Plec de prescripcions tècniques particulars que regeix la contractació basada relativa al suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari.

Exp. CB25AMCONSL1B006

Índex

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. Dins d'aquest context, els acords marc en matèria de ciberseguretat representen una eina essencial per a la implementació de solucions i serveis que reforcin la ciberseguretat de Catalunya, alineats amb l'Estratègia de Ciberseguretat 2019-2022 i la proposta per a la nova Estratègia 2023-2027.

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 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.

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 2024, presentada al Govern, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2024, tant pel que fa a la Generalitat com en diferents entitats del territori català.

En aquest sentit, l'Agència gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2025 va ser de més de 9.100 milions, en contraposició als 6.900 milions d'atacs del 2024. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 6.544 durant el 2025, un augment del 94% respecte els 3.372 de l'exercici anterior.

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

1.1 Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes del la nova estratègia de contractació

Avui en dia l'Agència té les següents funcions:

- **Gerència** s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació, la gestió de personal, la seguretat corporativa i la captació i gestió de fons que fomenta l'atracció de fons i gestions administratives ó la internacionalització de l'entitat.
- **Operacions** du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa (coneguda com SOC/CERT).
- **Desenvolupament d'Estratègia d'Àmbits** té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- **Producte** s'ocupa d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat.
- **Centre de Competència i Innovació** en Ciberseguretat (CCI) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Ciberseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector.
- **Certificació** en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

2 Antecedents

L'Agència de Ciberseguretat ha dissenyat i està desplegant un Model Integral de Ciberseguretat (en endavant, el Model), que té com a objectiu protegir els àmbits d'actuació públics més rellevants a Catalunya de les amenaces en ciberseguretat dirigides contra els seus sectors, i abordar les actuacions necessàries per a protegir-los dels ciberincidents que puguin impactar contra les diferents entitats que els conformen.

A tal efecte el Model preveu l'execució de les següents fases per al seu desplegament:

- **Diagnòstic:** identificació del grau actual d'exposició a les principals ciberamenaces que apliquen a l'àmbit.
- **Pla de seguretat:** determinació del pla de seguretat de cada entitat per tal de ser més resilient i reduir l'exposició a les amenaces més significatives, amb una orientació a assolir el compliment normatiu en l'Esquema Nacional de Seguretat i, quan correspongui, en altres normatives sectorials o específiques que siguin d'aplicació.
- **Integració operativa:** desplegament, a partir de les capacitats de protecció desplegades per les entitats, de les capacitats de prevenció, detecció i resposta, i dels processos i serveis associats a la integració amb l'Agència de Ciberseguretat de Catalunya.
- **Protecció:** activació i operació del serveis de monitorització i resposta 24x7 de l'Agència, i dels serveis i oficines necessàries per a la governança, comunicació, formació i evolució en la ciberseguretat.
- **Certificació:** procés de certificació mitjançant les auditories de la conformitat en l'Esquema Nacional de Seguretat.

Tota l'operació de la seguretat que contempla aquest Model gira al voltant del concepte "perímetre de ciberseguretat", entenent-se per perímetre el conjunt d'activitats i tecnologies desplegades i governades pel SOC/CERT, que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

En aquest context, durant el 2023, es va presentar i iniciar el desplegament del Model a l'àmbit universitari. Per poder donar continuïtat a la prestació de serveis, el CSUC i l'Agència van signar l'11 de desembre de 2025 la sol·licitud d'actuació AMS-CSUC-26-001, en el marc del Contracte Programa de l'Agència de Ciberseguretat de Catalunya 2024-2027.

Amb aquest acord, l'Agència de Ciberseguretat de Catalunya té, formalment, l'encàrrec de Govern manifestat per la Secretaria de Telecomunicacions i Transformació Digital, de continuar proveint durant el període 2026-2027 els serveis de ciberseguretat desplegats durant 2024 i 2025, per impulsar la protecció, la detecció, la resposta i la recuperació en vers incidents de ciberseguretat, així com per impulsar el compliment normatiu i legal en matèria de Ciberseguretat en l'àmbit públic universitari de Catalunya.

Més específicament, aquest acord amb CSUC inclou l'execució de les següents funcions i serveis recurrents, orientats a oferir capacitats de prevenció, protecció i resposta continua:

- Detecció i Monitorització d'amenaces (SOC 24x7)
- Millora casos d'ús SIEM (Use Case Factory)
- Resposta a Incidents
- Actualització de context amenaces de l'àmbit universitari
- 6 Certificacions de l'Esquema Nacional de Seguretat (ENS)
- Governança dels serveis

3 Descripció dels serveis objecte de la contractació basada

3.1 Context dels serveis objecte de la licitació

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient AM.01.2024, que regeix l'Acord Marc per l'entrega de serveis de consultoria per a l'Agència de Ciberseguretat de la Generalitat de Catalunya.

Concretament s'emmarca en el Lot 1 - Consultoria de Ciberseguretat inclosa la vessant d'arquitectura. Dins de dit lot s'inclouen les actuacions de suport a la governança de la ciberseguretat, les quals són plenament assimilables a l'objecte de la present licitació.

La licitació de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari té com a finalitat facilitar i reforçar les tasques operatives de:

- Control de qualitat dels resultats dels serveis prestats, identificant, posant remei, i prevenint els defectes i desviacions que puguin sorgir
- Recolzament en l'avaluació de l'impacte dels serveis prestats
- Suport al control i seguiment de la demanda de les universitats
- Manteniment de les dades de contacte i de context necessàries de les entitats destinatàries del servei
- Suport a la convocatòria de comitès i sales tècniques i a la gestió documental davant cibercrisis
- Generació i manteniment d'indicadors operatius i evolutius dels serveis prestats
- Anàlisi transversal i recurrent de la situació i exposició de les entitats de l'àmbit
- Preparació i presentació d'informes de seguiment dels serveis amb les universitats
- Suport en la realització de reunions de seguiment operatives amb les universitats
- Generació de memòries dels serveis a l'àmbit
- Suport per a l'impuls de la millora continua dels serveis per tal d'atendre les expectatives de les entitats.

Totes aquestes tasques es faran seguint les directrius i procediments definits per l'Agència. Addicionalment, aquest servei adoptarà els processos, procediments i models de relació que determini el servei de suport a la governança d'operació de l'Àrea d'Operacions (en endavant AOS), orientat a prestar servei principalment a la Generalitat de Catalunya, i garantirà una coordinació i comunicació efectiva i continuada entre les parts, per tal que les tasques a executar tinguin una coherència en quant a la seva prestació des d'un punt de vista transversal, i alhora contemplar les particularitats de l'entorn universitari.

3.2 Objecte i abast dels serveis

El servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari té per objecte finalitat facilitar i reforçar les tasques operatives de:

- Control de qualitat dels resultats dels serveis prestats, identificant, posant remei, i prevenint els defectes i desviacions que puguin sorgir
- Recolzament en l'avaluació de l'impacte dels serveis prestats
- Suport al control i seguiment de la demanda de les universitats
- Manteniment de les dades de contacte i de context necessàries de les entitats destinatàries del servei

- Suport a la convocatòria de comitès i sales tècniques i a la gestió documental davant cibercrisis
- Generació i manteniment d'indicadors operatius i evolutius dels serveis prestats
- Anàlisi transversal i recurrent de la situació i exposició de les entitats de l'àmbit
- Preparació i presentació d'informes de seguiment dels serveis amb les universitats
- Suport en la realització de reunions de seguiment operatives amb les universitats
- Generació de memòries dels serveis a l'àmbit
- Suport per a l'impuls de la millora continua dels serveis per tal d'atendre les expectatives de les entitats.

En aquest sentit, el servei està composat per les següents àrees de treball:

- Suport a la gestió del coneixement, per tal de disposar de la informació de context necessària per a poder respondre de manera eficient a qualsevol ciberamenaça que afecti als actius de l'àmbit universitari.
- Suport a l'entrega de valor dels serveis recurrents prestats respecte del reptes assolits i els beneficis que representen, així com la generació d'un relat consolidat del grau d'exposició i resiliència de l'àmbit envers les principals ciberamenaces.
- Suport al seguiment de l'activitat gestionada i de línies de millora dels serveis, mitjançant reunions periòdiques i la presentació de quadres de comandament.

Aquestes activitats es faran seguint les directrius i procediments definits per l'Agència.

Aquest servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari es basa en els següents principis transversals que regeixen el seu disseny:

- El servei **focalitzarà** la seva capacitat en **donar suport al seguiment** dels serveis que prestin a les universitats.
- El servei ha de **garantir que els serveis disposen d'informació de context de qualitat** per facilitar la gestió i resposta adient a les ciberamenaces.
- El servei **potenciarà missatges de valor** respecte els resultats de l'activitat operativa de l'àmbit, alineats amb la seva aportació al negoci i l'eficiència de l'operació de la seguretat.

Finalment, es destaquen els objectius globals que el servei ha d'assolir en la seva prestació, tenint en compte l'orientació cap a resultats que s'espera:

- Situar el servei com a referent dins l'Agència per canalitzar qualsevol demanda referent a la prestació de serveis a de ciberseguretat acordats amb les entitats de l'àmbit.
- Establir els canals oportuns per **proveir coneixement i context** de l'àmbit a qualsevol altra equip operatiu del SOC/CERT o l'Agència que participi en la prestació de serveis a les universitats.
- Dissenyar i assistir en la implantació i millora de quadres de comandament estratègics i tàctics per facilitar la presa de decisions informada per part de l'Agència.
- **Controlar la qualitat** dels serveis prestats a l'àmbit, a partir de la revisió d'indicadors d'activitat, així com el seguiment i gestió de peticions, queixes i línies de millora identificades per les entitats de l'àmbit.
- Garantir la **ciberamenaça com a element vehicular** de l'activitat operativa vinculada a l'àmbit.

- **Donar suport en el seguiment** de la prestació de serveis de l'Agència amb les entitats de l'àmbit.

A continuació es detallen els elements, característiques i objectius de les àrees de treball del servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari.

3.2.1 Suport a la Gestió del Coneixement

La funció de gestió i coneixement tindrà com a principals funcions:

- la definició i el manteniment del model de dades operatiu i de context, la qual assegurarà una estructura sòlida i coherent per a la gestió de la ciberseguretat;
- la gestió de la informació del context operatiu, la qual integrarà les dades rellevants sobre l'entorn i les amenaces per millorar la presa de decisions en relació a l'àmbit; i
- la gestió de la informació operativa de ciberseguretat, la qual consolidarà i estructurarà les dades generades per les operacions de seguretat per garantir-ne la disponibilitat, traçabilitat i utilitat d'aquestes

Definició i manteniment del model de dades operatiu i de context

Cal definir i mantenir un model que permeti aconseguir el màxim valor de les dades de l'àmbit tractades per l'Àrea d'Operacions, en endavant l'AOS donant suport a tots els nivells possibles, des de la presa de decisions a la recerca de noves solucions i models d'operació de la seguretat alineats amb els objectius estratègics de l'Agència. El model s'haurà de poder exportar, homogeneitzar o ser compatible amb el tractament de dades d'altres àmbits.

La definició del model s'ha de dur a terme per respondre a aspectes rellevants sobre la pròpia gestió de la dada i el seu cicle de vida coordinadament amb el servei de suport a la governança de l'operació de l'AOS (qui estableix les directrius transversals aplicables a tots els àmbits). Aquesta activitat inclourà com a mínim inclourà les següents tasques:

- Identificació de la informació mínima requerida per garantir una correcta operació de la seguretat dels actius dins de l'abast, procurant estandarditzar la tipologia de dades per tots els actius de les mateixes característiques.
- Classificació i priorització de les dades requerides per l'AOS per acomplir les seves funcions operatives.
- Alineament amb els equips tècnics corresponents per assegurar que les bases de dades i repositoris de l'AOS inclouen tota la informació requerida.
- Identificació de les fonts origen considerades vàlides per la recollida de les dades d'interès i definició dels canals/fluxos/mètodes establerts per actualitzar-la.
- Identificació de responsables o propietaris de la informació de les fonts de dades definides.
- Definició de criteris per al manteniment i conservació de la informació, incloent el període d'actualització, vigència i/o retenció. Aquest criteris hauran de complir els requeriments normatius o legals que puguin limitar o determinar els mètodes de tractament d'acord amb les directrius que marqui l'àrea corresponent de l'Agència.
- Identificació de les persones, serveis de l'Agència o ens als quals donar accés a la informació, ja sigui de manera directa amb accés als repositoris de l'AOS (permisos de lectura o edició, depenent del cas), o compartint amb aquests contingut més estàtic i estructurat (p.ex. Fets rellevants, informes mensuals).

Actualment, l'Agència gestiona un entorn molt complex on conviuen una gran varietat d'entorns tecnològics i usuaris dels sistemes d'informació (incloent estudiants i personal de les pròpies entitats universitàries).

D'igual forma, l'Agència, disposa d'un inventari de solucions de ciberseguretat, que agrupa les diferents solucions de ciberseguretat desplegades per les entitats, el qual requereix un manteniment i actualització constant.

Per tot plegat, el servei licitat haurà de donar suport en la implementació dels mecanismes necessaris per assegurar que els equips que presten servei a l'àmbit disposin, en tot moment, d'informació complerta i rellevant sobre l'actualitat de l'àmbit que pugui condicionar les tasques operatives i el seu esdevenir.

Gestió de la informació operativa de ciberseguretat

Com a part de l'activitat operativa, les funcions de d'operació de la seguretat generen gran quantitat d'informació de valor. Aquesta funció haurà de perseguir i assegurar que els equips operatius que presten servei a l'àmbit registrin adequadament tots els esdeveniments de seguretat produïts i gestionats per la seva part, així com analitzar-los des de un punt de vista més tàctic per identificar possibles tractaments agregats, necessitats de creuament de dades, i en general facilitar el coneixement de la situació de seguretat de l'àmbit en tot moment.

Caldrà dur a terme el seguiment i millora continua del registre de l'activitat operativa de l'àmbit, essent necessari generar la informació diària de l'estat de seguretat dels actius i facilitar que sigui accessible de manera àgil per a les parts que es defineixin.

A tall d'exemple, s'haurà de disposar d'informació mínima de tots els atacs, incidents, amenaces i vulnerabilitats gestionades de l'àmbit, permetent identificar el més crític, tipologia, origen i actius afectats.

Caldrà generar i automatitzar els inventaris i la seva informació associada provinent de les diferents eines que continguin informació dels mateixos i la seva activitat operativa relacionada (eina de tiqueting, bases de dades internes, Consoles EDR, Filtrat de continguts, SIEM, entre d'altres) per tal de que estiguin actualitzats i siguin accessibles per a la resta dels serveis operatius o altres consumidors que es defineixin. Per fer-ho, el servei s'haurà de coordinar amb l'equip intern de l'AOS de l'Evolució de Solucions per garantir la definició d'un model de dades adient i la integració tecnològica adient per mantenir tots els registres necessaris en els repositoris de l'AOS.

Addicionalment, caldrà definir i implementar els processos i controls adients per garantir la qualitat de la informació generada per la pròpia operativa i el seu registre als repositoris de l'AOS.

3.2.2 Suport al Seguiment i Gestió de l'operativa de l'àmbit

La funció de suport al seguiment i gestió de l'operativa de l'àmbit tindrà com a principals funcions el disseny i manteniment dels models de relació operatius per garantir una col·laboració eficient, la consolidació de la prestació dels serveis recurrents de qualitat a l'àmbit, el suport a la definició i seguiment de processos, alhora que reforçarà el seguiment dels objectius estratègics i tàctics de l'Agència per a l'àmbit; i el suport davant esdeveniments puntuals de ciberseguretat, garantint una resposta efectiva i estructurada.

Totes aquestes activitats es faran seguint les directrius i procediments definits per l'Agència.

Disseny i manteniment de models de relació

Serà funció d'aquest servei la definició dels mecanismes adients que permetin assegurar la correcta comunicació entre els diferents equips operatius que presten servei a l'àmbit, així com garantir la compartició d'informació de manera bidireccional amb les parts que s'acordin.

Com a mínim, haurà d'encarregar-se de les següents activitats:

- Identificació de serveis, amb els que interaccionar de manera periòdica per compartir informació operativa o de context de l'àmbit.
- Identificació d'aspectes a tractar i informació a compartir amb cadascun dels serveis amb els que s'identifiqui interacció periòdica.
- Suport a la determinació dels fluxos i canals de comunicació a utilitzar entre les parts interessades, incloent la formalització d'un model de relació que s'haurà de mantenir actualitzat durant la prestació del servei.
- Manteniment de les metodologies i protocols propis del servei per assegurar el correcte desplegament del model de ciberseguretat de l'Agència a l'àmbit objecte de la prestació.

Suport en el seguiment d'objectius de l'àmbit

El servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari assistirà als responsables de serveis de l'Agència a vetllar per l'assoliment dels objectius que emanen de la demanda formalitzada pel CSUC per a l'entorn universitari. Per fer-ho, es destaquen les principals tasques a portar a terme:

- Conèixer els objectius estratègics i tàctics relacionats amb l'àmbit .
- Assistir en el desplegament del model de ciberseguretat de l'Agència, tot atenent les expectatives de l'àmbit.
- Vetllar pel correcte càlcul i alimentació de mètriques i indicadors de l'activitat gestionada i del seguiment dels seveis a l'àmbit.
- Vetllar per la correcta disposició de quadres de comandament que permetin la visualització del compliment dels objectius i facilitin la presa de decisions de manera senzilla i àgil a l'àmbit.
- Donar suport en el seguiment periòdic corresponent del nivell d'objectius assolits per identificar i informar amb prou antelació de possibles desviaments o riscos de no compliment d'aquests objectius.
- Promoure la realització de tasques entre els serveis operatius per acomplir els objectius definits en els terminis acordats.

Suport davant esdeveniments puntuals de seguretat

Serà funció d'aquest servei actuar com a reforç de les capacitats de gestió dels equips operatius de l'àmbit davant situacions puntuals que requereixin d'un seguiment especial o addicional per part de l'àrea d'operacions de seguretat.

A continuació es detallen les accions i funcions principals a desenvolupar per part d'aquest subservei, individualment i de forma transversal, seguint sempre les directrius de l'Agència

- **Gestió de crisis:**
  - Suport a la gestió organitzativa i documental dels comitès de crisi i sessions tècniques endegats per l'Agència en el marc de la resposta a ciberincidents.

- Registrar i donar visibilitat de forma eficient i amb llenguatge intel·ligible de les accions acordades entre els diferents equips operatius en els comitès de crisis, mitjançant els canals adients per a cada tipologia i que l'Agència determini (per exemple actes de reunió).
- Conèixer i fer ús avançat de les eines implicades en el procés de gestió de crisi, tant les que estiguin vigents en el moment de l'adjudicació del contracte com les que es puguin incorporar durant la vigència del mateix
- Proposar millores a la metodologia i processos de gestió de crisis de l'Agència de forma coordinada amb el servei de suport a la governança de l'AOS, el servei de resposta a incidents i els responsables dels serveis de l'Agència afectats.
- Suport a la gestió organitzativa i documental dels comitès de seguiment i sessions tècniques endegats per l'Agència en el marc de la gestió proactiva de ciberamenaces.

▪ **De forma transversal**:

- Participar en la gestió de casos i esdeveniments importants on l'Agència determini que la presència del servei és necessària, donat l'impacte a negoci que pot tenir una potencial amenaça o incident de seguretat a l'àmbit.
- Establir i implantar procediments de revisió i modificació continus (individuals o globals) sobre la informació/documentació/eines emprades per garantir que el servei que en proporciona sigui amb qualitat. Per exemple, disposar de la documentació tècnica i funcional d'un servei actualitzada a la darrera versió o determinar modificacions en la informació emmagatzemada als repositoris actuals.
- Proporcionar informes d'incidències sobre els serveis gestionats des de la vessant organitzativa, proposant els canals de comunicació adients per augmentar l'eficiència i l'agilitat extrem a extrem.
- Analitzar, de forma continuada, l'execució dels processos de gestió de crisi amb l'objectiu de detectar, proposar i implantar punts de millora en els propis processos, els procediments relacionats i les eines de gestió emprades, en l'àmbit del propi servei o fora del mateix.

3.2.3 Suport a l'Entrega de valor

Serà funció del present contracte definir, desenvolupar i generar els conjunt de mètriques, indicadors i lliurables que permetin a l'Agència presentar les fites assolides en l'àmbit universitari.

Per assolir aquest objectiu serà primordial que el servei disposi d'un coneixement clar de com interactuen i quina activitat generen els serveis operatius, per així aportar una visió integrada i coherent en la construcció i evolució dels indicadors, quadres de comandament i lliurables.

Les principals tasques que haurà de desenvolupar el present servei són:

- Definició de mètriques i indicadors estratègics, alineats amb els objectius de l'Agència per a l'àmbit seguint les directrius proporcionades per l'Agència.
- Explotar el valor de les principals mètriques i indicadors generats pels equips operatius, permetent avaluar la consecució dels objectius estratègics i tàctics per a l'àmbit. Aquestes mètriques s'han de poder calcular i consumir mitjançant les eines que es disposen des de l'Agència. Actualment l'eina de presentació d'indicadors utilitzada és Microsoft Power BI.
- Disseny, evolució i millora de quadres de comandament tàctics i estratègics, que permeti disposar per part de l'Agència una visió complerta de l'estat dels indicadors dels diferents serveis.

- Alineament amb la resta de serveis operatius que presten servei a l'àmbit i govern de la dada, per la implementació del càlcul d'indicadors i el desenvolupament dels quadres de comandament definits.
- Suport en la definició de les diferents plantilles de lliurables per presentar el benefici aportat a l'Agència i l'àmbit per part dels serveis.
- Establiment d'un procediment de *reporting* periòdic del valor aportat a les entitats de l'àmbit.
- Recolzament a la l'Agència en la presentació del valor afegit pels serveis prestats a l'àmbit, com a resultat de l'activitat gestionada pels equips operatius.

3.2.4 Volumetries actuals

Per proporcionar una referència per al correcte dimensionament del servei es proporcionen algunes dades de volumetries observades actualment a l'entorn d'universitats.

Concepte	Quantitat / any
Entitats amb model desplegat i en execució de serveis recurrents	9
Casos rebuts i gestionats pel SOC/CERT a l'àmbit	4.832
Matrius d'escalat gestionades	17
Informes d'activitat gestionada i rebuda	13
Memòria de l'activitat operativa de l'àmbit	1
Activació de Comitès de Crisi	4

Durant l'esdeveniment d'operatius de ciberseguretat s'haurà d'estar preparat per assumir l'activitat necessària per atendre a la prestació del servei segons les necessitats pròpies de l'operatiu, tant de capacitat com d'horari, sense que això suposi, en els primers cinc operatius anuals, un cost addicional per l'Agència.

3.2.5 Lliurables del servei

El model de prestació del servei haurà de contemplar la definició, els continguts i la periodicitat dels lliurables del servei. Entre els lliurables es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Producte	**Periodicitat**
Informe d'activitat gestionada i rebuda de l'àmbit	Mensual
Informe d'activitat gestionada i rebuda per entitat	Mensual
Informe de seguiment de l'estat del desplegament de perímetre de sistemes d'informació	Mensual
Informe de seguiment de l'estat del desplegament de perímetre de persones	Mensual
Informe de fonts integrades a l'àmbit	Mensual
Informe de situació del servei	Setmanal
Fets rellevants de l'àmbit	Diari

Producte	Periodicitat
Memòria de l'activitat operativa l'àmbit	Anual
Presentació executiva del valor aportat per una o conjunt d'activitats específiques	Puntual

La relació de productes, la seva periodicitat i la seva pròpia estructura i continguts s'hauran de definir en la fase inicial abans de la prestació del servei. Aquests podran canviar amb el temps i durant el període d'execució dels serveis que es liciten, d'acord als requisits definits per l'Agència de Ciberseguretat. Els canvis s'acordaran entre l'adjudicatari i la pròpia Agència de Ciberseguretat, garantint no generar un impacte greu en cap de les dues parts.

3.2.6 Mètriques i indicadors

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar pel contractista. L'Agència es reserva el dret de modificar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Mètrica	Descripció
Comitès de crisi gestionats	Nombre de comitès de crisi gestionats des del servei en el marc de la gestió d'incidents de seguretat a l'àmbit.
Sales tècniques gestionades	Nombre de sales tècniques que es gestionen des del servei entre els serveis del SOC i amb l'entitat afectada per incident
Fets rellevants publicats	Nombre de fets rellevants publicats des del servei
Informes lliurats	Nombre d'informes emesos
Seguiments operatius amb entitats	Nombre de sessions de seguiment amb entitats
Retorn del control de qualitat recurrent	Nombre de defectes/errors subsanats
Peticions de millora i queixes resoltes	Nombre de peticions de millora correctament analitzades, classificades, tramitades i finalitzades (solucionades o descartades)
Millores dels serveis proposades	Nombre de propostes de millores

Addicionalment als diferents lliurables que pugui generar el servei, aquest també haurà de ser capaç de calcular i facilitar a la capa de "Governança de l'operació de l'AOS", funció encarregada de la construcció d'indicadors del SOC, totes aquelles mètriques requerides. Previ a fer la petició, s'haurà de definir i analitzar la seva viabilitat, determinant les fonts necessàries i dades necessàries.

3.3 Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, el servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari té els següents elements essencials:

- El servei de suport a la gestió dels serveis de ciberseguretat prestats a l'àmbit universitari haurà de comptar amb capacitats de lideratge i relacional excel·lents, visió tàctica i operativa per donar suport en l'alineament de la prestació dels diferents serveis amb els objectius de l'Agència i les necessitats de l'àmbit. Són aspectes clau d'aquest servei la capacitat de supervisió, ordenació i priorització de les tasques operatives, així com la seva capacitat d'adaptabilitat i resiliència a situacions canviants.

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- La periodicitat de les reunions de punt de control i l'entrega de lliurables serà acordada prèviament amb l'Agència.
- La documentació dels processos, procediments operatius i eines del serveis es trobaran actualitzades en tot moment.
- Sota un enfocament centrat en l'amenaça, aquest servei haurà d'assegurar que totes les activitats de detecció, protecció, prevenció i resposta a l'àmbit estiguin enfocades a la priorització i resolució de les necessitats tàctiques derivades del panorama de les ciberamenaces.
- El nombre d'entitats dins l'abast dels serveis d'aquesta licitació es distribueix en les 8 universitats públiques de Catalunya i el CSUC.

4 Condicions d'execució del servei

4.1 Horaris

El servei de consultoria 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 part d'això, caldrà disposar d'un format de guàrdia de 24x7 per tal de fer front als possibles comitès de crisis que puguin aparèixer.

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. Aquestes tasques poden incloure activitats crítiques com ara orquestracions addicionals, operatius especials o comitès de crisi per fer front a ciberincidents. Sovint, aquestes accions s'han de dur a terme fora de l'horari habitual, ja que per la pròpia casuística dels esdeveniments o comitès, es duen a terme fora dels horaris estàndards. Així mateix, i tal i com s'ha esmentat, l'assistència a comitès de crisi també poden requerir intervencions en moments no laborables, especialment en entorns amb alts requeriments de seguretat i continuïtat operativa.

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.

4.2 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.

Addicionalment, i d'acord amb certes activitats crítiques a les quals aquest servei ha de donar resposta, tal i com s'ha esmentat a l'apartat anterior, 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.

4.3 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.
- Capacitat de treball sota pressió.
- 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.

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

L'adjudicatari disposarà d'una figura que assumirà les tasques de **cap de servei / coordinador.** A aquest efecte, ha de assumir les següents responsabilitats addicionals a les descrites a l'acord marc on s'emmarca el present basat:

- El cap de servei és el responsable de garantir que el servei és prestat a l'Agència en les condicions, forma i qualitat pactades i requerides per l'Agència. En cas necessari, el cap de servei haurà d'establir els mecanismes i punts de control per assolir aquest objectiu.
- Garantir la transparència en el control de gestió per tal d'agilitzar el procés de seguiment i facturació.
- Gestionar altes i baixes del personal de l'adjudicatari conforme els protocols de l'Agència.
- Garantir que els lliurables realitzats s'entreguen a l'Agència en forma i qualitat esperats.
- Coordinar les tasques operatives del servei.
- Reportar al Responsable del Servei de l'Agència els indicadors operatius i de risc del servei.
- Vetllar per la millora continua en els processos i lliurables del servei.
- Gestionar les reunions i els conflictes que puguin aparèixer durant l'execució dels serveis.
- Construir i gestionar el pla de capacitat del servei.
- Establir els mecanismes de control necessaris per garantir que la informació que genera el servei es mantingui actualitzada en el repositori d'informació de l'Agència.

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.

4.3.1 Hores de dedicació

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **1.506 hores totals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes pels perfils indicats:

Perfil	Serveis recurrents
Consultor amb més de 3 anys d'experiència (1 FTE a un 100% de dedicació i 1 FTE amb almenys al 50% de dedicació)	**1.506 hores**

4.3.2 Perfils

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

PERFIL	REQUISITS
Consultor de ciberseguretat amb més de 3 anys d'experiència	Experiència professional mínima de 3 anys en projectes o serveis de ciberseguretat. Titulat universitari en l'àmbit de la Ciberseguretat, de les Tecnologies de la Informació i la Comunicació (TIC) o en altres disciplines que aportin competències directament aplicables. Haver participat i poder demostrar la seva involucració en mínim un projecte en els que hagi desenvolupat les següents funcions: • Lideratge de projectes o equips de treball multidisciplinars. • Gestió i operació de serveis de SOC. • Elaboració d'informes executius, incloent la definició i implantació de quadres de comandament, els quals incorporen visions estratègiques, operatives i tàctiques. • Definició i desplegament de processos de gestió de la seguretat. • Definició, implantació i automatització d'indicadors de servei, especialment en l'àmbit de la ciberseguretat. • Coneixements en: - Definició de projectes (metodologies, processos, eines, lliurables). - Eines de BI, especialment Microsoft PowerBI. - Eines de generació i presentació d'informació per fer més eficient la comunicació i presa de decisions. - Principals vulnerabilitats i defectes a les que poden estar subjectes infraestructures, plataformes i aplicacions, així com les propostes de mitigació cost/efectivitat més adients. - Principals amenaces i vectors d'atac que afecten a les organitzacions (per exemple, el catàleg d'amenaces que proposa l'organització NIST). • Suport i coordinació en la gestió de crisis i gestió de conflictes

PERFIL	REQUISITS
	• Suport administratiu en la planificació i formalització d'actes de reunions. • Habilitats comunicatives avançades i capacitat de coordinació i interlocució amb altres equips.

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei.

4.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat 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 basat. 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.

4.5 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 basat 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 basat ho requereix, aquest aspecte es podrà concretar en el contracte basat.

4.6 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. El licitador 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 l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

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

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

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

4.7 Gestió del coneixement

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

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.

4.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació:

- 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.
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics 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).

A la finalització del contracte, l'adjudicatari del contracte basat 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.

4.9 Control de Gestió

L'empresa adjudicatària del contracte basat, 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.

4.10 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.

El responsable 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

4.11 Contingència

L'adjudicatari haurà 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 del licitador, 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.

4.12 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 basat.

4.13 Seguretat

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

4.13.1 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 basat, 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.

4.13.2 Dades de caràcter personal

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

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

L'empresa adjudicatària del contracte basat 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 basat 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 basat el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte basat 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 basat 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 basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

4.13.4 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte basat 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 basat 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.

4.13.5 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), 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 basat haurà de garantir que disposa dels perfils amb la capacitació 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 capacitació 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.

4.13.6 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte basat 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 basat 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 basat 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.

4.13.7 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 basat 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.

4.13.8 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 basat 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 basat 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.

4.13.9 Accés a la informació

L'empresa adjudicatària del contracte basat 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.

4.13.10 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), 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.

4.14 Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment. 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 basat, 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 basat.
- Un informe de dedicació del basat 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 basat, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir o el termini d'implantació). 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 basat o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Si existeix cap especificitat en aquest sentit, es recollirà al basat corresponent.

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 basat 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.

4.15 Integració amb altres equips

L'adjudicatari del contracte basat 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, amenaces), 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.