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

Curs d'Especialització

1. Denominació

Ciberseguretat en Entorns de les Tecnologies de la Informació. (Reial decret 479/2020, de 7 d'abril)

2. Família professional.

Informàtica i comunicacions.

3. Competència general.

La competència general d'aquest curs d'especialització consisteix en definir i implementar estratègies de seguretat en els sistemes d'informació realitzant diagnòstics de ciberseguretat, identificant vulnerabilitats i implementant les mesures necessàries per 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) Elaborar i implementar plans de prevenció i conscienciació en ciberseguretat en l'organització, aplicant la normativa vigent.

b) Detectar i investigar incidents de ciberseguretat, documentant-los i incloent-los en els plans de securització de l'organització.

c) Dissenyar plans de securització contemplant les millors pràctiques per l'enfortiment de sistemes i xarxes.

d) Configurar sistemes de control d'accés i autenticació en sistemes informàtics, complint els requisits de seguretat i minimitzant les possibilitats d'exposició a atacs.

e) Dissenyar i administrar sistemes informàtics en xarxa i aplicar les polítiques de seguretat establertes, garantint la funcionalitat requerida amb un nivell de risc controlat.

f) Analitzar el nivell de seguretat requerit per les aplicacions i els vectors de atac més habituals, evitant incidents de ciberseguretat.

g) Implantar sistemes segurs de desplegat de programari amb l'adequada coordinació entre els desenvolupadors i els responsables de l'operació del programari.

h) Realitzar anàlisis forenses informàtics analitzant i registrant la informació rellevant relacionada.

i) Detectar vulnerabilitats en sistemes, xarxes i aplicacions, avaluant els riscos associats.

j) Definir i aplicar procediments per al compliment normatiu en matèria de ciberseguretat i de protecció de dades personals, implementant tant internament com en relació amb tercers.

k) Elaborar documentació tècnica i administrativa complint amb la legislació vigent, responent als requisits establerts.

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 estableix 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) Identificar els principis de l'organització i normativa de protecció en ciberseguretat, planificant les accions que cal adoptar en el lloc de treball per a l'elaboració del pla de prevenció i conscienciació.

b) Auditar el compliment del pla de prevenció i conscienciació de l'organització, definint les accions correctores que puguin derivar-se per incloure-les al pla de securització de l'organització.

c) Detectar incidents de ciberseguretat implantant els controls, les eines i els mecanismes necessaris per a la seva monitorització i identificació.

d) Analitzar i donar resposta a incidents de ciberseguretat, identificant i aplicant les mesures necessàries per a la seva mitigació, eliminació, contenció o recuperació.

e) Elaborar anàlisi de riscos per identificar actius, amenaces, vulnerabilitats i mesures de seguretat.

f) Dissenyar i implantar plans de mesures tècniques de seguretat a partir dels riscos identificats per garantir el nivell de seguretat requerit.

g) Configura sistemes de control d'accés, autenticació de persones i administració de credencials per preservar la privacitat de les dades.

h) Configura la seguretat de sistemes informàtics per a minimitzar les probabilitats d'exposició a atacs.

i) Configura dispositius de xarxa per complir amb els requisits de seguretat.

j) Gestionar la seguretat de sistemes informàtics en xarxa aplicant les polítiques de seguretat requerides per garantir la funcionalitat necessària amb el nivell de risc de xarxa controlat.

k) Aplicar estàndards de verificació requerits per les aplicacions per evitar incidents de seguretat.

l) Automatitzar plans de desplegat de programari respectant els requisits relatius a control de versions, rols, permisos i altres per aconseguir un desplegat segur.

m) Aplicar tècniques d'investigació forense en sistemes i xarxes en els àmbits de l'emmagatzematge de la informació no volàtil, dels dispositius mòbils, del Cloud i dels sistemes IOT (Internet de les coses), entre d'altres, per a l'elaboració d'anàlisis forenses.

n) Analitzar informes forenses identificant els resultats de la investigació per extreure conclusions i realitzar informes.

o) Combinar tècniques de hacking ètic intern i extern per detectar vulnerabilitats que permetin eliminar i mitigar els riscos associats.

p) Identificar l'abast de l'aplicació normativa dins de l'organització, tant internament com en relació amb tercers per definir les funcions i responsabilitats de totes les parts.

q) Revisar i actualitzar procediments d'acord amb normes i estàndards actualitzats per al correcte compliment normatiu en matèria de ciberseguretat i de protecció de dades personals.

r) Desenvolupar manuals d'informació, utilitzant eines ofimàtiques i de disseny assistit per ordinador per a elaborar documentació tècnica i administrativa.

s) Analitzar i utilitzar els recursos i oportunitats d'aprenentatge relacionats amb l'evolució científica, tecnològica i organitzativa el sector i les tecnologies de la informació i la comunicació, per mantenir l'esperit d'actualització i adaptar-se a noves situacions laborals i personals.

t) Desenvolupar la creativitat i l'esperit d'innovació per respondre als reptes que es presenten en els processos i en l'organització de la feina i de la vida personal.

u) 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 garantir entorns segurs.

v) Identificar i proposar les accions professionals necessàries per donar resposta a l'accessibilitat universal i al «disseny per a tothom».

w) Identificar i aplicar paràmetres de qualitat en els treballs i activitats realitzats en el procés d'aprenentatge, per valorar la cultura de l'avaluació i de la qualitat i ser capaços de supervisar i millorar procediments de qualitat.

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

Mòduls professionals	Durada (h)	Especialitat del cos de professorat
MP1. Incidents de ciberseguretat	99	PS507 / PS524 / PS525 / ESP
MP2. Enfortiment de xarxes i sistemes	132	PT602 / PT627 / ESP
MP3. Posada en producció segura	99	PT627 / ESP
MP4. Anàlisi forense informàtic	99	PT627 / ESP
MP5. Hacking ètic	99	PS507 / PS524 / PS525 / ESP
MP6. Normativa de ciberseguretat	66	PS507 / PS524 / PS525 / ESP
MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació	126	PS507 / PS524 / PS525 / PT602 / PT627 ESP

8. Assignació horària de professorat

Mòduls professionals	Grup ≤ 20 alumnes	Desdoblament (%)	Grup > 20 alumnes
MP1. Incidents de ciberseguretat	99	100	198

Mòduls professionals	Grup ≤ 20 alumnes	Desdoblament (%)	Grup > 20 alumnes
MP2. Enfortiment de xarxes i sistemes	132	100	264
MP3. Posada en producció segura	99	100	198
MP4. Anàlisi forense informàtic	99	100	198
MP5. Hacking ètic	99	100	198
MP6. Normativa de ciberseguretat	66	100	132
MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació	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 -manuals 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, noticies, 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 Cultius cel·lulars és necessari estar en possessió d'algun dels següents títols:

CFPS ICA0 Administració de Sistemes Informàtics en Xarxa

CFPS ICB0 Desenvolupament d'Aplicacions Multiplataforma

CFPS ICC0 Desenvolupament d'Aplicacions Web

CFPS EEC0 Manteniment Electrònic

CFPS EED0 Sistemes de Telecomunicacions i Informàtics

11. Espais formatius

Espai formatiu	Superfície m² (30 alumnes)	Superfície m² (20 alumnes)	Grau d'ús
Aula polivalent	45	30	40%
Laboratori (1)	180	140	30%
Aula tècnica	60	40	30%

(1) El Laboratori requerit per algun dels cicles formatius de grau superior que donen accés a aquest curs d'especialització es considerarà suficient, sempre que hi hagi compatibilitat horària.

12. Equipaments

Espai	Equipaments
Aula tècnica	Ordinador professor. Medis audiovisuals. Ordinadors alumnes. Sistemes de reprografia. Instal·lació de xarxa amb accés a Internet.

Espai	Equipaments
	Programari de control remot. Programari bàsic (sistemes operatius en xarxa). Programari d'aplicacions ofimàtiques, tractament d'imatges, entre altres. Programari específic per a virtualització, eines de monitorització basades en protocol snmp, eines de monitorització de serveis d'alta disponibilitat, entre altres. Servidors de Fitxers, Web, Bases de dades i aplicacions. Eines de clonació d'equips. Tallafocs, detectors d'intrusos, aplicacions d'Internet, entre altres. Sistemes Gestors de Bases de Dades. Servidors i clients. Entorns de desenvolupament, compiladors i intèrprets, analitzadors de codi font, empaquetadors, generadors d'ajudes, entre altres. Programari específic per a l'anàlisi, monitorització i explotació de vulnerabilitats de xarxes i serveis. Programari específic de diagnòstic, seguretat, antivirus entre altres.
Laboratori	Taules de treball individuals tipus taller (80-90 cm alt). Bastidor (rack) per a la instal·lació de servidors i dispositius addicionals. Ordinadors amb sistema operatiu de xarxa i connexió a Internet. Programari específic de diagnòstic, seguretat, antivirus i comunicacions, entre d'altres. Sistemes de reprografia i escàner. Servidors amb capacitat per a virtualitzar diferents escenaris, amb les tecnologies més avançades. Sistemes d'alimentació ininterrompuda. Mitjans audiovisuals. Tallafocs maquinari amb 8-12 ports LAN, 2-4 ports WAN, balanceig de càrrega, filtrat de continguts, autenticació d'usuaris, bloqueig de missatgeria instantània i d'aplicacions P2P, protecció de negació del servei, connexió remota segura a través de VPN, entre d'altres. Punts d'accés i dispositius extraïbles de connexió a xarxes sense fils. Dispositius mòbils i IoT. Sistemes de control d'accés físic: lectors de DNI electrònic, targetes RFID (Identificació per radiofreqüència), entre altres. Servidors de fitxers, web, Bases de dades i Aplicacions. Sistemes Gestors de Bases de Dades. Servidors i clients. Entorns de desenvolupament, compiladors i intèrprets, analitzadors de codi font, control de versions, empaquetadors, generadors d'ajuts, entre altres. Sistemes de control de versions. Simuladors de mòbils i IoT.

Espai	Equipaments
	Programari específic per a l'anàlisi, monitorització i explotació de vulnerabilitats de xarxes i serveis.
Aula polivalent	Ordinador professor. Mitjans audiovisuals. Ordinadors alumnes. Sistemes de reprografia. Instal·lació de xarxa amb accés a Internet.

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.

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
COMPETÈNCIES PROFESSIONALS, PERSONALS I SOCIALS	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		X					X

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**	**MÒDULS PROFESSIONALS**						
	MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
minimitzar l'impacte de qualsevol possible incident.							
e) Caracteritzar l'evolució dels sistemes de control industrial valorant el seu impacte en l'organització.		X					X
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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**	**MÒDULS PROFESSIONALS**						
	MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
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	X
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.	X	X	X	X	X	X	X

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**	**MÒDULS PROFESSIONALS**						
	MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
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	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	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	X

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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
OBJECTIUS GENERALS	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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	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
	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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	j) Aplicar metodologies d'anàlisis 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'anàlisis forense per a elaborar documentació tècnica i administrativa.			X				X
	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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	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
	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
	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

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	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
	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	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	X

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	t) Desenvolupar la creativitat i l'esperit d'innovació per respondre als reptes que es presenten en els processos i en l'organització de la feina i de la vida personal.	X	X	X	X	X	X	X
	u) 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 garantir entorns segurs.	X	X	X	X	X	X	X
	v) Identificar i proposar les accions professionals necessàries per donar resposta a l'accessibilitat universal i al «disseny per a tothom».	X	X	X	X	X	X	X
	w) Identificar i aplicar paràmetres de qualitat en els treballs i activitats realitzats en el procés d'aprenentatge, per valorar la cultura de	X	X	X	X	X	X	X

TÍTOL: **Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació**		**MÒDULS PROFESSIONALS**						
		MP1. Incidents de ciberseguretat	MP2. Enfortiment de xarxes i sistemes	MP3. Posada en producció segura	MP4. Anàlisi forense informàtic	MP5. Hacking ètic	MP6. Normativa de ciberseguretat	MP7. Projecte de ciberseguretat en entorns de les tecnologies de la informació
	l'avaluació i de la qualitat i ser capaços de supervisar i millorar procediments de qualitat.							