

Plec de prescripcions tècniques particulars que regeix la contractació dels continguts i la infraestructura de funcionament per a la Ciberacadèmia de l'Agència de Ciberseguretat de Catalunya

Índex

1. Introducció	4
2. Estructura de la contractació	6
3. Descripció dels serveis objecte de la contractació	7
3.1 Objecte i descripció	8
3.2 Continguts formatius de ciberseguretat	9
3.2.1 Matriu de matèries i unitats de continguts de ciberseguretat	11
3.2.2 Els nivells de maduresa de les unitats dels cursos	15
3.2.3 L'estructura dels continguts	16
3.2.4 Plantejament d'itineraris i dedicació mínima de formació	17
3.3 Serveis i les seves característiques	18
3.3.1 La qualitat dels lliurables	19
3.3.2 Propostes de millora dels continguts	20
3.4 Infraestructura i plataforma d'aprenentatge	22
3.4.1 Objecte i descripció de la plataforma	22
3.4.2 Serveis de la plataforma	22
3.4.3 Activitats i funcionalitats que s'esperen del servei	23
3.4.4 Productes del servei	29
3.4.5 Característiques generals del servei	34
3.4.6 Propostes de millora organitzativa	35
4. Equip de treball	36
4.1 Detall de l'activitat de l'equip	37
4.2 Definició i perfils requerits de l'equip de treball	38
4.2.1 Perfils principals per la Ciberacadèmia	38
4.2.2 Altres perfils de funcionament de la Ciberacadèmia	43
4.3 Organització de l'equip	49
5. Condicions d'execució del servei	51
5.1 Horaris	51
5.2 Localització física	51
5.3 Canvi de recurs	51
5.4 Control de rotació	52
5.5 Eines i equipament per a la prestació de serveis	52
5.6 Gestió del coneixement	53

5.7 Seguretat corporativa	54
5.8 Control de gestió	54
5.9 Documentació	55
5.10 Formació	55
5.11 Contingència	55
5.12 Metodologia, estàndars i lliurables	56
5.13 Seguretat	56
5.14 Assegurament de la qualitat i millora contínua	59
5.15 Seguiment del servei	59
5.16 Integració amb altres equips	60
5.17 Compromís amb el talent femení	60
5.18 Compromís amb el talent i la inclusió	61

1. Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

Amb un enfocament clar en la prevenció i detecció de ciberamenaces, la resposta efectiva davant incidents de ciberseguretat, la promoció de la cultura de ciberseguretat, i la col·laboració i coordinació amb diferents actors a nivell local i internacional, l'Agència opera dins de l'àmbit d'actuació definit per la llei, que marca les directrius d'actuació de l'Agència, les seves funcions, estructura orgànica i el règim de governança.

L'Agència sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil és l'encarregada d'establir i de liderar el servei públic de ciberseguretat i té com a objectiu garantir una Societat de la Informació segura i fiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Els avenços impulsats per l'Estratègia 2019-2022 han establert un sòlid punt de partida per a futures accions, incloent la consolidació de l'Agència com a entitat de referència. Aquests avenços no només han millorat la capacitat de resposta davant incidents sinó que també han promogut una major consciència i formació en ciberseguretat entre la ciutadania i les organitzacions. La nova Estratègia 2023-2027, "Una Catalunya cibersegura en una Europa Digital", s'orienta cap a reforçar la resiliència digital, protegir els serveis i infraestructures essencials, i assegurar que ciutadans i organitzacions es beneficiïn de tecnologies digitals de confiança.

En el marc de l'activitat gestionada per l'Agència, cal destacar que *segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2023, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2023, tant pel que fa a la Generalitat com en diferents entitats del territori català*. En aquest sentit, l'Agència gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació. En aquest sentit, i alineat amb la nova Estratègia, l'Agència ampliarà el seu perímetre d'actuació i per tant, incrementar el nivell de protecció, resiliència i prevenció de més àmbits.

Aquest contracte està finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel *Ministerio de Asuntos Económicos y Transformación Digital*, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials

d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l'intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d'impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el *Ministerio de Asuntos Económicos y Transformación Digital*, a través de la *Secretaría d'Estado de Digitalitzación e Inteligencia Artificial*, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

2. Estructura de la contractació

El present contracte té com a objectiu la contractació d'un conjunt integrat de serveis per al desplegament i funcionament de la Ciberacadèmia. Aquests serveis inclouen, d'una banda, l'elaboració i manteniment de continguts formatius de ciberseguretat per a diferents perfils professionals i, de l'altra, la provisió de la infraestructura tecnològica necessària per a la seva gestió, distribució i seguiment.

S'haurà de presentar una proposta integral que asseguri la coordinació efectiva entre la creació de continguts i l'entorn tecnològic que els suportarà, garantint-ne la compatibilitat, usabilitat i eficiència en l'experiència formativa. És imprescindible una proposta que contempli la interdependència funcional entre aquestes dues dimensions del servei —continguts i infraestructura—, assegurant-ne la màxima coherència operativa i el compliment dels terminis previstos de desplegament.

L'èxit del projecte dependrà de la capacitat de l'empresa per oferir una solució sinèrgica i ben integrada, on la qualitat pedagògica dels continguts es combini amb una plataforma tecnològica robusta, segura i escalable, capaç de donar suport al conjunt d'activitats formatives de la Ciberacadèmia.

D'altra banda, les accions formatives seran executades per professionals docents especialitzats, contractats a través dels serveis establert en l'Acord Marc per a la prestació de serveis de suport a les funcions de ciberseguretat en matèria de consultoria de l'Agència. Aquest personal docent actuarà de manera complementària als serveis objecte d'aquest contracte i serà coordinat per la mateixa Agència.

Finalment, la Ciberacadèmia també comptarà amb els serveis auxiliars de suport a l'alumnat i al professorat, que seran proveïts directament per l'Agència, assegurant una experiència de formació completa i de qualitat.

3. Descripció dels serveis objecte de la contractació

L'objecte d'aquesta contractació és la prestació d'un conjunt integrat de serveis per fer possible el funcionament de la Ciberacadèmia de l'Agència. Aquests serveis inclouen tant la creació i manteniment de continguts de capacitació en ciberseguretat com la provisió i gestió de la infraestructura tecnològica i operativa necessària per al desplegament, la gestió acadèmica i el seguiment de la formació.

L'objectiu general d'aquesta iniciativa és contribuir al desenvolupament d'una cultura sòlida de ciberseguretat i a la capacitació de professionals que treballen en empreses del sector, proveïdors de solucions i serveis d'alt valor afegit, així com d'altres agents que operen serveis de ciberseguretat en diversos àmbits.

Aquest projecte es desenvolupa en un context d'escassetat de professionals qualificats en ciberseguretat i té per objectiu principal contribuir a cobrir aquest dèficit mitjançant dos enfocaments complementaris:

- Upskilling: adquisició de noves habilitats o actualització de les existents per part de professionals ja actius en el sector, per tal de mantenir la seva competitivitat en el mercat laboral i facilitar el seu desenvolupament dins un pla de carrera.
- Reskilling: capacitació de professionals d'altres àmbits per facilitar la seva transició cap al sector de la ciberseguretat, en resposta a canvis en la demanda d'ocupació o a noves responsabilitats professionals.

La Ciberacadèmia actuarà com a entorn d'aprenentatge i punt de trobada per a iniciatives de col·laboració públic-privada, que inclouran professionals d'organismes públics, empreses i entitats sense ànim de lucre, amb l'objectiu de reforçar les seves capacitats i, per extensió, el teixit industrial del país en matèria de ciberseguretat.

Els continguts formatius que es dissenyin hauran d'estar alineats amb les funcions i perfils professionals definits a l'European Cybersecurity Skills Framework (ECSF) de l'ENISA, amb especial atenció als 11 perfils d'expertesa en ciberseguretat que aquest marc estableix. Els objectius específics d'aquesta contractació inclouen:

- La generació i disseny de continguts de qualitat i rellevants per als diferents programes formatius que es desplegaran a la Ciberacadèmia.
- L'elaboració d'itineraris formatius adaptats a necessitats reals del mercat, que ajudin a tancar les bretxes detectades en les àrees amb resposta lenta per part de l'oferta acadèmica tradicional.
- El foment de la formació contínua en àrees clau del model de desplegament de la ciberseguretat (Identificar, Protegir, Detectar, Respondre i Recuperar), on sovint hi ha dificultats per cobrir les necessitats de talent disponible.
- L'alineament amb les directrius de l'European Cyber Competence Centre (ECCC), contribuint a la construcció d'una comunitat europea sòlida de professionals en ciberseguretat.

Per tal de fer realitat aquests objectius, es requereix una infraestructura tecnològica i operativa que doni suport integral al desplegament de la Ciberacadèmia, incloent:

- Els recursos tecnològics per a l'allotjament, la distribució i el seguiment dels continguts.

- Els mecanismes de gestió acadèmica, incloent la matrícula, la traçabilitat del progrés dels alumnes i la generació d'indicadors.
- Les eines de suport a l'equip docent i als alumnes, i la coordinació general de totes les activitats.

Aquesta infraestructura haurà de garantir la robustesa, seguretat i escalabilitat necessàries per adaptar-se als diferents formats i escenaris formatius de la Ciberacadèmia, assegurant la màxima eficiència en la gestió dels serveis i la qualitat de l'experiència d'aprenentatge.

3.1. Objecte i descripció

L'objecte d'aquesta contractació és la provisió d'una solució integral per a la Ciberacadèmia de l'Agència, que inclogui tant l'elaboració i manteniment de continguts formatius especialitzats en ciberseguretat, com la disponibilitat, desplegament i gestió d'una infraestructura tecnològica i acadèmica que en faci possible la seva difusió, gestió i seguiment de manera eficient, escalable i segura.

Aquesta solució ha de respondre a l'objectiu estratègic de fomentar la cultura de la ciberseguretat i capacitar professionals en els perfils més demandats del sector, donant resposta a la carència actual de talent i promovent la millora contínua de les competències del capital humà implicat.

Els serveis objecte del contracte s'estructuren al voltant de dues grans àrees interrelacionades i interdependents:

A. Aprovisionament de continguts formatius i itineraris de capacitació en ciberseguretat

L'adjudicatari haurà de dissenyar, generar i mantenir actualitzats els continguts de formació en ciberseguretat, desenvolupats a partir d'una matriu de set matèries i compostat de diferents unitats didàctiques que cobreixin en quatre nivells de capacitació, des del nivell bàsic fins a l'expert. Els continguts han de permetre la formació de professionals que cobreixin totes les fases del model de desplegament de la ciberseguretat de l'Agència: diagnòstic, planificació, implementació, operació i auditoria.

Aquesta capacitació estarà orientada als onze perfils professionals definits per l'European Cybersecurity Skills Framework (ECSF) d'ENISA, que inclouen, entre altres, penetration testers, CISO, analistes d'intel·ligència d'amenaques, auditors, educadors i forenses digitals. El dotzè perfil que s'exclou dels continguts és l'expert en recerca en ciberseguretat (com tants altres perfils que poden aparèixer com necessaris), que podrà considerar-se en un futur quan hi hagi trajectòria de la Ciberacadèmia.

Un aclariment, en aquest plec es parla de "perfils professionals" o rols referits a l'enfocament de sortida d'especialització que s'ha d'assolir pels alumnes de la Ciberacadèmia amb programes formatius amb unes dedicacions òptimes. En cap cas cal confondre amb els perfils de contractació necessaris per a desenvolupar totes les activitats necessàries. En aquest darrer cas es parlarà de "perfils requerits".

Els continguts hauran de facilitar tant processos d'upskilling com de reskilling, mitjançant itineraris formatius estructurats i modulars, adaptats a les necessitats de cada perfil. Així mateix, caldrà contemplar la gestió acadèmica associada: planificació de cursos, calendarització, assignació de docents, organització de grups i seguiment del progrés de l'alumnat.

B. Infraestructura tecnològica i acadèmica

L'adjudicatari haurà de proporcionar i gestionar una infraestructura tecnològica completa i operativa que permeti la prestació efectiva dels serveis de formació. Aquesta infraestructura haurà d'incloure:

- Un sistema LMS (Learning Management System) que suporti l'aprenentatge síncron i asíncron.
- Gestió d'itineraris formatius, seguint els estàndards SIS (Student Information System) i funcionalitats de comercialització.
- Interoperabilitat amb altres plataformes educatives mitjançant estàndards com LTI.
- Compatibilitat amb SCORM per a la compartició i reutilització de continguts.
- Suport per a formats multimèdia i vídeo (streaming, live streaming, vídeo broadcasting) per a docència en línia.
- Funcionalitats per a la publicació oberta de cursos mitjançant microsites i la gestió d'inscripcions automàtiques.

La plataforma haurà d'assegurar la integració amb sistemes de seguretat corporatius, prioritzant la compatibilitat amb l'ecosistema de Microsoft utilitzat per l'Agència, i oferint funcionalitats com l'autenticació única (SSO) per a l'accés segur a aplicacions SaaS.

3.2. Continguts formatius de ciberseguretat

La Ciberacadèmia de l'Agència es dotarà d'un contracte per a:

- Generar els continguts necessaris i l'elaboració d'itineraris formatius. Les matèries i les unitats que componen aquests continguts es descriuen a la matriu de continguts a desenvolupar, preveient quatre diferents nivells, de nivell bàsic fins a nivell expert, que permetin formar els diferents professionals en ciberseguretat necessaris per cobrir totes les fases del seu model de desplegament de la ciberseguretat als diferents àmbits:
 1. Diagnòstic (anàlisi de febleses i riscos) amb professionals de pentesting i arquitectura.
 2. Pla de seguretat amb gestors de riscos i caps de seguretat (CISO).
 3. Integració amb implementadors de ciberseguretat, intel·ligència d'amenaques i resposta a incidents.
 4. Oficines recurrents: compliment legal, formació i conscienciació, anàlisi forense digital...
 5. Auditoria de certificació amb auditoria de ciberseguretat.

S'identifiquen, en primera instància, onze perfils professionals pels quals s'haurà d'oferir una capacitat que permeti un ràpid exercici pràctic, amb una diversitat de nivells d'accés. Segons la nomenclatura de perfils definida per l'ESCF d'ENISA aquest són:

1. Professionals de proves de penetració (Penetration Tester)
Realitza proves de penetració per identificar vulnerabilitats en els sistemes de l'organització i proposar solucions per corregir-les.
2. Auditor/a de ciberseguretat (Cybersecurity Auditor)
Realitza auditories per verificar el compliment de les polítiques de seguretat i identificar àrees de millora.
3. Cap de seguretat de la informació CISO (Chief Information Security Officer)

Responsable de la seguretat de la informació dins l'organització, defineix polítiques de seguretat, supervisa el compliment i gestiona incidents de ciberseguretat.

4. Consultor/a d'equips de resposta a incidents (Cyber Incident Responder)
Gestiona i respon a incidents de seguretat, minimitzant l'impacte i recuperant la normalitat operativa.
5. Expert/a en ciberseguretat legal (Cyber Legal, Policy & Compliance Officer)
Assegura que l'organització compleixi amb les regulacions i estàndards de seguretat, desenvolupant polítiques i proporcionant assessorament legal.
6. Expert/a en intel·ligència d'amenaques (Cyber Threat Intelligence Specialist)
Analitza i interpreta informació sobre amenaces cibernètiques per anticipar-se a possibles atacs i millorar les defenses.
7. Arquitecte/a de ciberseguretat (Cybersecurity Architect)
Dissenya l'arquitectura de seguretat de l'organització, integrant solucions tecnològiques per protegir les dades.
8. Educador/a de la ciberseguretat (Cybersecurity Educator)
Desenvolupa i imparteix programes de formació en seguretat per capacitar els empleats en pràctiques segures.
9. Expert/a en la implementació de la ciberseguretat (Cybersecurity Implementer)
Implementa solucions de seguretat en els sistemes de l'organització, garantint la protecció contra amenaces.
10. Expert/a en gestió de riscos (Cybersecurity Risk Manager)
Avalua els riscos de seguretat i proposa mesures per mitigar-los, garantint la protecció dels actius de l'organització.
11. Investigador/a forense digital (Digital Forensics Investigator)
Realitza anàlisis forenses per investigar incidents de seguretat, recopilant i preservant proves digitals.

En aquesta llista s'ha eludit altres perfils professionals, com l'expert en recerca de ciberseguretat, que requereix un nivell avançat en qualsevol d'aquestes capacitats, i altres que el mercat pot necessitar però encara no està identificat en l'ESCF.

- En aquest contracte, a banda dels continguts de ciberseguretat, s'haurà d'aportar les condicions per a desenvolupar i gestionar l'activitat acadèmica durant el període de contracte. Entre les gestions a realitzar hi haurà l'organització de les diferents àrees de coneixements/matèries a impartir per professors experts de ciberseguretat, en un calendari de curs, que optimitzi els recursos a disposició (materials didàctics, professorat i eines d'avaluació). S'haurà de preveure la gestió dels diferents grups d'alumnes que puguin consumir en diferents modalitats els cursos desenvolupats en tots els programes formatius disponibles.

3.2.2 3.2.1 Matriu de matèries i unitats de continguts de ciberseguretat

Aquesta és la distribució de continguts que es preveu desenvolupar amb una planificació durant el temps d'execució del contracte.

Les matèries de ciberseguretat de la Ciberacadèmia:

1. Fonaments de ciberseguretat
2. Seguretat de les aplicacions
3. Gestió d'identitats
4. Protecció i privacitat de dades
5. Ciberdefensa
6. Estructura organitzativa i processos empresarials
7. Habilitats interpersonals (*soft skills*)

Aquestes matèries de la ciberseguretat es desenvolupen en les unitats de continguts que poden tenir components específics per als diferents perfils professionals a qui s'adrecen i es distribueix per als quatre diferents nivells que s'alineïn segons la maduresa competencial. S'exposa a continuació de forma enunciativa però no limitativa les unitats previstes a desenvolupar.

Unitats a desenvolupar de Fonaments de ciberseguretat:

Fonaments de la ciberseguretat	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
1. Introducció a la ciberseguretat	Definició de ciberseguretat, evolució històrica, importància i impacte en les organitzacions. Casos pràctics d'incidents.
2. Estratègia i governança	Desenvolupament d'estratègies de ciberseguretat, governança (CSO, CISO), polítiques, rols i marcs normatius (CRISC, COBIT, CGEIT).
3. Seguretat física i de la infraestructura	Protecció d'accessos, vigilància, estructures de seguretat perimetral, tipus de firewalls, configuració de regles i dispositius (ex: IPTABLES).
4. Seguretat en l'endpoint i amenaces	Antivirus, EDR, detecció d'amenaces, bastionat de sistemes, seguretat en correu i missatgeria, phishing, i enginyeria social.
5. Continuitat del negoci i resiliència	Anàlisi d'impacte (BIA), pla de crisi, pla de continuïtat, simulacres i formació. Normatives com ISO 22301, NIS2, Cyber Resilience Act.
6. Seguretat industrial (OT)	Protocols industrials, models OT/IT/IOT, processos industrials, exemples de xarxes industrials i reptes de ciberseguretat en entorns OT.
7. Compliment normatiu	ENS, RGPD, LPIC, ISO 27001, NIS2, procediments i normes internes, desenvolupament de polítiques de seguretat i auditories.
8. Gestió d'actius	Inventari d'actius, cicle de vida, etiquetatge, CMDB, gestió de proveïdors i model de maduresa ITAM.
9. Avaluació i gestió del risc	Catàlegs d'amenaces, identificació d'actius crítics, metodologies (OCTAVE, FAIR), estratègies de mitigació i indicadors de seguiment.
10. Seguretat en el núvol i infraestructura virtual	Models de servei cloud (IaaS, PaaS, SaaS), responsabilitat compartida, seguretat de recursos, CSPM, DevSecOps, virtualització i arquitectura CSMA.

11. Gestió del risc de terceres parts	Avaluació del risc abans de la contractació (KYC, NDA, certificacions). Homologació i seguiment de proveïdors. Gestió del risc durant el servei (auditories pròpies i externes). Clausulats de seguretat. Gestió del risc a la finalització del servei (retorn de serveis, devolució d'informació sensible). STRIDE Threat Model.
12. Conscienciació i cultura de seguretat	Anàlisi del vector humà com a risc de seguretat. Elaboració d'un pla de conscienciació. Formació en comportaments segurs. Entrenament i simulacres d'enginyeria social.

Unitats a desenvolupar de Seguretat de les aplicacions:

Seguretat de les aplicacions	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
1. Cicle de vida del desenvolupament segur (SDLC)	Introducció al desenvolupament d'aplicacions, SDLC, bones pràctiques SDLC, arquitectura segura, models de maduresa, i normatives aplicables (LOPDGDD, RGPD, PCI DSS)
2. OWASP i vulnerabilitats d'aplicació	Coneixement del projecte OWASP i les seves eines (Top 10, SAMM, ASVS). Anàlisi detallada de vulnerabilitats comunes i com mitigar-les.
3. Proves de seguretat i gestió de vulnerabilitats	Coneixement pràctic de SAST, DAST, SCA, IAST. Gestió de vulnerabilitats, parxijat, eines de test i seguiment de seguretat d'aplicacions.
4. DevSecOps i maduresa del desenvolupament	Implementació de DevSecOps: integració de controls de seguretat en <i>pipelines</i> , definició de <i>security gates</i> , plataformes i eines (ASOC/ASPM).
5. Modelització d'amenaces	Conceptes i tècniques de <i>threat modeling</i> . Frameworks com STRIDE, PASTA, DREAD, MITRE ATT&CK. Productes i eines per a l'anàlisi d'amenaces.
6. Seguretat en aplicacions mòbils	Seguretat en aplicacions mòbils, riscos específics, millors pràctiques, simulació d'atacs i eines com MobSF.
7. Infraestructura segura	Disseny d'arquitectura segura (segmentació, DMZ, VPN, IDS/IPS, WAF), gestió d'identitats (IAM, MFA), control d'accés, encriptació i auditoria.
8. Seguretat en el núvol	Models IaaS/PaaS/SaaS, arquitectura de núvol, riscos OWASP Cloud, governança i responsabilitat compartida, seguretat de proveïdors, i eines CSPM/SSPM.

Unitats a desenvolupar de Gestió d'Identitats

Mòdul Gestió d'identitats	
Mòdul / Competència	Continguts en diferents nivells N1, N2, N3 i N4
1. Cicle de vida de l'usuari	Tipologia de comptes i identitats, àrees IAM/PAM/cIAM/IGA, fonts autoritzades, ABM (altes, baixes, modificacions), automatització, factors d'autenticació, biometria, auditoria i report. Gestió de certificats SSL: alta, renovació, revocació i seguiment.

2. Integració d'identitats	Sistemes cross-domain de gestió d'identitats, federació i delegació d'identitats, inici de sessió únic (SSO). Gestió de xifratge de correus electrònics mitjançant certificats i protocols segurs.
3. Gestió de rols	Control d'accessos basat en rols (RBAC), segregació de funcions, assignació i revisió periòdica dels rols.
4. Gestió d'accessos	Gestió d'accessos privilegiats (PAM), comptes amb privilegis, validació de dominis, gestió i monitoratge de sessions, llistes blanques i negres d'aplicacions.
5. Governança de la identitat	Polítiques de gestió d'identitats i certificats SSL, regulacions, campanyes de certificació, controls compensatoris, estàndards i bones pràctiques per la protecció de dominis i el compliment normatiu.

Unitats a desenvolupar de Protecció i Privacitat de Dades

Protecció i privacitat de dades	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
1. Fonaments de la protecció de dades i ciberseguretat	Tipologies de dades (personals, sensibles, estructurades/no estructurades), riscos, vulnerabilitats, pèrdua de reputació, context general de la ciberseguretat.
2. Legislació i regulacions en protecció de dades	RGPD, LOPDGGD, propietat intel·lectual, delictes digitals, Esquema Nacional de Seguretat, directiva NIS, ISO, normativa específica per a clients amb dades sensibles.
3. Xifratge de dades	Fonaments matemàtics, funcions hash, xifratge simètric i asimètric, xifratge per blocs i stream. Introducció a la criptografia aplicada.
4. Emmascarament i anonimització de dades	Privacitat en l'era digital, emmascarament, tokenització, anonimització, fabricació de dades, riscos de re-identificació.
5. Accés a les dades*	Principis i rols d'accés, eines d'accés (VPNs, autenticació, gestió d'identitats), tècniques d'accés, Deep Learning i Big Data.
6. Prevenció de fuga de dades	Identificació i classificació de dades sensibles, etiquetatge, assignació de mesures segons nivell de sensibilitat, eines DLP vs IRM.
7. Auditoria de protecció de dades*	Introducció i tècniques d'auditoria, estructura de bases de dades, consideracions legals i ètiques, accés, extracció i anàlisi de logs.
8. Avaluació de riscos i metodologies	Metodologies d'avaluació de riscos, impacte sobre drets i llibertats, identificació d'amenaques, mesures de mitigació i controls.

* Per enriquir l'experiència formativa, es planteja la incorporació de laboratoris especialitzats en els nivells 3 i 4 de formació. Aquests laboratoris oferiran un entorn pràctic on els alumnes podran aplicar de manera directa els seus coneixements teòrics, proporcionant experiències immersives per enfortir les seves habilitats en ciberseguretat.

Unitats a desenvolupar de Ciberdefensa

Ciberdefensa	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
1. Intel·ligència d'amenaçes	Cicle d'intel·ligència d'amenaçes, tipus d'intel·ligència (estratègica, tàctica, operativa, tècnica), kill chain, MITRE ATT&CK, IOC, OSINT, threat modelling, anàlisi de codi maliciós i d'infraestructures, ecosistema CTI (MISP, TIP, STIX, OpenCTI), orquestració, SOC de SOCs.
2. Operació del perímetre i detecció d'incidents	Gestió de vulnerabilitats (Nessus, Burp, CVSS, EPSS), SIEM, correlació d'esdeveniments, detecció per signatures i comportaments, regles SIGMA, detecció d'anomalies, enginyeria de deteccions, use case factory, automatització (SOAR), dashboards, IA/ML, monitorització de solucions.
3. Gestió i resposta activa davant d'incidents	Tipologia d'incidents, gestió del comitè de crisi, anàlisi d'intrusió, resposta i remediació (containment, erradicació, clean-room), lliçons apreses, comunicació d'incidents, gestió del ransomware, preparació i readiness d'incidents.
4. Anàlisi forense	Tècniques d'anàlisi forense en entorns Windows, Linux, mòbils i cloud, eines (KAPE, THOR, Velociraptor, volatility), accés a credencials, moviment lateral, recuperació d'evidències, cadena de custòdia, supertimelines, antiforense i gestió d'evidències.
5. Avaluació de l'exposició i test de penetració	Hacking ètic, metodologies (OSSTMM, PTES), vulnerabilitats i exploits, reconeixement, escalat de privilegis, evasió, accés a credencials, tunelització, moviments laterals, Active Directory, test de penetració, purple teaming, càlcul de l'exposició, informes, documentació.

Unitats a desenvolupar de Estructura organitzativa i processos empresarials

Estructura organitzativa i processos empresarials	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
Conceptes bàsics de l'estructura organitzativa	Definició i comprensió dels conceptes bàsics d'una organització i els seus nivells.
Funcions i rols en una organització	Descripció dels rols de l'alta direcció, gerents, tècnics, administratius i operatius.
Tipus d'estructures organitzatives	Característiques dels models jeràrquic, matricial, funcional...
Organigrames i la seva importància	Utilitat dels organigrames per a la gestió interna.
Cultura organitzacional	Importància de la cultura organitzacional en la identitat, motivació i coherència.
Valors i principis (missió, visió, valors)	Integració dels valors fundacionals en la gestió diària.
Ètica i integritat pública	Transparència, responsabilitat, equitat, servei al ciutadà i <i>compliance</i> .
Processos empresarials	Identificació, documentació i millora contínua de processos empresarials.
Polítiques i procediments	Implementació de polítiques i la seva coordinació amb els procediments operatius.
Gestió del canvi organitzacional	Estratègies de gestió del canvi, resistències i casos d'estudi.
Integració tecnològica i eines de gestió	Integració d'eines digitals en els processos organitzatius.

Ciberseguretat i aspectes tecnològics rellevants	Bones pràctiques en ciberseguretat aplicades a l'entorn empresarial.
--	--

Unitats a desenvolupar d'Habilitats interpersonals (soft skills)

Habilitats interpersonals (soft skills)	
Mòdul / competència	Continguts en diferents nivells N1, N2, N3 i N4
Comunicació efectiva	Desenvolupament d' habilitats de comunicació clara i efectiva.
	Maneig de la comunicació en situacions de crisi i amb diferents audiències.
Gestió del temps i prioritats	Estratègies per manejar múltiples tasques i projectes simultanis.
	Tècniques de prioritització en entorns d' alta pressió.
Lideratge i treball en equip	Desenvolupament d' habilitats de lideratge adaptatives.
	Foment d' un entorn de treball col·laboratiu i de suport.
Resolució de problemes i presa de decisions	Mètodes per abordar problemes complexos i prendre decisions efectives.
	Gestió de crisi i presa de decisions sota pressió.
Intel·ligència emocional	Desenvolupament d' empatia i consciència emocional.
	Maneig de conflictes i relacions interpersonals.

3.2.3 Els nivells de maduresa de les unitats dels cursos

Amb l'objectiu de garantir una alineació adequada entre els perfils professionals i els continguts formatius en matèria de ciberseguretat, es defineixen quins **nivells de maduresa competencial** han de preveure els contingut. Aquests nivells han de permetre l'establiment d'itineraris formatius progressius i modulars, adaptats a les necessitats específiques dels diferents perfils professionals o rols dins de l'organització.

En aquest sentit hi ha unitats que poden desenvolupar-se de manera diferent en nivells intermedi, avançat i superior. Principalment el que es prioritzarà en nivells més elevat és l'exercici pràctic dels alumnes per reforçar que coneixen i saben aplicar els coneixements.

Els quatre nivells següents representen l'evolució natural de la competència professional, des del coneixement bàsic fins al lideratge estratègic:

Nivell	Descripció	Capacitats associades
BÀSIC N1. Conversar (coneix)	L'alumne disposa de coneixement general sobre la competència i les seves implicacions en l'àmbit de la seguretat de la informació. Pot executar tasques senzilles sota supervisió.	- Coneixement bàsic i vocabulari específic - Principis generals d'integració amb sistemes - Comprensió dels principals ciber-incidents associats
INTERMEDI N2. Fer (aprèn, sap, esbrina)	L'alumne coneix suficientment i aplica processos concrets relacionats amb la competència i entén com s'implementen en els sistemes de l'organització. Actua amb autonomia funcional dins del seu lloc de treball.	- Ús operatiu d'eines i procediments - Coneixement funcional dels sistemes i tasques associades - Comprensió pràctica de les mesures de seguretat

AVANÇAT N3. Modificar (aplica, adapta, millora)	L'alumne disposa de coneixements avançats i pot adaptar, configurar o millorar sistemes i processos relacionats amb la competència. Treballa de manera autònoma i col·labora en l'evolució dels sistemes.	- Implementació i configuració de mesures específiques de seguretat - Avaluació de requisits de seguretat - Participació en definició i millora de processos i desenvolupaments
EXPERT N4. Liderar (transfereix)	L'alumne té un domini profund de la competència i capacitat per dissenyar estratègies, establir polítiques i liderar iniciatives de seguretat. Pot transferir coneixement i liderar la innovació.	- Coneixement expert i normatiu (estàndards, bones pràctiques) - Participació en fòrums i comunitats especialitzades - Certificacions reconegudes en l'àmbit de la competència

3.2.4 L'estructura dels continguts

Aquests continguts s'han d'estructurar en mòduls per a ser fàcilment digitalitzables en un LMS, que tinguin en compte els nivells (que contenen diferents unitats) i hauran de disposar aquesta composició mínima:

- Portada
- Introducció general del mòdul
- Índex de temes
- Unitats que desenvolupa aquest mòdul
- Repàs final del mòdul:
 - Resum final
 - Test de repàs
 - Cas pràctic final de mòdul amb solució basat en casos reals
- Bibliografia, legislació i enllaços d'internet d'interès general
- Annex o annexos sobre la temàtica i referències d'actualització dels continguts
- Avaluació final del mòdul o avaluació contínua composta per:
 - Avaluació final del mòdul qualificable
 - Cas pràctic qualificable amb solució
- Contraportada

Cada unitat haurà de contenir aquesta estructura mínima:

- Índex de continguts
- Introducció
- Objectius específics
- Continguts que apliquen al nivell específic
- Resum final amb les idees fonamentals
- Glossari de termes
- Bibliografia específica, enllaços d'interès i lectures recomanades
- Annex o annexos en cas de ser necessari a referències externes no avaluables
- Cas o casos pràctics amb solució
- Autoavaluació (vint preguntes tipus test) amb solució

3.2.5 Plantejament d'itineraris i dedicació mínima de formació

Per optimitzar la formació, es preveu agrupar els diferents perfils professionals en categories especialitzades, considerant nivells de maduresa i realitzant aquesta agrupació basant-nos en els criteris de la NIST ([National Institute of Standards and Technology](#)) on s'agrupen competències en el seu marc de ciberseguretat: "NICE Framework Competencies: Assessing Learners for Cybersecurity Work" IR 8355. La proposta d'itineraris formatius han estat dissenyats per fomentar sinergies entre rols afins, permetent als alumnes personalitzar la seva trajectòria. La inclusió de mòduls opcionals enriquirà la seva formació, oferint diverses possibilitats per al desenvolupament d'habilitats específiques.

La proposta es configura com una estimació aproximada que el servei de Coordinació d'activitat acadèmica haurà d'optimitzar des del punt de vista de la dedicació mínima en hores dels alumnes. Per dur a terme aquesta estimació, per poder entendre-ho s'ha ideat un escenari prenent com a referència els nivells de competències (N1, N2, N3 i N4) i ajustant les hores de formació corresponents a cada nivell:

Matèria de ciberseguretat / correspondència de nivell N1, N2, N3 i N4 amb perfils ciber	CISO	LEGAL	EDUCADOR	AUDITOR	RISC	INTEL·LIGÈNCIA	PENTESTER	ARQUITECTE	IMPLEMENTADOR	INCIDENTS	FORENSICS
Fonaments de la ciberseguretat	N3	N2	N2	N3	N3	N2	N2	N3	N2	N2	N2
Seguretat de les aplicacions	N1	-	-	-	-	N1	N3	N3	N4	N2	N1
Identitat Digital	N2	N1	-	N1	-	N2	N3	N2	N2	N2	N1
Protecció i privacitat de dades	N2	N4	-	N3	N3	N1	-	N2	N2	N1	N1
Ciberdefensa	N2	-	-	-	-	N4	N4	N2	N1	N4	N4
Estructura organitzativa i processos empresarials	N2	N2	N2	N2	N2	N1	N1	N2	N1	N1	N1
Habilitats interpersonals (<i>soft skills</i>)	N4	N3	N2	N3	N3	N1	N1	N4	N2	N1	N1

Matèria de ciberseguretat / correspondència d'hores previstes per perfils ciber											
	CISO	LEGAL	EDUCADOR	AUDITOR	RISC	INTEL·LIGÈNCIA	PENTESTER	ARQUITECTE	IMPLEMENTADOR	INCIDENTS	FORENSICS
Fonaments de la ciberseguretat	22	15	15	22	22	15	15	22	15	15	15
Seguretat de les aplicacions	2	-	-	-	-	2	6	6	8	4	2
Identitat Digital	4	2	-	2	-	4	6	4	4	4	2
Protecció i privacitat de dades	11	22	-	17	17	6	-	11	11	6	6
Ciberdefensa	12	-	-	-	-	38	38	12	4	38	38
Estructura organitzativa i processos empresarials	2	2	2	2	2	1	1	2	1	1	1
Habilitats interpersonals (<i>soft skills</i>)	3	2	1	2	2	1	1	3	1	1	1
TOTAL D'HORES	56	43	18	45	43	67	67	60	44	69	65

Aquests itineraris en detall, dissenyats per l'Agència, es trobaran disponibles per a poder revisar l'adjudicatari que hagi de crear els continguts específics que els apliquen per perfil. Existeix també una previsió del nombre dels diferents perfils de docents en ciberseguretat en funció de les àrees en les quals aquests han de ser especialistes per poder elaborar contingut formatiu i impartir les formacions sobre aquesta matèria.

3.3 Serveis i les seves característiques

De tot el que s'ha exposat prèviament es pot observar quins elements caracteritzen el sistema de contractació i digitalització de continguts:

La prestació haurà d'incloure la contractació i digitalització dels continguts formatius descrits anteriorment, que s'hauran de lliurar en format modular, per tal de facilitar la seva integració a la infraestructura digital de la Ciberacadèmia. Caldrà garantir la compatibilitat amb l'LMS utilitzat (formats SCORM, H5P, vídeos i altres recursos digitals equivalents.) i complir amb l'estructura mínima definida a l'apartat 3.2.3, preveient també la revisió i correcció dels materials segons els criteris de qualitat pedagògica i tècnica establerts.

El servei haurà de contemplar el disseny d'itineraris formatius adaptats a diferents nivells i perfils professionals del sector, mitjançant una modulació flexible que permeti itineraris personalitzats o d'especialització, tot vetllant per la coherència pedagògica entre els continguts, les activitats i el sistema d'avaluació.

S'haurà d'incloure una figura responsable de la coordinació de l'activitat acadèmica, encarregada de planificar el calendari de les activitats formatives, determinar-ne el format (síncron o asíncron) segons el programa, el nivell i les hores de dedicació, així com d'assignar els docents corresponents mitjançant la bossa d'hores disponible. Aquesta figura també haurà de fer el seguiment de l'execució formativa i gestionar possibles incidències.

Caldrà establir un mecanisme de revisió pedagògica i lingüística dels materials elaborats, que permeti validar-ne l'adequació i comprensibilitat per part del públic objectiu, així com proposar-ne les correccions o millores necessàries abans de la seva publicació.

El servei haurà de garantir l'acompanyament dels alumnes en els entorns virtuals d'aprenentatge, dinamitzant fòrums, tutories i espais d'interacció educativa, i oferint suport al procés formatiu a través d'eines digitals complementàries (microaprenentatges, recordatoris, reptes, o d'altres que es puguin proposar). L'adjudicatari també haurà de vetllar perquè els alumnes que accedeixin als cursos compleixin els criteris d'accés establerts per a cada itinerari, i oferir-los assessorament en la tria de rutes formatives d'acord amb el seu perfil professional. Així mateix, caldrà gestionar els processos de certificació i reconeixement d'aprenentatges que s'estableixin. S'haurà de preveure, si s'escau, la prestació de serveis auxiliars com:

- **Adaptació dels continguts a criteris d'accessibilitat universal**, garantint que els recursos digitals compleixin els estàndards WCAG 2.1 (nivell AA), especialment pel que fa a navegació, lectura, contrast, subtitulació i estructuració semàntica.
- **Traducció i/o adaptació lingüística dels continguts**, en funció dels col·lectius als quals s'adrecin els itineraris, amb especial atenció a la disponibilitat en català i castellà, i opcionalment en anglès o altres idiomes si el programa ho requereix.

Finalment, el servei haurà de contemplar la cerca activa d'acords amb empreses, institucions i altres actors del sector de la ciberseguretat, promovent aliances que facilitin accions conjuntes com certificacions, docència compartida o accés a infraestructures, amb l'objectiu d'incrementar el valor afegit de l'oferta formativa de la Ciberacadèmia.

3.3.1 La qualitat dels lliurables

Els continguts que es generin en el marc d'aquest contracte hauran de complir els següents requisits de qualitat:

- Idioma: Tots els continguts hauran d'estar redactats íntegrament en llengua catalana, seguint la normativa oficial de l'Institut d'Estudis Catalans. Caldrà garantir un ús correcte de la gramàtica, l'ortografia i la puntuació.
- Els continguts hauran de ser actualitzats i pertinents en el moment del lliurament. Es revisarà l'ús de dades o referències obsoletes, i s'exigirà la seva vigència informativa i al màxim alineada amb els informes disponibles de [Tendències de ciberseguretat](#).
- Coherència terminològica: La terminologia emprada haurà d'estar alineada amb el llenguatge propi de l'Agència. L'adjudicatari haurà de seguir les guies d'estil, manuals de redacció i altres documents de referència que l'Agència posi a disposició.
- Els textos hauran de tenir un registre adequat i ser comprensibles per a la tipologia d'alumnat destinatari. Caldrà adaptar el to i el nivell de complexitat segons les indicacions de l'Agència.
- Rigor i fiabilitat: La informació haurà de ser contrastada i procedent de fonts fiables. No s'admetran dades especulatives, ambigües o sense fonament documental.
- Els continguts s'hauran de lliurar seguint l'estructura, el format i les plantilles definides per l'Agència. En cas contrari, aquesta podrà sol·licitar-ne la correcció.

- Tots els continguts hauran de ser originals i lliures de plagi. En cas d'incloure contingut de tercers, s'haurà de comptar amb les autoritzacions pertinents i citar correctament les fonts o drets d'autoria.
- L'adjudicatari haurà de garantir una revisió completa del contingut (orto tipogràfica, de coherència i de qualitat) abans del lliurament.
- L'Agència es reserva el dret de revisar i, si escau, sol·licitar modificacions dels continguts lliurats en cas que no compleixin els requisits establerts, sense que això suposi cap cost addicional.
- Compliment dels terminis: Els lliuraments hauran de fer-se dins dels terminis acordats. Els retards reiterats o no justificats podran ser motiu de penalització o resolució del contracte.
- Criteris d'accessibilitat i inclusivitat: Els continguts hauran de vetllar per l'ús d'un llenguatge inclusiu i no sexista, i fomentar la representació de la diversitat, d'acord amb els valors de l'Agència. El [Pla estratègic de Dones en ciberseguretat de l'Agència de Ciberseguretat de Catalunya](#) parla de la formació i capacitació per a tothom, per una societat digital inclusiva, equitativa i sostenible.
- Adaptabilitat a canals i formats digitals: Quan s'especifiqui, els continguts hauran de ser aptes per a diferents canals de difusió (web, xarxes socials i/o newsletters) i respectar els requeriments tècnics corresponents.
- Metadades i traçabilitat: Els continguts hauran d'anar acompanyats, si es demana, de les metadades bàsiques (títol, autor, data, paraules clau, o d'altres que es puguin considerar) per facilitar-ne la gestió, cerca i publicació.

3.3.2 Propostes de millora dels continguts

L'empresa adjudicatària del contracte ha de tenir la capacitat d'usar eines de desenvolupament de capacitació que s'ajustin a la infraestructura disponible. Entre aquestes enumerem propostes que podran ser valorades:

- Disseny d'activitats formatives o de gamificació (*capture the flag, attack simulation*, ciber exercicis de defensa, simulació d'escenaris...).
- Disseny d'exercicis de pràctiques a diferents plataformes Cyber Range. Es relaciona el directori de la comunitat de proveïdors europeus gestionada per l'ECSO a l'Annex d'[European Cyber Range Community - ECSO](#) on s'exposen les eines adreçades a resoldre casos d'ús com:
 - **Educació en ciberseguretat** - Implementació de cursos i currículums bàsics i avançats.
 - **Investigació en ciberseguretat** - Investigació de nous mètodes de detecció i mitigació d'atacs.
 - **Resiliència cibernètica** - Capacitat de respondre i mantenir-se durant incidents de seguretat.
 - **Capacitats cibernètiques** - Desenvolupament de capacitats dels professionals de seguretat i investigació d'eines cibernètiques.

En molts casos aquest proveïdors proporcionen servei emulant virtualment diferents dispositius, servidors i xarxes que permeten integrar-se en plataformes LMS i també testear eines de codi obert o llicenciades de seguretat (Splunk, Nmap, Alien Vault, Metasploit...).

Algunes referències:

1. **Kypo Cyber Range**, llançada per CONCORDIA H2020, és una solució de ciberseguretat de codi obert especialment dissenyada per a l'educació. Aquesta plataforma redueix els costos associats a les solucions tradicionals de cyber range. Per instal·lar-la, es requereix OpenStack i un proveïdor d'OpenID Connect. <https://crp.kypo.muni.cz/>
2. **TryHackMe**, una plataforma de formació en ciberseguretat que ofereix laboratoris interactius i aules virtuals per a la pràctica de tècniques en entorns reals. Disposa de 900 laboratoris que cobreixen tant aspectes ofensius com defensius, amb contingut adaptat a tots els nivells d'experiència. La plataforma permet iniciar màquines virtuals vulnerables directament des d'un navegador, facilitant la configuració i l'accés als recursos necessaris per a l'aprenentatge. Inclou eines de gestió per als docents, que poden assignar tasques, monitoritzar el progrés dels alumnes i recomanar laboratoris que s'alineïn amb el seu pla d'estudi. <https://tryhackme.com/classrooms>
3. **UNIGE CRACK Multidomain CyberRange (CRACK MCR)**, desenvolupada per la Universitat de Gènova, ofereix escenaris multidomini que integren infraestructures IT/OT complexes, entorns de computació en núvol simulats, dispositius mòbils i centres d'operacions de seguretat (SOC). Opera per a activitats pràctiques durant els cursos i per a l'organització de competicions *Capture The Flag* i exercicis de defensa cibernètica. Utilitza frameworks de codi obert com CRACK - Cyber Range Automated Construction Kit i LiDiTe - Lightweight Digital Twin Environment. [GitHub - enricorusso/CRACK: Cyber Range Automated Construction Kit](#)
4. **UNINA Docker Security Playground** permet la creació d'escenaris interactius basats en contenidors amb infraestructures de xarxa complexes. És ideal per a la formació pràctica en ciberseguretat. Utilitza tecnologia Docker, que és lleugera i permet reproduir escenaris de xarxa reals. [GitHub - DockerSecurityPlayground/DSP: A Microservices-based framework for the study of Network Security and Penetration Test techniques](#)
5. **Vigrid** és una extensió de l'eina GNS3 que afegeix industrialització per a un ús massiu. Permet crear projectes que allotgen màquines virtuals sobre Qemu o Docker, amb capacitats d'emulació de CPU diverses. Utilitza tecnologies de codi obert per obrir GNS3 a un nou univers, incloent emulació de maquinari comercial. [GitHub - Vigrid is a Cyber Range redesign of the GNS3 tool able to virtualize almost any physical device on many CPU.](#)

Aquestes plataformes de codi obert poden integrar-se amb LMS mitjançant API d'experiència (xAPI) o SCORM per exportar dades de rendiment dels alumnes. Això permet una fàcil implementació i seguiment del progrés dels alumnes en escenaris de ciberseguretat.

- Eines complementàries a LMS que es vulgui proposar per les metodologies:
- **Isard Virtual Desktop Infrastructure (IsardVDI)**: plataforma al núvol de codi obert per a desplegar infraestructura digital de forma fàcil usant Docker i Docker Compose. Ofereix escenaris de pràctica, projectes, xarxes o laboratoris a l'alumnat. [IsardVDI · GitLab](#)
- **Nearpod**: plataforma interactiva d'aprenentatge, integrable amb altres recursos, que ofereix una varietat de funcionalitats per millorar l'experiència educativa: presentacions interactives afegint avaluacions formatives, simulacions i mitjans dinàmics, vídeos interactius amb preguntes integrades per comprovar la comprensió dels alumnes, gamificació i activitats. Permet avaluació en temps real en entorns híbrids. [How Nearpod works](#)
- **Kami**: ofereix diverses funcionalitats per millorar l'accessibilitat i la inclusió en l'aprenentatge dels alumnes. Aporta reconeixement de text, organitzadors gràfics, fonts per a dislèxia, dictat per veu, mode fosc i lectura en veu alta, ofereix subtítols, comentaris en vídeo i multimèdia. I personalització i inclusió, opcions per a grups específics per donar el suport necessari. [Kami](#)

3.4 Infraestructura i plataforma d'aprenentatge

3.4.1 Objecte i descripció de la plataforma

L'objecte del contracte és la contractació d'una solució tècnica per a la Ciberacadèmia amb els elements característics següents:

- Ha de ser un sistema que contingui les funcionalitats completes d'LMS (Learning Management System) que permeti suport per l'aprenentatge síncron i asíncron.
- Que permeti un sistema de gestió d'itineraris formatius.
- Que permeti la gestió de la formació segons els estàndards SIS (Student Information System) i que inclogui funcionalitats de comercialització.
- Que permeti la interoperabilitat de plataformes de l'ecosistema educatiu actual de la ciberseguretat (LTI – Learning tools interoperability).
- Que permeti la gestió bàsica de continguts i l'estàndard SCORM que facilita la compartició.
- Que integri el format vídeo en classes de professorat (permetent formats en vídeo streaming, live streaming o vídeo broadcasting) o suports multimèdia per les classes de professors.
- Que permeti la publicació oberta de cursos mitjançant landings o microsites específics i la gestió d'inscripcions automàtiques, sense necessitat de procés d'admissió formal, facilitant així l'accés directe a determinades accions formatives.

A la proposta que l'adjudicatari presenti se li demanarà com a requeriment la integració d'usuaris de sistemes de seguretat (prioritàriament del sistema de Microsoft en què treballa l'Agència). Tanmateix la solució pot aportar sistemes SSO (single sign-on) per accedir a aplicacions SaaS amb seguretat.

3.4.2 Serveis de la plataforma

El projecte de la Ciberacadèmia requereix de recursos tecnològics amb una clara connexió amb l'ecosistema educatiu actual de l'àrea de la ciberseguretat (que actualment proveeixen centres educatius públics i privats o que disposa el propi sector dedicat a la ciberseguretat de Catalunya).

En aquest sentit la solució tècnica proposada haurà de satisfer aquests objectius:

1. El de ser un LMS (*Learning Management System*), és el punt central per a un sistema de formació en línia. Connecta continguts CMS o el sistema de gestió SIS, sent també el punt de connexió d'altres plataformes educatives amb estàndards com LTI (*Learning Tools Interoperability*). Ofereix totes les funcionalitats necessàries per gestionar, impartir i avaluar la formació en línia. Ha d'incloure eines per crear diferents programes formatius, gestionar les inscripcions, fer seguiment històric del progrés dels alumnes participants i generar els informes detallats sobre el rendiment acadèmic de l'activitat formativa proposada pel professorat.
2. El sistema de gestió d'itineraris formatius: ha de permetre l'organització flexible de cursos i gestionar els diferents itineraris formatius i nivells basats en 4 grans àrees especialitzades de la ciberseguretat (govern, vigilància, seguretat i resiliència), els quals agrupen els 11 perfils professionals de ciberseguretat de l'ENISA, assegurant que compleixin amb els requisits acadèmics i professionals. Facilita la personalització dels plans d'estudi segons les necessitats i objectius individuals, combina mòduls compartits i facilita la reutilització de

continguts i l'adaptabilitat a diferents necessitats formatives. L'usuari ha de tenir una visió clara del progrés, la trajectòria personalitzada i les competències adquirides, optimitzant la seva experiència d'aprenentatge mitjançant la recomanació de continguts i activitats basades en el progrés.

3. El sistema SIS (*Student Information System*): que gestiona tota la informació acadèmica i administrativa dels alumnes, des de les inscripcions fins a les qualificacions, i connectable amb l'LMS. Ha de permetre gestionar les relacions amb els alumnes i potencials nous usuaris interessats en itineraris o cursos de ciberseguretat, millorant la comunicació i la comercialització de la Ciberacadèmia.
4. El sistema d'interoperabilitat de plataformes educatives (LTI): que ha de permetre la integració i interoperabilitat d'altres diferents plataformes educatives dins l'ecosistema de la ciberseguretat. Utilitzant l'estàndard LTI (*Learning Tools Interoperability*), facilita la connexió i l'ús conjunt de diverses eines i recursos educatius que ja existeixen en operació, millorant l'experiència d'aprenentatge. Aquesta interoperabilitat s'acordarà amb entitats i institucions amb qui s'estableixi xarxa de col·laboració desenvolupada amb la Ciberacadèmia, ja sigui per assignatures amb professorat específic o per recursos d'entrenament, pràctiques o demostradors (per exemple, continguts de *bootcamps*, *hands-on* o *lab-based training*, o *cyber range*).
5. El sistema de gestió de continguts, compatible amb estàndard SCORM: la gestió bàsica de continguts educatius i que és compatible amb l'estàndard SCORM (*Sharable Content Object Reference Model*). Això ha de facilitar la creació, compartició i reutilització de continguts formatius entre diferents plataformes LMS, assegurant la coherència i la qualitat de l'aprenentatge.
6. El sistema de publicació oberta i inscripció automàtica a través de *landings* o *microsites* específics: ha de permetre la creació i gestió d'espais web orientats a la difusió de cursos oberts, que no requereixin un procés d'admissió formal. Aquests espais han d'oferir una interfície intuïtiva per a l'usuari final, on es pugui consultar l'oferta formativa i realitzar la inscripció de manera directa i automàtica. Aquesta funcionalitat facilita l'accés immediat a determinades accions formatives, especialment aquelles orientades a la sensibilització, l'actualització o la formació inicial en ciberseguretat, i permet escalar la formació a col·lectius amplis. Així mateix, contribueix a la difusió i promoció de la Ciberacadèmia, reduint la càrrega administrativa i millorant l'eficiència del sistema de matriculació.

3.4.3 Activitats i funcionalitats que s'esperen del servei

Les solucions tècniques de les principals plataformes en línia que hi ha actualment al mercat són sistemes Moodle, Canvas, Blackboard, entre altres. Totes aquestes solucions són vàlides per la implementació ja que són propostes segures, robustes i abastament provades. Totes permeten funcionalitat completes, incloent la gestió d'usuaris, la creació i administració de cursos, el seguiment del progrés dels alumnes, la generació d'informes i la integració amb eines de col·laboració i comunicació.

Però és essencial per a la urgència en el termini d'execució d'aquest projecte per l'Agència que la solució proposada pugui consumir-se com un servei en línia en la màxima brevetat a l'iniciar l'activitat acadèmica segons el calendari planificat.

Per aquest motiu l'adjudicatari haurà d'aportar detall de com es proposa consumir la seva solució tècnica aportada, ja madura i testejada, i en quines condicions l'aporta externament com a servei accessible per a tots els usuaris i usuàries de la Ciberacadèmia, amb la marca visual de la Ciberacadèmia de l'Agència. Per això haurà d'indicar si existeixen condicions o requeriments de llicenciament per l'usuari (gestor, docent o alumnat) i descriure de forma transparent les condicions econòmiques necessàries.

Per entendre aquest consum previst pel servei tecnològic de plataforma de formació al núvol en modalitat SaaS (*Software as a Service*), tant al procés formatiu com operatiu, s'haurà d'especificar si compleix els requeriments mínims:

- Si permet l'escalabilitat per ajustar fàcilment els recursos segons la demanda de la Ciberacadèmia, escalant cap amunt o cap avall i evita restriccions del programari tradicional. Això facilita el creixement i l'adaptació ràpida a la necessitat.
- Si s'actualitza la tecnologia de manera automàtica i centralitzada al núvol per tal d'eliminar la necessitat d'actualitzacions manuals, estalviar temps i altres recursos de suport.
- Si és accessible des de qualsevol lloc amb connexió a Internet. Això promourà la col·laboració, la participació més àmplia en l'activitat formativa i permetrà major flexibilitat en desenvolupar-se amb modalitats síncrones o asíncrones, evitant desplaçaments amb l'accés remot.
- Si automatitza processos per tal de permetre executar tasques de gestió repetitives de manera eficient. Amb això es vol reduir errors, augmentar la productivitat i millora la satisfacció dels usuaris.
- Si permet la capacitat d'integració d'usuaris amb els sistemes de seguretat de Microsoft o de Google. Preferentment la gestió de SSO (single sign-on) per accedir a aplicacions SaaS amb més seguretat.

A continuació es descriuen les funcionalitats esperades de la solució tecnològica aportada:

1. Quant a les funcionalitats del LMS:

- Gestió de cursos: creació i administració de cursos amb eines intuïtives i simples.
- Avaluació: els professors puguin posar tasques i exercicis i corregir-les.
- Detall de progrés de l'alumne: proporcioni dades detallades i monitoritzi el progrés d'alumnes i identifiqui necessitats de suport. Ha de facilitar aquest seguiment del progrés dels alumnes, fins i tot, en els mòduls SCORM que hi hagi presents al curs, oferint informes detallats sobre el rendiment i les activitats completades.
- Gestió d'APIs (*Application Programming Interface*): connectable amb altres eines per comunicar-se i integrar-se. Permetent l'automatització de processos (per exemple, les qualificacions assolides pels alumnes per al SIS Sistema de gestió).

- Accessibilitat amb dispositius: sistemes d'accessibilitat amb APPs per a professors i alumnes, permetent accedir a les funcions del LMS des de qualsevol lloc.
2. Quant a les funcionalitats en els diferents itineraris, perquè siguin estructurats i adaptats als alumnes:
- Agrupament en mòduls: permeti organitzar el contingut dels cursos en unitats lògiques, com setmanes o temes, facilitant la navegació i l'accés seqüencial als materials.
 - Interfície personalitzable: ofereixi una vista d'entrada clara i organitzada, on els alumnes vegin els itineraris formatius que estan fent i accedeixin ràpidament als recursos necessaris.
 - Navegació de l'itinerari: permeti limitar i personalitzar enllaços de navegació per simplificar l'accés als continguts i millori l'experiència d'aprenentatge.
 - La generació de *badges* o insígnies digitals: que reconguin i certifiquin l'assoliment de competències específiques o la finalització de cursos dins un sistema d'itineraris formatius. Aquests elements poden servir de motivació pels alumnes, proporcionant un reconeixement visual i tangible dels seus èxits, i poden ser compartits a perfils professionals en CV o en plataformes d'intermediació laboral per demostrar les habilitats adquirides (LinkedIn, per exemple, on els reclutadors poden trobar ràpidament habilitats de ciberseguretat dels perfils).
 - Prerequisits i requisits: permeti configurar condicions que els alumnes han de complir abans de passar a la següent fase de l'itinerari, assegurant un progrés estructurat i coherent.
 - Integració d'eines externes: ha de permetre usar l'estàndard LTI per integrar matèries, pràctiques i recursos addicionals, enriquint els itineraris formatius amb continguts interactius i variats.
3. Quant a les funcionalitats de la solució del sistema de gestió SIS (*Student Information System*) integrable a l'LMS:
- Sincronització de dades: ha de permetre la sincronització automàtica de dades acadèmiques i administratives entre el SIS i el LMS, assegurant que la informació dels alumnes, cursos i gestió de les matriculacions estigui sempre actualitzada.
 - Importació de dades: que faciliti la importació massiva de dades des del SIS al LMS mitjançant un format d'arxius (per exemple l'estructura CSV), simplificant la integració de grans volums d'informació acadèmica.
 - Configuració personalitzada: ha de permetre adaptar les funcionalitats del SIS a les necessitats específiques dels sistemes de titulacions i certificacions professionals i universitàries existents al sistema educatiu de Catalunya, assegurant una gestió adequada segons els requisits.
 - Gestió de qualificacions: que faciliti la transferència de qualificacions des del LMS al SIS, permetent als professors sincronitzar les notes de manera manual o automàtica, garantint una gestió eficient i precisa.
 - Integració bidireccional: que ofereixi una integració bidireccional fent possible l'intercanvi de dades entre el SIS i LMS, millorant la coordinació i la gestió de la informació acadèmica.
 - *Customer Relationship Management* (CRM): a banda de la gestió administrativa dels alumnes des de les inscripcions fins a les qualificacions, ha de ser integrable o bé incloure un mòdul CRM que permeti gestionar les comunicacions o notificacions amb els alumnes i els

potencials nous usuaris de cursos. Aquesta integració és clau per automatitzar la comercialització de noves propostes formatives que es vagin incloent en el calendari de la Ciberacadèmia.

4. Quant a les funcionalitats del sistema d'interoperabilitat de plataformes educatives (LTI) que milloren l'experiència d'aprenentatge, hauria d'aportar:
 - Integració d'aplicacions i plataformes externes: ha de permetre la integració de diverses aplicacions educatives externes dins del LMS, facilitant l'accés a eines addicionals i altres recursos. Aquestes aplicacions externes poden arribar a complementar també els mòduls SCORM presents als cursos.
 - Configuració d'un centre d'aplicacions: administradors del LMS i formadors poden habilitar o deshabilitar les aplicacions a través d'un centre d'aplicacions permetent afegir noves funcionalitats a nivell de compte d'usuari o de curs.
 - Sincronització de dades: utilitza l'estàndard LTI (versions compatibles LTI 1.1, LTI 1.2 i LTI 1.3, preferentment aquesta darrera) per enviar informació verificable sobre els usuaris a plataformes de tercers, assegurant una integració segura i eficient.
 - Gestió simplificada d'eines LTI: amb la [versió LTI 1.3](#), la instal·lació i gestió d'eines LTI és més simplificada, reduint molt els passos necessaris i amb una interfície d'usuari.

Exemples de plataformes i aplicacions integrables amb l'LMS a través de la interoperabilitat LTI que tenen a veure amb serveis de formació en ciberseguretat:

- [Cisco Networking Academy](#): proporciona materials de formació en xarxes i ciberseguretat, amb laboratoris virtuals i simulacions que es poden accedir directament des del LMS.
 - [CodeHS](#): ofereix cursos de programació i ciberseguretat amb exercicis pràctics que es poden integrar al LMS per avaluar les habilitats dels alumnes.
 - [Cybrary](#): ofereix cursos interactius i laboratoris pràctics en ciberseguretat, permetent als alumnes aprendre i practicar habilitats en un entorn segur.
 - [Khan Academy](#): inclou continguts sobre ciberseguretat que es poden integrar a un LMS per complementar els cursos amb vídeos educatius i exercicis interactius.
 - [Palo Alto Networks Cybersecurity Academy](#): Proporciona recursos educatius i laboratoris pràctics en ciberseguretat, integrables amb un LMS per oferir una experiència d'aprenentatge completa.
5. Quant a les funcionalitats del sistema de gestió de continguts (CMS - *Content Management System*)
 - Editor de continguts: Ofereix eines per crear i editar continguts multimèdia, incloent vídeos, àudios, imatges i textos, millorant la qualitat dels materials educatius.

- Permeti crear cursos plantilla que es puguin sincronitzar amb altres cursos, assegurant que els continguts es mantinguin actualitzats i coherents. Ha de poder-se visualitzar-se directament format SCORM dins del LMS, assegurant una integració fluida i accessible per als alumnes.
 - Permeti organitzar i gestionar tots els fitxers del curs en un sol lloc, facilitant l'accés i la compartició de recursos. Eventualment aquests fitxers hauran de poder emmagatzemar-se en un suport extern proporcionat per l'Agència.
 - Eina d'importació/exportació: Faciliti la importació i exportació de continguts entre cursos, permetent als professors copiar materials didàctics de manera eficient. Concretament haurà de permetre importar fàcilment mòduls SCORM a aquest LMS, integrant-los directament en els cursos per a una experiència d'aprenentatge interactiva.
 - Permeti la compartició de recursos educatius: una biblioteca digital que permet als professors compartir i importar recursos educatius, facilitant la reutilització de continguts entre cursos i institucions
6. Quant a les funcionalitats d'integració de vídeo per les classes del professorat (permetent formats en vídeo streaming, live streaming o vídeo broadcasting) o multimèdia dins el LMS

La combinació de la formació en línia amb sessions virtuals brinda un enfocament equilibrat que aprofita els avantatges d'ambdós models educatius.

S'ha de preveure la utilització d'eines de suport a la gestió i creació de contingut multimèdia i que puguin integrar-se al LMS.

Els professors han de poder:

- Crear i organitzar contingut: crear, lliurar, allotjar i organitzar contingut de vídeo en una biblioteca de mitjans pròpia.
- Interacció i col·laboració: facilitar la interacció activa amb els alumnes a través de comentaris directament en la línia de temps del vídeo.
- Anàlisi i seguiment: proporcionar anàlisis detallades sobre qui ha vist els vídeos, durant quant de temps i quines parts han estat més interessants o confuses.
- Integració amb LMS: incrustar vídeos dins les unitats.
- Avaluació i feedback: crear qüestionaris dins dels vídeos, oferir feedback instantani i enviar les qualificacions directament al llibre de qualificacions.

I als alumnes hauria de permetre'ls:

- Participació activa: participar activament comentant en la línia de temps del vídeo i oferint feedback sobre el treball dels seus companys.
- Creació de contingut: crear i carregar els seus propis vídeos per a projectes i assignacions.
- Accés fàcil: accedir als vídeos des de qualsevol dispositiu i plataforma, facilitant l'aprenentatge en qualsevol moment i lloc.
- Interacció amb el contingut: respondre a qüestionaris integrats en els vídeos i rebre feedback instantani sobre les seves respostes.
- Col·laboració: col·laborar amb els seus companys a través de comentaris i discussions en els vídeos.

En aquesta llista s'anoten algunes eines que són referència al mercat:

- **Brightcove**: proveïdor global de solucions de vídeo en el núvol, anàlisi de rendiment i integració amb diverses plataformes.
<https://www.brightcove.com/es/solutions/live-streaming/>
- **Canvas Studio**: aprenentatge interactiu i col·laboratiu a través de vídeos. Permet incrustar vídeos en assignatures, discussions i pàgines de l'LMS Canvas.
<https://www.instructure.com/es/educacion-superior/productos/canvas/canvas-studio>
- **Kaltura**: plataforma de vídeo de codi obert que ofereix eines potents per a la gestió i processament de vídeos. Inclou widgets, integració amb LMS, i capacitats de gestió de contingut multimèdia.
<https://corp.kaltura.com/education-video-platform/>
- **VoiceThread**: plataforma que permet la creació de presentacions multimèdia interactives, on els usuaris poden comentar amb text, veu o vídeo i integració amb LMS.
<https://voicethread.com/products/highered/>
- **VIDIZMO**: plataforma de gestió de vídeos que ofereix solucions per a la formació, el màrqueting i la comunicació corporativa. Gestió de contingut multimèdia, anàlisi de rendiment i integració amb diverses plataformes.
<https://vidizmo.ai/enterprise-video-platform/use-cases/video-training-platform>

7. Quant a les funcionalitats del sistema de publicació oberta i inscripció automàtica a través de *landings* o *microsites* específics:

- Gestor de landings o microsites personalitzables: eina que permeti crear i gestionar espais web específics per a cada curs o grup de cursos, amb capacitat d'adaptar el contingut (imatges, textos, vídeos, enllaços i altres recursos digitals.) i la marca visual de la Ciberacadèmia.
- Catàleg de cursos en obert amb filtres i cercador: visualització clara i navegable de l'oferta formativa disponible sense requisits previs, amb opcions de filtre per temàtica, durada, nivell, dates o format.
- Sistema d'inscripció directa i automatitzada: formulari d'inscripció integrat que permeti registrar-se al curs amb dades bàsiques (nom, correu i altres dades identificatives mínimes) i que generi automàticament l'usuari dins el sistema LMS i/o SIS, assignant-lo al curs corresponent sense intervenció manual.
- Validació de correu i confirmació d'inscripció automàtica: enviament automàtic d'un correu de benvinguda amb informació d'accés i instruccions per iniciar el curs.
- Integració amb LMS per activació immediata: connexió directa amb el sistema LMS que permeti activar el curs per l'usuari un cop completada la inscripció, amb accés al contingut, calendari, recursos i activitats.
- Panell de control i estadístiques d'inscripció: espai de gestió per part de l'equip tècnic o de coordinació, des d'on es puguin consultar en temps real les dades d'inscripció, evolució de participació, conversió de visites i altres dades que es considerin necessàries.
- Compatibilitat amb campanyes de difusió i captació: capacitat d'integrar-se amb eines de màrqueting digital (Google Ads, xarxes socials, newsletters i altres canals digitals de promoció.) per facilitar la captació massiva d'usuaris i fer seguiment de la conversió.

- Suport multidioma i accessibilitat: possibilitat de publicar els cursos i formularis d'inscripció en més d'un idioma (com a mínim català, castellà i anglès), i garantir el compliment de criteris d'accessibilitat digital.

3.4.4 Productes del servei

Aquest servei es diferencia en dues parts. La primera que ha de permetre posar tot el sistema en marxa i, la segona, el manteniment, perfeccionament i actualització del sistema en funcionament:

I. Servei d'arrancada del sistema

Implementar un sistema LMS implica diverses fases per assegurar una configuració adequada i la incorporació d'usuaris amb diferents rols (administradors del sistema, gestors de grup, dinamitzadors i professors de diferents programes, alumnes de diferents grups o programes...).

Per aquest procés és necessari implicar l'equip format pels serveis:

- Integració de plataformes
- Configuració de itineraris i mòduls
- Coordinació d'activitat acadèmica
- Campanyes de màrketig inicials

Una descripció possible de les fases seria:

Fase 1: Planificació i preparació

- Identificar els requisits específics de la nova institució educativa, incloent-hi els tipus d'usuaris i les funcionalitats necessàries.
- Configuració inicial: establir els paràmetres bàsics del sistema, com la configuració del SSO (Single Sign-On) per facilitar l'accés segur i centralitzat.
- Formació inicial: preparar sessions de formació per a qui hagi d'administrar la plataforma, assegurant que comprenguin l'abast de totes les funcionalitats i la gestió del sistema.

Fase 2: Configuració del sistema

- Creació de rols i permisos: definir els rols dels tots els usuaris (administradors del sistema, gestors de grup, dinamitzadors i professors de diferents programes, alumnes de diferents grups o programes...) i assignar els permisos corresponents.
- Integració del SIS: configurar la integració amb el sistema SIS proposat per sincronitzar dades acadèmiques i administratives.
- Configuració de LTI: integrar aplicacions externes utilitzant l'estàndard LTI per aquells cursos que necessiten enriquir-se amb recursos addicionals.

Fase 3: Creació de continguts i itineraris formatius dels diferents programes previstos

- Importació de continguts: utilitzar el CMS per importar continguts SCORM, suport a l'edició en la pròpia plataforma si cal programar missatges automàtics pels usuaris i altres materials didàctics.

- Estructuració de cursos: crear i organitzar els programes de cursos amb diferents nivells i amb el programa d'itineraris formatius, definint mòduls, comuns i específics, requisits d'estudi i plans d'estudi.
- Configuració de serveis que permetin veure les funcionalitats dels itineraris en curs amb interfície personalitzable.

Fase 4: Incorporació d'usuaris

- El rol administrador: per incorporar els usuaris que administraran la plataforma, assignant-los rols i permisos per gestionar el sistema.
- El rol professor o dinamitzador: que registra el gruix de professors disponible, oferint-los formació sobre la creació/edició dels materials dels cursos, com funciona les pautes d'avaluació d'alumnes i quines eines disponibles addicionals poden usar.
- Gestor o coordinador de grups: incorporar els usuaris responsables de la gestió de grups d'alumnes i l'assignació de matèries a cada alumnes, assegurant que compreguin com funciona la configuració dels itineraris formatius.

Fase 5: Prova i ajustaments

- Prova pilot: realitzar una prova pilot amb un primer grup d'usuaris per identificar possibles problemes i ajustar la configuració.
- Ajustaments finals: fer els ajustaments necessaris basats en els resultats de la prova pilot, assegurant que el sistema estigui optimitzat per al seu ús complet.

Fase 6: Llançament

- Llançament oficial: posar en marxa el sistema per a tots els usuaris, assegurant que estiguin preparats per utilitzar-lo de manera efectiva.

Per aquest procés s'estima una duració d'entre 5 i 10 setmanes. En aquest sentit l'adjudicatari haurà de proporcionar una planificació detallada, identificant els punts crítics, i la previsió de recursos tècnics necessaris per l'arrancada que garanteixin un llançament exitós del sistema.

II. Serveis amb el sistema en marxa

Es preveu que es proporcioni suport tècnic continu per resoldre problemes als usuaris i oferir formació addicional segons sigui necessari.

Addicionalment al suport continu que s'espera del servei tècnic de configuració hi ha una sèrie de perfils requerits, amb dedicacions menys intensives, imprescindibles per complementar l'eficiència de la infraestructura:

- Servei d'admissió d'alumnes

Realitzar prospecció de mercat per identificar potencials alumnes interessats en els programes de formació de la Ciberacadèmia, entre els àmbits de relació de l'Agència.

Desenvolupar estratègies de captació de nous alumnes, incloent propostes de campanyes de màrqueting al responsable de campanyes i participació en esdeveniments del sector (Barcelona Cyber Security Congress, esdeveniments de captació de Talent IT, Hackathons...).

Administrar el procés d'admissió dels alumnes mitjançant l'eina CRM proporcionada per la plataforma per gestionar *leads qualificats*, incloent-hi la revisió de sol·licituds, la revisió de documentació i la comunicació amb els candidats.

Gestionar la documentació necessària per a l'admissió dels alumnes i assegurar que estigui completa i correcta. Treballarà coordinadament amb el servei de Compliment legal i normatiu en aspectes formatius per garantir la qualitat del procés i informar els alumnes sobre els requisits d'admissió establerts per la Ciberacadèmia.

Proporcionar orientació inicial als alumnes sobre els programes formatius disponibles (propostes de nivells i itineraris), ajudant-los a triar la proposta personalitzada que millor s'ajusti a les seves necessitats i objectius.

Facilitar la comunicació entre els alumnes i els perfils gestors de la Ciberacadèmia per assegurar la correcta inscripció.

Realitzar un seguiment inicial dels alumnes admesos per assegurar que s'integren correctament al sistema d'aprenentatge.

Proporcionar suport continu als alumnes durant els primers passos dins el sistema per garantir una adaptació òptima.

- Servei d'assessorament acadèmic

Proporcionar suport acadèmic a docents i alumnes, resolent dubtes que sorgeixen dins les diferents unitats i problemes que puguin sorgir durant el desenvolupament dels cursos. Ajudar els alumnes a resoldre problemes acadèmics que puguin sorgir durant el curs, oferint solucions i recursos adequats.

Ajudar els alumnes a ajustar-se als programes formatius i itineraris, proposant canvis o adaptacions personalitzades si la formació escollida no s'ajusta a les seves necessitats; per garantir que els alumnes superin els obstacles i aprofitin al màxim la seva formació.

Realitzar una anàlisi personalitzada de les necessitats i objectius d'alumnes per recomanar les millors opcions de formació, durant el desenvolupament d'itineraris segons el progrés acadèmic.

Realitzar un seguiment del progrés dels alumnes, proporcionant feedback constructiu i suggerint millores per al seu rendiment acadèmic.

Utilitzar eines d'avaluació per monitoritzar el desenvolupament dels alumnes i identificar àrees de millora.

Orientar els alumnes sobre com seguir formant-se un cop acabin la formació actual, proporcionant consells sobre cursos addicionals i oportunitats de desenvolupament professional.

Informar sobre les certificacions professionals existents i cursos de nivell expert que s'ofereixen des d'entitats de ciberseguretat de referència de la xarxa europea, com les que es troben a la Cybersecurity Higher Education Database (CyberHEAD).

Proporcionar recursos i eines de ciberseguretat per ajudar els alumnes a assolir els seus objectius acadèmics i professionals. Facilitar l'accés a materials didàctics, eines de pràctica i laboratoris de testeig de pentesting o forensics. Encaminar diferents alumnes a participar d'iniciatives de laboratori que s'organitzin des de la Ciberacadèmia.

- Dinamització d'activitat acadèmica o gestor/a de comunitats d'aprenentatge

El *networking* i la col·laboració és clau per desenvolupar i mantenir relacions amb actors del sector de la ciberseguretat, incloent-hi empreses, institucions acadèmiques i organitzacions professionals.

Cercar i negociar acords de col·laboració i sinèrgies amb els diferents actors, assegurant que beneficiïn la Ciberacadèmia i els seus alumnes per l'intercanvi de coneixements i recursos.

Proporcionar suport als membres de la comunitat d'aprenentatge, facilitant l'accés a recursos i oportunitats de col·laboració: a bootcamps amb situacions reals de ciberseguretat, pràctiques en entorns de virtualització...

Connectar els alumnes amb experts de la ciberseguretat que ofereixin perspectives valuoses als alumnes.

Avaluar l'eficàcia dels acords i col·laboracions establerts mesurant el feedback dels participants per identificar punts de millora.

Desenvolupar i mantenir relacions amb entitats de ciberseguretat de referència de la xarxa europea, com les que es troben a CyberHEAD d'ENISA.

- Servei tecno-pedagògic

L'adaptació a les necessitats canviants del sector mereix una mirada tècnico-pedagògica per tal de:

Planificar, coordinar i supervisar el projecte pedagògic de la Ciberacadèmia, assegurant que els objectius formatius es compleixin.

Desenvolupar cronogrames detallats i assignar recursos per garantir l'execució puntual i eficient dels projectes.

Ajudar a implementar la metodologia de formació, que s'adapti a les necessitats dels alumnes per fer efectiva la tasca acadèmica.

Incorporar tecnologies educatives per millorar l'experiència d'aprenentatge i fomentar la participació activa dels estudiants.

Assegurar que els continguts formatius són adequats, actualitzats i compleixen les expectatives de les necessitats del sector de la ciberseguretat.

Col·laborar amb experts del sector per garantir la rellevància i l'actualització contínua dels materials didàctics.

Liderar el projecte pedagògic, amb els perfils requerits implicats que garanteixi una execució efectiva i assegurar una implementació coherent i integrada del projecte.

Proporcionar suport acadèmic als docents i alumnes, resolent dubtes i problemes que puguin sorgir durant el desenvolupament de les activitats formatives.

Organitzar sessions de tutories per ajudar els docents a millorar les habilitats pedagògiques.

Avaluar l'eficàcia del programa de la Ciberacadèmia conjuntament amb el servei d'anàlisi de dades educatives.

- Compliment legal i normatiu en aspectes formatius

És important el procés de documentació dels aspectes formatius per al compliment de qualitat com aspectes legals.

Verificar que els continguts formatius i les microcredencials expedides compleixin amb els estàndards de qualitat establerts per les entitats certificadores. Cal pensar en un manual de qualitat, procediments documentats i registres del sistema (definició de formats per documentar l'evidència de l'acompliment).

També hi ha un rol derivat d'auditories internes: per avaluar la conformitat amb requisits d'ISO 9001 o aplicació d'accions correctives i preventives. Mantenir un registre detallat de tota la documentació relacionada amb les tramitacions oficials, incloent sol·licituds, certificacions i informes d'avaluació.

Assegurar que el procés de tramitació de microcredencials compleixi amb les regulacions i normatives vigents, tant a nivell nacional com internacional.

Revisar i validar amb el responsable d'admissions l'experiència acreditada dels professionals que sol·liciten les microcredencials, assegurant que compleixin els requisits necessaris.

Coordinació amb les entitats certificadores que vulguin col·laborar per garantir que les microcredencials expedides siguin reconegudes i acceptades a nivell professional.

Gestionar i resoldre qualsevol conflicte o discrepància que pugui sorgir durant el procés de tramitació de microcredencials.

- Anàlisi de les dades de la Ciberacadèmia

Permet la descripció de com funciona l'execució i monitoratge del servei, que permeti accionar mecanismes de control de qualitat, traçabilitat, supervisió de terminis i indicadors clau de rendiment (KPIs).

És molt important l'especificació dels processos clau per a l'execució i monitoratge del servei, incloent-hi mecanismes de control de qualitat de la formació, traçabilitat de les tasques i sistemes de retroalimentació.

Ha de fer anàlisi de les principals dades d'ús dels alumnes, rendiment, estabilitat, incidències i propostes de millora que s'han de tenir en compte.

Ha d'elaborar informes periòdics, *dashboards* i gestionar eines o espais compartits que permetin un accés proper al temps real a la informació clau del servei per prendre decisió.

- Servei d'innovació educativa

S'ha de preveure un procés per definir accions per la millora contínua del sistema i poder identificar oportunitats de millora.

En aquest sentit, l'ecosistema formatiu en ciberseguretat emergeix i s'adapta a la flexibilitat essencial per adaptar-se a les evolucions constants. És precís avaluar contínuament la modalitat de programes en funció de la retroalimentació dels alumnes a qui s'adreça (àmbits de relació de l'Agència), les

tendències del mercat i les necessitats canviants, assegurant així una oferta formativa sempre alineada amb les expectatives i demandes del públic objectiu.

Ha de poder gestionar projectes innovadors en coordinació amb l'Oficina d'Innovació de l'Agència amb la finalitat de promoure la inclusió i l'èxit educatiu de les activitats, així com oferir alternatives viables a gestors i docents en col·laboració.

També ha de posar la Ciberacadèmia en relació amb altres partners que participen de programes innovadors. Per exemple, els projectes d'investigació i innovació que aporten recursos en matèria de ciberseguretat: com el projecte europeu CONCORDIA, REWIRE, AICYBER, o programes de l'ECCC Cybersecurity Skills Alliance (CSA) i Advanced Cybersecurity Training Programs.

- Servei de suport i manteniment

Els responsables de configuració de la plataforma han de verificar periòdicament el funcionament adequat de la plataforma. Les diferents incidències o problemes tècnics que detectin gestors, docents i alumnes hauran d'abordar-se immediatament per minimitzar les interrupcions en l'aprenentatge.

3.4.5 Característiques generals del servei

De tot el que s'ha exposat prèviament es pot observar com, es descriuen elements que caracteritzen el sistema de formació e-learning per a la Ciberacadèmia:

1. Alta disponibilitat per accés als itineraris i recursos per tots els usuaris: gestors, docents i alumnes participants.
2. Escalabilitat per gestionar un nombre creixent i canviant d'usuaris en diferents cursos i itineraris sense comprometre el rendiment.
3. Possibilitats d'integració i seguiment d'informació de contactes (*leads qualificats*) que provenguin de subscripció de campanyes de màrqueting, formularis de contacte o d'enquestes d'interès o pre-inscripció en microsites de tercers.
4. Gestió eficient de grans volums de dades dels alumnes que demanen admissió, podent gestionar sol·licituds d'inscripció, qualificacions, historial acadèmic i certificacions de cursos realitzats.
5. Gestió documental, àgil i entenedora per tots els usuaris, que conformi una biblioteca de continguts (des d'elements singulars presents a les diferents unitats i mòduls fins a recull de gravacions de vídeo-streaming de classes de professors experts en les matèries), amb opcions de descàrrega i visualització offline.
6. Que permeti l'actualització dels continguts amb regularitat i que mantingui la qualitat esperada. La Ciberacadèmia ha de garantir que tots els materials i recursos que ofereix siguin extremadament útils i pertinents per als seus usuaris. Amb un elevat nivell de rellevància i utilitat, actuals i pràctics.
7. Proporcionar adaptabilitat als àmbits de treball de l'Agència, proporcionant informació valuosa als usuaris que els ajudi a assolir els seus objectius acadèmics i professionals.
8. Fàcil integració amb altres plataformes educatives i eines d'aprenentatge. La integració i interoperabilitat LTI és clau per a poder garantir les col·laboracions públic-privades que la Ciberacadèmia pugui establir. Per això la disponibilitat i gestió d'APIs per facilitar-la amb altres sistemes i aplicacions.
9. Disponibilitat de suport tècnic 24/7 per resoldre problemes tècnics i consultes.
10. Sistemes de tutorials i ajuda en línia per a utilitzar el sistema de forma efectiva, tan gestors, alumnes com docents.

11. Sistema amb mesures de protecció i seguretat robustes per evitar pèrdues d'informació. En tractar-se d'un sistema que té com a eix de treball principal la capacitat en la ciberseguretat és un entorn molt exposat atès que pot convertir-se en una diana molt temptadora o laminerera per a ciberdelinqüents, ja que al darrer hi haurà dades personals d'experts i alumnes en ciberseguretat d'institucions rellevants.
12. Capacitat de realitzar còpies de seguretat de tot el sistema implementat (amb totes les components: dades d'usuaris, continguts, configuració de modelatge i itineraris, interoperabilitat amb altres plataformes...) i poder restaurar-se tot el sistema en un període breu de temps.
13. Compliment de les normatives de privacitat i protecció de dades d'una entitat que certifica ENS i complirà condicions de proveïdor d'entitats públiques NIS2.
14. Evolució de la millora del rendiment acadèmic de la Ciberacadèmia i de la satisfacció d'alumnes amb presentació de ratis indicatius de forma transparent.

El dimensionament pressupostari del projecte s'ha realitzat prenent com a referència un escenari inicial de 200 usuaris simultanis a la plataforma LMS. No obstant això, a fi de garantir la sostenibilitat i escalabilitat del servei en fases posteriors, es preveu que la plataforma hagi de poder donar servei fins a 500 usuaris simultanis sense necessitat de canvis estructurals. Aquestes xifres s'utilitzen com a valors orientatius per definir els requisits mínims d'escalabilitat, i els licitadors hauran de justificar la capacitat de les seves solucions i, si escau, proposar capacitats superiors. En el moment de l'inici del contracte, l'empresa adjudicatària haurà d'aportar una taula detallada amb el preu cost/alumne plataforma.

3.4.6 Propostes de millora organitzativa

Amb l'objectiu d'augmentar el nivell de maduresa i l'eficiència del servei en una fase operativa es sol·licita al licitant que aportï per la infraestructura en marxa quines seran les característiques òptimes de treball de l'equip de perfils dedicats al contracte.

En aquest sentit per passar del procés d'arrancada del sistema al procés de sistema en marxa la reconfiguració de rols i funcions és essencial i han d'estar descrits en les propostes com serà l'organització del servei en cada cas.

4. Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, entre les quals es podrien determinar a efectes enunciatius les següents:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

El licitador proposarà un equip de treball (descriuint-ne els perfils, dedicació i pla de treball) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

En cap cas hi podrà haver transferència del personal intern de l'Agència o dels seus clients.

Responsable de la coordinació del servei

L'adjudicatari disposarà d'una figura que assumirà les tasques de responsable de coordinació del servei. A aquest efecte, ha de assumir les següents responsabilitats:

1. Coordinar transversalment les dues àrees clau del projecte:
 - Continguts formatius i itineraris de capacició.
 - Infraestructura tecnològica i acadèmica, assegurant la disponibilitat, integració i operativitat dels sistemes requerits (LMS, SIS, LTI, SCORM, SSO i altres components tecnològics necessaris pel funcionament del servei.).
2. Vetllar conjuntament amb el responsable de l'Agència pel compliment dels objectius estratègics del projecte, especialment en allò relatiu a:
 - El foment de la cultura de la ciberseguretat.
 - La capacició de talent en els perfils més demandats del sector.
 - La millora contínua de les competències del capital humà.
3. Assegurar la correcta interlocució amb l'Agència, mantenint una comunicació fluïda, proactiva i orientada a la resolució de necessitats, incidències i millores.

4. Establir i supervisar el pla de treball conjunt, calendaritzant fites, controlant terminis, i garantint la qualitat i coherència dels lliurables.
5. Alinear els diferents equips proveïdors i subministradors (pedagògics, tecnològics, de continguts, de suport tècnic i acadèmic), promovent una gestió integrada i col·laborativa.
6. Supervisar la implantació i l'evolució de la plataforma, incloent les funcionalitats LMS/SIS, gestió de grups, calendarització, inscripcions, publicació oberta de cursos i seguiment acadèmic.
7. Controlar la qualitat dels continguts (alineament amb el marc de matèries, nivells i perfils) i assegurar-ne la seva actualització constant en coordinació amb els experts en ciberseguretat.
8. Vetllar per la seguretat i escalabilitat de la solució, garantint la integració amb els sistemes corporatius de l'Agència i la compatibilitat amb l'ecosistema Microsoft.
9. Redactar informes de seguiment i d'assoliment d'objectius, amb indicadors clau de rendiment i avaluació del progrés del projecte.

4.1 Detall de l'activitat de l'equip

L'empresa adjudicatària haurà de fer una planificació per fases, amb el detall del calendari en què es preveuen fer els lliuraments, en temps i forma, de totes les matèries i unitats descrites. Aquesta planificació haurà de preveure les fases d'execució on es relacionin els principals actors implicats, la resposta de conformitat que s'espera de l'Agència i la identificació de les tasques principals, que permetin fer seguiment del camí crític i les desviacions per al desenvolupament total del projecte.

Fase	Objectiu	Tasques principals
1. Diagnosi i planificació	Identificar necessitats i definir l'estratègia dels programes formatius	- Coordinació amb promotors - Anàlisi de necessitats - Definició d'itineraris i objectius - Disseny preliminar dels programes - Redacció de l'informe de diagnosi i del pla d'actuació formativa.
2. Disseny pedagògic i continguts	Desenvolupar el projecte formatiu, fer un modelatge que respongui a les diferents opcions d'itineraris formatius i elaborar els materials didàctics	- Redacció dels continguts dels diferents itineraris - Adaptació a diferents perfils d'usuari: N1, N2, N3, N4, rols específics dins de l'ecosistema digital. - Disseny d'activitats i recursos - Supervisió metodològica i pedagògica - Enfocament competencial alineat amb el marc DigComp i ECSF, si s'escau. - Revisió i acceptació de l'Agència.
3. Digitalització i integració	Convertir els continguts al format digital i integrar-los al LMS	- Conversió multimèdia - Integració a la plataforma LMS - Creació d'elements interactius - Tests de qualitat tècnica - Adaptació a LMS institucional.
4. Posada en marxa i dinamització	Llançar els cursos i donar suport actiu a alumnes i docents	- Acompanyament i suport - Dinamització pedagògica - Monitoratge i resolució de dubtes - Elaboració dels informes d'ús i participació

5. Seguiment i millora contínua	Avaluar els resultats i fer ajustes	- Avaluació de resultats - Recollida de feedback - Proposta de millores - Ajustos metodològics o de contingut - Elaboració de l'informe final d'avaluació i millores proposades.
--	-------------------------------------	--

S'espera del licitador que completi aquestes fases i doni detall de tasques associades als perfils que requereix per l'activitat.

4.2 Definició i perfils requerits de l'equip de treball

S'identifiquen i es defineixen els perfil requerits que es consideren en el contracte:

4.2.1 Perfils principals per la Ciberacadèmia

PERFIL	REQUISITS	FUNCIONS
Especialista d'integració de plataformes	Formació acadèmica: • Graduat/ada universitari/ària (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la implantació i gestió de plataformes tecnològiques de formació. • Experiència en la configuració i manteniment de sistemes d'autenticació (SSO) i protocols de seguretat com SAML, OAuth o OpenID Connect. • Experiència en la integració de continguts SCORM i gestió de materials formatius digitals dins d'entorns virtuals d'aprenentatge. • Experiència en la integració de sistemes educatius mitjançant estàndards d'interoperabilitat com LTI. • Experiència en la coordinació tècnica de projectes formatius amb múltiples agents implicats (pedagògics, tecnològics i administratius). Competències tècniques: • Coneixements avançats de plataformes LMS (Moodle, Canvas o	• Coordinar la integració de tots els components tecnològics i formatius de la solució per a la Ciberacadèmia, assegurant una implantació funcional, escalable i segura. • Garantir el correcte desplegament i funcionament del sistema LMS, així com la seva integració amb altres sistemes com el SIS, el SSO i les aplicacions externes mitjançant LTI. • Configurar i supervisar la publicació dels continguts formatius, assegurant la seva accessibilitat, compatibilitat (SCORM) i alineació amb els itineraris de capacitació establerts. • Coordinar-se amb els equips tècnics i pedagògics per a l'adequada estructuració dels itineraris formatius i la personalització dels plans d'estudi segons els perfils professionals objectiu. • Supervisar el funcionament dels processos d'autenticació i accés segur a la plataforma, configurant protocols com SAML, OAuth o OpenID Connect en entorns Microsoft. • Donar suport a la sincronització de dades acadèmiques i administratives entre el LMS i el SIS, incloent la gestió de qualificacions, inscripcions i seguiment acadèmic.

	similars) i sistemes de gestió acadèmica (SIS). • Coneixements de bases de dades i processos de sincronització de dades acadèmiques. • Coneixements de protocols de seguretat, gestió d'identitats i interoperabilitat de sistemes educatius. • Capacitat per interpretar documentació tècnica i manuals de configuració de sistemes. • Nivell C1 de català.	• Monitorar el correcte funcionament de la interoperabilitat entre plataformes educatives, assegurant la integració segura i eficaç de serveis externs mitjançant estàndards LTI. • Elaborar informes tècnics de seguiment, identificar possibles incidències i proposar millores contínues en la infraestructura tecnològica i el funcionament integrat de la solució
Coordinació d'activitat acadèmica	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la coordinació de programes de formació, preferiblement en el sector de la ciberseguretat. • Experiència en la gestió de projectes pedagògics, incloent-hi la planificació, organització i supervisió de cursos formatius. • Experiència en la supervisió de recursos formatius, assegurant la correcta implementació dels plans de formació. • Experiència en establir i mantenir relacions amb promotors d'activitats formatives, facilitant la col·laboració i l'intercanvi de coneixements. • Coneixements específics sobre ciberseguretat, amb experiència en la implementació de programes de formació en aquest àmbit. • Coneixements sobre l'ús de plataformes LMS, assegurant la	• Crear i implementar plans de formació específics per a cada programa, assegurant que compleixin els objectius acadèmics i de capacitat. • Gestionar els recursos formatius necessaris per a la implementació dels programes, incloent-hi materials didàctics, plataformes tecnològiques i personal docent. • Planificació del calendari d'activitats formatives. • Establir i mantenir relacions amb promotors d'activitats formatives, facilitant la col·laboració i l'intercanvi de coneixements. • Assignació de docents per poder impartir la formació. • Supervisar l'execució dels programes de formació, assegurant que es compleixin els estàndards de qualitat i eficàcia. • Avaluar l'eficàcia dels plans de formació i proposar millores contínues basades en els resultats obtinguts. • Seguiment de l'execució formativa i resolució d'incidències. • Proporcionar suport als professors i alumnes, resolent dubtes i problemes que puguin sorgir durant el desenvolupament dels cursos.

	correcta integració i gestió dels continguts digitals. Competències tècniques: • Nivell C1 de català.	
Especialista de continguts teòrics en ciberseguretat	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). • Es requereix formació tècnica específica en ciberseguretat, ja sigui a través d'estudis universitaris reglats (grau, màster) o bé mitjançant certificacions professionals reconegudes que acreditin el domini dels fonaments de la ciberseguretat, com ara: SANS Institute (ex. GSEC), ISACA (ex. CSX Fundamentals), Fortinet NSE (ex. NSE 3 o superior) o altres equivalents com CompTIA Security+, Cisco CCNA Security, CEH, entre d'altres certificacions reconegudes en l'àmbit de seguretat. Experiència professional: • Cal que acrediti una experiència mínima de tres (3) anys en la creació de continguts didàctics, preferentment en entorns digitals. • Experiència en el desenvolupament de materials formatius per a plataformes d'aprenentatge virtual (e-learning). Coneixements lingüístics: • Nivell C1 de català. • Coneixements d'anglès amb un nivell mínim B2 del Marc Comú Europeu de Referència (MCER). Es valorarà nivell C1 o superior. Competències tècniques: • Experiència demostrable amb sistemes de gestió de l'aprenentatge	• Crear materials didàctics teòrics definits en l'apartat de continguts pels cursos en línia, assegurant que siguin clars, concisos i pedagògicament efectius. • Organitzar els continguts de manera lògica i coherent, facilitant l'aprenentatge progressiu dels alumnes. • Adaptar els materials didàctics per a diferents nivells de dificultat i perfils d'alumnes, garantint que siguin accessibles per a tots. • Incorporar recursos addicionals, com ara exemples pràctics, exercicis i casos d'estudi, per enriquir els materials didàctics.

	(LMS), especialment Moodle, Chamilo o altres entorns equivalents.	
Digitalitzador de continguts	Formació acadèmica: • Graduat/ada universitari/a (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la conversió de materials didàctics en formats digitals, en la integració de continguts digitals en plataformes LMS i en assegurar la compatibilitat dels continguts amb diverses plataformes educatives i dispositius. Competències tècniques: • Coneixements avançats en tecnologies educatives i plataformes LMS. • Capacitat per convertir materials didàctics en formats digitals accessibles, com ara vídeos, presentacions interactives i documents PDF. • Habilitats en la implementació d'elements interactius, com ara qüestionaris, simulacions i activitats pràctiques. • Capacitat per realitzar el manteniment dels continguts digitals, resolent qualsevol problema tècnic que pugui sorgir. • Capacitat per treballar en equip i col·laborar amb altres membres del personal acadèmic.	• Convertir materials didàctics en formats digitals accessibles, com ara vídeos, presentacions interactives i documents PDF. • Volcar els continguts digitals a una plataforma LMS (Learning Management System), assegurant la seva correcta configuració i funcionament. • Assegurar la compatibilitat dels continguts amb diverses plataformes educatives i dispositius, garantint una experiència d'usuari òptima. • Implementar elements interactius, com ara qüestionaris, simulacions i activitats pràctiques, per millorar l'experiència d'aprenentatge. • Realitzar el manteniment dels continguts digitals per garantir el seu bon funcionament i actualització, resolent qualsevol problema tècnic que pugui sorgir. • Proporcionar suport tècnic als usuaris de la plataforma LMS, ajudant-los a navegar i utilitzar els continguts digitals de manera efectiva.
Especialista de configuració d'itineraris i mòduls	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència:	• Configurar i organitzar cursos, mòduls i itineraris formatius dins del LMS. • Parametritzar activitats (tasques, qüestionaris, laboratoris) i carregar continguts SCORM/xAPI.

	• Cal que acrediti una experiència mínima de tres (3) anys en la gestió de projectes pedagògics i desenvolupament de metodologies de formació • Experiència en l'adequació de continguts formatius a diferents programes d'actuació • Experiència en el sector de la ciberseguretat i en la gestió acadèmica. Competències tècniques: • Nivell C1 de català. • Coneixements avançats en tecnologies educatives i plataformes LMS • Capacitat per desenvolupar i implementar itineraris formatius adaptats a les necessitats dels alumnes. • Habilitats en l'ús d'eines digitals per a la creació i gestió de continguts formatius.	• Definir requisits de progressió i itineraris personalitzats per als alumnes. • Gestionar rols i permisos vinculats als itineraris i mòduls. • Donar suport a docents i gestors en l'ús i adaptació dels itineraris a la plataforma. • Monitoritzar l'execució dels itineraris i proposar millores de configuració i usabilitat.
Responsable de marketing	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en el disseny i execució d'estratègies de màrqueting digital. • Experiència en la creació, gestió i optimització de campanyes publicitàries en canals com Google Ads, xarxes socials i <i>email marketing</i>. • Experiència en la creació i manteniment de <i>landings</i> o <i>microsites</i>, especialment per a iniciatives educatives o de captació massiva.	• Dissenyar i implementar l'estratègia de màrqueting digital per donar visibilitat a l'oferta formativa de la Ciberacadèmia i captar nous participants. • Crear i gestionar campanyes de difusió a través de canals digitals (Google Ads, xarxes socials, newsletters i altres canals de promoció digital.) amb orientació a resultats i optimització de la conversió. • Coordinar la creació i actualització dels <i>microsites</i> i <i>landings</i> dels cursos, assegurant una presentació atractiva, funcional i alineada amb la identitat visual de la Ciberacadèmia. • Gestionar el catàleg de cursos en obert, assegurant-ne una navegació intuïtiva, la segmentació adequada i la disponibilitat multidioma.

	• Experiència en l'ús de plataformes d'automatització de màrqueting i eines d'anàlisi (com Google Analytics, Meta Ads Manager, Mailchimp o similars). • Es valorarà experiència en projectes de formació en línia i/o en entorns relacionats amb la ciberseguretat. Competències tècniques: • Nivell C1 de català. • Coneixements de posicionament SEO/SEM, disseny d'estratègies de conversió i experiència d'usuari (UX). • Capacitat per treballar amb eines de gestió de continguts (CMS) i coneixement bàsic de maquetació web (HTML/CSS) per adaptar continguts visuals i textuais. • Capacitat d'anàlisi de dades i elaboració d'informes orientats a resultats i presa de decisions. • Coneixement dels requisits d'accessibilitat digital i multilingüisme en entorns web.	• Supervisar el funcionament dels sistemes d'inscripció automàtica i validació d'usuari, garantint una experiència fluida i sense friccions per a les persones usuàries. Monitorar les dades d'inscripció, participació i rendiment de les campanyes, elaborant informes periòdics amb indicadors clau (KPI) per a l'anàlisi de resultats i presa de decisions. • Proposar millores contínues per incrementar la captació d'alumnes, ampliar l'impacte de la comunicació i afavorir el posicionament de la Ciberacadèmia com a referent en formació en ciberseguretat. • Col·laborar amb l'equip tècnic per garantir la compatibilitat de la plataforma amb les eines de màrqueting i el bon funcionament dels sistemes de traçabilitat i seguiment. • Vetllar pel compliment dels criteris d'accessibilitat digital i per la publicació dels continguts i formularis en les llengües establertes (català, castellà i anglès).
--	--	---

4.2.2 Altres perfils de funcionament de la Ciberacadèmia

Altres perfils que poden ser requerits en el contracte:

PERFIL	REQUISITS	FUNCIONS
Especialista en admissió	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Experiència mínima de dos (2) anys en la gestió de processos d'admissió acadèmica. • Experiència en l'ús de sistemes de gestió comercial (leads qualificats i	• Realitzar prospecció de mercat i la captació de nous alumnes. • Administrar el procés d'admissió dels alumnes mitjançant un CRM, incloent-hi la revisió de sol·licituds, la revisió de documentació i la comunicació amb els candidats. • Proporcionar orientació inicial als alumnes sobre els programes de formació disponibles, ajudant-los a triar el curs que millor s'ajusti a les seves necessitats i objectius.

	CRM) per administrar el procés d'admissió. - Experiència en la prospecció de mercat, captació de nous alumnes i eines de captació digital. Competències tècniques: - Nivell C1 de català.	- Assegurar que els alumnes compleixin els requisits d'admissió establerts per la Ciberacadèmia; gestionant la documentació necessària per a l'admissió dels alumnes i assegurant que estigui completa i correcta. - Ajudar els alumnes en el procés d'inscripció, resolent dubtes i problemes que puguin sorgir. - Realitzar un seguiment inicial dels alumnes admesos per assegurar que s'integrin correctament a la Ciberacadèmia.
Especialista en assessorament acadèmic	Formació acadèmica: - Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: - Cal que acrediti una experiència mínima de dos (2) anys en assessorament acadèmic o orientació educativa. - Experiència en proporcionar suport continu als alumnes durant la seva formació. - Experiència en la resolució de problemes acadèmics i planificació del desenvolupament formatiu. Competències tècniques: - Nivell C1 de català. - Coneixements d'anglès amb un nivell mínim B2 del Marc Comú Europeu de Referència (MCER). Es valorarà nivell C1 o superior. - Coneixements avançats en tècniques d'assessorament acadèmic i orientació educativa. Capacitat per ajudar els alumnes a ajustar-se als cursos i proposar canvis o adaptacions si la formació escollida no s'ajusta a les seves necessitats.	- Proporcionar suport acadèmic continu als alumnes durant la seva formació, ajudant-los a superar dificultats i a mantenir-se motivats. - Ajudar els alumnes a ajustar-se als cursos, proposant canvis o adaptacions si la formació escollida no s'ajusta a les seves necessitats. - Orientar els alumnes sobre com seguir formant-se un cop acabin la formació actual, proporcionant consells sobre cursos addicionals i oportunitats de desenvolupament professional. - Ajudar els alumnes a resoldre problemes acadèmics que puguin sorgir durant el curs, oferint solucions i recursos adequats. - Realitzar un seguiment del progrés dels alumnes, proporcionant feedback constructiu i suggerint millores per al seu rendiment acadèmic. Proporcionar recursos i eines per ajudar els alumnes a assolir els seus objectius acadèmics i professionals.
Dinamització d'activitat acadèmica o	Formació acadèmica:	Desenvolupar i mantenir relacions amb actors del sector de la ciberseguretat, incloent-hi empreses,

gestor/a de comunitats d'aprenentatge	• Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la gestió de projectes pedagògics i elaboració de metodologies de formació. • Experiència en entorns acadèmics o del sector de la capacitat professional en la ciberseguretat. • Experiència en establir i mantenir relacions amb empreses, institucions acadèmiques i organitzacions professionals. • Experiència en la cerca i negociació d'acords de col·laboració i sinèrgies. • Experiència en la gestió de continguts formatius, incloent-hi la capacitat per obtenir continguts de manera àgil a través de col·laboracions externes Competències tècniques: • Nivell C1 de català. • Coneixements d'anglès amb un nivell mínim B2 del Marc Comú Europeu de Referència (MCER). Es valorarà nivell C1 o superior. • Coneixements avançats en tecnologies educatives i plataformes LMS. • Capacitat per desenvolupar i implementar metodologies de formació adaptades a les necessitats dels alumnes. • Habilitat en la gestió de projectes i coordinació d'equips.	institucions acadèmiques i organitzacions professionals. • Cercar i negociar acords de col·laboració i sinèrgies amb els diferents actors, assegurant que beneficiïn la Ciberacadèmia i els seus alumnes. • Posar en pràctica els acords establerts, coordinant amb els diferents departaments de la Ciberacadèmia per assegurar una execució efectiva. • Fomentar la col·laboració entre la Ciberacadèmia i els actors del sector, facilitant l'intercanvi de coneixements i recursos. • Proporcionar suport als membres de la comunitat d'aprenentatge, facilitant l'accés a recursos i oportunitats de col·laboració. Avaluar l'eficàcia dels acords i col·laboracions establerts, proposant millores contínues per assegurar la seva rellevància i impacte positiu.
Especialista tecno-pedagoc	Formació acadèmica: • Graduat/ada universitari/a en graus tecnològics o de la pedagogia (anteriorment diplomatures o llicenciatures). Acreditació amb cursos d'especialització, post-graus o màsters el seu currículum en	• Planificar, coordinar i supervisar els projectes pedagògics, assegurant que es compleixin els objectius acadèmics i de formació. • Desenvolupar i implementar metodologies de formació efectives, adaptades a les necessitats dels

	metodologia pedagògica i l'ús de tecnologies de la informació i la comunicació. Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la gestió de projectes pedagògics i desenvolupament de metodologies de formació • Experiència en l'adequació de continguts formatius a diferents programes d'actuació • Experiència en el sector de la ciberseguretat i en la gestió acadèmica. Competències tècniques: • Nivell C1 de català. • Coneixements avançats en tecnologies educatives i plataformes LMS • Capacitat per desenvolupar i implementar itineraris formatius adaptats a les necessitats dels alumnes. • Habilitats en l'ús d'eines digitals per a la creació i gestió de continguts formatius.	alumnes i als objectius de la Ciberacadèmia. • Assegurar que els continguts formatius siguin adequats, actualitzats i alineats amb les últimes tendències i necessitats del sector de la ciberseguretat. • Liderar els projectes pedagògics, coordinant amb els diferents departaments i actors implicats per garantir una execució eficient i efectiva. • Proporcionar suport acadèmic als professors i alumnes, resolent dubtes i problemes que puguin sorgir durant el desenvolupament dels cursos. Avaluar l'eficàcia dels programes de formació i proposar millores contínues per assegurar la qualitat i rellevància dels cursos.
Expert en compliment legal i normatiu	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en l'anàlisi i aplicació de normatives educatives, de protecció de dades i de drets digitals. • Experiència en l'assessorament legal en projectes de transformació digital en l'àmbit educatiu o institucional. • Experiència en la revisió i adaptació de polítiques i procediments per garantir el compliment legal de	• Revisar les normatives educatives i de protecció de dades per assegurar que el sistema LMS compleixi amb tots els requisits legals. Adaptar les polítiques del LMS segons les actualitzacions legislatives vigents, especialment l'adaptació als requeriments de microcertificacions relatives als continguts de ciberseguretat implementades. • Realització d'auditories periòdiques per verificar el compliment normatiu del sistema. • Identificar i mitigar els riscos legals associats a l'ús del LMS. • Proporcionar assessorament legal als administradors, gestors i professors

	sistemes tecnològics, especialment entorns LMS. • Experiència en la realització d'auditories normatives o de compliment legal en entorns educatius o de l'administració pública. • Es valorarà coneixement sobre la normativa europea i estatal vinculada a microcredencials, reconeixement d'aprenentatges i certificacions en l'àmbit de la ciberseguretat. Competències tècniques: • Nivell C1 de català. • Coneixements actualitzats sobre el Reglament General de Protecció de Dades (RGPD), normativa de transparència, accés a la informació i drets digitals. • Capacitat per interpretar i aplicar normatives específiques a l'àmbit educatiu digital. • Habilitats per comunicar i formar sobre temes legals a professionals no especialistes (docents, gestors, administradors). • Capacitat per identificar riscos jurídics i proposar mesures correctores o preventives.	sobre les implicacions normatives de les activitats formatives. • Elaboració d'informes de compliment per mantenir informat al director sobre l'estat legal del sistema.
Analista de dades educatives d'alumnes	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en l'anàlisi de dades, preferiblement en l'àmbit educatiu o institucional. • Experiència en l'extracció i tractament de dades des de sistemes LMS i/o SIS, incloent dades de rendiment acadèmic, inscripcions i qualificacions. • Experiència en l'elaboració d'informes analítics i dashboards per a la presa	• Recopilació de dades acadèmiques i administratives generades pel sistema LMS, incloent-hi informació sobre el rendiment dels alumnes, inscripcions i qualificacions. • Anàlisi continuu de les dades per identificar tendències, patrons i anomalies que puguin influir en la qualitat de l'ensenyament. Utilitzar tècniques estadístiques i de machine learning per crear models predictius. • Elaboració d'informes detallats que incloguin conclusions i recomanacions basades en l'anàlisi de dades. Presentar aquests informes educatius i econòmics al gestor de l'Agència per

	de decisions estratègiques en entorns formatius. • Es valorarà experiència en l'aplicació de tècniques de <i>machine learning</i> o estadística avançada per a la generació de models predictius. • Es valorarà coneixement dels indicadors clau de qualitat educativa i sistemes de seguiment del progrés dels estudiants. Competències tècniques: • Nivell C1 de català. • Habilitats per a l'elaboració d'informes i <i>dashboards</i> interpretables per perfils no tècnics i presentació de resultats a perfils gestors. • Coneixements avançats en anàlisi estadística, mineria de dades i visualització (Excel, Power BI, Tableau, R, Python o similars). • Coneixements de sistemes LMS (Moodle, Canvas...) i bases de dades relacionades amb la gestió acadèmica. • Capacitat per identificar patrons, anomalies i tendències que impactin en l'eficàcia dels programes formatius.	l'ajuda en la presa de decisions estratègiques.
Especialista d'innovació educativa	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Cal que acrediti una experiència mínima de tres (3) anys en la recerca, desenvolupament i implementació de metodologies educatives innovadores. • Experiència en el disseny i aplicació de projectes d'innovació educativa, especialment en entorns virtuals d'aprenentatge. • Experiència en la formació i acompanyament de docents i equips tècnics en l'ús de tecnologies	• Investigació de noves metodologies i tecnologies educatives en l'àmbit de la ciberseguretat que puguin ser integrades al LMS per millorar l'experiència d'aprenentatge. • Desenvolupament de projectes innovadors coordinat amb l'Oficina d'Innovació de l'Agència amb la finalitat de promoure la inclusió i l'èxit educatiu de l'activitat que es desenvolupa. • Oferir formació contínua als gestors, professors i administradors sobre les eines i metodologies que poden aportar millores innovadores en el procés. Fomentarà la participació i alineament en projectes europeus i de la recerca educativa.

	educatives i enfocaments pedagògics innovadors. • Es valorarà experiència en iniciatives educatives vinculades a l'àmbit de la ciberseguretat, així com en la participació en projectes europeus o de recerca educativa. • Es valorarà experiència en col·laboració amb oficines o departaments d'innovació dins d'organitzacions educatives o institucions públiques. Competències tècniques: • Coneixements sobre metodologies actives d'aprenentatge (ABP, flipped classroom, gamificació, entre d'altres). • Coneixement de tendències i eines emergents en educació digital i la seva integració a plataformes LMS. • Capacitat per avaluar l'impacte pedagògic de les innovacions aplicades i proposar millores fonamentades en dades. • Habilitats per a la comunicació i la formació d'equips docents i gestors. • Nivell C1 de català. • Coneixements d'anglès amb un nivell mínim B2 del Marc Comú Europeu de Referència (MCER). Es valorarà nivell C1 o superior.	• Promoure l'avaluació de l'eficàcia de les innovacions implementades i fer ajustaments segons sigui necessari per assegurar una millora contínua del servei.
--	---	---

Els requisits per aquests perfils que poden ser requerits són orientatius.

4.3 Organització de l'equip

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips per tal de donar resposta a les necessitats expressades en aquest plec.

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat de l'equip que donen servei a l'Agència.

L'estimació d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec serà de l'ordre de **15.600 hores per tot el temps de contracte**. Dins d'aquestes hores, s'estima el següent nombre d'hores anuals pels perfils requerits:

Perfil	Hores anuals estimades
Responsable de la coordinació del servei	1.500 hores
Especialista d'integració de plataformes	1.700 hores
Especialista de configuració d'itineraris i mòduls	1.700 hores
Coordinació activitat acadèmica	3.000 hores
Especialista de continguts teòrics en ciberseguretat	3.840 hores
Digitalitzador de continguts	1.920 hores
Responsable de campanyes de màrketing	750 hores
Altres perfils	1.190 hores

Els requisits anteriors s'han d'entendre com a hores aproximades, podent els licitadors ampliar-los i millorar-los a les seves ofertes. Dins d'altres es recullen tots aquells serveis i perfils que el licitant consideri necessaris per a l'adaptació de l'LMS SaaS proposada a components de col·laboració que puguin necessitar la Ciberacadèmia.

Tots els perfils hauran d'estar a disposició quan es requereixi per part de l'administració i en funció de les necessitats i el moment d'execució del contracte.

5. Condicions d'execució del servei

5.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 8x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 9:00h a 18:00h.

A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

5.2 Localització física

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Gerència de l'Agència (d'on depèn la comunicació, cultura en ciberseguretat i ecosistema), podria arribar a prestar/executar fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència, Carrer de Salvador Espriu, 45-51 de l'Hospitalet de Llobregat.

Addicionalment, es contempla que, de manera puntual i justificada segons les necessitats del servei, alguns professionals de l'empresa adjudicatària puguin haver de desplaçar-se a instal·lacions de clients de l'Agència (com ara serveis públics de la Generalitat de la Generalitat, món local, hospitals, centres d'educació o universitats) ubicats en diferents punts del territori de Catalunya. Aquest desplaçaments es planificaran i es limitaran als estrictament necessari per garantir la qualitat i continuïtat del servei.

5.3 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte ho requereix, aquest aspecte es podrà concretar en aquest.

5.4 Control de rotació

L'estabilitat dels recursos del servei amb coneixement i compromís és molt important per a la correcta prestació del servei.

L'empresa adjudicatària del contracte podrà fer canvis en l'equip de treball durant l'execució del contracte, però ho haurà de notificar per escrit a l'Agència amb una antelació mínima de 14 dies naturals, justificant el canvi i informant del perfil i característiques de la persona que s'incorpora. L'Agència comprovarà que la persona a incorporar compleix amb les condicions curriculars del component de l'equip que substitueixi.

L'empresa assumirà la selecció de les persones de nova incorporació, la coexistència en el servei del personal sortint i l'entrant sense cost per l'Agència, assegurant el correcte traspàs de coneixement en els següents 15 dies i duent a terme els controls necessaris per garantir-lo entenent, per tant, la no facturació d'aquests dies d'adaptació i traspàs. Sens perjudici que si s'escau es puguin aplicar els ANS corresponents per rotació excessiva.

En cap cas la substitució de personal suposarà un cost addicional, havent-se de garantir que el servei no es vegi afectat per aquest canvi. Si l'objecte del contracte ho requereix, aquest aspecte es podrà concretar en el contracte.

5.5 Eines i equipament per a la prestació de serveis

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura...) per la prestació del servei seran proporcionades per l'Agència. L'empresa haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

Quan l'adjudicatari es trobi en les instal·lacions de l'Agència, proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.
- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina ni tampoc ordinadors portàtils amb el programari habitual de l'Agència.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Accés a Internet via GPRS, UMTS.

- Cap altre recurs no especificat explícitament.

En conseqüència, l'adjudicatari haurà de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran d'ús exclusiu pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'Agència decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.

L'adjudicatari es compromet a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

5.6 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Àrea d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació contínua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació que derivi d'acord amb les directrius del CIC4Cyber.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'Agència, havent de proporcionar una descripció detallada del coneixement que es disposi i es generi al servei ofert, i tenint, per part de l'organització, accés a aquest coneixement en qualsevol moment.

L'Agència tal com s'ha indicat aportarà referències i s'involucrarà en la revisió dels continguts previstos en les graelles de matèries i unitats perquè és un coneixement imbricat en la seva operativa. En aquest sentit, l'adjudicatària haurà de facilitar accés als mòduls i unitat als diferents serveis de l'Agència dedicats al talent en ciberseguretat per revisar i aportar les referències a metodologies i eines interactives que poden usar-se en el procés de formació (per exemple, per a preparar proves d'accés o examen en processos d'admissió de recursos humans de l'Agència).

5.7 Seguretat corporativa

Un cop adjudicat el contracte, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés als equips i mitjans tècnic emprats pel personal de l'adjudicatari a les oficines de l'Agència, sempre que aquest accés sigui necessari i justificat per l'exercici de les funcions pròpies del servei contractat. Qualsevol accés fora d'aquest àmbit funcional es considerarà excepcional i requerirà autorització prèvia per part de l'Agència, atenent criteris de seguretat, proporcionalitat i traçabilitat.
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics de l'Agència per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

A la finalització del contracte, l'adjudicatari del contracte quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

5.8 Control de gestió

L'empresa adjudicatària del contracte, i en especial el cap de servei, haurà de col·laborar amb el responsable de la planificació pressupostària i el control de gestió de l'Agència per tal:

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de *forecast*.
- Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes:
 - Fitxer mestre de persones.

- Fitxer mestre de projectes i activitats.
- Estimació de recursos per projecte.
- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, que podran dur-se a terme en qualsevol de les instal·lacions involucrades en la prestació del servei, seran realitzades per personal de l'Agència o per tercers designats.

Quan les auditories no requereixin la col·laboració activa del personal de l'adjudicatari, es podran dur a terme sense notificació prèvia, sempre que no interfereixin en el desenvolupament normal del servei ni en els recursos de l'adjudicatari. En cas contrari, és a dir, quan sigui necessària la seva col·laboració, l'Agència emetrà una notificació amb un mínim de dues setmanes d'antelació.

5.9 Documentació

L'Agència és el propietari de tota la documentació elaborada per l'adjudicatari referent al servei prestat per aquest i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en el present contracte

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporcioni per tal efecte

5.10 Formació

El personal de l'empresa adjudicatària del contracte realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

5.11 Contingència

L'empresa adjudicatària elaborarà un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat de l'empresa, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
 - El personal necessari de l'adjudicatari per realitzar el servei i
 - Personal de l'Agència, o de tercers parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.

Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de l'Agència durant l'existència de la causa que doni lloc a la contingència.

5.12 Metodologia, estàndards i lliurables

L'organització del treball i execució del servei s'haurà d'adequar a les metodologies, estàndards i lliurables establerts per l'Agència vigents en el moment de l'execució del servei objecte del contracte.

5.13 Seguretat

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

L'empresa ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

L'empresa adjudicatària ha de posar en coneixement de l'Agència, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

2 Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària del contracte donarà compliment com a encarregat de tractament del que estableix el Reglament General de Protecció de Dades.

2.5.1 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.

En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària del contracte haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir amb l'ENS durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'Agència podrà requerir a l'empresa adjudicatària del contracte el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'Agència. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc web d'aquesta Secretaria. Si escau, l'empresa adjudicatària del contracte haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

2.5.2 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte haurà de presentar compromís exprés d'adscripció al contracte dels mitjans personals que s'especifiquin als plecs, complint amb els requeriments definits de formació, i acreditar la disposició efectiva dels mateixos.

2.5.3 Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte haurà de garantir que disposa dels perfils amb la capacitat i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitat per al personal que designi l'Agència per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'Agència, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al *Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC)* del *Centro Criptológico Nacional* o bé complir amb els criteris que estableixi l'*Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías*

de la Información del Centro Criptológico Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

2.5.4 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte i l'Agència o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'Agència.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'Agència.
- L'empresa adjudicatària del contracte haurà de participar en els mecanismes de coordinació que estableixi l'Agència i seguir els procediments establerts per aquest fi, per a poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

2.5.5 Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència.

2.5.6 Incidents de seguretat

El POC haurà de notificar a l'Agència qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària del contracte haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'Agència.

En cas que sigui necessari, l'empresa adjudicatària del contracte haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'Agència per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

2.5.7 Accés a la informació

L'empresa adjudicatària del contracte haurà de garantir l'accés del personal autoritzat de l'Agència a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'Agència i l'empresa establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

5.14 Assegurament i control de la qualitat i la millora contínua

L'empresa ha de vetllar per l'excel·lència i millora contínua dels processos, components tècnics i serveis sota el seu abast.

Per tal de garantir que s'aborda la qualitat i la millora, l'adjudicatari haurà d'elaborar, mantenir i executar un "Pla de Qualitat i Millora Contínua" que inclogui, entre d'altres:

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

5.15 Seguiment del servei

Les empreses adjudicatària haurà de presentar informes de de seguiment mensuals del servei d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

L'informe de seguiment haurà de tenir, com a mínim:

- Un informe de gestió dels serveis desenvolupats per a cada, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als Acords de Nivell de Servei (ANS) de cada contracte.
- Un informe de dedicació del contracte a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi contracte, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació, etc.). Per cada millora implantada s'establirà, sempre que sigui possible, un indicador que s'afegirà a l'informe de gestió dels serveis. La periodicitat de l'informe de seguiment serà mensual, quant al seguiment de les activitats i la implantació de les millores. La presentació de les propostes de millora es farà amb la periodicitat indicada en cada contracte o el que es determini per part del responsable del contracte de l'Agència.

Per el seguiment del servei, l'empresa haurà de generar i lliurar la informació necessària (dades mètriques i altres elements) que permeti a l'Agència governar, controlar i gestionar els serveis prestats, tant de manera individual com transversal i global.

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar en tots els àmbits del servei, seran definits per l'Agència. L'Agència podrà sol·licitar, durant la vigència del contracte, ampliacions i canvis en el contingut, periodicitat, canals i format de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'empresa es compromet a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'empresa es compromet a proporcionar informació veraç i contrastada, i haurà de disposar dels mecanismes necessaris per garantir-ho. L'Agència podrà dur a terme les auditories que consideri necessàries per a la seva verificació, obligant-se l'empresa a participar-hi de manera activa i diligent sense cap cost afegit per a l'Agència.

L'Agència podrà sol·licitar informació de forma immediata i l'empresa hi donarà resposta ràpida fora de la planificació establerta.

5.16 Integració amb altres equips

L'adjudicatari del contracte haurà de portar a terme les activitats d'integració amb la resta d'equips operatius que conformen l'Agència, tant amb personal intern com amb personal d'altres empreses contractistes.

Aquesta integració s'haurà de portar a terme tant a nivell de la operativa diària (per garantir l'execució dels processos de la cadena de valor de l'Agència) com a nivell tàctic i operatiu.

Tot i això, els models de relació han de garantir els següents punts:

- Participació de l'adjudicatari en els processos que l'afectin.
- Compartició d'informació sobre fets puntuals (incidències, alertes i/o vulnerabilitats), ja sigui amb l'Agència com directament amb altres proveïdors.
- Compartició d'informació sobre fets agregats (tendències, patrons) i sobre afectacions col·lectives als diferents clients de l'Agència.
- Eliminació de les sitges organitzatives.
- Creació d'un fons comú de coneixement sobre la seguretat de la informació.
- Creació de bucles de retroalimentació que facilitin una resposta àgil davant de qualsevol nova situació en matèria de seguretat.

5.17 Compromís amb el talent femení

El febrer de l'any 2022 l'Agència va aprovar el [Pla estratègic de Dones en ciberseguretat de l'Agència de Ciberseguretat de Catalunya](#) a l'àmbit de Catalunya, el qual es troba alineat amb les directrius i estratègies impulsades pel Govern de la Generalitat de Catalunya, com ara el Pla Estratègic de Polítiques d'Igualtat de Gènere, l'Estratègia de Ciberseguretat de Catalunya i el Pla Dona TIC, que té com finalitat fomentar la igualtat de gènere en el sector de la ciberseguretat i, en conseqüència, incrementar el número de dones que es dediquen a la ciberseguretat.

La situació de talent femení en l'àmbit de la ciberseguretat evidencia que, segons dades disponibles dels cursos acadèmics 2023-24:

- només el 7,1% d'alumnes de Cicles formatius de grau superior o de cursos d'Especialització dedicats a la ciberseguretat dins la Formació Professional eren dones.
- només el 20,1% d'alumnes de màsters o post-graus dedicats a la ciberseguretat en les universitats eren dones.
- només el 17,8% de certificacions professionals en ciberseguretat van ser obtingudes per dones.
- només el 8% de beques d'estudis de ciberseguretat (FP o universitaris) han estat destinades a dones.

Aquesta situació resumeix una tendència globalment decreixent respecte altres cursos i entre els motius que provoquen aquesta baixa representació de la dona en el sector té a veure amb estereotips de gènere, la manca de models a seguir i la consciència de l'àmbit. A més cal afegir que les dones se senten menys inclinades a postular-se per a adoptar perfils professionals o rols amb major responsabilitat on intervé la ciberseguretat.

Per deixar palès aquest compromís i voluntat per impulsar iniciatives que permetin donar a conèixer i captar el talent femení, atenent a l'objecte de la contractació l'Agència preveu criteris per fomentar el talent femení i la seva presència en el camp de la ciberseguretat.

Per això, és important que la presència en els rols requerits per la Ciberacadèmia equilibri aquesta situació per a donar major referència també per a l'alumnat que sigui objectiu en les campanyes de difusió i captació. Les eines de màrqueting digital (Google Ads, xarxes socials, newsletters i altres canals digitals de promoció.) han de facilitar la representació de dones en ciberseguretat en la captació massiva d'usuaris i fer seguiment de la conversió tenint en compte el gènere dels participants.

La participació de la dona en la diversitat de perfils requerits per la Ciberadèmia ha de ser viable per a l'adjudicatari atès que són molts els nivells d'expertesa i capacitats que es demanen en aquest contracte: capacitats de coordinació de serveis, especialistes de gestió acadèmica i docència, dinamitzadors de col·lectius en ciberseguretat, compliment legal acadèmica, digitalització de continguts, aprovisionament de diversitats de camps de les matèries específiques dels continguts de ciberseguretat...

5.18 Compromís amb el talent i la inclusió

L'Estratègia de la Ciberseguretat de Catalunya 2019-2022, així com la proposta per a la nova Estratègia 2023-2027, reconeixen com un dels seus pilars la generació, captació i conservació de talent. I, es que, en un context d'escassetat de perfils especialitzats en el sector, l'Agència té la voluntat d'impulsar iniciatives que fomentin el desenvolupament de nous professionals de ciberseguretat. A la vegada, dites estratègies de ciberseguretat també preveuen com un dels objectius centrals de les polítiques públiques el coneixement i accés de la societat a la comunicació i tecnologies de la informació.

Doncs bé, atenent aquests dos elements l'Agència té el compromís de fomentar la inclusió de persones amb discapacitat dins dels seus programes de talent ja que aquest tipus de perfil aporta un doble valor en la seguretat de les xarxes: (i) permet resoldre conflictes i vulnerabilitats amb perspectives diverses i, per tant, més completa i (ii) assegura que l'objectiu "d'accés" de la ciutadania a les solucions de seguretat sigui total.

Per deixar palès aquest compromís i voluntat, l'Agència preveu en el present contracte criteris per fomentar la inclusió en la generació de talent i la seva presència en el camp de la ciberseguretat.

Existeixen programes que s'orienten a donar ocupació de persones amb discapacitat en sectors emergents. Avui dia diferents programes de formació amb atenció a col·lectius prioritaris com persones amb discapacitat s'han començat a enfocar a la ciberseguretat com a factor de capacició i inclusió laboral. Un exemple, la Fundació Prevent organitza el programa NIO amb HUB4T TecnoCampus.

La participació de persones amb discapacitat en la diversitat de perfils requerits per la Ciberadèmia ha ser viable per a l'adjudicatari atès que són molts els nivells d'expertesa, amb competències tècniques i transversals, que es demanen en aquest contracte.

