SOC / Servei d'Ocupació de Catalunya

Catálogo de Especialidades Formativas

PROGRAMA FORMATIU

Resposta a incidents de ciberseguretat

G146NCEF-001-00

Setembre 2021

SOC / Servei d'Ocupació de Catalunya

IDENTIFICACIÓ DE L'ESPECIALITAT I PARÀMETRES DE L'CONTEXT FORMATIU

Denominació de l'especialitat:	RESPOSTA A INCIDENTS DE CIBERSEGURETAT
Família Professional:	INFORMÀTICA I COMUNICACIONS
Àrea Professional:	SISTEMES I TELEMÀTICA
Codi:	IFCT124
Nivell de qualificació professional:	4

Objectiu general

Identificar les característiques dels atacs informàtics, programar eines de detecció, i reaccionar per aturar l'atac (contenir) i recuperar el funcionament dels processos de negoci.

Relació de mòduls de formació

Mòdul 1	Gestió de resposta a incidents.	10 hores
Mòdul 2	Recollida de dades i gestió d'alarmes	40 hores
Mòdul 3	Recomanacions de bones pràctiques i marc regulador	24 hores
Mòdul 4	Desenvolupament d'una resposta a un incident de ciberseguretat.	12 hores

Modalitats d'impartició

Presencial

Teleformació

Durada de la formació

Durada total en qualsevol modalitat d'impartició	86 hores
Teleformació	Durada total de les tutories presencials: 12 hores

Requisits d'accés de l'alumnat

Acreditacions / titulacions	Complir com a mínim algun dels requisits següents: - Títol de Grau o equivalent - Títol de Postgrau (Màster) o equivalent - Títol de Tècnic Superior (FP Grau Superior) o equivalent de la família professional Informàtica i Comunicacions - Certificat de professionalitat de nivell 3 de la família professional Informàtica i Comunicacions
Experiència professional	En cas de no disposar de certificació o acreditació/titulació es requereix experiència professional mínima de 2 anys en tasques relacionades amb la gestió de xarxes o sistemes informàtics.

Modalitat de teleformació	A més del que s'ha indicat anteriorment, l'alumnat ha de tenir les destreses suficients per a ser usuaris de la plataforma virtual en la qual es recolza l'acció formativa.

Justificació dels requisits de l'alumnat

Per tal d'acreditar els coneixements adquirits n'hi haurà prou amb aportar el justificant d'haver finalitzat els estudis, o el resguard d'haver-lo sol·licitat, o l'expedient acadèmic dels estudis realitzats.

En cas de requerir la justificació de l'experiència laboral, l'alumnat haurà d'aportar un certificat de l'empresa, indicant les tasques a les quals s'ha dedicat i el percentatge de la jornada laboral dedicat a les tasques relacionades amb la formació que ens ocupa.

Prescripcions de formadors i tutors

Acreditació requerida	Complir com a mínim algun dels requisits següents: - Llicenciat, Enginyer, Màster en alguna especialitat TIC relacionada amb aquesta formació, o el títol de Grau corresponent o altres títols equivalents. - Diplomat, Enginyer Tècnic, o el títol de Grau corresponent o altres títols equivalents. - Tècnic Superior de la família professional Informàtica i Comunicacions.
Experiència professional mínima requerida	Es requeriran 2 anys d'experiència en tasques relacionades amb els temes abordats en aquesta formació.
Competència docent	Experiència docent o investigadora acreditable en l'àmbit de la ciberseguretat, de al menys 60 hores en modalitat presencial
Modalitat de teleformació	A més de complir amb les prescripcions establertes anteriorment, els tutors-formadors han d'acreditar una formació mínima de 30 hores, o experiència mínima de 60 hores, en aquesta modalitat i en la utilització de les tecnologies de la informació i comunicació.

Justificació de les prescripcions de formadors i tutors

Els formadors han d'acreditar la seva titulació i aportar alguna justificació de docència impartida en la modalitat escollida.

Requisits mínims d'espais, instal·lacions i equipaments

Espais formatius	Superfície m2 per a 15 alumnes	Increment Superfície / alumne (màxim 30 alumnes)
Aula de gestió	45 m2	2,4 m2 / alumne

Espai Formatiu	Equipament
Aula de gestió	- Taula i cadira per al formador - Taules i cadires per a l'alumnat - Material d'aula - Pissarra - PC instal·lat en xarxa amb possibilitat d'impressió de documents, canó amb projecció i Internet per al formador - PC's instal·lats en xarxa i Internet amb possibilitat d'impressió per als alumnes. - Programari específic per a l'aprenentatge de cada acció formativa: · Sistema operatiu Windows · Plataforma per a l'execució de sistemes i aplicacions virtualitzades · Eina de SIEM

La superfície dels espais i instal·lacions estaran en funció de la seva tipologia i del nombre d'alumnes. Tindran com a mínim els metres quadrats que s'indiquen per a 15 alumnes i l'equipament suficient per als mateixos.

En cas que augmenti el nombre d'alumnes, fins a un màxim de 30, la superfície de les aules s'incrementarà proporcionalment (segons s'indica a la taula pel que fa a m2/ Alumne) i l'equipament estarà d'acord amb aquest augment.

Les instal·lacions i equipaments hauran de complir la normativa industrial i higiénico-sanitària corresponent i respondran a mesures d'accessibilitat i seguretat de l'alumnat.

En el cas que la formació s'adreci a persones amb discapacitat es realitzaran les adaptacions i els ajustaments raonables per assegurar-ne la participació en condicions d'igualtat.

Aula virtual

Si s'utilitza l'aula virtual han d'acomplir-se les següents indicacions.

• **Característiques**
- La impartició de la formació mitjançant aula virtual s'ha d'estructurar i organitzar de manera que es garantitzi en tot moment que existeixi connectivitat sincronitzada entre les persones formadores i l'alumnat participant així com bidireccionalitat en les comunicacions.
- S'haurà de comptar amb un registre de connexions generat per l'aplicació de l'aula virtual on s'identifiqui, per a cada acció formativa desenvolupada a través d'aquest mitjà, les persones participants a l'aula, així com les seves dates i temps de connexió.

En modalitat de teleformació, les tutories presencials s'utilitzaran en espais formatius de les característiques i amb els equipaments necessaris indicats anteriorment.

Per a impartir la formación en modalitat de **teleformació**, s'ha de disposar del següent equipament.

Plataforma de teleformació:

La plataforma de teleformació que s'utilitzi per impartir accions formatives ha d'allotjar el material virtual d'aprenentatge corresponent, posseir capacitat suficient per desenvolupar el procés d'aprenentatge i gestionar i garantir la formació de l'alumnat, permetent la interactivitat i el treball cooperatiu, i reunir els següents requisits tècnics d'infraestructura, programari i serveis:

- **Infraestructura**

- Tenir un rendiment, entès com a número d'alumnes que suporti la plataforma, velocitat de resposta de servidor als usuaris, i temps de càrrega de les pàgines web o de descàrrega d'arxius, que permeti:

    - Suportar un nombre d'alumnes equivalent a el nombre total d'alumnat en les accions formatives de formació professional per a l'ocupació que estigui impartint el centre o entitat de formació, Garantint un allotjament mínim igual al 'total de l'alumnat d'aquestes accions, considerant que el nombre màxim d'alumnes per tutor és de 80 i un nombre d'usuaris concurrents de el 40% d'aquest alumnat.
    - Disposar de la capacitat de transferència necessària perquè no es produeixi efecte retard en la comunicació audiovisual en temps real, havent de tenir el servidor en el qual s'allotja la plataforma un ample de banda mínim de 300 Mbs, suficient en baixada i pujada.

- Estar en funcionament 24 hores a el dia, els 7 dies de la setmana.

- **Programari:**

- Compatibilitat amb l'estàndard SCORM i paquets de continguts IMS.

- Nivells d'accessibilitat i interactivitat dels continguts disponibles mitjançant tecnologies web que com a mínim compleixin les prioritats 1 i 2 de la Norma UNE 139803: 2012 o posteriors actualitzacions, segons l'estipulat en el capítol III del Reial Decret 1494/2007, de 12 de novembre .

- El servidor de la plataforma de teleformació ha de complir amb els requisits que estableix la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, de manera que el responsable d'aquesta plataforma ha d'identificar la localització física del servidor i el compliment del que estableix sobre transferències internacionals de dades en els articles 40 a 43 de l'esmentada Llei Orgànica 3/2018, de 5 de desembre, així com, en el que sigui aplicable, al Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques respecte del tractament de dades personals i la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95 / 46 / CE.

- Compatibilitat tecnològica i possibilitats d'integració amb qualsevol sistema operatiu, base de dades, navegador d'Internet dels més usuals o servidor web, havent de ser possible utilitzar les funcions de la plataforma amb complements (plug-in) i visualitzadors compatibles. Si es requereix la instal·lació addicional d'algun suport per funcionalitats avançades, la plataforma ha de facilitar l'accés a la mateixa sense cost.

- Disponibilitat del servei web de seguiment (operatiu i en funcionament) de les accions formatives impartides, d'acord amb el model de dades i protocol de transmissió que estableix l'annex V de l'Ordre / TMS / 369/2019, de 28 de març.

- **Serveis i suport**

- Sustentar el material virtual d'aprenentatge de l'especialitat formativa que a través d'ella s'imparteixi.

- Disponibilitat d'un servei d'atenció a usuaris que doni suport tècnic i mantingui la infraestructura tecnològica i que, de forma estructurada i centralitzada, atengui i resolgui les consultes i incidències tècniques de l'alumnat. Les formes d'establir contacte amb aquest servei, que seran mitjançant telèfon i missatgeria electrònica, han d'estar disponibles per a l'alumnat des de l'inici fins a la finalització de l'acció formativa, mantenint un horari de funcionament de matí i de tarda i un temps de demora en la resposta no superior a 48 hores laborables.

- Personalització amb la imatge institucional de l'administració laboral corresponent, amb les pautes d'imatge corporativa que s'estableixin.

Amb l'objecte de gestionar, administrar, organitzar, dissenyar, impartir i avaluar accions formatives a través d'Internet, la plataforma de teleformació integrarà les eines i recursos necessaris per a aquesta finalitat, disposant, específicament, d'eines de:

- Comunicació, que permetin que cada alumne pugui interaccionar a través del navegador amb el tutor-formador, el sistema i amb els altres alumnes. Aquesta comunicació electrònica ha de dur-se a terme mitjançant eines de comunicació síncrones (aula virtual, xat, pissarra electrònica) i asíncrones (correu electrònic, fòrum, calendari, tauler d'anuncis, avisos). Serà obligatori que cada acció formativa en modalitat de teleformació disposi, com a mínim, d'un servei de missatgeria, un fòrum i un xat.
- Col·laboració, que permetin tant el treball cooperatiu entre els membres d'un grup, com la gestió de grups. Mitjançant aquestes eines ha de ser possible realitzar operacions d'alta, modificació o esborrat de grups d'alumnes, així com creació de «escenaris virtuals» per al treball cooperatiu dels membres d'un grup (directoris o «carpetes» per a l'intercanvi d'arxius, eines per a la publicació dels continguts, i fòrums o xats privats per als membres de cada grup).
- Administració, que permetin la gestió d'usuaris (altes, modificacions, esborrat, gestió de la llista de classe, definició, assignació i gestió de permisos, perfils i rols, autenticació i assignació de nivells de seguretat) i la gestió d'accions formatives.
- Gestió de continguts, que possibiliten l'emmagatzematge i la gestió d'arxius (visualitzar arxius, organitzats en carpetes -directoris- i subcarpetes, copiar, enganxar, eliminar, comprimir, descarregar o carregar arxius), la publicació organitzada i selectiva dels continguts d'aquests arxius, i la creació de continguts.
- Avaluació i control del progrés de l'alumnat, que permetin la creació, edició i realització de proves d'avaluació i autoavaluació i d'activitats i treballs avaluables, la seva autocorrecció o la seva correcció (amb retroalimentació), la seva qualificació, l'assignació de puntuacions i la ponderació de les mateixes, el registre personalitzat i la publicació de qualificacions, la visualització d'informació estadística sobre els resultats i el progrés de cada alumne i l'obtenció d'informes de seguiment.

Material virtual d'aprenentatge:

El material virtual d'aprenentatge per a l'alumnat mitjançant el qual s'imparteixi la formació es concretarà en el curs complet en format multimèdia (que mantingui una estructura i funcionalitat homogènia), havent d'ajustar a tots els elements de la programació (objectius i resultats d'aprenentatge) d'aquest programa formatiu que figura en el Catàleg d'Especialitats Formatives i el contingut compleixi aquests requisits:

- Com a mínim, ser l'establert en l'esmentat programa formatiu del Catàleg d'Especialitats Formatives.
- Estar referit tant als objectius com als coneixements / capacitats cognitives i pràctiques, i habilitats de gestió, personals i socials, de manera que en el seu conjunt permetin aconseguir els resultats d'aprenentatge previstos.
- Organitzar-se a través d'índexs, mapes, taules de contingut, esquemes, epígrafs o titulars de fàcil discriminació i seqüenciats pedagògicament de tal manera que permeten la seva comprensió i retenció.
- No ser merament informatius, promovent la seva aplicació pràctica a través d'activitats d'aprenentatge (auto avaluables o valorades pel tutor-formador) rellevants per a l'adquisició de competències, que serveixin per verificar el progrés de l'aprenentatge de l'alumnat, fer un seguiment de les seves dificultats de aprenentatge i prestar-li el suport adequat.

- No ser exclusivament textuals, incloent variats recursos (necessaris i rellevants), tant estàtics com interactius (imatges, gràfics, àudio, vídeo, animacions, enllaços, simulacions, articles, fòrum, xat, etc.). de forma periòdica.
- Poder ser ampliats o complementats mitjançant diferents recursos addicionals als que l'alumnat pugui accedir i consultar a voluntat.
- Donar lloc a resums o síntesi i a glossaris que identifiquin i defineixin els termes o vocables bàsics, rellevants o claus per a la comprensió dels aprenentatges.
- Avaluar la seva adquisició durant la finalització de l'acció formativa a través d'activitats d'avaluació (exercicis, preguntes, treballs, problemes, casos, proves, etc.), que permeten mesurar el rendiment o l'exercici de l'alumnat.

Altres especificacions

Tecnologia i equips	La plataforma de teleformació inclourà una eina que permeti la connexió síncrona de docents i alumnes, amb sistema incorporat d'àudio, vídeo i possibilitat de compartir arxius, la mateixa pantalla o altres aplicacions tant pel docent com per l'alumnat, amb registre dels temps de connectivitat.

Ocupacions i llocs de treball relacionats

- 27191013 Auditors-assessors informàtics
- 2711 Analistes de sistemes
- 2723 Analistes de xarxes informàtiques
- 27231014 Analistes i desenvolupadors de xarxes informàtiques
- 2722 Administradors de sistemes i xarxes
- 3811 Tècnics en operacions de sistemes informàtics
- 3812 Tècnics en assistència a l'usuari de tecnologies de la informació
- 3813 Tècnics en xarxes
- 27111046 Enginyers tècnics en informàtica de sistemes
- 27191022 Enginyers tècnics en informàtica en general
- 2729 Especialistes en bases de dades i en xarxes informàtiques no classificats sota altres epígrafs

Requisits oficials de les entitats o centres de formació

Estar inscrit en el Registre d'entitats de formació (Serveis Públics d'Ocupació)

DESENVOLUPAMENT MODULAR

MÒDUL DE FORMACIÓ 1: GESTIÓ DE RESPOSTA A INCIDENTS

OBJECTIU

Identificar les diferents estratègies, models d'actuació i formes d'implantació en la resposta a incidents, en funció de les característiques de l'atac, coordinant les actuacions de l'equip de resposta assignat.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 10 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Descripció d'un equip de resposta a incidents.
  - Estructura organitzativa.
  - Distribució de funcions i operació
- Organització d'un equip de resposta a incidents
  - Creació de procediments, polítiques i plans per a resposta a incidents
- Identificació de serveis
  - Serveis reactius
  - Serveis proactius
  - Gestió de la ciberseguretat
- Relació de les fases en la resposta a incidents:
  - Detecció de l'incident.
  - Anàlisis de dades i identificació de l'incident.
  - Contenció i erradicació de l'incident.
  - Recuperació de l'incident.
  - Notificació de l'incident per regulació.
- Localització i contacte dels equips de coordinació i resposta a Incidents de ciberseguretat: CSIRTs
  - Agència de Ciberseguretat de Catalunya: models d'interrelació i servei
  - Fòrums internacionals: FIRST, TERENA, Trusted Introducer
  - Agents nacionals: INCIBE, CCN-CERT, CNPIC
  - Associació nacional d'equips de resposta a incidents: CSIRT.ES

Habilitats de gestió, personals i socials

- Assimilació de les funcions i objectius dels organismes nacionals i internacionals de coordinació i suport als equips de resposta a incidents.
- Intercanvi d'idees mitjançant les eines de col·laboració ofertes per cadascun d'ells i abast de la col·laboració esperada d'aquests, tant per a membres de les seves organitzacions, com per a equips de resposta no vinculats.
- Valoració de les fonts d'informació sobre els atacs coneguts i les recomanacions de detecció i mitigació d'aquests.
- Rigor e la selecció, recomanació i automatització de les reaccions de resposta a cada tipus d'incident detectat

- Implicació en la supervisió, avaluació, documentació i comunicació de la resposta dels tècnics encarregats de dur a terme les accions reactives recomanades
- Prescripció de l'ús de les eines col·laboratives per optimitzar els recursos emprats en la resposta a incidents
- Avaluació del risc i la política de protecció de dades i sistemes corporatius a les estratègies de resposta a incidents recomanades per organismes nacionals i internacionals

MÒDUL DE FORMACIÓ 2: RECOLLIDA DE DADES I GESTIÓ D'ALARMES

OBJECTIU

Categoritzar les fonts d'informació de les dades implicades en incidents de ciberseguretat

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 40 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Recull de dades significatives:
  - Identificació de les fonts de dades internes d'un centre d'operacions de seguretat, mitjançant eines de monitorització de xarxa i sistemes informàtics.
  - Identificació de fonts de dades externes: Anàlisi d'intel·ligència de l'atac (investigació, Threat Intelligence) i Intel·ligència en fonts obertes (OSINT)
  - Recollida d'evidències digitals: recerques cegues, preservació de la confidencialitat de les dades, preservació de la cadena de custòdia i gestió de còpies de seguretat.
- Anàlisi de dades d'intrusions
  - Avaluació de l'impacte potencial de la intrusió i determinació del nivell d'alerta corresponent
  - Detecció d'intrusions (IDS)
  - Protecció contra intrusions (IPS)
  - Gestió de dades
  - Anàlisi forense: Conèixer les bones pràctiques de recollida d'evidències digitals, per a mantenir la seva validesa en cas de realitzar-se una denúncia pels danys soferts.
- Correlació de dades i generació d'alarmes
  - Gestió de logs dels diferents sistemes i serveis
  - Sistemes de gestió d'esdeveniments de seguretat (SIEM)
  - Homogeneïtzació de les dades. Filtrat i normalització de les fonts.
  - Tractament de les alarmes: automatització de respostes i comunicació de l'escenari de l'incident
  - Altres eines: Orquestració i automatització (SOAR),visualització de dades, generació automàtica d'informes

Habilitats de gestió, personals i socials

- Col·laboració amb els membres dels equips de recollida i anàlisi de dades, així com amb experts externs
- Designació de rols i responsabilitats als membres dels equips de treball, assignació de tasques i distribució de torns.
- Valoració de la utilitat de les dades recopilades i de l'impacte dels atacs en els processos de negoci i els actius de l'organització.
- Compromís amb la identificació i avaluació de fonts de dades, tant externes com internes, obertes o ocultes en programes, memòria o altres sistemes d'emmagatzematge extern o en el núvol.
- Rigor en la discriminació de dades verídiques de falsos
- Responsabilitat en la protecció dels actius digitalitzats i dades sensibles de la corporació

MÒDUL DE FORMACIÓ 3: RECOMANACIONS DE BONES PRÀCTIQUES I MARC REGULADOR

OBJECTIU

Aplicar la normativa, eines i estàndards corresponents en la detecció i resposta a incidents de ciberseguretat.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 24 hores

Teleformació: Durada de les tutories presencials: 0 hores

RESULTATS D'APRENENTATGE

Coneixements / Capacitats cognitives i practiques

- Interpretació, selecció i aplicació de les eines i els estàndards internacionals i nacionals de detecció i resposta a incidents de ciberseguretat
  - MITRE ATT & CK
  - SIGMA (Security Management Services)
  - SIEM (OSSIM)
  - IDS (SNORT)
  - RTIR
  - OTRS
  - LUCIA
- Classificació de normatives de protecció de dades personals
  - RGPD de la UE (Reglament General de Protecció de Dades Europeu)
  - LOPD-GDD (Llei orgànica de protecció de dades i Garantia de drets digitals espanyola)
- Adequació a l'Esquema Nacional de Seguretat
  - Metodologia d'anàlisi i gestió de riscos (MAGERIT)
  - Eines d'anàlisi, avaluació i gestió de riscos (PILAR)
- Aplicació de la Directiva NIS
  - Proveïdors de serveis essencials

- Impacte en les empreses subministradores

- Definició dels principis de l'ètica professional
  - En la resposta a incidents
  - En la captura i custòdia d'evidències

Habilitats de gestió, personals i socials

- Responsabilitat en la protecció dels actius digitalitzats i dades sensibles de la corporació.
- Sensibilització dels requisits legals aplicables als processos de negoci de la corporació.

MÒDUL DE FORMACIÓ 4: DESENVOLUPAMENT D'UNA RESPOSTA A UN INCIDENT DE CIBERSEGURETAT

OBJECTIU

Aplicar eines i tècniques d'anàlisi i gestió de la resposta a un incident de ciberseguretat.

DURADA EN QUALSEVOL MODALITAT D'IMPARTICIÓ: 12 hores

Teleformació: Durada de les tutories presencials: 12 hores

RESULTATS D'APRENENTATGE

Coneixements / Capacitats cognitives i pràctiques

- Extracció d'informació
  - D'una font de dades de trànsit en una xarxa corporativa
  - De fonts OSINT
- Automatització dels processos de detecció d'intrusions.
  - Integració de fonts de dades en una eina SIEM
  - Selecció dels paràmetres per a la detecció i generació d'alarmes rellevants
- Gestió de la resposta a un incident de seguretat informàtica
  - Identificació de fonts de cooperació per optimització de la resposta a un incident de ciberseguretat
  - Planificació d'actuacions i procediments
  - Resolució d'un ciberincident.

Habilitats de gestió, personals i socials

- Col·laboració amb altres membres de l'equip de treball.
- Eficiència en la utilització d'eines habituals en els centres d'operacions de seguretat i equips de resposta a incidents
- Rigor en la redacció d'informes de resultats
- Constància en la programació d'activitats de recollida i classificació de dades.

Resultats que obligatòriament han de adquirir-se en presencial

- Extracció d'informació
  - D'una font de dades de trànsit en una xarxa corporativa
  - De fonts OSINT
- Automatització dels processos de detecció d'intrusions.
  - Integració de fonts de dades en una eina SIEM
  - Selecció dels paràmetres per a la detecció i generació d'alarmes rellevants
- Gestió de la resposta a un incident de seguretat informàtica
  - Identificació de fonts de cooperació per optimització de la resposta a un incident de ciberseguretat
  - Planificació d'actuacions i procediments
  - Resolució d'un ciberincident.

ORIENTACIONS METODOLÒGIQUES

La impartició de la docència es durà a terme complementant:

- Introducció de conceptes teòrics i metodològics
- Estudi de casos en què s'hagin aplicat aquests
- Realització d'exercicis pràctics per demostrar les capacitats adquirides.

AVALUACIÓ DE L'APRENENTATGE EN L'ACCIÓ FORMATIVA

- L'avaluació tindrà un caràcter teòric-pràctic i es realitzarà de forma sistemàtica i contínua, durant el desenvolupament de cada mòdul i a la fi del curs. En les avaluacions programades es poden agrupar coneixements de diversos mòduls.
- Es realitzarà una avaluació inicial de caràcter diagnòstic per detectar el nivell de partida de l'alumnat.
- L'avaluació es durà a terme mitjançant els mètodes i instruments més adequats per comprovar els diferents resultats d'aprenentatge, i que garanteixin la fiabilitat i validesa de la mateixa.
- Cada instrument d'avaluació s'acompanyarà del corresponent sistema de correcció i puntuació en el qual s'expliciti, de forma clara i inequívoca, els criteris de mesura per avaluar els resultats assolits pels alumnes.
- La puntuació final assolida s'expressarà en termes d'Apte / No Apte.