



Orientacions als centres educatius per a organitzar el Curs d'especialització en Ciberseguretat en Entorns de les Tecnologies d'Operació

Curs d'Especialització

1. Denominació

Ciberseguretat en Entorns de les Tecnologies d'Operació. (Reial decret 478/2020, de 7 d'abril)

2. Família professional.

Electricitat i electrònica.

3. Competència general.

La competència general d'aquest curs d'especialització consisteix a definir i implementar estratègies de seguretat en les organitzacions i infraestructures industrials realitzant diagnòstics de ciberseguretat, identificant vulnerabilitats i implementant les mesures necessàries per a mitigar-les aplicant la normativa vigent i estàndards del sector, seguint els protocols de qualitat, de prevenció de riscos laborals i respecte ambiental.

4. Competències professionals, personals i socials

- a) Determinar perfils de risc de les organitzacions identificant bones pràctiques, estàndards i normativa aplicable.
- b) Verificar alineació dels equips i sistemes de les organitzacions en relació als principis de la seguretat informàtica i dels riscos de ciberseguretat.
- c) Elaborar informes de ciberseguretat relatius a sistemes i entorns industrials tant a nivell tècnic com organitzatiu i avaluant els elements de seguretat desplegats.
- d) Aplicar estratègies de ciberseguretat en les fases dels projectes industrials per a minimitzar l'impacte de qualsevol possible incident.
- e) Caracteritzar l'evolució dels sistemes de control industrial valorant-ne l'impacte en l'organització.
- f) Establir la configuració de sistemes de control industrial minimitzant els riscos de l'organització.
- g) Aplicar les metodologies reconegudes en el sector valorant els escenaris de risc tecnològic en xarxes industrials.
- h) Identificar vulnerabilitats i establir la configuració de dispositius de xarxes minimitzant els escenaris de risc.
- i) Realitzar anàlisi forenses en sistemes i xarxes industrials detectant vulnerabilitats en l'organització.

- j) Integrar les normes i procediments de seguretat física, operacional i de ciberseguretat en entorns d'operació minimitzant els riscos.
- k) Elaborar documentació tècnica i administrativa d'acord amb la legislació vigent i amb els requeriments del client.
- l) Adaptar-se a les noves situacions laborals, mantenint actualitzats els coneixements científics, tècnics i tecnològics relatius al seu entorn professional, gestionant la seva formació i els recursos existents en l'aprenentatge al llarg de la vida.
- m) Resoldre situacions, problemes o contingències amb iniciativa i autonomia en l'àmbit de la seva competència, amb creativitat, innovació i esperit de millora en el treball personal i en el dels membres de l'equip.
- n) Generar entorns segurs en el desenvolupament del seu treball i el del seu equip, supervisant i aplicant els procediments de prevenció de riscos laborals i ambientals, d'acord amb el que s'estableix per la normativa i els objectius de l'organització.
- o) Supervisar i aplicar procediments de gestió de qualitat, d'accessibilitat universal i de «disseny per a tothom», en les activitats professionals incloses en els processos de producció o prestació de serveis

5. Capacitats clau

Són les capacitats transversals que afecten diferents llocs de treball i que són transferibles a noves situacions de treball. Entre aquestes capacitats destaquen les d'autonomia, d'innovació, d'organització del treball, de responsabilitat, de relació interpersonal, de treball en equip i de resolució de problemes.

L'equip docent ha de potenciar l'adquisició de les competències professionals, personals i socials i de les capacitats clau a partir de les activitats programades per desplegar el currículum d'aquest cicle formatiu.

6. Objectius generals

- a) Analitzar bones pràctiques, estàndards d'aplicació i normativa per a definir perfils de risc.
- b) Definir i incorporar requisits de ciberseguretat en totes les fases d'un projecte industrial per a evitar possibles incidents.
- c) Identificar i analitzar les tecnologies avançades d'aplicació en entorns OT (Tecnologies de l'operació) per a verificar l'alineació amb els principis de seguretat informàtica i els riscos de ciberseguretat.
- d) Analitzar la convergència de les pràctiques professionals en els entorns OT i IT (Tecnologies de la informació) i les exigències que suposa per a aplicar estratègies de ciberseguretat i caracteritzar l'evolució dels sistemes de control industrial.

- e) Definir i parametritzar sistemes de control industrial conforme als requisits establerts i controls d'auditoria per a establir la configuració d'aquests.
- f) Identificar i caracteritzar equips i configuracions de xarxes industrials per a realitzar llistats de possibles vulnerabilitats.
- g) Avaluar nivells de risc associats a les xarxes d'instal·lacions industrials per a identificar vulnerabilitats.
- h) Seleccionar i emprar diferents eines per a realitzar anàlisis forenses.
- i) Definir i aplicar configuracions en xarxes industrials minimitzant riscos per a integrar els requeriments de seguretat.
- j) Aplicar metodologies d'anàlisi forense en sistemes SCADA, DCS, PLC, robòtica industrial, dispositius IoT (Internet de les coses) i xarxes industrials per a integrar procediments de seguretat.
- k) Realitzar informes per a la presentació de resultats i conclusions d'anàlisi forense per a elaborar documentació tècnica i administrativa.
- l) Determinar la normativa i els procediments aplicables a la seguretat física, a la seguretat operacional i a la ciberseguretat per a integrar normes i procediments de seguretat.
- m) Definir i aplicar metodologies per a la gestió integral de riscos de seguretat en entorns de l'operació
- n) Desenvolupar manuals d'informació per als destinataris, utilitzant les eines ofimàtiques i de disseny assistit per ordinador per a elaborar la documentació tècnica i administrativa.
- o) Desenvolupar la creativitat i l'esperit d'innovació per a respondre als reptes que es presenten en els processos i en l'organització del treball i de la vida personal.
- p) Analitzar i utilitzar els recursos i oportunitats d'aprenentatge relacionats amb l'evolució científica, tecnològica i organitzativa del sector i les tecnologies de la informació i la comunicació, per a mantenir l'esperit d'actualització i adaptar-se a noves situacions laborals i personals.
- q) Avaluar situacions de prevenció de riscos laborals i de protecció ambiental, proposant i aplicant mesures de prevenció personals i col·lectives, d'acord amb la normativa aplicable en els processos de treball, per a garantir entorns segurs.
- r) Identificar i proposar les accions professionals necessàries, per a donar resposta a l'accessibilitat universal i al «disseny per a tothom».
- s) Identificar i aplicar paràmetres de qualitat en els treballs i activitats realitzats en el procés d'aprenentatge, per a valorar la cultura de l'avaluació i de la qualitat i ser capaços de supervisar i millorar procediments de gestió de qualitat

7. Taula de mòduls professionals, durada i especialitat de professorat

Mòduls professionals	Durada (h)	Especialitat del cos de professorat
MP1. Ciberseguretat en projectes industrials	99	PS512 Organització i projectes de fabricació mecànica PS524 Sistemes electrònics PS525 Sistemes electrotècnics i automàtics Especialista
MP2. Sistemes de control industrial segurs	99	PS512 Organització i projectes de fabricació mecànica PS524 Sistemes electrònics PS525 Sistemes electrotècnics i automàtics Especialista
MP3. Xarxes de comunicacions industrials segures	132	PT602 Equips electrònics PT606 Instal·lacions electrotècniques Especialista
MP4. Anàlisi forense en ciberseguretat industrial	132	PT602 Equips electrònics PT606 Instal·lacions electrotècniques Especialista
MP5. Seguretat integral	132	PS512 Organització i projectes de fabricació mecànica PS524 Sistemes electrònics PS525 Sistemes electrotècnics i automàtics Especialista

Mòduls professionals	Durada (h)	Especialitat del cos de professorat
MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació	126	PS512/ PS524/ PS525 PT602/ PT606 ESP

8. Assignació horària de professorat

Mòduls professionals	Grup ≤ 20 alumnes	Desdoblament (%)	Grup > 20 alumnes
MP1. Ciberseguretat en projectes industrials	99	100	198
MP2. Sistemes de control industrial segurs	99	100	198
MP3. Xarxes de comunicacions industrials segures	132	100	264
MP4. Anàlisi forense en ciberseguretat industrial	132	100	264
MP5. Seguretat integral	132	100	264
MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació	126	100	252

9. Incorporació de la llengua anglesa al Curs d'especialització

Les necessitats d'un mercat de treball integrat a la Unió Europea fan que la llengua anglesa esdevingui fonamental en la inserció laboral de l'alumnat dels cursos d'especialització. D'altra banda cal donar resposta al compromís amb els objectius educatius sobre l'anglès plantejats per als propers anys per la pròpia Unió Europea. Amb la finalitat d'incorporar i normalitzar l'ús de la llengua anglesa en situacions professionals habituals i en la presa de decisions en l'àmbit laboral, s'hauran de dissenyar activitats d'ensenyament-aprenentatge que incorporin la utilització de la llengua anglesa, en tots mòduls professionals del curs d'especialització d'acord amb el resultat d'aprenentatge i criteris d'avaluació següents:

Resultat d'aprenentatge

1. Interpreta informació professional en llengua anglesa -manuais tècnics, instruccions, catàlegs de productes i/o serveis, articles tècnics, informes, normativa, entre d'altres-, aplicant-ho en les activitats professionals més habituals.

Criteris d'avaluació

- 1.1. Aplica en situacions professionals la informació continguda en textos tècnics o normativa relacionats amb l'àmbit professional.
- 1.2. Identifica i selecciona amb agilitat els continguts rellevants de novetats, articles, notícies, informes i normativa, sobre diversos termes professionals.
- 1.3. Analitza detalladament les informacions específiques seleccionades.
- 1.4. Actua en conseqüència per donar resposta als missatges tècnics rebuts a través de suports convencionals -correu postal, fax- o telemàtics -correu electrònic, web.
- 1.5. Selecciona i extreu informació rellevant en llengua anglesa segons prescripcions establertes, per elaborar en llengua pròpia comparatives, informes breus o extractes.
- 1.6. Complimenta en llengua anglesa documentació i/o formularis del camp professional habituals.
- 1.7. Utilitza suports de traducció tècnics i les eines de traducció assistida o automatitzada de textos.

10. Requisits d'accés al curs d'especialització:

Per a accedir al Curs d'Especialització en Ciberseguretat en entorns de les tecnologies d'operació és necessari estar en possessió d'algun dels següents títols:

Tècnic/a superior en Sistemes Electrotècnics i Automatitzats

Tècnic/a superior en Automatització i Robòtica Industrial

Tècnic/a superior Manteniment Electrònic

Tècnic/a superior en Sistemes de Telecomunicacions i Informàtics

Tècnic/a en Mecatrònica Industrial.

11. Espais formatius

Espai formatiu	Superfície m ² (30 alumnes)	Superfície m ² (20 alumnes)	Grau d'ús
Aula polivalent	45	30	15%
Aula d'informàtica ⁽¹⁾	120	80	35%
Laboratori de sistemes automàtics ⁽¹⁾	180	120	25%
Taller de sistemes automàtics ⁽¹⁾	200	130	25%

(1) Els espais requerits per al cicle formatiu de grau superior d'Automatització i Robòtica Industrial, que dona accés a aquest curs d'especialització, es consideraran suficients, sempre que hi hagi compatibilitat horària

12. Equipaments

Espai	Equipament
Aula polivalent	Sistema de projecció. Ordinadors en xarxa i amb accés a Internet. Dispositius d'emmagatzematge en xarxa. Escàner. Sistemes de reprografia. Equips audiovisuals
Aula d'informàtica	Sistema de projecció. Ordinadors en xarxa i amb accés a Internet. Escàner. Plotter. Programes de gestió de projectes. Sistemes de reprografia. Equips audiovisuals. Programari de disseny i simulació de sistemes d'automatització i robòtica industrial. Programari de desenvolupament de sistemes de control de l'operació SCADA.

Espai	Equipament
Laboratori de sistemes automàtics	<p>Sistema de projecció.</p> <p>Ordinadors en xarxa i amb accés a Internet.</p> <p>Sistemes de reprografia.</p> <p>Programari d'aplicació.</p> <p>Elements mesuradors i captadors, especialment amb tecnologies integrades de comunicacions, tipus IoT.</p> <p>Elements actuadors, especialment amb tecnologies integrades de comunicacions, tipus IoT.</p> <p>Elements de comandament i maniobra.</p> <p>Elements de protecció.</p> <p>Transformadors.</p> <p>Polímetres.</p> <p>Fonts d'alimentació.</p> <p>Freqüencímetres.</p> <p>Autòmats programables.</p> <p>Oscil·loscopis.</p> <p>Injector de senyals.</p> <p>Eines i màquines portàtils de mecanitzat per a electricitat. Bancs d'assajos, control, regulació i acoblament de màquines elèctriques estàtiques i rotatives.</p> <p>Pinces amperimètriques.</p> <p>Tacòmetres.</p> <p>Diversos tipus de motors.</p> <p>Fonts d'alimentació.</p> <p>Transformadors monofàsics.</p> <p>Transformadors trifàsics.</p> <p>Arrencadors progressius.</p> <p>Elements i entrenadors de comunicacions industrials.</p> <p>Equipaments i elements de mesurament i control.</p> <p>Equipament per a la realització d'assajos.</p>

Espai	Equipament
Taller de sistemes automàtics	Sistema de projecció. Ordinadors en xarxa i amb accés a Internet. Sistemes de reprografia. Equips i eines de mecanitzat manual. Equipaments i elements de mesurament i control. Equipament per a la realització de mesuraments i verificació d'elements. Mecanismes. Panells modulars per al muntatge de sistemes. Elements per a muntatge i simulació de sistemes hidràulics, pneumàtics, electro-hidràulics i electro-pneumàtics. Eines portàtils per a mecanitzat. Simuladors d'estacions: distribució, verificació, processament, robot i uns altres. Autòmats programables. Equips de verificació i mesura. Programari d'aplicació.

13. Relació de les competències professionals, personals i socials, i els objectius generals amb els mòduls professionals.

Els resultats d'aprenentatge i els continguts dels mòduls professionals capaciten a l'alumnat per a assolir les competències professionals, personals i socials (CPPeS) i els objectius generals (OG).

La taula 1 relaciona les competències professionals, personals i socials (CPPeS) amb els mòduls professionals.

COMPETÈNCIES PROFESSIONAL, PERSONALS I SOCIALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
a) Determinar perfils de risc de les organitzacions identificant bones pràctiques, estàndards i normativa aplicable.	X					X
b) Verificar alineació dels equips i sistemes de les organitzacions en relació a els principis de la seguretat informàtica i dels riscos de ciberseguretat.		X				X
c) Elaborar informes de ciberseguretat relatius a sistemes i entorns industrials tant de nivell tècnic i organitzatiu avaluant els elements de seguretat desplegats.		X				X
d) Aplicar estratègies de ciberseguretat en les fases dels projectes industrials per a minimitzar l'impacte de qualsevol possible incident.	X					X
e) Caracteritzar l'evolució dels sistemes de control industrial valorant el seu impacte en l'organització.		X				X

COMPETÈNCIES PROFESSIONAL, PERSONALS I SOCIALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
f) Establir la configuració de sistemes de control industrial minimitzant els riscos de l'organització.		X				X
g) Aplicar les metodologies reconegudes en el sector valorant els escenaris de risc tecnològic en xarxes industrials			X			X
h) Identificar vulnerabilitats i establir la configuració de dispositius de xarxes minimitzant els escenaris de risc.			X			X
i) Realitzar anàlisi forenses en sistemes i xarxes industrials detectant vulnerabilitats en l'organització				X		X
j) Integrar les normes i procediments de seguretat física, operacional i de ciberseguretat en entorns d'operació minimitzant els riscos.					X	X
k) Elaborar documentació tècnica i administrativa d'acord amb la legislació vigent i amb els requeriments del client.	X	X	X	X	X	X
l) Adaptar-se a les noves situacions laborals, mantenint actualitzats els coneixements científics, tècnics i tecnològics relatius al seu entorn	X	X	X	X	X	X

COMPETÈNCIES PROFESSIONAL, PERSONALS I SOCIALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
professional, gestionant la seva formació i els recursos existents en l'aprenentatge al llarg de la vida.						
m) Resoldre situacions, problemes o contingències amb iniciativa i autonomia en l'àmbit de la seva competència, amb creativitat, innovació i esperit de millora en el treball personal i en el dels membres de l'equip.	X	X	X	X	X	X
n) Generar entorns segurs en el desenvolupament del seu treball i el del seu equip, supervisant i aplicant els procediments de prevenció de riscos laborals i ambientals, d'acord amb el que s'estableix per la normativa i els objectius de l'organització	X	X	X	X	X	X
o) Supervisar i aplicar procediments de gestió de qualitat, d'accessibilitat universal i de «disseny per a tothom», en les activitats professionals incloses en els processos de producció o prestació de serveis.	X	X	X	X	X	X

La taula 2 relaciona els objectius generals (OG) amb les mòduls professionals.

OBJECTIUS GENERALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial assegurances	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
a) Analitzar bones pràctiques, estàndards d'aplicació i normativa per a definir perfils de risc.	X					X
b) Definir i incorporar requisits de ciberseguretat en totes les fases d'un projecte industrial per a evitar possibles incidents	X					X
c) Identificar i analitzar les tecnologies avançades d'aplicació en entorns OT per a verificar l'alineació amb els principis de seguretat informàtica i els riscos de ciberseguretat.		X				X
d) Analitzar la convergència de les pràctiques professionals en els entorns OT i IT i les exigències que suposa per a aplicar estratègies de ciberseguretat i caracteritzar l'evolució dels sistemes de control industrial.		X				X
e) Definir i parametritzar sistemes de control industrial conforme a requisits establerts i controls d'auditoria per a establir la configuració d'aquests.		X				X

OBJECTIUS GENERALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial assegurances	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
f) Identificar i caracteritzar equips i configuracions de xarxes industrials per a realitzar llistats de possibles vulnerabilitats			X			X
g) Avaluar nivells de risc associats a les xarxes d'instal·lacions industrials per a identificar vulnerabilitats.			X			X
h) Seleccionar i emprar diferents eines per a realitzar anàlisis forenses.				X		X
i) Definir i aplicar configuracions en xarxes industrials minimitzant riscos per a integrar els requeriments de seguretat.			X			X
j) Aplicar metodologies d'anàlisi forense en sistemes SCADA, DCS, PLC, robòtica industrial, dispositius IoT i xarxes industrials per a integrar procediments de seguretat.				X		X
k) Realitzar informes per a la presentació de resultats i conclusions d'anàlisi forense per a elaborar documentació tècnica i administrativa.				X		X

OBJECTIUS GENERALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial assegurances	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
l) Determinar la normativa i els procediments aplicables a la seguretat física, a la seguretat operacional i a la ciberseguretat per a integrar normes i procediments de seguretat.					X	X
m) Definir i aplicar metodologies per a la gestió integral de riscos de seguretat en entorns de l'operació.					X	X
n) Desenvolupar manuals d'informació per als destinataris, utilitzant les eines ofimàtiques i de disseny assistit per ordinador per a elaborar la documentació tècnica i administrativa	X	X	X	X	X	X
o) Desenvolupar la creativitat i l'esperit d'innovació per a respondre als reptes que es presenten en els processos i en l'organització del treball i de la vida personal.	X	X	X	X	X	X
p) Analitzar i utilitzar els recursos i oportunitats d'aprenentatge relacionats amb l'evolució científica, tecnològica i organitzativa del sector i les tecnologies de la informació i la comunicació, per a mantenir l'esperit d'actualització i adaptar-se a noves situacions laborals i personals	X	X	X	X	X	X

OBJECTIUS GENERALS	MP1. Ciberseguretat en projectes industrials	MP2. Sistemes de control industrial assegurances	MP3. Xarxes de comunicacions industrials segures	MP4. Anàlisi forense en ciberseguretat industrial	MP5. Seguretat integral.	MP6. Projecte de Ciberseguretat en entorns de les tecnologies d'operació
q) Avaluar situacions de prevenció de riscos laborals i de protecció ambiental, proposant i aplicant mesures de prevenció personals i col·lectives, d'acord amb la normativa aplicable en els processos de treball, per a garantir entorns segurs.	X	X	X	X	X	X
r) Identificar i proposar les accions professionals necessàries, per a donar resposta a l'accessibilitat universal i al «disseny per a tothom».	X	X	X	X	X	X
s) Identificar i aplicar paràmetres de qualitat en els treballs i activitats realitzats en el procés d'aprenentatge, per a valorar la cultura de l'avaluació i de la qualitat i ser capaces de supervisar i millorar procediments de gestió de qualitat.	X	X	X	X	X	X