AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Salvador Espriu, 45-51
S08908 L'Hospitalet de Llobregat
Tel. 93 557 42 40

Plec de Prescripcions Tècniques

Contractació dels serveis per al Projecte de desenvolupament, disseny i construcció de la Ciberacadèmia ("CAC") per a l'Agència de Ciberseguretat de Catalunya

—Exped.: COS.02.2022—

1. Introducció

1.1 L'Agència de Ciberseguretat de Catalunya

L'Agència de Ciberseguretat de Catalunya (l'Agència, en endavant) és una entitat de dret públic de l'Administració de la Generalitat de Catalunya que actua amb plena autonomia orgànica i funcional, objectivitat i independència tècnica i professional, i resta adscrita al Departament de la Vicepresidència i de Polítiques Digitals i Territori de la Generalitat de Catalunya.

L'Agència actua en compliment de la Llei 15/2017 de 25 de juliol de 2017, de l'Agencia de Ciberseguretat de Catalunya.

Aquest marc legislatiu estableix l'Agència de Ciberseguretat de Catalunya com a entitat encarregada d'executar i de governar les polítiques públiques i l'estratègia en matèria de Ciberseguretat de la Generalitat de Catalunya, sent l'organisme que governa la Ciberseguretat del sector públic a Catalunya.

L'Agència com a encarregada d'establir i de liderar el servei públic de Ciberseguretat, té com a objectiu garantir una Societat de la Informació segura i confiable 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.

Com a organisme competent en matèria de Ciberseguretat, l'Agència es responsabilitza de l'establiment i el seguiment dels programes d'actuació en matèria de Ciberseguretat, 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.

Així mateix, en les funcions que li són pròpies, l'Agència és l'ens idoni per gestionar les tasques necessàries per assolir aquest objectiu de protecció de la informació i la infraestructura TIC de les institucions i ciutadania de Catalunya i, en especial la del Govern de la Generalitat.

Sens perjudici de l'anterior, és important destacar que l'activitat de l'Agència no se circumscriu només a l'àmbit de l'Administració pública. L'Agència treballa també amb el teixit empresarial català per construir un ecosistema segur a Catalunya per combatre les ciberamenaces.

Finalment, l'Agència està implicada amb tots els organismes pertinents per aconseguir que la ciberseguretat esdevingui un sector econòmic fort a Catalunya durant els propers anys, i perquè cada vegada hi hagi més professionals qualificats en aquest sector a casa nostra.

1.1.1 Objectius estratègics:

L'Agència de Ciberseguretat de Catalunya neix amb el repte de fer un país cibersegur, i lidera l'Estratègia de Ciberseguretat de la Generalitat de Catalunya 2019-2022, on s'estableix una estratègia operativa de Ciberseguretat basada en la maduresa del govern del risc, fonamentada en l'acció preventiva, en detriment de la reacció com a únic mecanisme de protecció.

L'Agència organitza la seva activitat per mitjà d'un model de governança de la Ciberseguretat des d'on es desenvolupen les funcions de protecció, prevenció i resiliència dels sistemes d'informació i les infraestructures TIC de la Generalitat de Catalunya. Aquestes funcions, juntament amb la de governança de la Ciberseguretat, conformen la cadena de valor de l'entitat amb una clara orientació a la millora de la maduresa en matèria de Ciberseguretat i aportant en tot moment una perspectiva de risc i impacte al negoci.

L'Agència fonamenta la seva activitat estratègica en quatre pilars:

- Desplegament d'un Servei Públic de Ciberseguretat executant polítiques públiques.

- Impuls d'una Cultura de Ciberseguretat que permeti assolir una ciutadania digital plena, conscient i capacitada per a l'ús de les TIC i, en especial, en matèria de Ciberseguretat.

- Garant de la Ciberseguretat de l'Administració de la Generalitat de Catalunya i del seu sector públic i de la resta d'entitats i institucions públiques, així com dels ens locals.

- Potencialment del sector econòmic de la Ciberseguretat com a sector estratègic, mitjançant polítiques d'innovació, creació de talent i dinamització del sector productiu.

Aquest enfocament estratègic es complementa mitjançant la priorització de les actuacions destinades a cobrir els objectius prioritaris en matèria de Ciberseguretat de la Generalitat de Catalunya respecte a la resta, vetllant de manera particular pels sistemes d'informació sobre els quals se sustenta l'activitat més crítica de l'Administració.

Així mateix, conseqüència directa dels quatre pilars estratègics de l'Agència en sorgeixen les seves funcions més essencials, que són les següents:

a) Prevenir i detectar incidents de ciberseguretat i respondre-hi, desplegant les mesures de protecció pertinents.

b) Planificar, gestionar, coordinar i supervisar la ciberseguretat en l'àmbit de l'Administració de la Generalitat i el seu sector públic.

c) Exercir les funcions d'equip de resposta a emergències (CERT) competent a Catalunya.

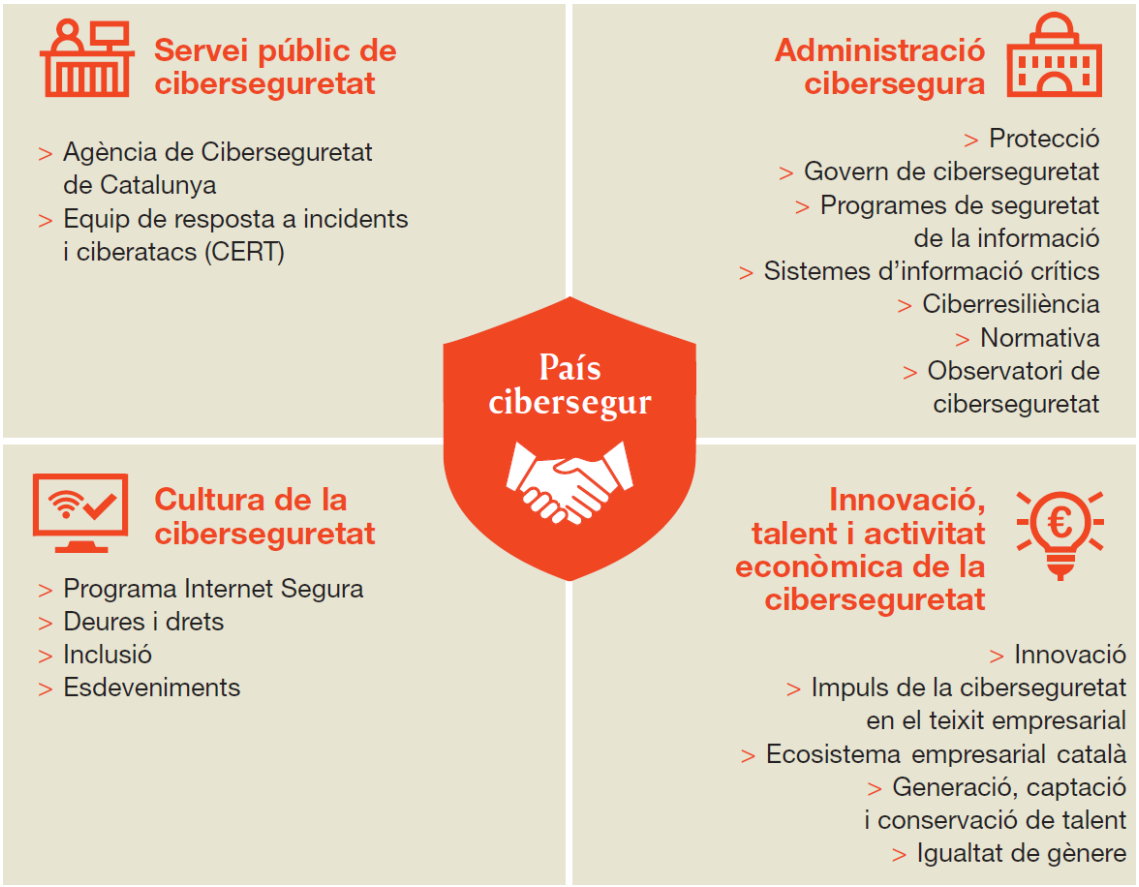
d) Minimitzar els danys i el temps de recuperació en cas de ciberatac.

e) Actuar com a suport, en matèria de ciberseguretat, de qualsevol autoritat competent per a l'exercici de les seves funcions públiques.

f) Investigar i analitzar tecnològicament els ciberincidents i ciberatacs.

g) Recollir les dades pertinents de les entitats que gestionen serveis públics o essencials a Catalunya per conèixer l'estat de la seguretat de la informació, informar-ne el Govern i proposar les mesures adequades.

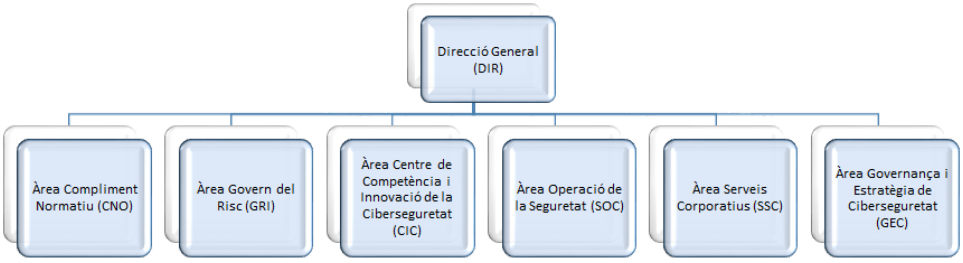
h) Donar suport als responsables de la continuïtat dels serveis i les infraestructures de les tecnologies de la informació i la comunicació de la Generalitat i de les altres administracions públiques que ho requereixin.



Aquesta estratègia i funcions de l'Agència es despleguen a la Generalitat de Catalunya i són extensibles als diferents àmbits d'actuació de l'entitat.

1.1.2 L'estructura de l'Agència de Ciberseguretat de Catalunya i el Centre d'Innovació i Competència en Ciberseguretat (CIC).

L'Agència està estructurada en àrees dependents de la Direcció General.



Il·lustració 1. Organigrama de l'Agència

Els serveis objecte de la present licitació es troben dins de l'àrea d'Estratègia de la Seguretat de l'Agència, que fins recentment vetllava per evolucionar els serveis de l'Agència, interpretava el risc en seguretat de la informació i conscienciava i formava a la ciutadania i les administracions públiques, però que ha evolucionat durant 2022 per esdevenir el **Centre d'Innovació i Competència en Ciberseguretat (CIC)**.

L'estructura de dit Centre d'Innovació s'inspira en els centres de competència per tal de proporcionar experiències per al suport a projectes o programes, per actuar com a repositori del coneixement intern, construir *pools* d'eines i recursos de capacitació de professionals i innovació en ciberseguretat, atraure finançament i incrementar solucions innovadores. Aquest centre és un conglomerat de diferents components bàsics (*building blocks*) que tenen els objectius següents:

– Impuls de la Innovació

– Transferència tecnològica

– Impuls del sector i l'activitat de Ciberseguretat de Catalunya

Aquests objectius s'alineen amb els eixos estratègics de l'Agència i més específicament el CIC treballa per a la cohesió de l'ecosistema de Ciberseguretat, la captació de fons internacionals, l'estímul a la transferència de coneixement, l'estímul a solucions innovadores,

el foment de la capacitació i el foment de la investigació i la recerca.

Estructura de *building blocks* dels àmbits de servei del CIC

Alguns exemples de propostes de valor que permet el CIC són:

– Mapatges d'activitats i capacitats dels membres de l'ecosistema per a participar en projectes conjunts.

– Creació de consorcis i propostes alineades amb els programes de l'Estat i la UE per a participar en convocatòries (*Calls)*, etc.

– Programes específics d'obtenció de competències per a la generació de talent.

– Creació de laboratoris i potenciació de hubs tecnològics per a donar resposta als reptes del sector.

– Desenvolupament d'activitats de vinculació d'oferta i demanda (matchmaking supply/demand) per afavorir el creixement i l'activitat de l'ecosistema de ciberseguretat.

Així doncs, amb el CIC, l'Agència posa a disposició capacitats en:

▪ El coneixement de la Comunitat i l'Ecosistema i la facilitat d'accés.

▪ El disseny i desenvolupament de productes adaptats als reptes del sector per a millorar la capacitació i obtenció de finançament.
▪ L'experiència en la prestació de serveis públics.
▪ La gestió de recursos especialitzats i l'eficiència organitzativa per a obtenir resultats en tots els àmbits d'actuació.

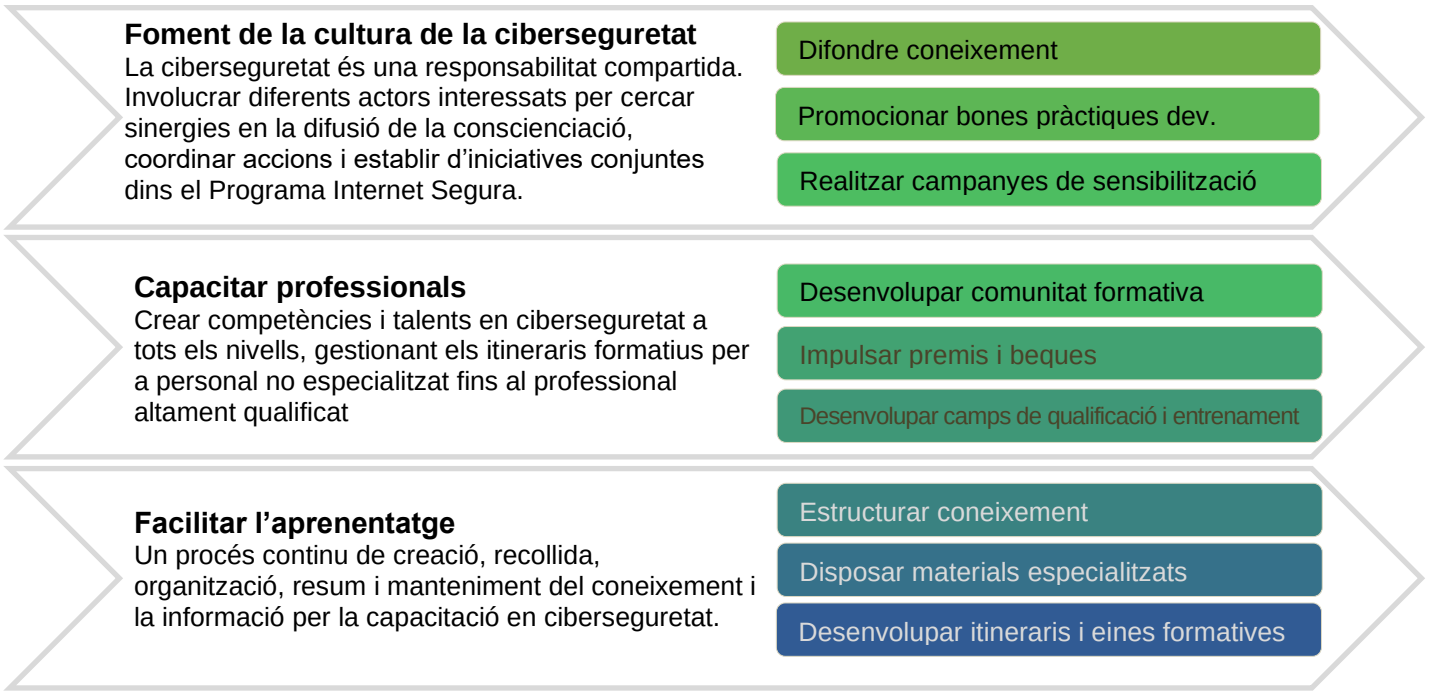
A partir d'aquests objectius, propostes de valor i capacitats per cada una les línies de serveis del CIC es desvetllen els principals públics d'interès (stakeholders):

Stakeholders	
sector públic	Generalitat de Catalunya, administracions locals...
	universitats i centres de recerca i innovació...
sector privat	Sector de la ciberseguretat, teixit empresarial i patronals,
	organitzacions (professionals, consumidors,)

2. OBJECTE I ABAST DELS SERVEIS DE LICITACIÓ

L'objecte de la present licitació és la contractació dels serveis de disseny i construcció d'estratègies i eines per al desenvolupament de programes específics d'obtenció de competències per a la generació de talent en Ciberseguretat. .

Per aconseguir l'anterior, resulta necessari crear una acadèmia de ciberseguretat o ciberacadèmia on es plantegen els objectius següents:



2.1 Descripció del servei

Com s'ha observat, el servei objecte de la present licitació es pot dividir en tres grans àmbits de servei, les quals tenen tres accions estratègiques vinculades. A continuació s'exposarà l'abast de cadascuna d'aquestes línies així com de les accions vinculades:

2.1.1 Àmbits de serveis de foment de la cultura de la Ciberseguretat

L'objectiu general és ampliar el potencial del programa Internet Segura per la coordinació d'accions i iniciatives conjuntes per la difusió del coneixement amb major impacte.

Els objectius específics dels projectes d'innovació són:

- Dinamitzar els diferents grups de treball adreçats al sector de professionals de la ciberseguretat de la comissió interdepartamental Internet Segura (Digital Community Alliance DCA, entitats TIC de professionals de Catalunya, ...).
- Promoure de bones pràctiques de sensibilització en el teixit empresarial de Catalunya.
- Creació i estímul de comunitats threat hunters (evolucionant el concepte de les bug bounties) per a corregir les vulnerabilitats crítiques de ciberseguretat dels actius TIC de Catalunya.
- Capacitació de professionals en ciberseguretat d'entitats dedicades als col·lectius en risc.

2.1.1.1 Difondre coneixement

– Promoure programes per a conscienciar a professionals que volen desenvolupar productes i serveis segurs, i difondre la necessitat de realitzar activitats per a detectar vulnerabilitats i fer-hi front a tot l'ecosistema (threat hunters, etc.).

2.1.2.2Promocionar bones pràctiques de desenvolupament

– Promocionar per a professionals dedicats a software developers de programes de pràctiques de *privacy, security by design* i *by default* per a conscienciar i difondre la gestió de la seguretat i privacitat de les dades de les persones des del mateix moment del disseny i desenvolupament actuals i futurs.
– Promocionar de pràctiques de programació segura i *SecDevOps* per al sector de professionals de ciberseguretat, conscienciant i difonent la necessitat d'introduir la seguretat des del disseny, fomentant el desenvolupament segur amb formació i informació i l'ús d'eines d'anàlisi, aconseguint reduir els costos.

2.1.3.3 Realitzar campanyes de sensibilització

– Dinamitzar ecosistema de partners públic-privats per a l'increment d'impactes de campanyes a la ciutadania.

Amb aquestes actuacions es vol dotar a l'ecosistema d'elements experts de conscienciació i difusió multi-canals, tals com, per exemple, altaveus de conscienciació, bases de treball per a les comunitats bug bounties i de recerca o eines de difusió de prevenció, entre d'altres.

2.1.2 Àmbits de serveis de capacitar professionals

L'objectiu general és la capacitació especialitzada de professionals per a generar talent amb les activitats de formació, d'entrenament amb eines especialitzades i col·laborant amb l'ecosistema de formació en ciberseguretat existent a Catalunya.

Els objectius específics dels projectes d'innovació són:

- Formar i/o entrenar individualment o col·lectivament a professionals.
- Posar a disposició de l'ecosistema un entorn de **Cyber Ranges** dins el node de ciberseguretat del **Digital Innovation Hub (DIH4Cat)**.
- Realitzar els exercicis de capacitació que precisa el SOC de l'Agència i d'altres Administracions.
- Oferir a l'ecosistema un entorn per a la realització de ***cyber tests*** d'aplicacions...

2.1.2.1 Desenvolupar comunitat formativa

– Posar a disposició de la comunitat els entorns reals per a la formació i entrenament de professionals de l'Agència i de la comunitat

2.1.2.2 Impulsar premis i beques

– Desenvolupar activitats de foment i retenció de talent de la comunitat impulsant premis o sistemes de beques en funció del diferents perfils objectiu (ajuts a alumnes de postgrau amb necessitat específica de suport educatiu, beques de col·laboració...)

2.1.2.3 Desenvolupar camps de qualificació i entrenament

– Dissenyar, preparar i realitzar exercicis de qualificació i capacitació. Aquests s'orienten a determinar la capacitació per a activitats laborals específiques en els perfils de ciberseguretat en base a l'e-CF[1].

L'acadèmia de ciberseguretat ha de posar a disposició una plataforma de simulació d'entorns reals i dissenyat específicament per a la formació per a:

- Entrenament de professionals (interns de l'Agència en primera fase, posteriorment per altres administracions Generalitat de Catalunya i Administracions locals, i finalment per la comunitat de ciberseguretat).
- Tests d'aplicacions i millora de l'estratègia de l'ecosistema.
- Pràctiques, competicions i exercicis de ciberseguretat.

També ha de dotar a l'ecosistema d'uns eina d'intercanvi de coneixement i desenvolupament a nivell local i internacional.

Una llista de programes específics orientatius a dissenyar i construir:

- Programes de suport a la formació professional especialitzada IT i OT
- Programa d'upskilling a nivells 2, 3 i 4
- Programa de reciclatge professional (reskilling), coordinat amb pla estratègic Dona Cyber.
- Disseny de competicions d'atac/defensa, *Capture the Flag, cyber league, cyber challenges*
- Estructurar serveis de *cyber range,* amb administració de casos d'ús sectorials, simuladors i *boot camps per DIH4Cat*

2.1.3 Àmbits per facilitar l'aprenentatge

L'objectiu general és la construcció d'un espai virtual d'aprenentatge que faciliti l'experiència d'ensenyament-aprenentatge per a generar coneixement.

Els objectius específics dels projectes d'innovació són:

- Promoure i enfortir l'ecosistema local, nacional i internacional de ciberseguretat, a través de la col·laboració i esperit de comunitat dels diversos agents de l'ecosistema (desplegar el coneixement del CIC).
- Possibilitar un aprenentatge constant, flexible i rigorós mitjançant les eines tecnològiques i mètodes didàctics òptims.
- Garantir l'accés a l'aprenentatge i formació en ciberseguretat a la ciutadania.

2.1.3.1 Estructurar coneixement

[1] ***16234-1 European e-Competence Framework (e-CF)*** proporciona una referència de competències aplicades al lloc de treball de les Tecnologies de la Informació i la Comunicació https://ecfusertool.itprofessionalism.org/explorer i es tenen en compte els equivalents en els EQF levels https://europa.eu/europass/en/description-eight-eqf-levels

– Posar a disposició de la comunitat formativa mètodes de generació del coneixement i retenir-lo.

2.1.3.2 Disposar materials especialitzats

– Dotar a la comunitat de diversos elements per aconseguir l'aprenentatge amb la combinació d'elements pedagògics essencials i eines tecnològiques (mòduls EVA, guies, infografies, exercicis pràctics interactius H5P...).

– Dotar d'un hub-portal d'accés a usuaris interessats en les activitats promogudes o recollides per la ciberacadèmia.

– Posar a disposició de l'ecosistema un catàleg d'habilitats, capacitats i especialitats en ciberseguretat, càpsules, biblioteques, stacks, guies i feedback de l'acadèmia (exemple: comunitat Alumni).

2.1.3.3 Desenvolupar itineraris i eines formatives

– Posar a disposició de l'ecosistema itineraris formatius d'especialització en ciberseguretat amb mitjans propis o de *partners* (xarxes socials, *meetups i meetings* en general).

Amb aquestes actuacions es podrà posar a disposició una organització de formadors/es en xarxa.

Dotació a l'ecosistema de continguts formatius multisectorials especialitzats en ciberseguretat.

Disposició d'experts professionals mentors en ciberseguretat de la comunitat formativa.

Una llista d'actuacions orientatives a dissenyar i construir:

- Administració de xarxes territorials resultants de formació a formadors
- Administració de comunitat de mentors experts cyber
- *Gestió d'un hub-portal* d'accés a usuaris de la ciberacadèmia de cursos i continguts de ciberseguretat especialitzats (comunicació i manteniment d'una comunitat alumni)
- Gestió d'una plataforma de cursos d'autoformació en ciber per a diferents canals
- Tests d'orientació als diferents itineraris i avaluació d'skills certificables

2.4 Activitats del servei

- Actualitzar la estratègia i el seu pla de associat, en el disseny de continguts, el seu desplegament, la col·laboració amb els continguts existents i plataformes de formació, així com programes de fabricants privats i públics cercant la seva col·laboració.
- Desenvolupar, actualitzar i oferir programes específics de ciberseguretat i proveir material educatiu per a la formació i la conscienciació basats en el contingut, el mètode i les eines innovadores que els alumnes de l'acadèmia de ciberseguretat necessitin.

- Organitzar, dissenyar i oferir activitats de conscienciació sobre ciberseguretat, seminaris, cursos, exercicis pràctics per a diferents itineraris formatius.
- Supervisar, avaluar i informar sobre l'eficàcia de la formació assolida per la ciberacadèmia.
- Disseny d'avaluació i sistemes d'informació sobre el rendiment de les tipologies d'alumnat participant.
- Trobar enfocs de capacitació de professionals en ciberseguretat orientats a mercat establint convenis amb agents implicats, valorant solucions i continguts de mercat i marcs de referència en definició d'skills i competències cyber internacionals, com Cybernet, Enisa, ECSO, NIST, etc...
- Establir convenis de col·laboració continuada amb universitats, centres tecnològics, altres acadèmies IT amb qui trobar punts de col·laboració, empreses dedicades a la formació en ciberseguretat per a formació oficial, ocupacional, continuada o especialitzada.
- Definir un model de negoci de la cyberacademy, identificant ingressos i fons de finançament i capacitat de captura d'aquests fons.
- Definir un model de negoci dels nostres partners i negociar l'adquisició de components de la cyberacademy.
- Detectar i mantenir un ecosistema de formadors i formadors de formadors.
- Intergrar i desenvolupar les eines de cyberrange i de modalitats innovadores que s'apropin a l'experiencia del usuari i no només als conceptes.

2.5 Productes del servei

El servei serà responsable de coordinar la definició, desenvolupament i desplegament de la Cyber Academy vetllant per garantir l'alineament per a l'acompliment de fites i objectius del propi CIC.

Amb l'objectiu de garantir el seguiment, suport i aprovació de les accions que involucrin terceres parts i la futura presa de decisions haurà de mantenir informat a responsables de línies de servei del CIC.

– Calendari amb el pla d'accions realitzades i previstes.
– Documentació d'actes i reunions de l'activitat sorgida amb l'ecosistema formatiu amb qui es vol formalitzar activitat.
– Pla de qualitat, evolució i innovació del servei amb actualització trimestral.

El desenvolupament de la cyberacademy té com abast la pròpia Agència, Generalitat, mon local i els seus proveïdors, les entitats del ecosistema prestadors de formació, els canals orientats a les empreses com DIH4CAT o el DCA, les empreses del sector Ciber i les que siguin objecte de transformació digital, així com els professionals o potencial talent, bé sigui en FP, universitats i màsters o bé en la formació informal orientada a upskilling i reskilling de professionals.

La cyberacademy també tindrà presents iniciatives de talent com el Barcelona Digital Talent o el pla dona TIC o més concretament el Pla dona cyber. Així com les necessitats dels agents de formació continua del Servei d'Ocupació o les principals representats de les empreses o dels treballadors.

Així mateix, fruit de les tasques del servei, es requerirà una important tasca de documentació per tal de formalitzar els avenços realitzats en potencials productes o serveis projectats i la definició de programes específics amb les components bàsiques que els defineixin (possibles acords amb projectes europeus o entitats relacionades, tipologia de proveïdors a implicar, definició d'actuacions i abast, finançament, canals de difusió...).

- Convenis i acords de col·laboració.
- Presentacions executives per presentar els programes a stakeholders.
- Mapatge de l'ecosistema identificat en els programes.
- Altra documentació detallada.

3. Condicions d'execució del servei

3.1. Equip Humà

L'adjudicatari serà responsable d'un seguit de funcions dirigides a enfortir la seva acció externa, teixint accions col·laboratives per a la constitució d'una societat més cibersegura, a partir de la millora del coneixement, les habilitats i les competències en Ciberseguretat de la ciutadania i professionals de Catalunya. L'adjudicatari ha de ser conscient de l'especial rellevància d'aquesta tasca i, per tant, de la necessitat d'aportar un equip amb recursos amb les següents habilitats:

– Actitud altament proactiva, autònoma i experiència contrastable en cadascun dels àmbits de referència.

– Capacitat d'interrelació i coordinació amb altres projectes de les línies de serveis del CIC.

– Destresa comunicativa i interpersonal.

– Habilitat per identificar, analitzar i resoldre problemes.

– Capacitat de treball en equip amb orientació a objectius col·lectius del CIC.

– Capacitat de treball en entorns complexos i sota pressió.

Per tal de donar resposta a les necessitats descrites per a la creació i el manteniment dels productes descrits anteriorment, el CIC requereix la incorporació del recurs mínim assenyalat a la solvència tècnica del Quadre-resum de característiques del Plec de Clàusules Administratives Particulars. Addicionalment als requeriments mímims, seguidament s'assenyala les capacitats desitjables de l'esmentat perfil i les funcions bàsiques a desenvolupar.

Perfil	Requeriments mínims	Funcions bàsiques orientatives
Coordinador d'acadèmia de Ciberseguretat (perfil expert)	• Perfil desitjables on s'ha aportat experiència: *Cybersecurity educator* *Cybersecurity Awareness Specialist* *Cybersecurity Trainer* • Presentació de participació en disseny o autoria en: — material educatiu en capacitació avançada en ciberseguretat	• Dissenya, desenvolupa i endegar programes de conscienciació, formació i educació en temes relacionats amb la Ciberseguretat. • Planifica actuacions formatives en base a itineraris de capacitació a diferents nivells i mitjançant l'administració de convenis de

	— plans de creació de capacitació en matèria de recursos humans en ciberseguretat — Desenvolupament de polítiques educatives, formatives i de sensibilització en ciberseguretat — Desenvolupament de programes de sensibilització, educació i formació en matèria de ciberseguretat — projectes de creació d'infraestructura educativa (valorable en ciberseguretat) — projectes d'infraestructura de ciberexercicis o simuladors de ciberseguretat • Participació com a ponent, en ponències, xerrades professionals o en tallers formatius. • Participació en publicacions de ciberseguretat, disseny de campanyes de sensibilització de ciberseguretat. • Capacitat de lideratge.	col·laboració (entorn DIH4Cat i DCA ciberseguretat). • Coordina programes de sensibilització i capacitació per a professionals amb necessitats d'assolir nivells avançats de temàtiques de ciberseguretat de forma accelerada (per exemple, *boot camp* o ciberexercicis). • Utilitza mètodes, tècniques i instruments pedagògics i formatius especialitzats per a comunicar i millorar la cultura, les capacitats, els coneixements i les aptituds dels destinataris de les accions formatives en matèria de ciberseguretat. • Dissenya cyber tests d'aplicacions i entorns de gestió i estructuració del coneixement. • Promou la importància de la ciberseguretat i estableix mecanismes per consolidar-la en les organitzacions amb qui s'estableixin convenis.

2.5.2 Dedicació mínima

Perfil	**FTE**
Coordinador d'acadèmia de Ciberseguretat	1
Total	**1**

El servei requereix l'actualització d'indicadors de referència que permetin efectuar el recolzament en el seguiment, la gestió i governança, i amb l'anàlisi de l'evolució de l'activitat serveixi en la presa de decisions. A continuació, es detallen alguns d'aquests indicadors més bàsics:

- Avenç de l'evolució de l'activitat i el lliurament de productes.
- Planificació de les accions per àmbits definits.

- Accions realitzades el darrer mes i previstos pel proper.
- Nombre d'oportunitats en curs i acords assolits / convenis signats.
- Impacte obtingut de les accions.(per sectors o tipologies)
- Eficàcia de la formació.
- Rendiment i diversitat de l'alumnat participant (nivells assolits, gènere, ...)

Si s'escau, en concordança amb la resta de línies de serveis del CIC, els indicadors de mesura i seguiment seran integrats en els Repositoris d'indicadors i d'informació de l'Agència, per posteriorment ser visualitzats en eines que faciliten la gestió dels mateixos, com ara eines de *business intelligence*. Aquest procés de càrrega d'informació i visualització dels indicadors és funció del servei de Govern de la Dada de l'Agència, amb el que l'adjudicatari s'ha de coordinar per garantir una correcta càrrega d'indicadors establerts, i l'evolució dels mateixos.

3.3 Horari

Els serveis en règim presencial es desenvolupen amb els horaris laborals de l'Agència. Aquests corresponen amb els del centre de treball de l'Hospitalet de Llobregat. Es pacten amb l'àrea del Centre de Competència i Innovació en Ciberseguretat i orientativament es situa en la franja de les 9:00h i les 18:00h.

A petició expressa de l'Agència, hi ha tasques que podrien realitzar 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, es consensuarà 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.

3.4 Localització

L'equip prestatari del servei podrà treballar de forma presencial o remota des de les seves pròpies instal·lacions, i es consensuarà de forma conjunta. En qualsevol cas, és responsabilitat del licitador explicitar la metodologia de treball proposada per evitar cap perjudici en la qualitat del desenvolupament del servei. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació del servei.

3.5 Rotació de recursos

L'Agència tindrà dret a exigir justificadament a l'adjudicatari 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 tal de garantir la correcta prestació, dimensionament i organització del servei. Aquesta substitució ha de ser efectiva en un termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència al cap de servei. L'adjudicatari haurà de presentar en un termini màxim de 10 dies 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.

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 dels personal que donen servei a l'Agència evitant, sempre que sigui possible, la rotació del perfil corresponent al cap de servei.

L'excessiva rotació del personal podrà ser penalitzada (apartat 5.1). Així mateix, les hores dedicades pel personal de l'adjudicatari a la transició i/o formació del personal sortint i entrant en cas de substitució no serà facturable. S'acordarà entre l'adjudicatari i l'Agència el temps estimat de transició per cada substitució que es produeixi, essent el període mínim establert per a la transició de 4 dies laborables.

Quan la rotació sigui necessària (baixes, etc.) l'adjudicatari haurà d'acreditar la idoneïtat del nou personal prèvia incorporació dels nous recursos.

3.6 Eines i equipament per la prestació del servei

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

– Ubicació física adequada per al desenvolupament i prestació del servei, a les instal·lacions de l'Agència.

– Accés a Internet a través de la xarxa 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.

– Eines corporatives de correu, paquet ofimàtic i eines col·laboratives Office 365.

– Accés a la plataforma de col·laboració i compartició d'informació entre els treballadors de l'Agència (Confluence).

– Accés al servidor de fitxers del Centre d'Innovació i Competència en Ciberseguretat de l'Agència (Servfile).

L'Agència no proveirà:

–Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina.

–Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.

–Ordinadors portàtils (PCs) o altres dispositius mòbils.

–Accés a Internet via comunicacions mòbils.

–Eines per al control de canvis i la gestió de versions.

–Cap altre recurs no especificat explícitament.

En conseqüència, l'adjudicatari haurà de:

–Subministrar tots els elements de maquinari, assumir el cost del llicenciament del programari i serveis, així com del seu manteniment, durant la durada del contracte, que siguin necessaris per complir amb els requeriments d'aquest capítol. 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'Agència.

–Permetre l'administració, maquetat i supervisió dels equips per part de Desplegament i manteniment de solucions de l'Agència.

S'ha de realitzar una proposta homogènia de maquinari, programari i de tots aquells accessoris i equipaments auxiliars que siguin necessaris per què l'equip pugui executar les seves funcions amb eficàcia. S'ha de tenir en compte les especificacions donades pel responsable del servei d'Enginyeria de Sistemes d'Informació a fi de garantir la compatibilitat amb el sistema de maquetat, així com amb el compliment dels requeriments de Seguretat Corporativa. L'equip portàtil o de sobretaula que l'adjudicatari posi a disposició haurà d'estar maquetat per l'Agència amb el programari i les llicències que l'adjudicatari proporcioni. Per facilitar la gestió, l'Agència posa a disposició de l'adjudicatari la possibilitat d'utilitzar una maqueta pròpia de l'Agència, assumint el mateix adjudicatari els costos de llicenciament del programari (sistema operatiu, paquet ofimàtic, antivirus, etc.).

Tot el sistema de maquetació serà responsabilitat del adjudicatari el seu manteniment i oportuna actualització segons les necessitats de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en referència a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei. Per aquest motiu es fa imprescindible que l'adjudicatari tingui presents les consideracions següents:

–L'Agència decideix la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.

–L'Agència decideix com implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.

–L'adjudicatari es compromet a assumir i adaptar-se a aquestes tecnologies i sistemes per donar el servei de suport, així com participar activament en la transició i amb la formació si es requereix sense cost addicional per l'Agència.

3.7 Seguretat corporativa

Tant l'adjudicatari com el seu personal s'haurà de sotmetre a les polítiques i regulacions internes que estableix Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

–Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la

prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.

–Facilitar l'accés 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 normes i polítiques que estableix Seguretat Corporativa tant en el moment de la seva incorporació com després de canvis importants de les polítiques, normes o regulacions.

–Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de Desplegament i manteniment de solucions 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 (GDPR, LOPDGDD, LSSI, etc.).

A la finalització del contracte, l'adjudicatari 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 Orientació a objectius

L'adjudicatari orientarà la seva activitat i la facturació de la mateixa a l'assoliment d'objectius i/o fites, de manera que qualsevol acció fora d'aquest marc no podrà ser justificada i no serà subjecta al pagament per part de l'Agència.

– Encàrrec formal d'objectius/fites:
- Es realitzaran reunions específiques on l'adjudicatari i el Centre d'Innovació i Competència en Ciberseguretat organitzaran i acordaran els objectius i/o fites a assolir.
- Entre els objectius/fites s'hi inclou la generació dels productes de servei detallats en el punt anterior.
- Es podran orientar els objectius/fites com a blocs d'encàrrecs o conjunts de tasques.

– Estimació de l'esforç i llum verda a l'execució:
- L'adjudicatari realitzarà una estimació de les hores a consumir que seran les hores subjectes a facturació al compliment de l'objectiu/fita.
- És responsabilitat de l'adjudicatari que els objectius/tasques quedin ben definits i siguin prou acurats per dur a terme la seva execució.
- Una vegada quantificat l'esforç, el Centre d'Innovació i Competència en Ciberseguretat haurà de validar-lo i donar llum verda a la seva execució, i posteriorment serà responsabilitat de l'adjudicatari dur a terme l'encàrrec.

– Acceptació:
• La facturació per a l'esforç destinat a l'assoliment d'objectius/fites es realitzarà una vegada el resultat final d'aquestes sigui acceptat pel Centre d'Innovació i Competència en Ciberseguretat.
• Si la fita no es compleix, ja sigui fora de la data acordada o amb una qualitat i forma deficients o diferents a les acordades, l'adjudicatari podrà ser subjecte a una penalització.

3.10 Control econòmic de la prestació del servei

L'adjudicatari prestarà tot el suport requerit pel servei de Planificació Pressupostària i Control de Gestió de l'Agència per tal de:

– Definir un model de transparència en termes de capacitat i execució dels serveis previstos en l'abast contractual.

– Donar compliment als procediments de facturació en temps i forma en allò establert.

– Conformar les factures en coherència amb el serveis prestats reconeguts d'acord amb els informes de serveis, i les corresponents actes vinculants, segons els procediments vigents.

– Exercir la gestió del contracte, facilitant la previsió del dimensionament de les capacitats futures del servei (Forecast).

– Desenvolupar la funció de *reporting* mitjançant les eines proporcionades per l'Agència amb els conceptes següents:

- 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.
- 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. L'adjudicatari suportarà els costos d'auditories adjudicades a tercers i gestionades per l'Agència, destinant al seu finançament un màxim del 0,7% de l'import anual dels serveis contractats.

3.11 Propietat i validació de la documentació

L'Agència és la propietària 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.

El responsable de línia de servei de l'Agència serà el 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 la present licitació.

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

3.12 Formació

Els perfils adscrits a l'execució del servei disposaran de la formació adequada per al desenvolupament de les seves tasques. Sens perjudici d'aquesta qüestió, si s'escau, el personal de l'adjudicatari realitzarà formació continuada que garanteixi l'actualització i l'adquisició de coneixements que pugui ser de valor pels serveis de l'Agència. L'adjudicatari haurà de reservar un 5% del seu temps per tasques de formació i certificació (en matèries relacionades amb l'activitat del contracte) i aquest temps no serà facturat a l'Agència, valorant-se la disposició d'un pla de formació per al personal de l'adjudicatari destinat a l'Agència. Aquest pla es coordinarà amb les activitats i accions de formació pròpies de l'Agència.

Així mateix durant la fase de devolució del servei a un nou adjudicatari, el proveïdor sortint resta obligat a formar als treballadors de la nova empresa en totes les eines, processos inventaris, procediments operatius específics per a prestar el servei objecte del contracte.

4. Acords de nivell de servei i model de penalitzacions

5.1 Acords de nivell de servei

L'adjudicatari resta obligat al compliment de l'execució total de les prestacions recollides en les ofertes que doni compliment al present plec segons el previst a l'Annex 1 i a les prescripcions del contracte.

Així mateix, la prestació de serveis de l'adjudicatari haurà de complir uns estàndards de qualitat mínims que permetin fer-ne un aprofitament adequat i donin resposta a les necessitats de l'Agència. En cas que els serveis no assoleixin aquests mínims de qualitat requerits es considerarà l'existència d'un incompliment d'acord amb el model recollit en la clàusula especifica estipulada al respecte al Plec de Clàusules Administratives Particulars.

6. Fases de la prestació

Els licitadors hauran de presentar dins la seva oferta tècnica el pla d'actuació detallat per tal de garantir les fases següents, si s'escau atenent a la situació actual de l'Agència:

6.1 Inici de la prestació

És el període que va des de l'entrada en vigor del contracte fins l'estabilització dels serveis en els nivells establerts en aquest plec. La transició tindrà una durada màxima d'UN (1) mes des de la data d'adjudicació. Aquest període no serà objecte de remuneració.

Durant l'inici de la prestació es duran a terme les següents activitats:
• **Adquisició del coneixement de l'estat actual del Servei i el seu model de gestió i metodologia.** El nou adjudicatari parlarà amb el responsable de la línia de servei de l'Agència per tal d'entendre el funcionament i estat actual del servei.
• **Generació i implantació dels models de relació amb els diferents serveis operatius**. Els serveis hauran d'establir les relacions amb la resta d'àrees de l'Agència, així com els proveïdors TIC de la Generalitat de Catalunya.

6.2 Prestació

Es considera la fase normal de la prestació del servei. Comença quan la fase d'inici de prestació hagi acabat fins **quinze dies** abans de que finalitzi la prestació del servei.

Durant aquesta fase, estan vigents els plans de millora continua dels serveis; per aquesta raó els ANS s'han de revisar com a mínim cada mes, per tal d'adaptar-los a l'evolució en la prestació dels serveis i a les variacions atenent a les necessitats de l'Agència.

6.3 Devolució

Fase que s'emmarca al final de la prestació, un cop s'hagi comunicat la finalització del contracte o de la seva pròrroga, i que comença quinze dies abans de l'extinció d'aquest. Durant aquesta fase hi haurà coexistència amb un nou adjudicatari fins que es transfereixin els serveis a aquest.

L'adjudicatari haurà de procurar la metodologia, eines i recursos necessaris per tal de traspassar adequadament el servei a altres possibles futurs adjudicataris.

Tot el material generat i desenvolupat, incloent desenvolupaments en Sistemes d'Informació, és propietat de l'Agència i romandrà, amb tota la seva documentació, a l'Agència un cop acabada la prestació del servei.

Tal i com s'ha descrit anteriorment, els mitjans tècnics que el proveïdor sortint hagi proporcionat per tal de desenvolupar la seva tasca hauran de ser degudament esborrats i tota la informació traspassada a qui l'Agència designi.

La devolució de les eines es regirà segons l'estipulat a l'apartat 4 d'aquest plec i en les condicions acordades amb l'adjudicatari.

L'Hospitalet de Llobregat, en la data de la signatura electrònica

Santiago Romeu Sala
Responsable de Línia de Servei Ciència i Analítica de dades
Agència de Ciberseguretat de Catalunya

ANNEX 1

Indicadors i nivells de servei ("ANS")

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Salvador Espriu, 45-51
S08908 L'Hospitalet de Llobregat
Tel. 93 557 42 40

Tipus	Nom	Descripció	Fórmula de càlcul / eines	Periodicitat	Llindar Inicial (Li)	Llindar Final (Lf)	Penalització Màxima
Personal	Rotació de personal	Índex de rotació del personal presencial en el servei	Índex de rotació de personal = (((A + D)/2) *100)/ES A = Admissions de personal presencial en el servei dins del període considerat. D = Desvinculacions de personal presencial en el servei dins del període considerat. ES = Número d'efectius del servei segons s'estableix en la proposta de servei pel període considerat; si hagués alguna ampliació del servei en número de recursos humans durant el període considerat, es considerarà el valor ponderat al temps d'aplicabilitat	Mensual	N/A	N/A	% Índex de Rotació x Import de la factura mensual
Personal	Termini per la reposició de Recursos	Termini de substitució d'un recurs per un altre, tant sigui per baixa o per rotació de personal	Dies de desviament respecte el termini de reposició de recursos definit	Per recurs	5 dies	15 dies	Dedicació equivalent a les hores de no disponibilitat del recurs
Personal	No disponibilitat del personal	L'incompliment de l'horari de servei, la no disponibilitat de servei o la no presència en el lloc de treball en qualsevol moment del període contractat	Hores no disponibles per causes no justificades	Mensual	N/A	N/A	Dedicació de 2h de servei per cada hora de no disponibilitat

Tipus	Nom	Descripció	Fórmula de càlcul / eines	Periodicitat	Llindar Inicial (Li)	Llindar Final (Lf)	Penalització Màxima
Qualitat	Qualitat dels lliurables	Grau de satisfacció del l'Agència respecte les condicions acordades dels lliurables	Puntuació de 1 a 10 segons enquestes de satisfacció de l'Agència	Per lliurable	8	5,5	20% del cost mensual del servei
Terminis	Disponibilitat dels lliurables	Disponibilitat dels lliurables respecte la data d'entrega acordada	Dies desviats respecte la data d'entrega establerta	Per lliurable	2 dies	6 dies	10% del cost mensual del servei
Gestió	Qualitat del reporting i indicadors del servei (periodicitat mín. mensual)	Grau de satisfacció del client respecte dels informes de reporting	Puntuació de 1 a 10 segons enquestes de satisfacció al client endegades pel propi adjudicatari.	Mensual	8	5,5	20% del cost mensual del servei