DOSSIER DE FORMACIÓ

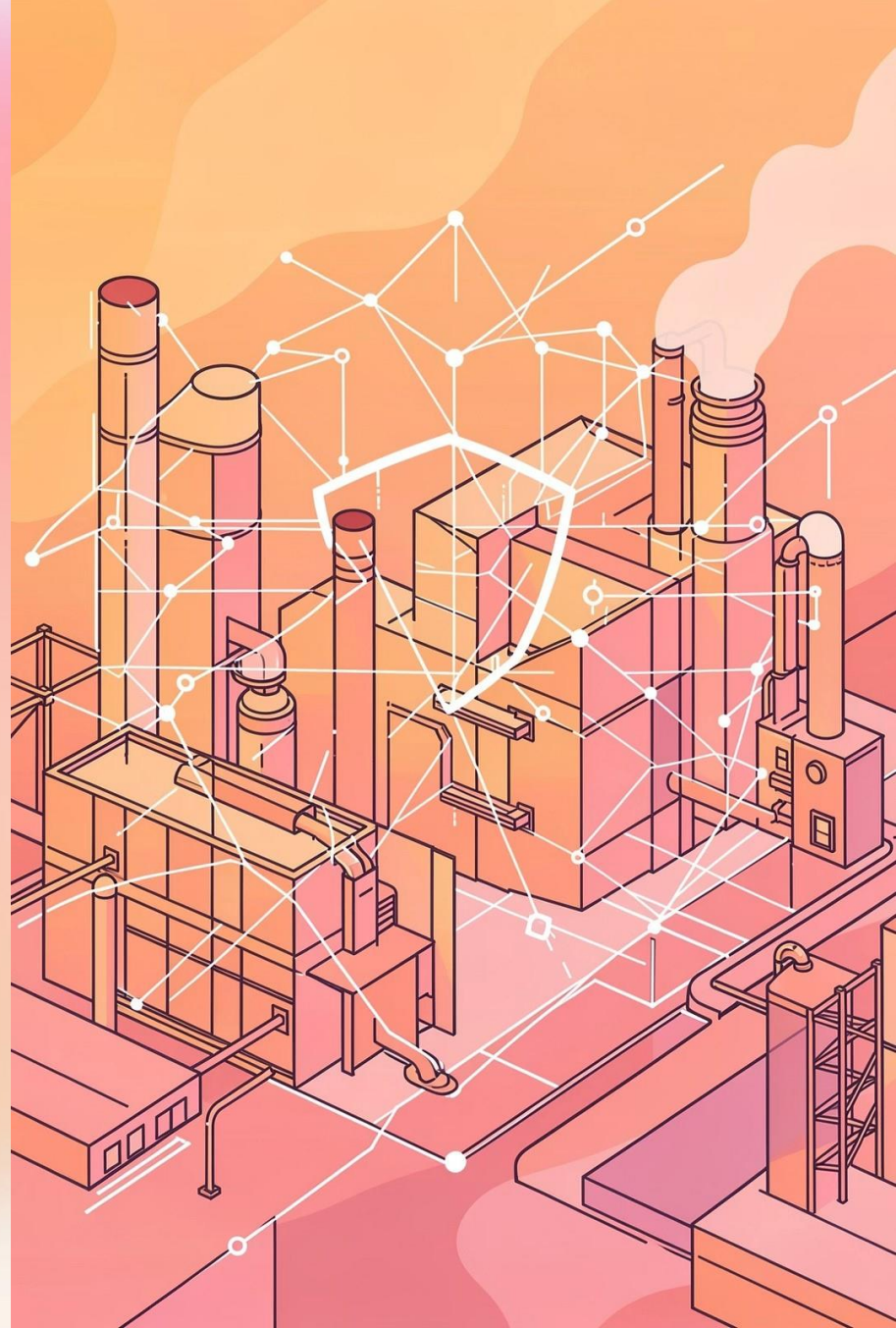
CIBERSEGURETAT INDUSTRIAL I GESTIÓ DEL RISC

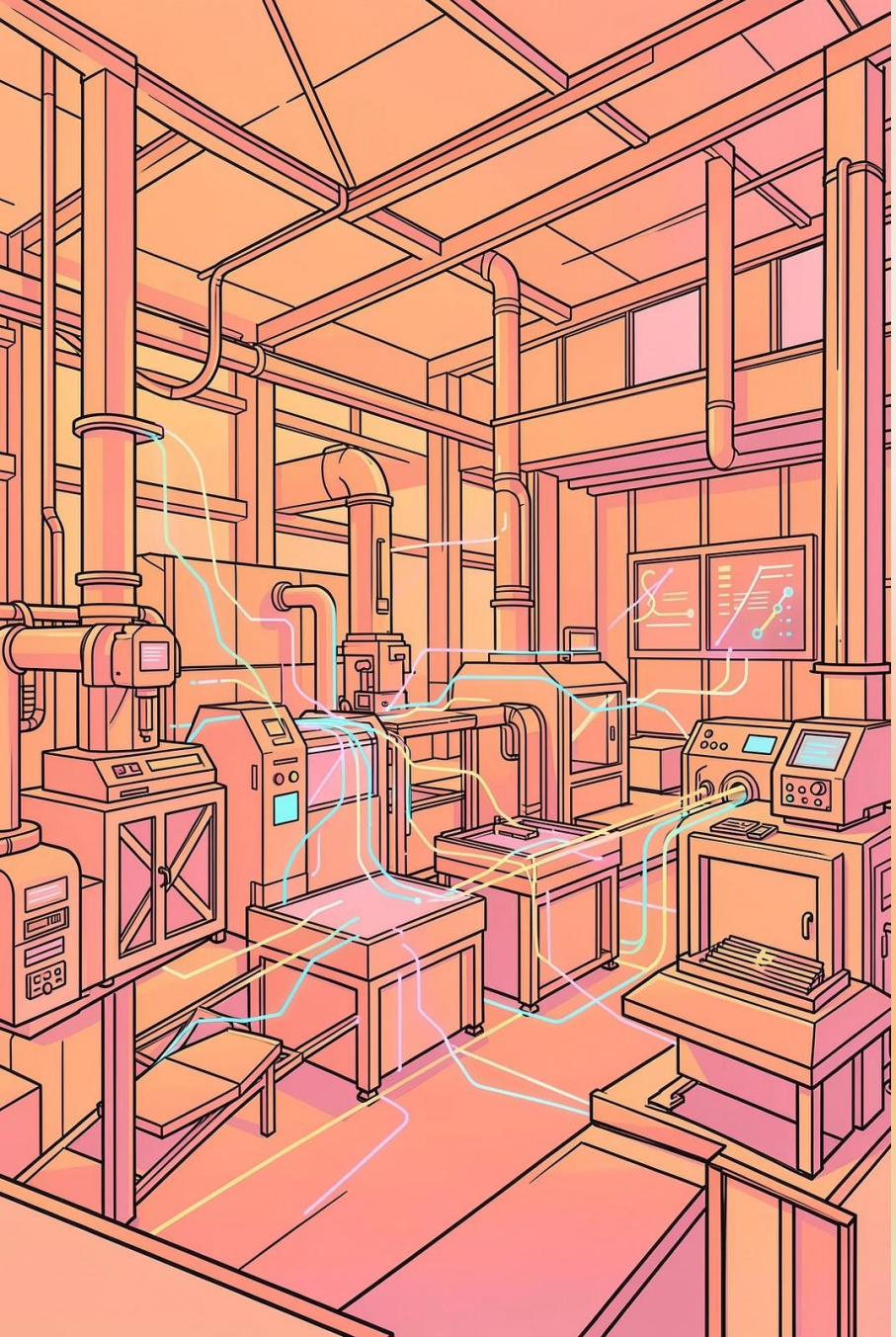
2 Jornades · 4 hores totals

Impartit per: **Joaquim Elcacho Gelonch**

CEO 3 INCYBER

Especialista en Ciberseguretat Industrial, Gestió de Riscos i Protecció d'Infraestructures Crítiques





01 PRESENTACIÓ

La digitalització i la Indústria 4.0 han incrementat exponencialment la superfície d'atac de les organitzacions. La ciberseguretat ja no és un problema exclusivament tècnic: és un risc empresarial que afecta a la continuïtat operativa, la producció i la reputació.

Aquest curs ofereix una visió estratègica i pràctica per comprendre i gestionar els riscos de ciberseguretat en entorns empresarials i industrials.

02 OBJECTIUS

Al finalitzar la formació, els assistents seran capaços de:

- **Entendre el impacte real del cibercrim en la indústria.**
- **Diferenciar clarament entre riscos IT i OT.**
- **Aplicar un model estructurat d'anàlisi de riscos.**
- **Identificar mesures tècniques i organitzatives prioritàries.**
- **Comprendre les obligacions derivades de NIS2.**
- **Definir les bases d'un Pla Director de Ciberseguretat.**

03 ESTRUCTURA DEL CURS

Jornada 1 (2 hores)

Context, amenaces i gestió del risc

Indústria 4.0 i nova superfície d'atac

- Evolució industrial 1.0 → 4.0
- Digitalització, IoT i automatització
- Com canviar el risc en entorns connectats

Fonaments de Ciberseguretat

- Confidencialitat, integritat i disponibilitat
- Concepte de risc (Probabilitat x Impacte)
- Diferències entre IT i OT

OT vs IT: Prioritats diferents

- Disponibilitat com a prioritat industrial
- Risc físic vs risc digital
- Casos reals d'impacte en infraestructures

Amenaces actuals

- Crim organitzat digital
- Ransomware
- Phishing
- Casos reals en indústria i grans corporaions

Exercici pràctic: Introducció a matriu de riscos.

03 ESTRUCTURA DEL CURS

Jornada 2 (2 hores)

Mesures pràctiques i compliment normatiu

Gestió del risc en 6 passos

- Definició de l'abast
- Identificació d'actius
- Amenaces i vulnerabilitats
- Avaluació i tractament dels ris

Mesures tècniques prioritàries

- Segmentació i microsegmentació
- Model de zones (Purdue)
- Backups 3-2-1
- Diferència entre backup, snapshot i replicació
- Control d'accessos i autenticació forta

Mesures organitzatives clau

- Formació i conscienciació
- Política de seguretat
- Pla de continuïtat de negoci
- Pla Director de Seguretat

NIS2 i obligacions regulatòries

- Sectors afectats
- Gestió d'incidents
- Seguretat en la cadena de subministrament
- Requisits organitzatius mínims

Conclusió: Com iniciar el roadmap de millores en l'empresa.

04 METODOLOGIA

- Enfocament estratègic i pràctic
- Casos reals i exemples aplicats
- Llenguatge accessible per a perfils tècnics i no tècnics
- Espai de debat i preguntes

05 PERFIL DE PARTICIPANTS

- Direcció general
- Responsables IT / OT
- Producció i manteniment
- Qualitat i compliment normatiu
- Comandaments intermedis

06 ENTREGABLES

Els assistents rebran:

- **Plantilla bàsica de matriu de riscos**
- **Checklist de ciberseguretat industrial**
- **Guia resumida de mesures prioritàries**
- **Certificat d'assistència**