

Plec de prescripcions tècniques particulars que regeix la contractació del manteniment dels serveis de la CiberAcadèmia

Índex

1. Introducció	4
1.1 Estructura de la contractació	5
2. Descripció dels serveis objecte de la contractació.....	5
2.1 Objecte i abast dels serveis.....	6
2.1.1 Situació actual de la CiberAcadèmia i ecosistema tecnològic.....	7
2.1.2 Actuacions formatives específiques en l'àmbit de la salut	9
2.2 Serveis objecte del contracte i característiques.....	9
2.2.1 Servei d'admissions, captació i orientació de participants	10
2.2.2 Servei de gestió acadèmica i suport a l'alumnat.....	10
2.2.3 Servei de compliment legal, normatiu i de qualitat.....	10
2.2.4 Servei de suport i manteniment tècnic de les plataformes	11
2.2.5 Servei de manteniment pedagògic i actualització de continguts	11
2.2.5.1 La qualitat dels lliurables	11
2.2.5.2 Propostes de millora.....	12
2.2.6 Servei de digitalització de continguts formatius	13
2.2.7 Governança, transició i seguiment de la CiberAcadèmia.....	14
2.3 Equip de treball	15
2.3.1 Definició dels perfils de l'equip de treball.....	15
2.3.2 Organització de l'equip de treball	22
2.3.3 Perfils.....	22
3 Condicions d'execució del servei	29
3.1 Horaris	29
3.2 Localització física.	29
3.3 Canvi de recurs.....	29
3.4 Control de rotació.....	30
3.5 Eines i equipament per a la prestació de serveis.....	30
3.6 Gestió del coneixement.....	31
3.7 Seguretat Corporativa	31
3.8 Control de Gestió	32
3.9 Documentació.	33
3.10 Formació.....	33
3.11 Contingència	33
3.12 Metodologia, estàndards i lliurables	34
3.13 Seguretat	34
3.13.1 Deure de confidencialitat.....	34
3.13.2 Dades de caràcter personal	34

3.13.3	Compliment del marc legal de ciberseguretat i del marc normatiu intern	34
3.13.4	Capacitat tècnica.....	35
3.13.5	Adquisició de productes/eines i productes o serveis de seguretat.....	35
3.13.6	Interconnexions.....	35
3.13.7	Verificació del compliment i auditoria	36
3.13.8	Incidents de seguretat.....	36
3.13.9	Accés a la informació	36
3.14	Assegurament i control de la qualitat i la millora contínua	36
3.15	Seguiment del servei.....	37
3.16	Integració amb altres equips	38

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 de Ciberseguretat 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 de Ciberseguretat, cal destacar que, segons recull la Memòria de l'Agència de Ciberseguretat de Catalunya de 2025, l'entitat ha continuat tenint un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat, tant pel que fa a la Generalitat de Catalunya com en diferents entitats del territori català. Aquest àmbit d'actuació comporta un elevat nivell d'activitat operativa. Més concretament, durant l'any 2025 l'Agència va gestionar un total de 6.544 incidents únics de seguretat, gairebé el doble dels 3.372 incidents gestionats durant el 2024 i molt per sobre dels 2.670 incidents gestionats durant el 2023.

En aquest marc, i amb la voluntat d'impulsar la capacitació i el desenvolupament del talent en ciberseguretat, l'Agència va impulsar la construcció i posada en funcionament de la CiberAcadèmia, concebuda com un entorn integral de capacitació especialitzada en ciberseguretat. Aquest projecte ha permès definir i desenvolupar els itineraris i continguts formatius, així com configurar l'ecosistema tecnològic i les eines necessàries per donar suport a l'activitat formativa de la CiberAcadèmia.

A partir d'aquesta primera fase, resulta necessari garantir la continuïtat de la CiberAcadèmia mitjançant el manteniment, l'actualització i l'evolució dels seus diferents components pedagògics, acadèmics, operatius i tecnològics. En conseqüència, el present contracte té per objecte la prestació integral dels serveis necessaris per garantir-ne el correcte funcionament, incloent el manteniment pedagògic i l'actualització continuada dels continguts formatius, la digitalització i adaptació dels materials d'aprenentatge, la gestió acadèmica i el suport a l'alumnat, els processos d'admissió, captació i orientació de participants, el compliment legal, normatiu i de qualitat de les activitats formatives, l'anàlisi de dades i el monitoratge del rendiment del servei, així com el suport i

manteniment tècnic de les plataformes que donen servei a la CiberAcadèmia. Aquests serveis es presten de manera coordinada per garantir la qualitat pedagògica, la sostenibilitat operativa, la millora contínua i l'alineament de l'oferta formativa amb les necessitats del sector de la ciberseguretat.

1.1 Estructura de la contractació

El contracte té com a objectiu la contractació de serveis per al manteniment de la CiberAcadèmia de l'Agència de ciberseguretat de Catalunya.

2. Descripció dels serveis objecte de la contractació

L'objecte del contracte és garantir el manteniment operatiu, pedagògic, tecnològic i analític dels serveis de la CiberAcadèmia de l'Agència de Ciberseguretat de Catalunya, assegurant la creació i actualització continuada de continguts formatius, la gestió acadèmica, el suport a l'alumnat i docents, l'admissió i orientació de participants, el compliment normatiu i la disponibilitat tècnica de les plataformes formatives.

Aquesta iniciativa té com a finalitat impulsar la capacitat en matèria de ciberseguretat adreçada als professionals del sector —tant de l'àmbit privat com del públic—, incloent empreses proveïdores de serveis i solucions de ciberseguretat, operadors de serveis crítics i professionals que desenvolupen funcions especialitzades en aquest camp.

L'encàrrec respon a la necessitat d'abordar el dèficit de talent especialitzat, reforçar la competitivitat dels professionals i afavorir el desenvolupament continu de les seves competències mitjançant processos d'*upskilling* i *reskilling*:

- Upskilling: adquisició o actualització d'habilitats i coneixements per mantenir els professionals competius en el seu rol actual, adaptant-se a les evolucions tecnològiques o organitzatives del sector de la ciberseguretat.
- Reskilling: adquisició de noves capacitats que permetin als professionals pivotar cap a altres perfils o responsabilitats, en resposta a canvis en la demanda del mercat o en les necessitats de les organitzacions.

La CiberAcadèmia es configura com un espai que faci possible materialitzar col·laboracions público-privada, en el qual puguin participar professionals d'organismes públics, empreses i entitats sense ànim de lucre, amb l'objectiu d'enfortir les capacitats del sector i contribuir a la consolidació d'un ecosistema robust en matèria de ciberseguretat.

Els continguts formatius que es dissenyin i mantinguin en el marc del contracte s'alinearan amb les capacitats requerides pels 11 perfils del marc European Cybersecurity Skills Framework (ECSF) d'ENISA, garantint que la formació responen a les funcions professionals de referència i als estàndards europeus.

L'execució i manteniment dels serveis de la CiberAcadèmia es duran a terme a través dels perfils especialitzats descrits en aquest plec, incloent el tecnopedagog, els especialistes en assessorament acadèmic i admissions, l'expert en compliment normatiu i el tècnic de suport i plataformes, els quals asseguraran una operació integral del servei en totes les seves dimensions: pedagògica, tecnològica, acadèmica i de qualitat.

2.1 Objecte i abast dels serveis

L'objecte del present contracte és la prestació integral dels serveis de manteniment, actualització i operació de la CiberAcadèmia de l'Agència de Ciberseguretat de Catalunya, incloent-hi la creació i revisió continuada de continguts formatius, la digitalització dels continguts, la gestió acadèmica, l'admissió i orientació de participants, el compliment legal i normatiu de les activitats formatives, l'anàlisi de dades de rendiment i l'operació i manteniment tècnic de les plataformes que suporten el servei.

El servei té com a finalitat garantir que la CiberAcadèmia manté una oferta formativa actualitzada, alineada amb les necessitats del sector i operativament sostenible, tot contribuint a incrementar les competències dels professionals de la ciberseguretat a Catalunya i donar resposta al dèficit existent de talent especialitzat.

Així mateix, el contracte té per objecte assegurar la disponibilitat dels recursos pedagògics, tecnològics i operatius que permetin desplegar itineraris de upskilling i reskilling, d'acord amb els perfils professionals i funcions del *European Cybersecurity Skills Framework* (ECSF) d'ENISA.

L'abast del servei comprèn totes les activitats necessàries per garantir el funcionament continuat, la qualitat i la millora permanent de la CiberAcadèmia. Aquest abast inclou el manteniment pedagògic i l'actualització contínua dels continguts formatius, assegurant que aquests s'adeqüen metodològicament i tècnicament a les necessitats dels diferents itineraris i als perfils professionals definits en l'ECSF. També incorpora la supervisió de la coherència pedagògica dels materials, la revisió dels itineraris establerts i l'adaptació dels continguts en funció de l'evolució del sector.

El servei inclou igualment la gestió acadèmica i el suport a l'alumnat, amb l'acompanyament necessari perquè els participants puguin resoldre incidències o dificultats durant el transcurs de la formació, i amb la provisió d'orientació sobre els itineraris formatius més adients, així com sobre les oportunitats de desenvolupament professional que se'n deriven. Aquesta gestió comporta el seguiment del progrés acadèmic, la coordinació amb els docents i el suport continu als participants des de la seva incorporació fins a la finalització del programa formatiu.

Pel que fa al servei d'admissions, l'abast inclou la prospecció i captació de participants potencials, la gestió completa del procés d'admissió mitjançant eines CRM, la revisió de sol·licituds i documentació, la validació del compliment dels requisits d'accés i la comunicació amb els candidats durant tot el procés. El servei comprèn també la seva orientació prèvia a l'inici de la formació i el seguiment inicial de la seva integració dins la CiberAcadèmia.

Pel que fa al compliment legal i normatiu, el servei engloba totes les actuacions necessàries per garantir que els processos formatius de la CiberAcadèmia compleixen els estàndards de qualitat i les normatives vigents. Això inclou la revisió de procediments interns, el manteniment dels registres documentals, la verificació de la conformitat amb estàndards com la ISO 9001, la coordinació amb entitats certificadores i la gestió de possibles incidències o discrepàncies que puguin sorgir en la tramitació de microcredencials i altres acreditacions.

L'abast del servei inclou igualment les funcions d'anàlisi de dades i monitoratge del funcionament de la CiberAcadèmia. Aquestes tasques impliquen la recopilació, validació i explotació de les dades generades pel servei, la definició i seguiment d'indicadors clau de rendiment, l'elaboració d'informes periòdics i la generació de quadres de comandament que facilitin una presa de decisions informada.

Així mateix, comporta la supervisió de la traçabilitat de les activitats i la proposta de millores basades en l'anàlisi dels resultats obtinguts.

Finalment, el servei comprèn el suport i manteniment tècnic de les plataformes de la CiberAcadèmia, assegurant la seva disponibilitat i el correcte funcionament dels entorns digitals i de les eines col·laboratives. Això inclou la resolució d'incidències tècniques, la configuració de classes virtuals i espais de treball, la gestió de repositoris de continguts i la coordinació amb l'equip pedagògic i els docents per garantir que les necessitats tecnològiques del servei estan adequadament cobertes.

Actualment, el funcionament de la CiberAcadèmia es basa en un ecosistema tecnològic existent que inclou la plataforma Canvas com a sistema de gestió de l'aprenentatge (LMS), l'entorn Hack The Box (HTB) per al desenvolupament de laboratoris pràctics i activitats basades en reptes, Articulate 360 com a eina de creació i digitalització de continguts formatius, i Zoom per a la realització de sessions formatives síncrones, classes virtuals i activitats en directe, mitjançant l'extensió de la llicència corresponent.

L'adjudicatari haurà de garantir la compatibilitat operativa, la correcta integració i el suport dels serveis objecte del contracte dins d'aquest entorn tecnològic, sense perjudici de l'evolució futura de les eines, prèvia validació per part de l'Agència de Ciberseguretat de Catalunya.

2.1.1 Situació actual de la CiberAcadèmia i ecosistema tecnològic

La CiberAcadèmia de l'Agència de Ciberseguretat de Catalunya constitueix la iniciativa de referència de l'Agència orientada a la capacitació, especialització i desenvolupament del talent en ciberseguretat. Actualment, la CiberAcadèmia disposa d'una oferta formativa estructurada en nou itineraris formatius alineats amb els perfils professionals definits per l'European Cybersecurity Skills Framework (ECSF) d'ENISA.

Els itineraris actualment disponibles corresponen als perfils professionals d'auditor/a de ciberseguretat, cap de seguretat de la informació, consultor/a d'equips de resposta a incidents, educador/a de ciberseguretat, expert/a en ciberseguretat legal, expert/a en gestió de riscos, expert/a en implementació de ciberseguretat, investigador/a forense digital i professional de proves de penetració.

Els itineraris comparteixen continguts i competències comunes, fet que permet establir passarel·les i recorreguts de desenvolupament professional entre diferents perfils. Aquesta aproximació facilita tant processos d'upskilling com de reskilling dins del sector de la ciberseguretat.

L'activitat formativa es desenvolupa principalment sobre la plataforma Canvas LMS, que actua com a entorn central de gestió de l'aprenentatge i constitueix el punt únic d'accés a l'ecosistema tecnològic de la CiberAcadèmia. Sobre aquesta plataforma s'articulen la resta de sistemes i eines que donen suport a l'activitat formativa, acadèmica i administrativa mitjançant mecanismes d'integració estàndard, principalment basats en Learning Tools Interoperability (LTI) i sistemes d'autenticació unificada (SSO). Aquesta arquitectura permet oferir una experiència integrada a l'alumnat i al personal de gestió, facilitant l'accés als diferents recursos i entorns d'aprenentatge sense la necessitat de gestionar credencials o accessos independents per a cadascuna de les plataformes.

Cada itinerari es compon de diferents mòduls formatius que poden tenir un caràcter transversal o específic en funció del perfil professional objectiu. Els principals blocs de contingut actualment disponibles són fonaments de ciberseguretat, habilitats transversals (soft skills), estructura organitzativa, gestió d'identitats, protecció de la dada, seguretat en les aplicacions i operacions de ciberseguretat.

Com a requisit previ per a l'accés als itineraris formatius, les persones candidates han de superar una prova de nivell disponible dins de la mateixa plataforma Canvas, dissenyada en H5P. Aquesta prova, ajustada a cada perfil, té com a objectiu verificar que l'alumne disposa dels coneixements previs necessaris per seguir amb garanties l'itinerari formatiu seleccionat.

Tots els cursos segueixen una estructura pedagògica comuna. Cada itinerari incorpora un mòdul introductori de presentació del perfil professional i, posteriorment, els diferents mòduls formatius segueixen una seqüència homogènia formada per una presentació del mòdul, els objectius d'aprenentatge, els continguts a desenvolupar, un repte inicial, els continguts interactius elaborats amb l'eina Articulate 360, els laboratoris pràctics desplegats a la plataforma Hack The Box i un espai final de consolidació dels aprenentatges que inclou el resum del mòdul, la resolució del repte plantejat, els punts clau, les referències bibliogràfiques, el glossari de termes i l'avaluació final corresponent.

Els continguts digitals es gestionen mitjançant un model de reutilització basat en SCORM Proxy, que permet compartir objectes formatius comuns entre diferents itineraris i cursos. Aquest mecanisme facilita el manteniment dels continguts, ja que qualsevol actualització efectuada sobre un contingut compartit es propaga automàticament a tots els cursos que el referencien, evitant actualitzacions manuals duplicades, reduint el risc d'inconsistències i millorant l'eficiència operativa de la plataforma.

La component pràctica dels itineraris es desplega principalment mitjançant laboratoris a la plataforma Hack The Box, integrada amb l'entorn formatiu de Canvas LMS. Aquesta integració permet als participants accedir als laboratoris i activitats pràctiques utilitzant els mecanismes d'autenticació unificada existents, garantint una experiència contínua entre els continguts teòrics i els entorns pràctics d'aprenentatge.

Addicionalment, la CiberAcadèmia disposa d'eines de suport a la dinamització i seguiment de les activitats formatives. En aquest sentit, l'entorn incorpora la integració amb Zoom per a la realització de sessions síncrones, seminaris, tutoritzacions i altres activitats de formació en directe.

Per a la gestió administrativa i acadèmica dels participants, la CiberAcadèmia disposa del sistema d'informació de l'estudiant OpenSIS, que permet mantenir el registre dels alumnes, efectuar-ne el seguiment i consolidar l'històric de participació en els diferents programes formatius.

Un cop l'alumnat supera satisfactòriament totes les activitats i avaluacions requerides de l'itinerari corresponent, la plataforma genera el procediment necessari per a l'emissió del certificat acreditatiu per part de l'Agència de Ciberseguretat de Catalunya. Addicionalment, al final de cada itinerari es recull la valoració de l'alumnat mitjançant una enquesta de satisfacció.

Actualment, l'accés als cursos es promou principalment a través de la pàgina web pública de la CiberAcadèmia; <https://ciberseguretat.gencat.cat/ca/ciberacademia>. Tanmateix, es considera

necessari evolucionar els processos d'admissió, captació, orientació i selecció de participants per tal de disposar d'un model escalable que permeti gestionar de manera eficient l'increment progressiu del nombre de persones interessades en participar en els programes formatius.

Les plataformes Canvas LMS, Hack The Box i OpenSIS es presten sota un model Software as a Service (SaaS), essent responsabilitat de l'adjudicatari garantir el correcte suport funcional, operatiu i de gestió dels serveis associats a aquestes plataformes en coordinació amb l'Agència.

2.1.2 Actuacions formatives específiques en l'àmbit de la salut

En el marc dels serveis objecte del contracte, l'Agència podrà requerir la realització d'actuacions específiques de capacitació adreçades a professionals TIC de l'àmbit de la salut, especialment de centres hospitalaris i entitats sanitàries de Catalunya.

Aquestes actuacions es desenvoluparan mitjançant els itineraris formatius existents de la CiberAcadèmia corresponents als perfils de Professional de proves de penetració i Cap de seguretat de la informació, incloent tots els serveis associats previstos en aquest plec, tals com els processos d'admissió, la gestió acadèmica, l'assessorament i seguiment de l'alumnat, el manteniment de continguts, la digitalització de materials formatius i el suport i manteniment de les plataformes tecnològiques.

A aquests efectes, el contracte incorpora una partida econòmica variable destinada a donar cobertura a aquestes actuacions formatives específiques abans de finals de 2027. L'execució d'aquesta partida estarà condicionada a les necessitats efectives de capacitació que determini l'Agència durant la vigència del contracte, sense que això impliqui la incorporació de nous serveis ni la modificació de l'objecte contractual.

2.2 Serveis objecte del contracte i característiques

Els serveis objecte del present contracte es configuren com un conjunt integrat de prestacions orientades a garantir el funcionament eficient, la qualitat pedagògica, la sostenibilitat operativa i la millora contínua de la CiberAcadèmia de l'Agència de Ciberseguretat de Catalunya.

Es defineix un cicle formatiu complet el conjunt ordenat d'activitats formatives en ciberseguretat, agrupades en itineraris de cursos i adreçades a uns perfils acadèmics determinats, que es desenvolupen dins d'un període temporal concret a la plataforma formativa de la CiberAcadèmia.

El cicle inclou la planificació dels cursos, la configuració dels grups d'alumnes, la definició de les dates d'inici i finalització, les condicions d'inscripció i accés, el seguiment de la progressió, l'avaluació o validació de l'aprofitament i el tancament dels itineraris previstos.

Un cicle formatiu complet ha de garantir que cada participant pugui iniciar i acabar els cursos assignats dins del termini establert, i que l'organització pugui disposar d'evidències suficients sobre la participació, la finalització i, si escau, l'acreditació de l'aprenentatge assolit.

Els serveis que han de permetre completar un cicle formatiu s'estructuren són els següents:

2.2.1 Servei d'admissions, captació i orientació de participants

El servei d'admissions té com a objectiu garantir una gestió eficient, transparent i traçable del procés d'incorporació de participants a la CiberAcadèmia. L'adjudicatari serà responsable de dur a terme les tasques de prospecció i captació de perfils potencials alineats amb els objectius estratègics de la CiberAcadèmia, així com de gestionar de manera integral el procés d'admissió mitjançant eines CRM (actualment es fa amb el suport d'OpenSIS). Aquesta gestió inclou la recepció, revisió i validació de les sol·licituds, la verificació del compliment dels requisits d'accés establerts, la comunicació continuada amb els candidats al llarg de tot el procés, així com la configuració, manteniment i actualització dels formularis d'inscripció i admissió i dels mecanismes de recollida i tractament de la informació necessària per a la valoració de les candidatures, garantint-ne la traçabilitat, la qualitat de les dades recollides i la seva integració amb les eines de gestió utilitzades per la CiberAcadèmia.

Així mateix, el servei haurà de permetre gestionar adequadament els processos d'admissió en aquells casos en què la demanda de participació superi les places disponibles en els diferents itineraris formatius. A aquest efecte, l'adjudicatari haurà de donar suport a l'Agència en la definició, aplicació i seguiment dels mecanismes necessaris per prioritzar les candidatures, garantint la transparència, la traçabilitat i l'alineament dels participants seleccionats amb els objectius de capacitat de la CiberAcadèmia, tenint en consideració aspectes com el perfil professional, l'experiència acreditada, els objectius formatius, els resultats obtinguts en les proves d'accés i qualsevol altre criteri que l'Agència determini.

Igualment, l'adjudicatari proporcionarà l'orientació prèvia a l'inici de la formació i realitzarà el seguiment inicial de la correcta integració dels participants dins la CiberAcadèmia.

2.2.2 Servei de gestió acadèmica i suport a l'alumnat

L'adjudicatari proporcionarà un servei integral de gestió acadèmica orientat a garantir una experiència formativa de qualitat al llarg de tot el cicle de vida de l'alumnat dins la CiberAcadèmia.

Aquest servei inclourà el seguiment individualitzat del progrés acadèmic dels participants, així com la coordinació operativa amb el professorat i amb la resta d'agents implicats en el desenvolupament de les activitats formatives.

L'empresa adjudicatària serà responsable de la gestió de les incidències acadèmiques que es puguin produir i del suport continu als participants durant tota la seva trajectòria formativa, assegurant igualment una orientació acadèmica adequada sobre els itineraris formatius més ajustats al perfil i als objectius professionals de cada participant. A més, el servei comprendrà el suport en les fases d'incorporació i de finalització dels programes formatius, garantint una transició ordenada i coherent entre les diferents etapes del procés formatiu.

2.2.3 Servei de compliment legal, normatiu i de qualitat

L'adjudicatari haurà de garantir que totes les activitats formatives i els processos associats al funcionament de la CiberAcadèmia compleixen la normativa vigent i els estàndards de qualitat aplicables. Aquest servei comprendrà la revisió i el manteniment dels procediments interns vinculats als processos formatius, així com la gestió i actualització dels registres documentals necessaris.

L'adjudicatari haurà de verificar el compliment dels estàndards de qualitat que resultin d'aplicació, com ara la norma ISO 9001, i coordinar-se amb les entitats certificadores i els organismes competents corresponents. Així mateix, serà responsable de la gestió de les possibles incidències, no conformitats o discrepàncies que puguin sorgir en relació amb la tramitació de microcredencials, certificacions o altres tipus d'acreditacions.

2.2.4 Servei de suport i manteniment tècnic de les plataformes

L'adjudicatari garantirà el funcionament continu, segur i eficient de les plataformes tecnològiques que donen suport a la CiberAcadèmia. Aquest servei comprendrà el manteniment operatiu de les plataformes digitals i la supervisió de la seva disponibilitat, així com la resolució d'incidències tècniques i la prestació de suport de segon nivell. Igualment, l'adjudicatari serà responsable de la configuració i gestió de les aules virtuals, dels entorns de treball col·laboratiu i dels repositoris de continguts, i es coordinarà amb l'equip pedagògic i amb el professorat per assegurar que les necessitats tecnològiques del servei estan adequadament cobertes. El servei inclourà també el suport tècnic necessari per garantir el correcte desplegament de les activitats formatives en modalitat digital.

2.2.5 Servei de manteniment pedagògic i actualització de continguts

L'empresa adjudicatària haurà de prestar un servei continu de manteniment, revisió i actualització dels continguts formatius de la CiberAcadèmia, assegurant-ne la vigència tècnica, l'adequació metodològica i l'alineació amb les necessitats del sector de la ciberseguretat.

Aquest servei inclou la revisió periòdica dels continguts formatius existents amb l'objectiu d'adaptar-los a l'evolució de les tecnologies, de les amenaces, de la normativa aplicable i de les bones pràctiques del sector de la ciberseguretat. Així mateix, comprèn l'actualització i millora dels materials formatius d'acord amb els itineraris d'upskilling i reskilling definits, garantint en tot moment la coherència pedagògica entre els diferents mòduls, cursos i itineraris.

Els continguts hauran d'estar alineats amb els perfils professionals i les funcions establerts pel European Cybersecurity Skills Framework (ECSF) d'ENISA. El servei inclou igualment la proposta d'adaptacions o millores metodològiques derivades de l'avaluació dels resultats formatius i de l'anàlisi del feedback recollit tant de l'alumnat com del professorat.

2.2.5.1 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 dels continguts abans del seu lliurament, incloent-hi la revisió ortotipogràfica, de coherència interna i de qualitat tècnica.
- 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, newsletters, etc.) 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, etc.) per facilitar-ne la gestió, cerca i publicació.

2.2.5.2 Propostes de millora

L'empresa adjudicatària del contracte ha de tenir la capacitat d'usar eines de desenvolupament de capacitació que s'ajustin a la infraestructura disponible:

- 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. **eSBARD EDU (aktios:)** plataforma **PaaS de formació pràctica en ciberseguretat** adreçada a centres educatius i entitats, orientada a entrenar equips en tècniques d'atac i defensa mitjançant **laboratoris virtuals, simuladors de ciberatacs reals, reptes tipus CTF, exercicis Red Team i Blue Team**, entorns accessibles des de navegador i sense instal·lació local, amb possibilitat de desplegar laboratoris propis, reutilitzar-los, editar-los, adaptar els reptes per nivell o rol, monitorar l'activitat dels usuaris i col·laborar amb altres institucions. www.aktios.com/landing-esbardedu
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.

- Actualment hi ha un servei d'Azure Blob Storage que s'usa com servei d'emmagatzematge d'objectes (principalment vídeos de caràcter formatiu). El propi CANVAS compta amb un repositori de vídeos en l'entorn nadiu però com a còpia de seguretat s'usa el servei Blob Storage, i no està integrat al CANVAS per oferir funcions bàsiques de visualització de vídeos. Queda pendent la connexió amb un visualitzador, amb experiència similar a l'streaming de Youtube però amb vídeos interns, que integri els documents formatius multimèdia (per exemple, de sessions de Zoom realitzades) per a la seva revisió.

2.2.6 Servei de digitalització de continguts formatius

L'adjudicatària proporcionarà un servei de digitalització de continguts orientat a garantir que els materials formatius de la CiberAcadèmia siguin adequadament adaptats, estructurats i disponibles en formats digitals per al seu consum en entorns d'aprenentatge en línia.

Aquest servei inclourà la transformació i adaptació de continguts teòrics i materials existents, facilitats per l'Agència o generats per altres serveis del contracte, en recursos digitals multimèdia i interactius,

adequats a l'autoaprenentatge i coherents amb els itineraris i mòduls formatius definits assegurant-ne la correcta visualització, navegabilitat, usabilitat i funcionament tècnic, així com la seva compatibilitat amb les eines d'autoria i les plataformes formatives utilitzades per la CiberAcadèmia.

L'empresa adjudicatària serà responsable de la preparació, estructuració i integració dels continguts digitalitzats dins la plataforma formativa de la CiberAcadèmia, assegurant-ne la correcta visualització, navegabilitat, usabilitat i funcionament tècnic. Així mateix, el servei comprendrà el suport en la incorporació d'activitats, qüestionaris i altres elements d'avaluació associats als continguts.

El servei de digitalització es prestarà de manera coordinada amb el servei de manteniment pedagògic i actualització de continguts i amb el suport i manteniment de plataformes, amb l'objectiu de garantir la coherència pedagògica dels materials, la seva adequació als diferents nivells formatius i el compliment de criteris bàsics d'accessibilitat i qualitat dels recursos digitals.

2.2.7 Governança, transició i seguiment de la CiberAcadèmia

Amb l'objectiu de garantir la continuïtat dels serveis de la CiberAcadèmia, l'adjudicatari haurà de dur a terme les activitats necessàries de governança, transició i seguiment dels serveis objecte del contracte.

Aquest servei comprendrà la presa de coneixement del funcionament actual de la CiberAcadèmia, dels continguts formatius disponibles, de les plataformes tecnològiques, dels procediments operatius existents i de la documentació associada al servei.

Així mateix, l'adjudicatari haurà de definir i mantenir els mecanismes de governança i seguiment necessaris per garantir la qualitat del servei, monitorar-ne l'execució, identificar incidències, riscos i oportunitats de millora, i proposar les actuacions necessàries per assegurar el correcte funcionament, manteniment i millora contínua de la CiberAcadèmia. En el marc d'aquestes funcions, l'adjudicatari haurà de recopilar, validar, analitzar i explotar les dades generades pels diferents serveis, processos i plataformes de la CiberAcadèmia, definir i fer el seguiment dels indicadors clau de rendiment (KPI), elaborar informes periòdics i mantenir quadres de comandament que permetin disposar d'una visió integrada de l'estat dels serveis, de l'activitat formativa i dels resultats assolits. A partir de l'anàlisi de les dades obtingudes, l'adjudicatari haurà de formular recomanacions i propostes de millora orientades a l'optimització contínua dels serveis, processos, continguts i plataformes.

En el marc d'aquest servei, l'adjudicatari haurà de lliurar com a mínim els productes següents:

- a) Pla de transició i presa de coneixement del servei, incloent l'inventari dels itineraris formatius, continguts, plataformes, integracions, processos acadèmics, procediments d'admissió, mecanismes de certificació, sistemes de qualitat i documentació associada al servei, en el termini màxim d'un mes des de l'inici del contracte.
- b) Posada en funcionament ordinària dels serveis objecte del contracte, incloent els serveis de manteniment pedagògic, digitalització de continguts, admissions, gestió acadèmica, suport a l'alumnat, compliment normatiu, qualitat i manteniment de plataformes, en el termini màxim de dos mesos des de l'inici del contracte.

c) Primer informe integral de seguiment del servei, incloent indicadors d'activitat i rendiment dels processos d'admissió, participació, seguiment acadèmic, taxa de finalització, estat dels continguts formatius, incidències acadèmiques i tècniques, ús de les plataformes, compliment dels requisits de qualitat i propostes de millora, en el termini màxim de tres mesos des de l'inici del contracte. Posteriorment, l'adjudicatari haurà d'elaborar un informe equivalent per cada cicle formatiu complet executat durant la vigència del contracte.

d) Pla d'actualització i millora continuada de la CiberAcadèmia, incloent propostes de manteniment i actualització dels continguts, millora dels processos d'admissió i orientació acadèmica, optimització dels indicadors de seguiment, adequació dels itineraris formatius, millora de l'experiència de l'alumnat i optimització de les plataformes tecnològiques que donen suport al servei, en el termini màxim de quatre mesos des de l'inici del contracte.

2.3 Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte basat 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.

L'adjudicatari proposarà un equip de treball (descriuint-ne els perfils, dedicació, pla de treball, etc.) 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.

No es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus clients.

2.3.1 Definició dels perfils de l'equip de treball

Per donar resposta a les necessitats descrites per a la realització dels serveis descrits anteriorment, l'Agència de ciberseguretat de Catalunya sol·licita perfils concrets.

2.3.1.1 Coordinador del servei

L'adjudicatari haurà de disposar d'una figura responsable de coordinació del servei, que actuarà com a interlocutor principal amb l'Agència i serà responsable de la direcció operativa i la correcta execució del contracte.

Haurà de planificar el calendari global del cicle, coordinar els equips implicats, garantir l'execució dels serveis en termini i qualitat, fer seguiment dels indicadors del servei, elevar riscos i incidències a l'Agència i assegurar el tancament ordenat del cicle amb els informes de resultats, lliurables i propostes de millora.

A aquest efecte, assumirà les funcions següents:

1. Coordinar transversalment totes les àrees del servei, assegurant la coherència entre els àmbits pedagògic, acadèmic, tecnològic, analític i de qualitat.
2. Planificar, supervisar i fer el seguiment de l'execució dels serveis, garantint el compliment de fites, terminis i nivells de qualitat.
3. Actuar com a interlocutor únic amb l'Agència, gestionant la comunicació, les incidències, les necessitats i les propostes de millora.
4. Coordinar els equips i perfils adscrits al contracte, assegurant una gestió integrada i eficient dels recursos.
5. Supervisar el funcionament dels serveis i de les plataformes tecnològiques, garantint la seva disponibilitat, estabilitat i evolució.
6. Vetllar per la qualitat dels continguts, dels processos formatius i del servei en el seu conjunt, així com pel compliment normatiu aplicable.
7. Definir i fer el seguiment dels indicadors clau de rendiment (KPI) del servei, assegurant la recopilació, validació i explotació de les dades necessàries per avaluar l'activitat, el rendiment dels serveis i l'assoliment dels objectius de la CiberAcadèmia.
8. Elaborar i mantenir actualitzats els informes de seguiment i els quadres de comandament del cicle formatiu en procés, incloent indicadors de rendiment, dades d'activitat, estat dels serveis, incidències, riscos i propostes de millora.
9. Impulsar la millora contínua del servei mitjançant l'anàlisi dels resultats, indicadors i feedback dels usuaris, formulant recomanacions orientades a l'optimització dels continguts, els processos, les plataformes i els serveis de la CiberAcadèmia.

2.3.1.2 Tecnopedagog

Expert en gestió en projectes pedagògics, que aporta metodologia de formació i que adequa els continguts desenvolupats al projecte pedagògic de la CiberAcadèmia per a incloure els interessos dels diferents usuaris a la modulació i itineraris més adequats per assolir l'objectiu de capacitat professional.

Haurà de dissenyar i revisar l'arquitectura pedagògica dels itineraris, validar la coherència entre objectius, activitats, avaluacions i competències, adaptar els continguts als diferents perfils i nivells, orientar el professorat en l'ús de metodologies actives i proposar millores a partir del retorn de l'alumnat i dels resultats d'aprenentatge.

Comptarà d'una contrastada experiència en el sector de la ciberseguretat i en la gestió acadèmica.

2.3.1.3 Digitalitzador/a de continguts

Professional especialitzat en la transformació i adaptació de continguts formatius a formats digitals, responsable de garantir que els materials de la CiberAcadèmia siguin accessibles, interactius i adequats al consum en entorns d'aprenentatge en línia.

Adapta i digitalitza continguts teòrics i materials existents proporcionats per l'Agència o generats per altres perfils del contracte, integrant-los correctament als mòduls i itineraris formatius de la plataforma. Dona suport en la creació de recursos multimèdia, activitats, qüestionaris i materials d'avaluació, en coordinació amb el servei de tecnopedagogia.

Transforma els materials formatius en recursos digitals interactius, assegurar-ne la correcta estructura, navegació, accessibilitat i compatibilitat amb Canvas LMS, Articulate, H5P, SCORM o altres estàndards aplicables, incorporar activitats i qüestionaris, verificar el funcionament tècnic dels recursos i preparar les versions definitives per a la publicació, treballant de manera coordinada amb el tècnic de suport i manteniment de plataformes.

Comptarà amb experiència en digitalització de continguts formatius per a entorns d'e-learning i en l'ús d'eines de creació i gestió de continguts digitals, preferentment en entorns tecnològics o formatius.

2.3.1.4 Tècnic/a admissions

Especialista en processos d'admissió i captació de talent formatiu, responsable de gestionar de manera integral el procés d'incorporació de participants a la CiberAcadèmia i de garantir que els itineraris formatius arribin als perfils professionals més adequats d'acord amb els objectius estratègics de l'Agència. Contribueix al projecte pedagògic assegurant que els candidats accedeixin als itineraris més alineats amb el seu nivell de coneixements, experiència prèvia i objectius professionals.

S'encarrega de la prospecció i captació de potencials participants dins dels àmbits de relació de l'Agència, i col·labora en la definició i execució d'accions de promoció i captació de talent, incloent-hi la participació en esdeveniments, iniciatives de difusió i activitats sectorials relacionades amb la ciberseguretat i el talent digital.

Gestiona de forma integral el procés d'admissió mitjançant les eines de gestió habilitades per la CiberAcadèmia, actualment OpenSIS i els sistemes associats. Entre les seves funcions s'inclouen la configuració, manteniment i actualització dels formularis d'inscripció i admissió, la revisió i validació de les sol·licituds i de la documentació aportada, la verificació del compliment dels requisits d'accés, la gestió de les proves de nivell, la valoració de candidatures i la comunicació continuada amb els candidats durant tot el procés.

Treballa coordinadament amb el servei de compliment legal i normatiu i amb els equips de gestió acadèmica per garantir la traçabilitat, transparència i qualitat del procés d'admissió, vetllant pel correcte tractament de la informació i el compliment dels requisits establerts per la CiberAcadèmia.

Quan la demanda de participació superi les places disponibles, dona suport a l'Agència en l'aplicació dels criteris de selecció i prioritització establerts, tenint en consideració aspectes com el perfil professional, els objectius formatius, l'experiència acreditada, els resultats de les proves d'accés i qualsevol altre criteri determinat per l'Agència.

Proporciona orientació inicial als candidats sobre els diferents itineraris formatius disponibles, els perfils professionals associats al European Cybersecurity Skills Framework (ECSF) i les possibles trajectòries d'especialització, ajudant-los a identificar els recorreguts formatius més adequats al seu perfil i objectius professionals.

Realitza el seguiment inicial dels participants admesos per assegurar-ne la correcta incorporació als entorns digitals de la CiberAcadèmia, facilitant la seva integració en les plataformes, els processos acadèmics i les metodologies d'aprenentatge utilitzades.

Comptarà amb experiència contrastada en gestió de processos d'admissió, captació de talent formatiu, orientació acadèmica i relació amb candidats, preferentment en l'àmbit tecnològic o de la ciberseguretat, així com en l'ús d'eines CRM, sistemes d'informació acadèmica i plataformes de gestió de l'aprenentatge.

2.3.1.5 Especialista en assessorament acadèmic

Especialista en suport acadèmic i orientació formativa, responsable de garantir l'acompanyament i seguiment dels participants al llarg de tot el seu recorregut dins la CiberAcadèmia, des de la seva incorporació fins a la finalització dels itineraris formatius i acreditació del curs. Contribueix al projecte pedagògic oferint assessorament expert, resolució d'incidències acadèmiques, orientació personalitzada i suport continuat a l'alumnat per afavorir el progrés i la consecució dels objectius formatius i professionals associats als diferents perfils de la CiberAcadèmia.

Dóna suport acadèmic continu als participants, orienta els participants abans i durant el cicle, resolent dubtes relacionats amb els continguts formatius, l'estructura dels itineraris que millor s'adapta al seu perfil i objectius professionals, les activitats d'avaluació i l'ús de les eines d'aprenentatge. Realitza el seguiment del progrés acadèmic de l'alumnat mitjançant les funcionalitats disponibles a Canvas LMS, identificant possibles dificultats de continuïtat de l'aprenentatge, situacions de baixa participació o risc d'abandonament, i proposant les actuacions de suport que corresponguin.

Acompanya l'alumnat en la selecció i adaptació dels itineraris formatius, proporcionant orientació sobre els diferents perfils professionals de l'ECSF i les possibles trajectòries d'especialització, upskilling o reskilling disponibles dins la CiberAcadèmia.

Facilita l'accés als recursos formatius, continguts digitals, laboratoris pràctics de Hack The Box i altres activitats d'aprenentatge, donant suport als participants en la utilització dels diferents entorns tecnològics que conformen la CiberAcadèmia. coordinant-se amb docents i suport tècnic.

Participa en activitats de dinamització de la comunitat d'aprenentatge, incloent-hi sessions informatives, seminaris, tutories grupals, webinars i altres activitats síncrones desenvolupades a través de les eines habilitades per la CiberAcadèmia, contribuint a fomentar la participació i el compromís dels participants.

Treballa de forma coordinada amb els equips de tecnopedagogia, admissions i suport de plataformes per garantir una experiència formativa coherent, personalitzada i alineada amb els objectius de capacitat de la CiberAcadèmia.

Comptarà amb experiència contrastada en orientació acadèmica, seguiment educatiu i suport a l'alumnat, preferentment en entorns de formació en línia i plataformes LMS, així com en la utilització d'eines de videoconferència, comunicació i dinamització d'activitats formatives.

2.3.1.6 Tècnic en compliment legal i normatiu

Professional expert en qualitat, documentació i normativa formativa, responsable de garantir que tots els processos educatius, continguts i microcredencials de la CiberAcadèmia compleixin els estàndards de qualitat i les regulacions aplicables. Aporta rigor metodològic i assegura la traçabilitat documental, contribuint al posicionament de la CiberAcadèmia com a referent de confiança en l'àmbit de la formació en ciberseguretat.

Vetlla perquè el cicle compleixi la normativa aplicable, els requisits de qualitat i els procediments interns, revisa la documentació vinculada a admissions, certificació i protecció de dades, i mantén els registres necessaris.

Verifica que els continguts formatius i les microcredencials compleixin els requisits establerts per les entitats certificadores, definint i mantenint manuals de qualitat, procediments documentats i formats per recollir evidències de l'acompliment. Supervisa i actualitza el sistema de qualitat en coordinació amb els responsables pedagògics.

Participa en processos d'auditoria interna per avaluar la conformitat amb ISO 9001, així com en la implementació d'accions correctives i preventives. Manté un registre exhaustiu de tota la documentació relacionada amb sol·licituds, certificacions i informes d'avaluació.

Assegura el compliment de les regulacions vigents en la tramitació de microcredencials a nivell nacional i internacional, i valida, conjuntament amb el responsable d'admissions, l'experiència acreditada dels professionals que les sol·liciten.

Coordina la relació amb entitats certificadores externes per garantir el reconeixement i la validesa professional de les microcredencials expedides. Gestiona i resol conflictes o discrepàncies que puguin sorgir durant el procés, assegurant un tractament transparent i diligent.

Comptarà amb una expertesa sòlida en sistemes de qualitat, normatives formatives i gestió documental, preferiblement en entorns certificats i vinculats a l'àmbit tecnològic o universitari.

2.3.1.7 Tècnic de suport i manteniment de plataformes i eines col·laboratives

Professional especialitzat en l'administració, configuració, integració i suport funcional de les plataformes digitals que conformen l'ecosistema tecnològic de la CiberAcadèmia, responsable de garantir la continuïtat del servei, la disponibilitat dels entorns d'aprenentatge i el correcte funcionament de les eines utilitzades per alumnes, docents i equips de gestió.

Supervisa de forma continuada l'estabilitat, disponibilitat i rendiment de les diferents plataformes que formen part de la CiberAcadèmia, incloent-hi Canvas LMS, Hack The Box, OpenSIS, Zoom i la resta d'eines integrades. Intervé davant incidències tècniques o funcionals reportades pels usuaris, coordinant-ne la resolució i minimitzant-ne l'impacte sobre l'activitat formativa.

És responsable de configurar i mantenir els espais del cicle formatiu a Canvas LMS, OpenSIS, Hack The Box, Zoom i altres eines integrades, gestionar altes, accessos, rols i permisos, donar suport de segon nivell a incidències tècniques, supervisar la disponibilitat dels entorns, prepara aules virtuals i repositoris, verificar integracions LTI o Single Sign-On (SSO) i es coordina amb l'equip pedagògic per garantir la continuïtat operativa.

Vetllarà perquè els alumnes puguin accedir als diferents recursos i entorns d'aprenentatge de forma integrada i sense interrupcions.

Dóna suport a la gestió dels continguts digitals i a les eines emprades per al seu desplegament, incloent-hi Articulate, H5P, paquets SCORM i els mecanismes de reutilització de continguts basats en SCORM Proxy. Així mateix, col·labora amb els equips pedagògics i de digitalització per garantir que els materials formatius es publiquen i actualitzen correctament dins de l'ecosistema tecnològic existent.

Proporciona suport tècnic i funcional als equips de gestió, al professorat i a l'alumnat en l'ús de les diferents eines de la CiberAcadèmia, incloent-hi la configuració de sessions síncrones, webinars i activitats virtuals mitjançant Zoom, així com el seguiment de les incidències associades als laboratoris pràctics de Hack The Box.

Treballa coordinadament amb els equips de tecnopedagogia, gestió acadèmica, admissions i anàlisi de dades per garantir que la infraestructura tecnològica dona resposta a les necessitats operatives i acadèmiques de la CiberAcadèmia.

Comptarà amb experiència contrastada en administració de plataformes LMS, gestió d'integracions entre sistemes, suport a entorns d'aprenentatge digital i administració de serveis SaaS. Es valorarà

especialment experiència en Canvas LMS, Hack The Box, OpenSIS, Zoom, estàndards LTI, mecanismes SSO, gestió de continguts SCORM i eines de creació de continguts digitals com Articulate i H5P.

Matriu RACI de rols i responsabilitats dels perfils descrits

Perfil -> Activitat del cicle formatiu complet	1. Coord. del servei	2. Tecno- pedagog	3. Digitalit. continguts	4. Tècnic/a d'admissions	5. Especialista en asses. acadèmic	6. Tècnic en compliment legal i normatiu	7. Tècnic de suport de manteniment de plataf. i eines col·lab.
Planificació del calendari, abast i recursos del cicle	A/R	C	C	C	C	C	C
Disseny pedagògic dels itineraris, mòduls i activitats	A	R	C	I	C	C	C/R
Actualització i manteniment pedagògic dels continguts	A	R	C	I	C	C	C
Digitalització, integració i prova tècnica dels recursos formatius	A	C	R	I	I	C	C/R
Configuració dels cursos, grups, rols, accessos i entorns digitals	A	C	C	C	C	I	R
Captació, admissió i selecció de participants	A	I	I	R	C	C	C
Orientació inicial i assignació d'itineraris formatius	A	C	I	C	R	I	I
Seguiment acadèmic, suport a l'alumnat i gestió de consultes	A	C	I	I	R	I	C
Suport tècnic, incidències de plataforma i continuïtat operativa	A	I	C	I	C	I	R
Compliment legal, qualitat, protecció de dades i evidències d'auditoria	A	C	C	C	C	R	C
Avaluació, certificació, microcredencials i tancament acadèmic	A	C	I	C	R	C/R	C
Informes de resultats, indicadors, lliurables i propostes de millora	A/R	C	I	C	C	C	C

Llegenda RACI: R = responsable d'executar l'activitat, A = responsable últim de garantir-ne el resultat i validar-ne el lliurament, C = perfil consultat o que aporta criteri expert, I = perfil informat del progrés o del resultat de l'activitat.

2.3.2 Organització de l'equip de treball

L'adjudicatari haurà 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 aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **5.859 hores** estimades per a l'execució dels serveis durant la vigència inicial del contracte. Dins d'aquestes hores, s'estima el següent número d'hores pels perfils indicats:

Perfil	Hores estimades
Coordinador/a del servei	1.290
Tecno-pedagog/a	1.148
Digitalitzador/a de continguts	321
Tècnic/a admissions	458
Especialista assessorament acadèmic	1.254
Especialista en compliment legal i normatiu	117
Especialista suport de manteniment de plataformes i eines col·laboratives	1.271

Els requisits anteriors s'han d'entendre com hores estimades per desenvolupar els serveis, i l'adjudicatari haurà d'oferir preu unitari per perfil a la seva oferta.

2.3.3 Perfils

Els requeriments mínims dels perfils professionals que poden compondre l'equip són els següents:

PERFIL	REQUISITS	FUNCIONS
Coordinador del servei	Formació acadèmica: • Titulació universitària (grau, llicenciatura o equivalent), preferentment en àmbits tecnològics, educatius, de gestió o similars. Experiència professional: • Experiència mínima de cinc (5) anys en coordinació o gestió de serveis o projectes complexos.	• Coordinar transversalment totes les àrees del servei, assegurant la coherència i integració dels àmbits pedagògic, acadèmic, tecnològic, analític i de qualitat. • Exercir com a interlocutor principal amb l'Agència, gestionant la comunicació, les incidències, les necessitats i les propostes de millora del servei. • Planificar, supervisar i fer el seguiment de l'execució del servei, garantint el

	• Es valorarà experiència en projectes vinculats a l'elearning, formació digital o ciberseguretat. Competències tècniques: • Nivell C1 de català. • Capacitat de planificació, seguiment i control de serveis. • Coneixement de metodologies de gestió de projectes i serveis (planificació, control de terminis, gestió de riscos). • Coneixement d'entorns tecnològics de formació (LMS i eines associades).	compliment de fites, terminis i nivells de qualitat establerts. • Coordinar i alinear els equips i perfils adscrits al contracte, assegurant una gestió eficient dels recursos i una correcta distribució de tasques. • Supervisar el funcionament dels serveis i de les plataformes tecnològiques, garantint la seva disponibilitat, estabilitat i adequació a les necessitats del servei. • Vetllar per la qualitat dels continguts, dels processos formatius i del servei en el seu conjunt, així com pel compliment dels requisits normatius aplicables. • Definir, mantenir i fer el seguiment dels indicadors clau de rendiment (KPI) del servei, garantint la disponibilitat d'informació fiable per a l'avaluació dels resultats i la presa de decisions. • Coordinar la recopilació, validació, anàlisi i explotació de les dades generades pels diferents serveis, processos i plataformes de la CiberAcadèmia, assegurant-ne la traçabilitat i qualitat. • Elaborar i mantenir actualitzats els quadres de comandament i mecanismes de monitoratge necessaris per proporcionar una visió integrada de l'activitat, el rendiment i l'evolució de la CiberAcadèmia. • Impulsar la millora contínua del servei mitjançant l'anàlisi de resultats, incidències, indicadors i feedback dels usuaris, formulant propostes de millora basades en evidències. • Elaborar i presentar informes periòdics de seguiment del servei, incloent l'estat d'execució, indicadors de rendiment, dades d'activitat, incidències, riscos i propostes de millora. • Coordinar la gestió del coneixement i la documentació associada al servei,
--	---	--

		garantint-ne l'actualització i disponibilitat per a l'Agència.
Tecno- pedagog/a	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • 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 i necessitats. • Experiència en el sector de la ciberseguretat i en la gestió acadèmica. • Experiència en supervisió i coordinació d'accions formatives i recursos docents. Competències tècniques: • Nivell C1 de català. • Coneixements 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.	• Planificar, coordinar i supervisar projectes pedagògics alineats amb els objectius de la CiberAcadèmia. • Desenvolupar i implementar metodologies de formació efectives. • Dissenyar, adaptar i desenvolupar continguts formatius, assegurant-ne la qualitat, actualització i alineació amb les tendències del sector de la ciberseguretat i amb els itineraris formatius definits. • Definir l'estructura pedagògica dels continguts, incloent la conceptualització de mòduls, unitats didàctiques, activitats i recursos d'aprenentatge. • Coordinar amb altres equips l'execució pedagògica i metodològica dels programes, així com la generació i evolució dels continguts. • Donar suport acadèmic a docents i alumnes durant el desenvolupament dels cursos. • Avaluar l'eficàcia dels programes de formació i dels continguts, i proposar millores contínues. • Supervisar la integració de continguts en plataformes LMS i garantir-ne la coherència pedagògica i funcional.
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	• Produir, transformar i adaptar els continguts formatius definits pel servei de tecnopedagogia a formats digitals, multimèdia i interactius per al seu consum en entorns d'aprenentatge en línia. • Volcar els continguts digitals a la plataforma LMS (Learning Management System), assegurant la seva correcta configuració i funcionament.

	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.	• 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 Tècnic/a en admissions	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència professional: • 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 CRM). • Experiència en prospecció de mercat i captació de nous alumnes. • Experiència en eines i estratègies de captació digital, esdeveniments i accions sectorials. Competències tècniques:	• Realitzar prospecció de mercat i accions de captació de nous alumnes. • Administrar el procés d'admissió mitjançant el CRM, incloent revisió de sol·licituds i documentació. • Comunicar-se amb candidats durant totes les etapes del procés d'admissió. • Configurar, mantenir i actualitzar els formularis d'inscripció i admissió, així com els mecanismes de recollida de la informació necessària per a la valoració de les candidatures. • Proporcionar orientació inicial sobre els programes formatius i itineraris disponibles. • Validar que els candidats compleixin els requisits d'admissió. • Ajudar en els processos d'inscripció i resolució de dubtes.

	• Coneixements en eines CRM i sistemes d'admissió acadèmica. • Capacitat de comunicació amb candidats, gestió de documentació i validació de requisits. • Competències per orientar l'alumnat sobre programes formatius i itineraris.	• Realitzar un seguiment inicial de l'alumnat admès per assegurar una integració adequada al sistema de formació. • Participar en esdeveniments de captació, fires i activitats sectorials de promoció de la CiberAcadèmia.
Especialista en assessorament acadèmic	Formació acadèmica: • Graduat/ada universitari/a (anteriorment diplomatures o llicenciatures). Experiència: • 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 resolució de problemes acadèmics i orientació durant el desenvolupament formatiu. • Es valorarà experiència en entorns d'aprenentatge en línia (e-learning) i en plataformes LMS. Competències tècniques: • Nivell C1 de català. • Coneixements avançats en tècniques d'assessorament acadèmic i orientació educativa. • Capacitat per proposar adaptacions o canvis en els itineraris segons les necessitats de l'alumnat. • Coneixements funcionals de plataformes LMS, preferentment Canvas LMS, per al seguiment acadèmic, monitoratge del progrés dels participants i gestió de les activitats formatives. • Coneixements en eines de videoconferència i dinamització d'activitats formatives en línia,	• Proporcionar suport acadèmic continu als alumnes durant el seu procés formatiu. • Ajudar els alumnes a ajustar-se als itineraris formatius i proposar adaptacions quan calgui. • Oferir orientació sobre formació posterior, itineraris professionals i oportunitats de desenvolupament en l'àmbit de la ciberseguretat. • Resoldre incidències i problemes acadèmics que sorgeixin durant el curs, oferint recursos i mecanismes de suport adequats. • Realitzar el seguiment del progrés acadèmic dels participants mitjançant les eines disponibles a la plataforma LMS. • Identificar alumnes amb dificultats d'aprenentatge, baixa participació o risc d'abandonament i proposar actuacions de suport específiques. • Facilitar eines i recursos per assolir els objectius acadèmics i professionals definits pels participants. • Donar suport a les activitats de dinamització de la comunitat d'aprenentatge, incloent-hi sessions informatives, tutories grupals, webinars i activitats síncrones desenvolupades a través de les eines habilitades per la CiberAcadèmia. • Coordinar-se amb els perfils de tecnopedagogia, admissions i suport de plataformes per garantir una experiència formativa coherent durant tot el cicle de vida de l'alumnat.

	preferentment Zoom o eines equivalents. • Capacitat per interpretar indicadors acadèmics i identificar situacions de risc d'abandonament o dificultats en l'aprenentatge.	
Especialista en compliment legal i normatiu en aspectes formatius	Formació acadèmica: • Graduat/ada universitari/ (anteriorment diplomatures o llicenciatures). Experiència: • Experiència mínima de tres (3) anys en gestió de qualitat, documentació i compliment normatiu en entorns formatius o certificadors. • Experiència en auditories internes, revisió de procediments i gestió de registres documentals. • Experiència en tramitació, validació i verificació de credencials formatives o certificacions professionals. Competències tècniques: • Nivell C1 de català. • Coneixement de sistemes de qualitat (ISO 9001 o equivalents). • Capacitat de gestió documental i seguiment de processos formatius. • Competències en relació amb entitats certificadores.	• Verificar el compliment dels estàndards de qualitat en continguts i microcredencials. • Mantenir manuals de qualitat, procediments, formats i registres. • Participar en auditories internes i aplicar accions correctives i preventives. • Assegurar el compliment normatiu en la tramitació de microcredencials. • Revisar i validar l'experiència acreditada dels sol·licitants de microcredencials. • Coordinar-se amb entitats certificadores externes. • Gestionar conflictes o discrepàncies durant els processos de certificació.
Especialista de suport i manteniment de plataformes i eines col·laboratives	Formació acadèmica: • Graduat/ada universitari/a o formació professional de l'àmbit tecnològic, preferentment en informàtica, sistemes, telecomunicacions o disciplines afins. Experiència: • Experiència mínima de dos (2) anys en administració, configuració o suport de plataformes de formació en	• Supervisar el funcionament, estabilitat i disponibilitat de les plataformes que conformen l'ecosistema de la CiberAcadèmia. • Resoldre incidències tècniques i funcionals reportades per gestors, docents i alumnes. • Configurar, mantenir i administrar els espais formatius i les diferents eines que integren l'ecosistema tecnològic de la CiberAcadèmia.

	línia o entorns digitals d'aprenentatge • Experiència en gestió d'incidències tècniques i suport a usuaris en entorns formatius. • Experiència en configuració i manteniment d'integracions entre plataformes mitjançant estàndards d'interoperabilitat o mecanismes d'autenticació. • Experiència en administració de serveis SaaS i plataformes cloud. • Es valorarà especialment experiència en entorns Canvas LMS, Hack The Box, OpenSIS, Zoom o eines equivalents. Competències tècniques: • Coneixements en administració de plataformes LMS i sistemes de gestió acadèmica. • Coneixements en integracions basades en Learning Tools Interoperability (LTI), xAPI i mecanismes d'autenticació unificada (SSO). • Coneixements en gestió i publicació de continguts digitals mitjançant estàndards SCORM. • Coneixements en eines de creació i manteniment de continguts digitals com Articulate 360, H5P o equivalents. • Coneixements en plataformes de videoconferència ZOOM i col·laboració digital. • Capacitat d'anàlisi i resolució d'incidències tècniques i funcionals.	• Gestionar i donar suport a les integracions existents entre Canvas LMS, Hack The Box, OpenSIS, Zoom i la resta de plataformes utilitzades. • Administrar els mecanismes d'autenticació i accés, incloent-hi els serveis d'Single Sign-On (SSO) i les integracions basades en LTI i APIs. • Donar suport a la publicació, manteniment i actualització dels continguts digitals, incloent-hi la gestió de paquets SCORM i dels mecanismes de reutilització de continguts basats en SCORM Proxy. • Configurar i donar suport a sessions síncrones en ZOOM, webinars i activitats virtuals. • Coordinar-se amb els perfils de tecnopedagogia, digitalització de continguts, assessorament acadèmic i admissions per garantir la correcta operació de les plataformes. • Mantenir actualitzats els entorns tecnològics i proposar millores orientades a garantir la disponibilitat, usabilitat i qualitat del servei.
--	---	---

S'entén que aquests perfils es corresponen amb els rols identificats per l'Agència per a la prestació dels diferents serveis previstos. L'empresa adjudicatària haurà d'organitzar el desplegament i la coordinació de l'equip respectant, en tot cas, els perfils, requisits i dedicacions estimades establerts en aquest plec.

3 Condicions d'execució del servei

3.1 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.

3.2 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 Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

Adicionalment, s'ha de contemplar la possibilitat que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

3.3 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.

3.4 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.

3.5 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'adjudicatari 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, els adjudicataris hauran 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 Seguretat Corporativa de l'Àrea de Tecnologia i Organització 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.
- Els adjudicataris es comprometen 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.

En el cas de les eines formatives i de gestió de l'aprenentatge, l'adjudicatari haurà d'utilitzar i donar suport a les plataformes i eines definides per l'Agència com a entorn tecnològic de referència del servei, adaptant-se a la seva evolució durant la vigència del contracte, sense que això suposi cap cost addicional.

3.6 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions 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 continua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'organització, 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.

3.7 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 per Seguretat Corporativa de l'Àrea de Tecnologia i Organització 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 en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix Seguretat Corporativa de l'Àrea de Tecnologia i Organització 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 del servei de Mitjans Tècnics 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.

3.8 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, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació.

3.9 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris 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 plec.

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

3.10 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.

3.11 Contingència

Els adjudicataris hauran de proveir 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'adjudicatari, 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 terceres 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.

3.12 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.

3.13 Seguretat

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

3.13.1 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, o el que s'especifiqui en el contracte, 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.

3.13.2 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.

3.13.3 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 de Ciberseguretat 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 de Ciberseguretat. 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.

3.13.4 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.

L'empresa adjudicatària del contracte ha de garantir que tot el personal sigui conscienciat, rebi formació i informació sobre els seus deures, obligacions i responsabilitats en matèria de seguretat derivats de la legislació, del marc normatiu intern i dels procediments i directrius aplicables, recordant les possibles mesures disciplinàries aplicables i el seu deure de confidencialitat respecte a la informació a la que tingui accés.

3.13.5 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 de Ciberseguretat 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 Centre Criptològic 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 Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

3.13.6 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.

3.13.7 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 de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.13.8 Incidents de seguretat

El POC haurà de notificar a l'Agència de Ciberseguretat 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 de Ciberseguretat.

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 de Ciberseguretat per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

3.13.9 Accés a la informació

L'empresa adjudicatària del contracte haurà de garantir l'accés del personal autoritzat de l'Agència de Ciberseguretat 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 de Ciberseguretat i l'empresa establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

3.14 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.

3.15 Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment de cada contracte 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 de Ciberseguretat.

Pel control i seguiment del servei s'utilitzaran dades, mètriques i informes (en endavant informació) que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, el mecanisme de seguiment i avaluació del servei. Aquesta informació es pot fer extensible a altres Unitats, Àrees, Direccions de l'Agència o tractar-se d'anàlisi puntual.

L'empresa adjudicatària del contracte és la responsable de generar i lliurar la informació que es determini en els diferents àmbits del servei, la qual ha de permetre a l'Agència governar, controlar i gestionar els serveis prestats objecte del contracte, tant des d'una òptica 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.

3.16 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, vulnerabilitats, etc.), 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.