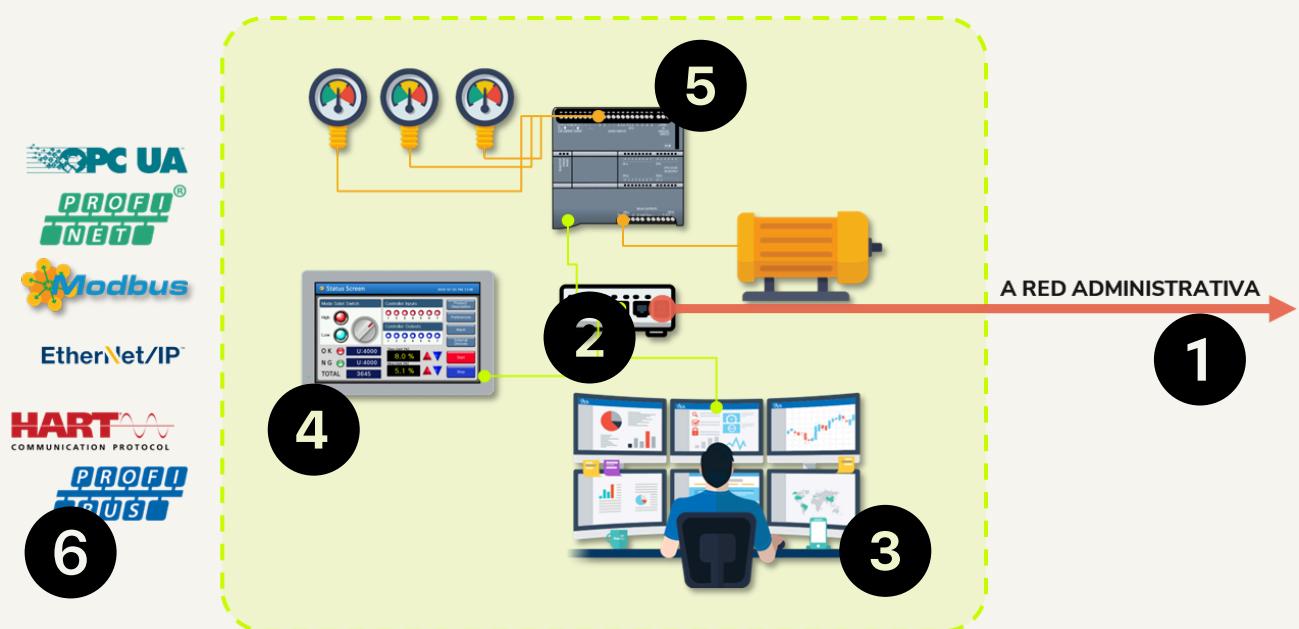
6.



Notas adicionales:

# PUNTOS VULNERABLES

Esta sección es para que puedas anotar las áreas vulnerables más comunes de los sistemas industriales.



1.

2.

3.

4.

5.

6.

# VULNERABILIDADES CONOCIDAS

Algunos de los malware más famosos, que han causado estragos a lo largo y ancho del mundo.



## **Stuxnet [2010]:**

un malware extremadamente sofisticado que infectó sistemas SCADA, dirigido específicamente a las centrifugadoras de enriquecimiento de uranio en Irán. Fue el primer ataque conocido que causó daño físico a equipos industriales mediante software.

## **Industroyer [2016]:**

herramienta maliciosa creada para atacar redes eléctricas. Fue responsable de un apagón en Ucrania, afectando la distribución de energía mediante la manipulación directa de los sistemas de control de subestaciones.

## **Wannacry [2017]:**

ransomware que se propagó rápidamente por el mundo, cifrando archivos de empresas, hospitales y organismos públicos. Explotó una vulnerabilidad en sistemas Windows, provocando interrupciones críticas en servicios de salud y transporte.

## **ILOVEYOU [2000]:**

gusano que llegó a millones de usuarios a través de un correo con un archivo adjunto disfrazado de carta de amor. Se propagó masivamente y eliminó archivos de los sistemas infectados, causando grandes pérdidas económicas.

## **Petya / NotPetya [2017]:**

disfrazado de ransomware, su verdadero propósito era la destrucción de datos. Afeció infraestructuras críticas y grandes compañías multinacionales, paralizando operaciones enteras y provocando daños millonarios. Lo llamativo, es que usaba el famoso servicio de almacenamiento en la nube Dropbox para propagarse.

## **BlackEnergy [2015]:**

malware utilizado principalmente en Europa del Este para atacar sistemas de energía e infraestructuras industriales. Se infiltraba mediante correos maliciosos y permitía a los atacantes tomar control remoto de sistemas críticos.



“

**La frase más  
peligrosa del  
idioma es “Eso  
siempre lo  
hicimos así”**

-

Grace Hopper

Desarrolladora del primer  
compilador, creadora del lenguaje  
COBOL, y la razón por la que le  
decimos “bug” a los errores en un  
programa

# OSINT - OPEN SOURCE INTELLIGENCE

## EL ARTE DE SABER BUSCAR

**OSINT (Open Source Intelligence)** es la recopilación y análisis de información obtenida de fuentes públicas y accesibles, como redes sociales, sitios web, foros, medios de comunicación y bases de datos abiertas.

Esta práctica permite obtener datos valiosos sin la necesidad de acceder a sistemas privados o protegidos. Se utiliza tanto en ciberseguridad como en inteligencia militar, investigaciones criminales o análisis de riesgos, ya que puede revelar información crítica sobre personas, empresas o infraestructuras a partir de **lo que está disponible libremente en internet**.



# PASOS PARA HACER PENTESTING

Cada vez que nos encontremos con un sistema industrial, debemos tomar los recaudos necesarios. SIEMPRE debemos tener permiso para identificar vulnerabilidades.



# NOTAS DE CLASE

Puedes anotar aquí todo lo que quieras, o creas conveniente

# NOTAS DE CLASE

Puedes anotar aquí todo lo que quieras, o creas conveniente

# NUESTROS ALUMNOS

ÉSTOS SON ALGUNOS DE LOS TESTIMONIOS QUE DEJARON NUESTROS ALUMNOS EN GOOGLE.



## SERGIO D. VELAZQUEZ

Buen día ! Excelente introducción al mundo de los PLC. Además de muy buena combinación entre teoría y práctica! Y sobre todo muy buena asistencia de los profes para evacuar inquietudes!



## JORDAN MENDEZ

Excelente capacitación, muy buena explicación, se destaca mucho el acompañamiento del profesor para con los alumnos. Siempre tuve una buena experiencia con los cursos que tome de la página, muy recomendables



## SEBASTIÁN LÓPEZ

Sorprendido gratamente por el alto nivel que se puede apreciar tanto en la calidad educativa, en el espacio de capacitación y en el material de aprendizaje. Sumamente recomendable.



## PABLO HRBACEK

Contenido muy amplio de tecnologías actuales que permite realizar una solución completa. Excelente predisposición del profe a consultas fuera de las clases.



# POR TIEMPO LIMITADO

POR MUY POCOS DÍAS A PARTIR DE ÉSTA FECHA PUEDEN ADQUIRIR  
NUESTRO PAQUETE DE CAPACITACIONES

## CERTIFICACIÓN AVANZADA EN INDUSTRIA 4.0

Programa cuidadosamente diseñado para comenzar a desarrollar soluciones de Industria 4.0 en un mundo en el que la automatización industrial está cambiando rápidamente.  
**No es necesaria experiencia previa**, ya que todos los temas se ven desde el comienzo.

El paquete consta de 6  **cursos** en total, desarrollados con las últimas tecnologías:

- Python nivel I – Introducción y primeros pasos
- Python nivel II – El camino hacia la industria 4.0
- Python nivel III – Aplicaciones y análisis de datos
- Ciberseguridad Industrial – Nivel 1: Fundamentos
- Ciberseguridad Industrial – Nivel 2: Prácticas y pentesting de equipos reales
- Open CV – Reconocimiento de imágenes con IA

MAS INFO  
(Grupo VIP)



**POR TIEMPO LIMITADO, CON TU COMPRA ADEMÁS, TE REGALAMOS**

- Acceso a los 3 niveles de la academia de inglés técnico
- Curso “Arma tu CV”
- Acceso a la IA de Ingelearn, entrenada para entornos industriales
- Acceso a la bolsa de trabajo
- Grupo exclusivo de Whatsapp y Discord

**DISPONIBLE PARA CUALQUIER  
LUGAR DEL MUNDO  
FINANCIAMIENTO EN CUOTAS**



**TODOS** nuestros cursos son:

- Tuyos, de por vida
- A tu ritmo
- Acompañados por el instructor
- Con ejercicios para resolver
- Con prácticas de situaciones reales

- Accesibles 24/7, los 365 días del año
- Con objetivos y metas claras
- Con plataforma propia
- Certificados
- Repetibles las veces que quieras

# ¡GRACIAS!

Por acompañarnos éstas tres jornadas de capacitación. Esperamos que te hayan sido de utilidad, y que te hayas llevado nuevas herramientas, para poder impulsar tu curiosidad.

**Queremos verte crecer.**

Compartí tus avances de tu cuaderno de trabajo con nosotros.

¡Etiquetanos en tus historias!

