Generalitat de Catalunya
Centre de Telecomunicacions i Tecnologies de la Informació

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS QUE REGEIX LA CONTRACTACIÓ DELS SERVEIS DE COMPUTACIÓ SOBRE UNA REGIÓ DE NÚVOL PÚBLIC SOBIRÀ A CATALUNYA

Expedient núm.: CTTI-2026-111

ÍNDEX DE CONTINGUTS

1 ANTECEDENTS I CONTEXT DE LA NECESSITAT

El CTTI, d'acord amb l'article 2.1 de la Llei 15/1993, de 28 de desembre, per la qual es crea el Centre de Telecomunicacions de la Generalitat de Catalunya i l'article 4.1 dels Estatuts del CTTI, recollits en el Decret 26/1999, de 9 de febrer, pel qual s'aprova l'Estatut del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya, té entre d'altres funcions:

- La planificació tècnica i l'establiment de les directrius de la gestió i explotació dels sistemes de telecomunicacions i informàtics que siguin necessaris per al funcionament de la Generalitat.
- La coordinació, la supervisió i el control de l'execució dels sistemes i dels serveis de telecomunicacions i d'informàtica aptes per a satisfer les necessitats de l'Administració de la Generalitat de Catalunya en aquesta matèria.
- La realització de la gestió de forma directa o indirecta de l'execució de les infraestructures necessàries per implantar les xarxes i els serveis de telecomunicacions i informàtics requerits i la seva explotació i manteniment posteriors.
- L'establiment i la fixació de les especificacions tècniques dels terminals d'usuaris en l'àmbit de les telecomunicacions i la informàtica per garantir-ne la correcta connectivitat a les xarxes.

Mitjançant l'Acord de Govern GOV/144/2011, de 18 d'octubre, s'encarregà al Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (en endavant el CTTI) la provisió centralitzada i la gestió de solucions TIC de l'Administració de la Generalitat de Catalunya i el seu sector públic.

Així mateix, l'Acord de Govern GOV/169/2024, de 30 de juliol, actualitza el model de relació entre el Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya i l'Administració de la Generalitat de Catalunya i el seu sector públic en relació amb la provisió centralitzada i la gestió de solucions TIC.

En compliment d'aquest mandat, actualment, el CTTI disposa dels contractes de serveis de CPD següents:

Contracte	Serveis	Proveïdor	Termini
CTTI/2023/8/1-PRO-1	Serveis de cloud computing (cloud privat i cloud públic) Serveis de gestió de projectes *(prestats en cada contracte a diferents departaments i organismes)*	T-SYSTEMS ITC IBERIA, S.A.U.	01/04/25 - 31/03/27
CTTI/2023/8/2-PRO-1		UTE KYNDRYL SEIDOR	01/04/25 - 31/03/27
CTTI/2023/8/3-PRO-1		UTE KYNDRYL SEIDOR	01/04/25 - 31/03/27
CTTI/2023/8/4-PRO-1		T-SYSTEMS ITC IBERIA, S.A.U.	01/04/25 - 31/03/27
CTTI-2019-20148-1	Serveis de plataforma Mainframe	KYNDRYL ESPAÑA, S.A.	04/06/20 - 3/06/26
CTTI-2019-20148-2	Serveis de cloud computing (cloud privat)	T-SYSTEMS ITC IBERIA, S.A.U.	04/06/20 - 3/06/26

En aquestes contractacions s'estableix un mecanisme d'ajust contractual que regula les condicions i procediments pels què l'empresa adjudicatària de cada lot juntament amb el CTTI, haurà de migrar les agrupacions tecnològiques construïdes en base als serveis sol·licitats, a l'adjudicatari o adjudicataris del futur model de serveis de CPD, el qual es projecta amb el present Acord Marc.

Cal tenir en compte que en un món digital, on l'evolució tecnològica és constant i contínua, el consum de serveis de computació al núvol són un instrument estratègic per acompanyar els programes de transformació digital i tecnològica de les organitzacions. L'adopció del paradigma de computació al núvol no només permet optimitzar recursos i reduir costos, sinó que també impulsa la innovació i millora l'eficiència operativa, garanteix major flexibilitat, facilita l'escalabilitat de les solucions, millora la seguretat i resiliència de les infraestructures digitals i facilita una gestió més eficient de les dades. Paral·lelament, la computació al núvol implica una major gestió de les dependències tecnològiques i geopolítiques.

En aquest sentit, l'Acord de Govern 64/2025, de 18 de març, pel qual s'aprova el Marc estratègic d'impuls de la implantació i el desenvolupament de centres de dades a Catalunya, posa de relleu la necessitat creixent d'emmagatzematge i processament d'informació, així com la seva gestió de manera segura i més sostenible econòmicament, socialment i mediambientalment, i que entre els diferents eixos d'actuació defineix aspectes i accions específiques, com per exemple:

- La coordinació estratègica de projectes, amb l'objectiu que Catalunya disposi de centres de dades multi-propòsit, atesa la tipologia diversa de serveis, com poden ser les infraestructures científiques i tècniques singulars, la intel·ligència artificial o l'accés a núvols públics o privats impulsats per companyies i operadors tecnològics.
- Coordinar la planificació i l'impuls de les infraestructures digitals necessàries per al desenvolupament adequat d'un ecosistema de centres de dades a Catalunya.
- Promoure l'atracció d'inversions empresarials que generin valor econòmic al territori i llocs de treball qualificats.
- Orientar el foment de les inversions en centres de dades a Catalunya amb l'objectiu d'impulsar la sobirania tecnològica quant a emmagatzematge i processament de dades a diferents escales i abast (Europa, Estat espanyol i Catalunya), perquè Catalunya disposi d'un ecosistema de centres de dades per als diferents propòsits i necessitats de processament, latència i especialització en objectius de computació, especialment d'intel·ligència artificial i d'altres tecnologies digitals avançades.
- Aprofitar la capacitat de compra pública del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya per atraure inversions per part de les companyies tecnologies que presten servei a la Generalitat de Catalunya en centres de dades o ubicacions de les seves regions de núvol públic o privat, com a condició necessària en el marc de la sobirania de les infraestructures digitals.

Per tant, és imprescindible que la Generalitat de Catalunya disposi d'una estratègia pròpia per a la provisió, adopció i ús de solucions (serveis, plataformes i infraestructures digitals) de núvol per a la migració, modernització i creació de sistemes i aplicacions, imprescindibles per a la provisió de serveis digitals de l'Administració.

L'estratègia sobre la provisió, adopció i ús del núvol per a la millora i modernització dels serveis digitals, i per assegurar l'autonomia en la seva governança, determina les diferents modalitats de núvol aplicables a la Generalitat de Catalunya i el seu Sector Públic, així com els seus criteris d'aplicació.

L'estratègia és multi-núvol i contempla les següents modalitats:

- **Núvol públic**, on tota la infraestructura és propietat i està gestionada per un proveïdor extern privat, que ofereix serveis a través d'una plataforma digital per al desenvolupament, manteniment i evolució dels sistemes i aplicacions. En aquesta modalitat, els recursos de computació són compartits i abstrets per prestar servei a múltiples organitzacions. D'aquesta manera, hi ha una responsabilitat compartida en la gestió, atès que el proveïdor es responsabilitza del manteniment, continuïtat, actualització i evolució de tota la infraestructura tecnològica, així com de la seguretat de la plataforma, alhora que ofereix un catàleg de serveis al núvol amb preu públic per facilitar el desenvolupament i l'escalabilitat dels sistemes i aplicacions. D'altra banda, l'organització que l'utilitza es responsabilitza de la configuració dels serveis, del codi de les aplicacions que hi allotja i del seu ús.
- **Núvol privat**, amb els recursos de computació dedicats exclusivament a una única organització, i que pot estar allotjat en un centre de dades propi o instal·lacions d'un proveïdor especialitzat, però sempre amb un accés restringit a l'organització propietària. Normalment té un catàleg de serveis més reduït que un núvol públic i disposa d'infraestructura pròpia o gestionada per tercers, permetent un control total sobre les polítiques de seguretat, compliment normatiu i protecció de dades.
- **Núvol públic sobirà**, que ofereix els avantatges d'un núvol públic (escalabilitat, flexibilitat, eficiència i prestacions funcionals) però amb un major control sobre la gestió de les dades, la seguretat i el compliment normatiu, garantint que les dades s'emmagatzemen en el marc de la Unió Europea respectant la regulació sobre protecció de dades, impedint que empreses o governs estrangers hi tinguin accés sense autorització, operat per entitats locals o en col·laboració amb proveïdors de núvol global sota regulacions estrictes, assegurant el compliment de normatives específiques per a sectors sensibles com la sanitat, la defensa o l'administració pública, i habilitant com a mínim una regió a Catalunya.

A nivell europeu s'han desenvolupat un conjunt de normatives vigents que afecten als serveis al núvol. Aquestes normatives europees com el General Data Protection Regulation, la Data Act, la Cybersecurity Act o la AI Act, es complementen amb iniciatives comunitàries com GAIA-X (amb l'objectiu de crear una infraestructura de dades interoperable i segura), i l'EU Cloud Rulebook (l'harmonització de les regles que afectes els serveis de núvol a Europa) entre d'altres, que permeten habilitar una major sobirania digital a diferents nivells.

El desplegament d'aquesta estratègia multi-núvol híbrida, habilitant i incorporant la modalitat de núvol públic sobirà, connectat a les infraestructures de la Generalitat de Catalunya, és clau per assegurar la continuïtat dels serveis crítics, la protecció de les dades de l'administració pública, la capacitat d'innovació i el lideratge tecnològic dins l'espai europeu per part de Catalunya. Aquest model redueix la dependència tecnològica i els riscos associats, reforça la seguretat digital i, com a valor afegit, impulsa la creació d'un ecosistema d'empreses, talent i recerca al voltant de la tecnologia de núvol i la intel·ligència artificial.

A més, la implementació de l'estratègia planteja avantatges operatius i econòmics, atès que les empreses proveïdores de serveis de núvol públic incorporen de manera ràpida i continuada les innovacions tecnològiques i les plataformes d'intel·ligència artificial, fet que permet al sector públic accedir a capacitats d'alt valor afegit i facilitant un ús racional i eficient dels recursos públics, ja que ajusta la despesa al consum real i fomenta la sostenibilitat econòmica de les infraestructures TIC.

En un exercici de transparència d'aquesta estratègia el CTTI va realitzar una consulta preliminar al mercat per contrastar respecte la viabilitat d'implantar una regió de núvol públic sobirà a Catalunya (CPM-2025-002). En el marc d'aquesta consulta es van definir tots els requeriments considerats essencials que ha de satisfer una infraestructura de núvol públic sobirà a Catalunya. Aquests requeriments es van agrupar en diferents famílies que cobrien tots els aspectes necessaris per assolir l'estratègia definida, com per exemple, requeriments de seguretat, de compliment normatiu, territorials, de govern i control, de connectivitat i de resiliència.

Els resultats de la consulta van evidenciar l'interès, la capacitat i les perspectives dels agents econòmics, i van ratificar la viabilitat d'una licitació d'una regió de núvol públic sobirà a Catalunya.

Per tal de donar compliment als projectes del Govern, el CTTI ha desenvolupat aquesta licitació, mitjançant Acord Marc, per donar resposta a una part del nou model de CPD, en concret tots els serveis d'infraestructura de núvol públic sobirà

Per tant, la present licitació ha de garantir els serveis objecte de la mateixa, la prestació dels quals és essencial pel correcte funcionament del serveis que presta la Generalitat de Catalunya i el seu sector públic a la seva ciutadania, així com evolucionar els serveis de CPD amb els objectius estratègics de la Generalitat de Catalunya.

2 OBJECTE DE LA LICITACIÓ

El present Acord Marc (AM) té com objecte l'homologació d'un proveïdor per a la prestació dels serveis de núvol públic per a la Generalitat de Catalunya i el seu sector públic sobre una regió de núvol públic sobirà europeu a Catalunya.

Una regió de núvol públic sobirà és una infraestructura de serveis al núvol situada dins del territori català que garanteix la gestió, el control i la supervisió dels recursos per part d'una entitat subjecta íntegrament a la regulació europea. Aquesta regió evita dependències de proveïdors o matrius situades fora de la Unió Europea, assegurant la sobirania tecnològica, l'autonomia de gestió, la seguretat, el compliment normatiu i la sostenibilitat mediambiental. Els serveis que s'hi ofereixen són multi-client (multi-tenant), aïllats i protegits entre ells, amb garanties d'alta disponibilitat i utilització majoritària de programari de codi obert per afavorir la independència tecnològica.

Aquests serveis de núvol públic sobirà es prestaran en les següents modalitats:

- Serveis de cloud computing
    - Provisió de serveis de cloud computing, basats en infraestructures d'ús públic, sobre les que la Generalitat de Catalunya pugui disposar d'un o varis espais de treball propis (tenants propis) sobre els quals pugui desplegar les seves solucions TIC adaptades a les necessitats de la Generalitat de Catalunya, aplicant els marcs de govern TIC i les mesures de seguretat de sobirania i autonomia requerides.
- Serveis de facilitació
    - Provisió de serveis per facilitar la implantació de solucions TIC sobre els serveis de cloud computing (Núvol Públic Sobirà)
        - Serveis d'assessorament
        - Serveis de suport tècnic
        - Serveis de formació

3 DESCRIPCIÓ DELS SERVEIS A PRESTAR

Els serveis a prestar son:

- Serveis de cloud computing
- Serveis de facilitació

3.1 Serveis de cloud computing

En aquest apartat es presentaran de manera detallada els requeriments específics que han de complir tant la pròpia regió de núvol públic sobirà com els serveis que aquesta haurà de prestar. A més, s'inclouran els requisits que han de satisfer tant el licitador com tots els actors de l'ecosistema de la regió de núvol públic sobirà implicats, amb l'objectiu d'assegurar la plena sobirania de la regió i garantir el compliment dels estàndards i les directrius establertes per la Unió Europea.

Els requeriments definits per als serveis de la regió de núvol públic sobirà estan totalment alineats amb el *Cloud Sovereignty Framework*[1] de la Unió Europea, així com amb la normativa sobre la qual s'ha de regir la construcció de la regió. Aquesta alineació garanteix que tant els controls de govern com la gestió de la infraestructura de la regió i els serveis respecten els estàndards europeus, assegurant la protecció de dades, la transparència i la independència respecte a entitats externes a la UE. D'aquesta manera, la solució proposada dona resposta a les exigències de seguretat, control regulador i sobirania digital que estableixen les directrius europees.

Per aquest tipus d'infraestructures i serveis, l'UE estableix cinc nivell de sobirania:

Sovereignty Effective Assurance Levels	**Descripció**
SEAL-0	**Sense sobirania**: Servei, tecnologia o operacions sota control exclusiu de tercers no pertanyents a la UE, governats completament en jurisdiccions no pertanyents a la UE.
SEAL-1	**Sobirania jurisdiccional:** la legislació de la UE s'aplica formalment amb una aplicabilitat pràctica limitada; servei, tecnologia o operacions sota control exclusiu de tercers no pertanyents a la UE.
SEAL-2	**Sobirania de dades:** Dret de la UE aplicable i exigible, amb dependències materials no pertanyents a la UE restants; servei, tecnologia o operacions sota control indirecte de tercers no pertanyents a la UE.
SEAL-3	**Resiliència digital**: Dret de la UE aplicable i exigible, actors de la UE que exerceixen una influència significativa però no plena; servei, tecnologia o operacions sota control marginal de tercers no pertanyents a la UE.

[1] https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en

Sovereignty Effective Assurance Levels	Descripció
SEAL-4	**Sobirania digital completa:** tecnologia i operacions sota el control total de la UE, subjectes només a la legislació de la UE, sense dependències crítiques fora de la UE.

L'aplicació del mencionat framework aportarà un sòlid resultat doncs complementa el conjunt de requeriments tecnològics concrets de la licitació amb les salvaguardes específiques del grau de sobirania requerit.

El conjunt de requeriments i salvaguardes de sobirania s'estructuren en les següents famílies:

Família	Objectiu de sobirania	Funció de l'objectiu
EST	Sobirania estratègica	Avaluar el grau en què els serveis d'un proveïdor de núvol estan ancorats dins de l'ecosistema legal, financer i industrial de la Unió Europea. Avalua l'estabilitat de la propietat, la influència en la governança i l'alineació amb les prioritats estratègiques de la UE.
LEG	Sobirania legal	Avaluar l'entorn legal, l'exposició a autoritats estrangeres i l'aplicabilitat dels drets que regeixen els serveis d'un proveïdor de núvol. Determina fins a quin punt els serveis estan ancorats en la jurisdicció europea i aïllats de reclamacions legals externes.
DIA	Sobirania de la dada i algorísmia IA	Avaluar el focus en la protecció, el control i la independència dels actius de dades i els serveis d'IA dins de la UE. Aborda com es protegeixen les dades, on es processen i el grau d'autonomia que els clients conserven sobre les capacitats d'IA.
OPE	Sobirania operacional	Avaluar i mesurar la capacitat pràctica dels proveïdors de núvol per gestionar, donar suport i desenvolupar una tecnologia independentment del control no europeu. Se centra en la continuïtat de les operacions, la disponibilitat de competències i la resiliència contra les dependències externes.
TEC	Sobirania tecnològica	Avaluar el grau d'obertura, transparència i independència de la pila tecnològica subjacent, garantint que els actors de la UE puguin interoperar, auditar i desenvolupar solucions sense estar lligats a sistemes propietaris estrangers.
SEG	Sobirania de seguretat i compliment	Avaluar i mesurar fins a quin punt les operacions de seguretat, les obligacions de compliment i les mesures de resiliència es controlen dins de la UE, garantint la independència de jurisdiccions estrangeres i la garantia operativa a llarg termini.

Família	Objectiu de sobirania	Funció de l'objectiu
MED	Sostenibilitat mediambiental	Avaluar l'autonomia i la resiliència dels serveis al núvol a llarg termini en relació amb el consum d'energia, la dependència i l'escassetat de matèries primeres.

En el moment d'activació de la regió de núvol públic sobirà, l'empresa homologada haurà de demostrar de manera exhaustiva i verificable l'assoliment dels objectius de sobirania definits per al nivell SEAL-3 per a totes les famílies de sobirania indicades (Estratègica, Legal, de la Dada i Algorísmia IA, Operacional, Tecnològica, de Seguretat i Compliment, i Sostenibilitat Mediambiental).

Reconeixent que el concepte de SEAL-3 pot implicar que el dret de la UE sigui aplicable i exigible amb una influència significativa d'actors de la UE, però amb un control marginal de tercers no pertanyents a la UE sobre servei, tecnologia o operacions, s'acceptaran propostes que per a aquells aspectes específics que puguin presentar un repte per a l'acompliment estricte del SEAL-3 en la seva màxima expressió, demostrin mecanismes clars i controls compensatoris eficaços per assegurar la protecció dels objectius de sobirania definits per a cada família.

Aquests mecanismes hauran de garantir que, malgrat possibles dependències tecnològiques o operatives marginals fora de la UE, les dades i les operacions crítiques romanen sota control i jurisdicció europea, sense comprometre la seguretat, la resiliència digital ni la protecció de dades de la Generalitat de Catalunya.

Serà necessària la presentació d'una anàlisi de riscos detallada per a qualsevol excepció proposada, juntament amb les mesures de mitigació corresponents.

3.1.1 Requeriments de sobirania estratègica

ID-Req	Descripció del requeriment
EST-01	L'empresa homologada haurà de garantir que la gestió efectiva, el control i l'accés a les dades i sistemes de la regió de núvol públic sobirà es realitza exclusivament des de la jurisdicció de la UE, mitjançant personal ubicat a la UE i subjecte a la legislació europea. Es permetrà la intervenció d'actors o personal amb seu fora de la UE per a funcions de suport especialitzat (p. ex., desenvolupament de producte o suport de nivell 3 del fabricant) sempre que es demostrin mecanismes clars i eficaços de separació, control, auditabilitat i aprovació explícita per part de la Generalitat de Catalunya, assegurant que en cap cas es pugui accedir a dades de client o a controls crítics de la infraestructura sense autorització i sota la supervisió d'entitats de la UE, i que qualsevol accés es realitzi d'acord amb la legislació de la UE.
EST-02	Com a mínim dos centres de procés de dades (CPD) de la regió de núvol públic sobirà han d'estar ubicats dins del territori de Catalunya, i han de complir amb les característiques de Tier III. Aquests CPD's podran ser propis de l'empresa homologada o subcontractats a altres proveïdors. En cas de subcontractació, l'empresa homologada haurà de demostrar la capacitat de mantenir el control total sobre la sobirania de la regió de núvol desplegada sobre aquests CPDs, incloent la gestió de les dades i l'operació, d'acord amb els requisits de sobirania d'aquesta licitació.
EST-03	La regió de núvol públic sobirà proposada ha de tenir connexió amb una altre regió pública sobirana del propi licitador (regió addicional), ubicada a Europa i fora del territori de Catalunya, amb la mateixa base tecnològica i que acompleixi els requisits d'aquesta licitació. En cas que, a la data d'adjudicació, la regió addicional no acompleixi la totalitat d'aquests requisits, l'empresa homologada disposarà d'un termini màxim de 24 mesos per remeiar-ho. Aquesta regió addicional no pot estar connectada a regions cloud no sobiranes fora de la Unió Europea, i s'haurà d'evidenciar que disposa de comercialització activa en el moment de la publicació de la present licitació. Aquest model segueix les millors pràctiques d'arquitectures resilients i amb alta disponibilitat dels grans proveïdors de serveis de núvol públic (Amazon, Microsoft, Google, etc.), i per tant garanteix una arquitectura multi-regió robusta i provada del núvol públic sobirà. Aquesta estratègia permetrà a la Generalitat de Catalunya: • Assegurar la continuïtat del servei, garantint que els serveis crítics es mantinguin actius i les dades de l'Administració Pública protegides fins i tot davant fallades que afectin tota la regió catalana. • Optimitzar l'operativa mitjançant l'ús d'una base tecnològica idèntica a totes les regions que facilita l'automatització i la gestió eficient.

ID-Req	Descripció del requeriment
	• Garantir la sobirania i seguretat, mantenint totes les dades i operacions dins de la Unió Europea, reduint els riscos geopolítics i assegurant el compliment normatiu.
EST-04	La regió de núvol públic sobirà ha d'estar formada per un mínim de 3 zones de disponibilitat i 2 CPD's físics (d'acord a requisit EST-02), que han de permetre que els serveis s'executin en modalitat actiu-actiu-actiu (els que tècnicament ho permetin) o actiu-passiu amb failover automàtic els que no. El CPD que disposi de 2 de les 3 zones de disponibilitat tindrà la categorització de CPD primari. Les 3 zones de disponibilitat han de permetre a serveis que requereixen d'arbitratge per a seleccionar el màster, poder executar-se amb les recomanacions dels fabricants de la plataforma de programari subjacent.
EST-05	L'empresa homologada facilitarà accés al seu full de ruta de l'estratègia del núvol públic sobirà: • Proporcionar accés al full de ruta del catàleg de serveis (API i portal). • Notificar l'actualització de versió amb la informació necessària. • Disposar de calendaris d'actualitzacions i canvis planificats.
EST-06	El catàleg de serveis de la regió de núvol públic sobirà ofertada tindrà com a mínim les mateixes capacitats i funcionalitats que el catàleg de serveis de la regió addicional (EST-03) en el moment de la publicació de la present licitació. Caldrà aportar url d'accés a dit catàleg de serveis.
EST-06	La llista de preus del catàleg de serveis de la regió de núvol públic sobirà haurà de ser pública, amb preus equivalents a la regió addicional, i el percentatge de l'increment anual de preus no podrà superar el percentatge de l'increment mig dels núvols públics que operen en territori europeu.
EST-07	L'empresa homologada ha d'incorporar nous serveis, funcionalitats o tecnologies emergents al catàleg de serveis de forma regular.
EST-08	El licitador considerarà i facilitarà una estratègia de migració progressiva des de tecnologies o serveis actualment basats fora de la Unió Europea cap a alternatives de solucions i plataformes europees quan aquestes estiguin disponibles i que compleixin els requisits de qualitat, seguretat, escalabilitat i sostenibilitat exigits. Aquesta orientació s'emmarca en la voluntat de reforçar la sobirania digital, la resiliència tecnològica i l'autonomia estratègica europea, i no té com a objectiu limitar la llibertat tecnològica dels licitadors ni condicionar la seva participació en el procediment. La coexistència temporal de solucions de diferents orígens i l'adopció gradual de noves tecnologies s'entenen com a escenaris raonables dins d'un procés d'evolució tecnològica. Els licitadors descriuran com les seves propostes contribueixen a aquest objectiu a mitjà o llarg termini, aportant una visió alineada amb els principis de sobirania digital i d'ecosistema tecnològic europeu.

3.1.2 Requeriments de sobirania legal

ID-Req	Descripció del requeriment
LEG-01	La gestió de la infraestructura i els serveis del núvol estaran sota el control d'una entitat sotmesa als aspectes jurídics i regulatoris europeus, evitant dependències operatives o legals que puguin permetre a jurisdiccions o matrius situades fora de la Unió Europea accedir a dades o sistemes sense autorització conforme a la legislació de la UE (p. ex. Cloud Act EEUU). Pel que fa a les operacions de desenvolupament de plataforma i enginyeria de producte, el licitador haurà de demostrar mesures de control, segregació i auditabilitat que impedeixin l'accés no autoritzat a dades de clients per part de personal no subjecte a la jurisdicció de la UE i garantir que qualsevol intervenció externa estigui supervisada i aprovada per entitats basades a la UE, assegurant que les dades sensibles del client romanen protegides dins la jurisdicció de la UE.
LEG-02	Ha de complir el Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya, disponible al Portal de Seguretat de l'Agència de Ciberseguretat de Catalunya.
LEG-03	En cas de conflicte entre el model operatiu estàndard d'un núvol públic global (autoservei intern, escalats internacionals, recursos distribuïts) i els requisits de sobirania locals, prevaldran els criteris de sobirania (GDPR/NIS2/ENS). Això implica que l'arquitectura i els processos del tenant s'adaptaran per bloquejar qualsevol operació que contravingui la localització UE (p. ex. segmentant entorns o aplicant controls de sortida de dades). Totes les disputes i interpretacions s'abordaran donant prioritat al compliment de la normativa comunitària i nacional de seguretat sobre disposicions de proveïdors internacionals El licitador haurà de garantir i evidenciar que les operacions crítiques del servei, incloent l'accés a dades de client, la gestió d'incidències i el manteniment de la infraestructura, es realitzen exclusivament des de territori europeu i sota la legislació de la UE. Per a les operacions de desenvolupament de plataforma i enginyeria de producte, el licitador haurà de demostrar mesures de control i segregació que assegurin la no-exposició a jurisdiccions o entitats fora de la UE.
LEG-04	Ha de disposar de les certificacions següents: ISO 9001, ISO 22301, ISO 27001, 27017 i 27018. Per a les instal·lacions de centre de procés de dades (CPD's), haurà de complir amb les característiques de Tier III i aportar la certificació EN 50600 o una acreditació equivalent reconeguda internacionalment que acrediti el compliment d'estàndards de disseny i operació de centre de dades.

3.1.3 Requeriments de sobirania de la dada i algorísmia IA

ID-Req	Descripció del requeriment
DIA-01	Ha de garantir l'estricte confinament de l'emmagatzematge i el processament a jurisdiccions europees, sense recurs a tercers països de fora de la UE.
DIA-02	Ha de garantir que només el client, no l'empresa homologada, tingui el control efectiu sobre l'accés criptogràfic a les seves dades.
DIA-03	Ha de facilitar la visibilitat de quan, on i qui accedeix a les dades, inclosa l'auditabilitat de l'ús del model d'IA, mecanismes que garanteixin l'eliminació irreversible de les dades, amb proves verificables.
DIA-04	El catàleg de serveis d'IA haurà d'incloure i prioritzar models de llenguatge grans (LLM) de codi obert i/o desenvolupats per proveïdors amb operació sobirana a la UE. El licitador podrà proposar mecanismes per a la integració segura i sobirana de models d'IA de 'líders de mercat ' (no necessàriament d'origen UE) sempre que es garanteixi que el processament d'inferència i de dades es realitza exclusivament dins de la infraestructura de la regió sobirana i sota control jurídic de la UE. Igualment, quan s'utilitzin models o tecnologies d'IA originàries de fora de la UE, el licitador haurà de demostrar la seva integració al serveis de la regió sobirana i operació de manera que s'asseguri un control efectiu per part d'entitats de la UE i la minimització de dependències que puguin comprometre la sobirania de les dades.
DIA-05	Per als serveis d'Intel·ligència Artificial, el licitador ha de garantir que la inferència i, si escau, l'entrenament o fine-tuning de models que utilitzin dades del client, es realitzen íntegrament dins la infraestructura de la regió de núvol sobirana a la UE, sota la legislació europea. L'entrenament de models des de zero fora de la infraestructura de la regió de núvol sobirana, no serà excloent per als models fonamentals pre-existents, sempre i quan no utilitzin dades de client per l'entrenament.

3.1.4 Requeriments operacionals

ID-Req	Descripció del requeriment
OPE-01	Ha de garantir que el suport operacional de nivell 1 i 2, i la gestió de la infraestructura i els serveis, sigui realitzat per operadors ubicats dins de la UE i subjectes a la legislació de la UE. Per al suport de nivell 3 o d'enginyeria de producte, es requeriran plans detallats per a la minimització de la dependència de recursos no comunitaris i la demostració de salvaguardes robustes que impedeixin l'accés no autoritzat a dades o sistemes per part de personal fora de la UE.
OPE-02	Ha d'assegurar l'existència de talent amb l'experiència per operar i mantenir el servei, i que pertanyin a empreses amb seu a la UE.

ID-Req	Descripció del requeriment
OPE-03	Ha de garantir que el suport operatiu que impliqui accés a dades de client o control de la infraestructura es realitzi exclusivament des de dins de la UE, sota control d'entitats subjectes a la legislació de la UE. Per a casos excepcionals que puguin requerir assistència de personal extern a la UE (per exemple, per a la resolució d'errors de programari de fabricant), s'hauran d'implementar mecanismes de control estricte, traçabilitat completa i aprovació prèvia del CTTI, garantint que cap dada sensible abandoni la jurisdicció de la UE.
OPE-04	Disponibilitat de documentació tècnica completa i coneixements operatius que permeten l'autonomia d'operació a llarg termini.
OPE-05	Els serveis consumits han de poder garantir una disponibilitat mínima del 99.95%

OPE-06	Ha de disposar de mecanismes d'observabilitat i telemetria dels serveis contractats en formats oberts i interoperables que facilitin la integració amb els sistemes d'observabilitat existents a CTTI, incloent:
	• Suport explícit i obligatori d'OpenTelemetry per a:
	  ○ Mètriques.
	  ○ Logs estructurats.
	  ○ Traces distribuïdes
	  ○ Telemetria en general
	• Disponibilitat d'agents i exportadors nadius o compatibles amb Open Telemetry Collector.
	• JSON estructurat per a logs i esdeveniments.
	• Syslog RFC5424 per a integració amb sistemes de seguretat.
	• Capacitats de filtratge i segmentació de telemetria per etiquetes, compte, subscripció, recurs, servei o component.
	• Exportació directa de dades mitjançant:
	  • OTel Collector, agents nadius o compatibles.
	  • API REST.
	  • Connectors i subscripcions a esdeveniments (EventBridge, Azure Events, Pub/Sub Events).
	  • Streaming cap a repositoris externs d'emmagatzematge.
	• Possibilitat de configurar pipelines Open Telemetry governats pel CTTI, incloent:
	  • filtratge,
	  • agregació,
	  • conversió,
	  • routing de dades,
	  • re-procés i encaminament multiplataforma.
	• Compromís de mantenir schemas Open Telemetry estables, documentats i versionats.
	• Notificació de qualsevol canvi en schemas, APIs, formats o comportaments de telemetria amb una antelació mínima de 90 dies.

ID-Req	Descripció del requeriment
	• Suport de telemetria en entorns multicloud i híbrids, garantint formats i semàntica consistents.
OPE-07	Ha de generar i posar a disposició, com a mínim, els elements següents: • Logs d'activitat administrativa (IAM, API calls). • Logs de xarxa (flow logs, connexions, bloquejos). • Logs de seguretat • Logs del servei gestionat (operatius, errors, canvis interns). • Esdeveniments de configuració i canvi d'estat dels recursos. • Mètriques de rendiment: CPU, memòria, IO, latències, throughput, QPS. • Mètriques de disponibilitat: health checks, error rates, saturació, estats de vida del servei. • Integració nativa d'emmagatzemament centralitat de logs amb xifrat en repòs.
OPE-08	Ha de disposar de capacitats de creació d'alertes via API i d'integració amb sistemes externs amb informació mínima (recurs afectat, severitat, timestamp, mètrica i valor).
OPE-09	Ha de disposar d'una pàgina d'estat dels diferents serveis que composen el núvol públic sobirà ("status page")
OPE-10	Ha de disposar d'un sistema centralitzat dels elements de govern de la regió en diferents comptes i subscripcions.
OPE-11	Ha de disposar capacitats d'integració amb eines de FinOps (p.e.: Apptio)
OPE-12	Ha de disposar d'un sistema nadiu d'auditoria de logs per controlar canvis en recursos cloud de xarxes.
OPE-13	Ha de disposar d'un sistema nadiu de mètriques de monitorització i alertes de recursos cloud de xarxes amb possibilitat d'extracció de mètriques amb eines externes.
OPE-14	Ha de disposar d'un sistema de segmentació i aïllament de recursos a nivell de gestió.
OPE-15	Ha de disposar de mecanismes de desplegament de rols i polítiques natives per una governança efectiva dels recursos de xarxa.
OPE-16	Ha de disposar d'una cobertura de suport de 24x7 amb canal de suport multicanal (web i telèfon), i amb idioma de suport en català i/o castellà.
OPE-17	S'ha de notificar qualsevol incident significatiu en ≤24 hores (avís inicial amb informació preliminar) i proporcionar un informe més complet en ≤72 h (incloent una avaluació inicial de l'impacte). Posteriorment, s'ha d'elaborar un informe final detallat en ≤1 mes descrivint la causa, l'impacte i les mesures correctores aplicades. Es designaran rols, responsabilitats i canals d'escalament interns i

ID-Req	Descripció del requeriment

	externs per a cada fase, i es generaran evidències auditables (logs, comunicacions) de totes les accions.
	• Detecció i notificació de les incidències
	  ○ Detecció i comunicació de les incidències en els serveis.
	  ○ Proporcionar un canal programàtic (API status) per consultar estat, actualització i causa arrel.
	• Comunicació i participació operativa
	  ○ Designar un punt d'escalat 24x7 per a incidències crítiques.
	  ○ Participar en remot en els Comitès de Crisi convocats pel CTTI.
	  ○ Proporcionar informe preliminar en ≤ 24 hores, incloent:
	  ▪ causa arrel,
	  ▪ abast del servei,
	  ▪ línia de temps,
	  ▪ mesures correctores,
	  ▪ mesures preventives.

OPE-18	Ha de disposar d'un servei de suport addicional (Enterprise Support) amb els següents temps de resposta davant incidències sobre les solucions TIC desplegades pel client • Resposta incidència crítica: <= 15 minuts • Resposta incidència alta: <= 1 hora • Resposta incidència mitjana: <= 4 hores
OPE-19	Gestió notificació de canvis i anàlisi d'impacte • Comunicació de canvis disruptius (amb afectació al servei) amb 90 dies d'antelació. • Comunicació de deprecacions tecnològiques de serveis amb ≥ 12 mesos d'antelació. • Comunicació de manteniments planificats (sense afectació al servei) amb ≥ 21 dies.

3.1.5 Requeriments de sobirania tecnològica

ID-Req	Descripció del requeriment
TEC-01	Ha de ser multitenant: qualsevol empresa, organització o institució pública pot adquirir serveis de la regió de núvol públic sobirà, que estaran totalment aïllats i securitzats entre les diferents organitzacions.
TEC-02	Ha de disposar de capacitats d'hibridació per permetre de forma natural i estàndard l'extensió sobre infraestructures de núvol privat.
TEC-03	El licitador haurà de demostrar, sense ànim limitatiu, compromís amb l'ús de programari de codi obert en la construcció de la seva plataforma de núvol

ID-Req	Descripció del requeriment
	sobirana, prioritzant-lo per a components clau i facilitant així la independència tecnològica i la portabilitat dels serveis a través d'estàndards oberts i APIs ben documentades. El licitador haurà de detallar l'ús de components de codi obert versus propietaris i justificar-ne la selecció en termes de sobirania i funcionalitat, així com la seva integració amb estàndards oberts.
TEC-04	Ha de disposar d'un catàleg de serveis de cloud computing amb un abast i funcionalitats equivalents als catàlegs de serveis dels hiperescalars públics. Aquesta equivalència s'entén com la provisió de serveis que vagin més enllà del bàsic IaaS o IaaS amb plataformes instal·lades, i que incloguin serveis propis per al desenvolupament d'aplicacions cloud-native. El catàleg ha de comprendre, entre d'altres, serveis de computació, contenidors gestionats, funcions serverless, emmagatzematge, bases de dades autogestionades (SQL/NoSQL), solucions de seguretat, caché distribuïda, observabilitat, solucions d'IA i solucions de BigData, amb les capacitats de disponibilitat, pagament per ús, resiliència i escalabilitat integrades en els serveis. Aquesta equivalència no implica la necessitat de replicar la totalitat exhaustiva de tots els serveis que puguin oferir els grans proveïdors de núvol públic, sinó d'assegurar una oferta robusta, moderna i competitiva que suporti una àmplia gama de càrregues de treball i models de desenvolupament per als casos d'ús de l'Administració Pública.

TEC-05	Ha de disposar de capacitats de còmput i emmagatzematge amb suport per a diferents càrregues de treball:
	• propòsit general, optimitzades per memòria o per CPU
	• GPU per a projectes d'IA sobirana o processament massiu de dades
	• Emmagatzematge multinivell
	  ○ Block Storage
	  ○ Object Storage
	  ○ File Storage.

TEC-06	Qualsevol nou servei o funcionalitat incorporada al catàleg haurà de complir les premisses de sobirania jurídica i tècnica exigides en aquesta licitació, amb un enfocament en la garantia que el control, la gestió i el processament de dades es mantenen dins de la jurisdicció de la UE. Per a tecnologies de 'mercat estàndard' amb origen fora de la UE, s'acceptarà la seva integració sempre que el licitador pugui demostrar la implementació de controls compensatoris i salvaguardes que assegurin el compliment de la sobirania de dades i operacions dins la UE.
TEC-07	El catàleg disposarà de les darreres versions estables de les tecnologies de plataforma utilitzades (ex. Kubernetes, motors de bases de dades, etc.)
TEC-08	Ha de permetre definir polítiques corporatives i etiquetes (tags) per classificar recursos (dades, màquines, serveis) segons criteris de sobirania, criticitat, centre de cost, etc. amb possibilitat d'integrar aquesta informació amb la CMDB o eines de gestió d'actius per facilitar la governança

ID-Req	Descripció del requeriment
TEC-09	Ha de disposar de capacitat d'integració amb altres tecnologies a través d'API o protocols ben documentats i no propietaris, mesura en què la solució s'adhereix a estàndards governats públicament i àmpliament adoptats, reduint la dependència de proveïdors únics.
TEC-10	Ha de disposar d'un Framework d'IaC, equivalent a Terraform com a estàndard de mercat i adoptat a CTTI, per la definició, versionat, i automatització de tota la infraestructura així com que doni suport a tots elements del catàleg i aspectes de configuració.
TEC-11	Ha de disposar de serveis de pipelines d'integració contínua per a la creació i canvi de recursos. Fer *policy-as-code* per aplicar regles de seguretat (*drift detection* per detectar desalineaments). Integrar escàners automatitzats de vulnerabilitats i compliance sobre imatges de VM i contenidors, apropant-se a un model DevSecOps
TEC-12	Possibilitat d'establir segmentació de xarxa.
TEC-13	Ha de disposar de desplegament d'arquitectures tipus Hub & Spoke o similars, per compartir recursos de xarxa i seguretat amb múltiples càrregues de treball aïllat en els spokes.
TEC-14	Ha de desplegar un sistema nadiu de DNS per recursos cloud,
TEC-15	Ha de disposar de com a mínim 2 punts d'interconnexió (mínim 10 Gbps) a la regió sobirana per establir connexions privades amb les operadores que determini el CTTI.
TEC-16	Ha de disposar d'intercanvi de rutes estàtiques i dinàmiques, cap altres xarxes privades.
TEC-17	Ha de desplegar serveis nadiu per la traducció d'adreces de xarxa
TEC-18	Ha de disposar d'adreçament públic sota demanda o rang d'adreçament propi.
TEC-19	Ha de disposar d'un Marketplace que faciliti la integració de solucions de proveïdors de software independents.

3.1.6 Requeriments de sobirania de seguretat i compliment

ID-Req	Descripció del requeriment
SEG-01	Ha de complir el Marc Normatiu de Ciberseguretat de la Generalitat de Catalunya: https://portal.ciberseguretat.cat.
SEG-02	Ha d'acreditar que els serveis que presta en relació amb l'objecte del contracte disposen de les declaracions/certificacions de conformitat amb la categoria alta de l'ENS.

ID-Req	Descripció del requeriment
	L'empresa homologada haurà de mantenir aquesta certificació durant tota la vigència del contracte.
SEG-03	Ha de complir l'RGPD a nivell europeu i la LOPDGDD. L'empresa homologada actuarà com a encarregat del tractament, d'acord amb el previst a l'article 3 de l'ENS per als sistemes que tracten dades personals. Pel que fa a la seguretat, l'adjudicatari implementarà les mesures establertes en el Marc de Ciberseguretat per a la Protecció de Dades (MCPD) de la Generalitat, corresponents al **nivell alt**. Aquesta implementació i nivell de compliment seran incorporats al model de compliment normatiu de Ciberseguretat de la Generalitat de Catalunya. A aquests efectes, l'empresa homologada, com a encarregat del tractament, es compromet a subscriure i complir l'encàrrec de tractament que s'adjunti com annex al contracte.
SEG-04	Ha de complir amb els controls establerts per la NIS2.
SEG-05	Haurà de complir tota aquella normativa europea relacionada que entri en vigor amb posterioritat a la homologació del licitador, dins els terminis d'adaptació, aplicació o compliment que estableixi la pròpia normativa. Així mateix es compromet a implementar totes les mesures necessàries per garantir l'alineament continuat amb qualsevol actualització, modificació o nova disposició europea aplicable al servei, subministrament o actuació objecte del contracte.
SEG-06	Ha d'assegurar l'alineament dels seus controls de seguretat i governança amb les guies i esquemes d'ENISA.
SEG-07	Ha de facilitar el compliment de les obligacions vigents de l'AI Act (Reglament d'Intel·ligència Artificial de la UE) en el moment de la publicació de la licitació i haurà de demostrar una estratègia clara i un full de ruta detallat per a la preparació i el compliment de les futures obligacions una vegada aquestes normatives i les seves guies d'implementació estiguin plenament operatives. S'esperarà la capacitat de facilitar el compliment d'aquestes normatives per als serveis desplegats per la Generalitat de Catalunya, comprometent-se a adaptar els serveis en els terminis establerts per la legislació aplicable.
SEG-08	Ha de facilitar el compliment de les obligacions vigents de la Data Act (Reglament de la UE que estableix normes sobre l'accés, l'ús i la compartició de dades) en el moment de la publicació de la licitació.
SEG-09	Ha d'estar preparat per l'acompliment del reglament DORA per aquells sistemes d'informació o solucions que així ho requereixin.
SEG-10	Ha d'estar preparat per l'acompliment del reglament EHDS per aquells sistemes d'informació o solucions que així ho requereixin.
SEG-11	Ha d'estar adherit a l'EU Cloud Code of Conduct i assegurar un nivell de compliment 2 o 3.

ID-Req	Descripció del requeriment
SEG-12	Ha d'evidenciar que l'empresa homologada adoptarà i aplicarà els principis i controls del GAIA-X Trust Framework, i que disposa de procediments i evidències per demostrar-ho, disposant de credencials verificables de conformitat (GAIA-X Compliance Verifiable Credentials) emeses per entitat reconeguda dins l'ecosistema GAIA-X per a tots o part dels serveis del seu catàleg degudament declarats.
SEG-13	D'acord amb el model de responsabilitat compartida del núvol públic, l'empresa homologada ha de disposar dels elements de seguretat necessaris, gestionats, per garantir la seguretat preventiva, proactiva i reactiva de la infraestructura del núvol objecte del servei.
SEG-14	D'acord amb el model de responsabilitat compartida del núvol públic, l'empresa homologada ha de disposar de tots els serveis de seguretat nadius necessaris per tal que els usuaris de la regió de núvol públic sobirà puguin garantir la seguretat dels seus serveis d'acord a la normativa de seguretat vigent. Com ara entre d'altres: • Protecció en front atacs a la disponibilitat en diferents protocols de comunicació. • Gestió de vulnerabilitats de la infraestructura (VM, contenidors, etc.). • Detecció i protecció d'amenaces (intents d'intrusió, execució de codi maliciós, monitorització de l'activitat d'usuaris, etc.). • Gestió segura de les identitats (IAM, etc.). • Capacitats de resposta i automatització en front la gestió d'incidents de seguretat.
SEG-15	Anàlisi de riscos de seguretat. D'acord amb la normativa vigent, l'empresa homologada haurà de disposar d'un anàlisi de riscos de seguretat del servei/infraestructura objecte de la licitació i el corresponent pla de mitigació, associat.
SEG-16	Ha de disposar de mecanismes hardware de seguretat (HSM) que permetin la generació, gestió i emmagatzematge de claus de xifrat (CMK) sota el control exclusiu del client. Les claus mestres de xifrat hauran de residir i rotar exclusivament dins la jurisdicció de la UE. El licitador haurà de detallar l'arquitectura de gestió de claus, incloent l'esquema de "split-key" o mecanismes equivalents que garanteixin la sobirania i el control total de les claus per part del contractant dins la UE, amb registres auditables (complint ENS Art. 22).
SEG-17	Ha de disposar de capacitats d'integració de la consola d'administració dels tenants configurats pel client sobre la regió cloud amb estàndards de mercat: OIDC preferentment, o SAML.
SEG-18	Ha de disposar de capacitats d'integració amb plataformes de seguretat de productes CNAPP i SIEM nadius o de tercers.

ID-Req	Descripció del requeriment
SEG-19	Ha de disposar de Centres d'Operacions de Seguretat (SOCs) i equips de resposta a incidents ubicats i operant sota la jurisdicció exclusiva de la Unió Europea per a la gestió directa dels serveis objecte d'aquesta licitació. En cas que per la naturalesa de la tecnologia es requereixi la intervenció de personal o sistemes de suport global (fora de la UE), el licitador haurà d'establir protocols clars que garanteixin la sobirania de dades i operacions, la no-exposició a jurisdiccions externes i l'aprovació prèvia del CTTI per a qualsevol accés a dades o sistemes sensibles.
SEG-20	D'acord a la normativa europea, ha d'informar de forma transparent i diligent sobre penetracions o vulnerabilitats, disposant d'autonomia de mitigació.
SEG-21	Ha de permetre realitzar auditories de seguretat i compliment independents amb accés complet, per part d'entitats de la UE, per part d'entitats reguladores estatals o locals, com per exemple el CTTI o l'Agència de Ciberseguretat de Catalunya.
SEG-22	Ha de permetre implantar controls estrictes d'accés: autenticació multifactor (MFA), principi de mínim privilegi, *Single Sign-O*n i polítiques de control de privilegis (PAM, o tipus JIT) i polítiques d'accés condicional. *Hardenitzar* les polítiques IAM i establir *guardrails* (per exemple, límits de permisos codificats) per prevenir configuracions insegures. Definir procediments d'«emergència» (*break-glass*) controlats i amb auditories pels casos en què calgui accedir amb privilegis extrems.
SEG-23	Ha de disposar d'una arquitectura zero-trust i segmentació per configurar la xarxa amb segmentació avançada (ACL, microseguretat, VPN, *gateways* segurs, NFGW, etc) per implementar un model de confiança zero
SEG-24	L'empresa homologada haurà de garantir l'accés del personal autoritzat del CTTI o l'Agència de Ciberseguretat de Catalunya a la informació de seguretat i compliment (procediments, registre d'incidents, traces, entre d'altres). Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat.

3.1.7 Requeriments de Sostenibilitat Mediambiental

ID-Req	Descripció del requeriment
ENV-01	Compliment de la ISO 50001 en el moment de posada en marxa de la regió a Catalunya o declaració de compromís per obtenir la certificació en un termini màxim de 12 mesos des de la posada en marxa de la regió a Catalunya.
ENV-02	Compliment de la ISO 14001 en el moment de posada en marxa de la regió a Catalunya o declaració de compromís per obtenir la certificació en un termini màxim de 12 mesos des de la posada en marxa de la regió a Catalunya..

ENV-03	L'empresa homologada haurà de garantir la utilització d'energia renovable o de baixa emissió de carboni per alimentar les infraestructures i operacions de la regió de núvol públic sobirà. Es valorarà la capacitat d'alimentació directa i es requerirà un compromís amb un percentatge mínim d'energia verda, amb un pla detallat i verificable per assolir progressivament el 100% mitjançant acords de compra d'energia o certificats d'energia renovable.

3.1.8 Requeriments de gestió del tenant de la Generalitat de Catalunya

Com a part essencial dels requeriments, es requereix que l'empresa homologada realitzi la gestió del tenant de núvol públic sobirà per a la Generalitat de Catalunya. L'empresa homologada haurà de configurar, operar i governar el tenant (inclòs el domini d'identitat, les subscripcions o projectes, la jerarquia de recursos i les polítiques corporatives de seguretat), garantint que totes les dades i metadades gestionades resideixin i es processin exclusivament dins del territori contractat (Catalunya) i en tot cas dins la Unió Europea.

ID-Req	Descripció del requeriment
GET-01	L'empresa homologada realitzarà l'avaluació i configuració del tenant realitzant entre d'altres les següents activitats: • Revisió del domini d'identitat i estructura de subscripcions/projectes: Crear una jerarquia de recursos inicial amb polítiques corporatives adequades. Determinar els perfils i rols necessaris per a cada equip. • Classificació de la informació i geo-fencing: Permetre la catalogació de totes les dades i serveis del tenant segons el seu nivell de sensibilitat, habilitant l'aplicació d'etiquetes (tags) corporatives per facilitar la governança (classificació, propietari funcional, residència, centre de cost).
GET-02	L'empresa homologada haurà de proposar estratègies d'estalvi en la facturació del servei, explorant diferents modalitats de contractació disponibles al núvol públic, com ara la contractació per períodes més petits, reserves anticipades, o qualsevol altra tipologia que permeti optimitzar els costos. Aquestes propostes hauran de ser detallades i justificades, amb l'objectiu de garantir una gestió eficient i sostenible dels recursos contractats.
GET-3	L'empresa homologada caldrà que faciliti de forma pública instruccions detallades respecte com consumir i/o configurar els serveis del núvol públic sobirà, incloent blueprints, plans i procediments operatius, *runbooks* per a tasques rutinàries i *playbooks* per a escenaris d'emergència.
GET-04	L'empresa homologada inclourà anualment en el servei (i per tant, sense cost) 4 cursos de formació del seu catàleg de formació escollits pel CTTI, adreçats al personal que CTTI determini, orientat a serveis concrets del cloud i bones pràctiques.

3.2 Serveis de facilitació

La finalitat dels serveis de facilitació és disposar d'un equip de treball específic durant un termini acotat, diferent de l'equip d'operació dels serveis de cloud computing, per tal d'atendre necessitats puntuals de suport a la resta de proveïdors que construeixen o mantenen solucions TIC per a la Generalitat de Catalunya i/o a les àrees TIC del CTTI, i assegurar els calendaris de cada projecte d'aprovisionament dels serveis de cloud computing que es requereixi, o bé per disposar d'un suport ampliat per realitzar tasques fora del servei d'explotació estàndard.

Aquest element de catàleg s'estructura en els següents sub-elements de servei:

- Serveis d'assessorament
- Serveis de suport tècnic
- Serveis de formació

3.2.1 Servei d'assessorament

Realització d'activitats d'assessorament a CTTI sobre la millor estratègia d'utilització dels serveis de cloud computing del núvol públic sobirà a l'hora de construir solucions TIC, per garantir la màxima resiliència, autonomia i assoliment de sobirania.

3.2.2 Servei de suport tècnic

Realització d'activitats d'acompanyament als proveïdors de les solucions TIC que es despleguin sobre el núvol públic sobirà, com per exemple en els següents aspectes:

- Aprovisionament via IaC (Infraestructure as Code)
- Migracions de BBDD's
- Containerització (Estratègies rehost i replatform)
- Gestió de notificacions del servei (CMDB)
- Suport a proves funcionals i validacions amb l'Agència de Ciberseguretat
- Configuració de pipelines (https://canigo.ctti.gencat.cat/plataformes/ghec/)
- Suport post-producció per a garantir la estabilitat del sistema.
- Assignació i gestió de Tags
- Implementació de pràctiques FinOps
- Revisió de consums
- Càlcul i repartiment de costos
- Suport a definicions de disseny
- Suport a serveis de continuïtat
- Suport a observabilitat i automatització

CTTI podrà afegir altres tasques que puguin necessàries per assegurar la qualitat de solucions TIC que utilitzen els serveis de cloud computing d'aquesta licitació.

Aquestes tasques de suport tècnic es poden dur a terme tant dins com fora de l'horari normal del servei. A tall d'exemple d'aquest tipus de tasques de suport a aplicacions:

- Suport fora d'hores per una migració de dades.
- Suport de cap de setmana per una posada en marxa d'una nova funcionalitat de l'aplicació (que no ha requerit aprovisionament d'infraestructures).
- Etc.

No formen part d'aquest concepte les tasques associades a les activitats específiques d'operació i administració de les solucions TIC desplegades sobre la regió de núvol públic sobirà.

En el cas que l'empresa homologada identifiqui un volum de peticions de servei excessives, ho posarà en coneixement de l'interlocutor assignat pel CTTI al projecte d'implantació per tal que es pugui reconduir la situació ràpidament.

3.2.3 Servei de formació reglada

L'empresa homologada haurà de proporcionar un catàleg de cursos de formació específicament dissenyat per respondre a les necessitats de cada servei ofert que garanteixi una adaptació òptima a les diferents solucions i serveis del núvol públic sobirà de l'empresa homologada. Aquest catàleg ha d'incloure formació tant tècnica com funcional, abastant des de la gestió de recursos, l'arquitectura de solucions, la seguretat, la configuració de serveis, fins a l'administració d'infraestructures i el manteniment de sistemes. D'aquesta manera, es facilita que les empreses que utilitzin els serveis i els equips tècnics puguin adquirir competències pràctiques i teòriques que afavoreixin la integració, el desplegament i l'optimització de les funcionalitats del núvol, així com el compliment dels requisits d'arquitectura, de seguretat i eficiència operativa. El catàleg ha de ser ampli, actualitzat periòdicament i accessible per a tot l'equip implicat en la gestió i ús dels serveis del núvol públic sobirà, assegurant una formació contínua alineada amb l'evolució tecnològica i les necessitats específiques de cada projecte.

Cada curs tindrà un cost associat (excepte els inclosos com a part del servei).

Aquesta formació haurà d'incloure com a mínim:

- **Serveis específics del núvol públic sobirà**: networking, seguretat, gestió de recursos, monitoratge, ...
- **Pràctiques avançades**: infraestructura com a codi (IaC), automatització de desplegaments, integració contínua i DevOps.
- **Àmbits d'innovació**: AIOps, FinOps, arquitectures serverless i altres tecnologies emergents.
- **Bones pràctiques i optimització**: ús eficient dels recursos, seguretat i governança.
- **Actualitzacions tecnològiques**: novetats i evolució dels serveis del núvol públic sobirà.

A més, puntualment el CTTI podrà demanar sessions específiques a banda del propi catàleg de formació del licitador, per tal de cobrir necessitats específiques o novetats tecnològiques.

4 CONDICIONS D'EXECUCIÓ

Les següents condicions d'execució es consideren requeriments generals d'obligat compliment per part de l'empresa homologada.

4.1 Estructura organitzativa per prestar el servei

Dins d'aquest capítol es defineix l'equip de treball per a la prestació del servei, que amb caràcter de mínims han de formar l'estructura organitzativa que proposi l'empresa homologada pel servei demandat, així com de forma il·lustrativa les principals funcions, que no úniques, que hauran de desenvolupar.

Els recursos humans assignats al contracte per l'empresa homologada han de tenir la qualificació necessària per a poder garantir amb èxit la prestació del servei i la seva evolució futura.

El CTTI es reserva el dret de demanar el canvi d'algun recurs si detecta que no és capaç de complir amb les mínimes exigències que són necessàries per a prestar un servei d'aquesta dimensió. En aquest cas, l'empresa homologada haurà de presentar un pla de canvi del/s recurs/os, que haurà de ser aprovat pel CTTI.

En cada basat d'Acord Marc, l'empresa homologada haurà de presentar un esquema organitzatiu correctament dimensionat que asseguri la cobertura del servei que es descrigui en el plec corresponent a cada basat.

4.1.1 Rols i perfils requerits per la prestació del servei

L'empresa homologada haurà de definir clarament les funcions que realitzaran tots i cadascun dels perfils. Pels diferents perfils descrits, el proveïdor haurà de definir, identificar i detallar clarament quins d'ells s'encarregarà de liderar i dur a terme el desenvolupament dels objectius d'aquest contracte.

L'horari d'atenció d'aquests rols serà de dilluns a divendres, de 08:00 a 18:00 hores, respectant en tots els casos els Acords de Nivell de Servei (SLA) establerts. En cas d'atenció a incidents que afectin a la disponibilitat del servei, siguin o no de seguretat, l'horari d'atenció del rol del responsable de seguretat s'ajustarà a un servei 24x7.

Les funcions mínimes que hauran d'assumir aquests perfils associats a la prestació del servei són les següents:

- **Responsable de compte:** Aquesta figura és única per l'empresa homologada. És la figura de referència per tots els contractes basats entre el CTTI i l'empresa homologada i el darrer responsable de la prestació del conjunt de serveis i projectes de l'empresa homologada. El responsable de compte ha de tenir capacitat executiva sobre el servei, especialment si s'articula alguna UTE. Aquesta figura es mantindrà durant tota la vida del contracte o contractes entre el CTTI i l'empresa homologada, en la gestió comercial, durant la provisió del servei i fins a la devolució d'aquest. Ha de ser garant de l'existència dels mecanismes de relació en la seva organització per portar a terme els acords

presos entre CTTI i l'empresa homologada. En cas que es produeixin canvis en l'abast i/o cost dels serveis que impliquin una modificació contractual, és el responsable de vehicular-ho.

- **Rol principal**: Figura única dins l'empresa homologada, amb capacitat decisòria sobre l'acord marc amb el CTTI.
- **Responsabilitats clau**:
  - Vetllar pel compliment dels objectius de l'acord marc (serveis i obres) segons terminis, qualitat i pressupost.
  - Responsable màxim dels àmbits econòmic, contractual, organitzatiu i estratègic.
  - Consolidar i aportar al CTTI les informacions tant objectives com subjectives; valorades (informació fiable i de qualitat) que permetin la presa de decisions operatives i estratègiques al llarg de la vida de l'Acord Marc.
  - Ser l'interlocutor principal amb el CTTI en matèria jurídica-legal per a tots els serveis/contractes prestats per l'empresa homologada. Serà el responsable de la formalització de les interpretacions realitzades respecte als contractes vigents, quan aquestes impliquin modificacions contractuals.
  - Ser el responsable que el CTTI rebi els informes de gestió acordats, tant amb indicadors econòmic-financers com d'altres, així com de realitzar el seguiment del model econòmic acordat amb l'empresa homologada.
  - Ser el responsable que l'empresa homologada faciliti la informació relativa al procés de facturació, segons el model i format definit pel CTTI, així com col·laborar en el procés de la conciliació.
  - Interlocutor principal amb el CTTI per qüestions d'alt nivell, incloent resolució de conflictes i decisions crítiques.
  - En cas d'UTE, garanteix la coordinació entre les empreses participants.
- **Perfil:** direcció, coneixement profund del contracte, capacitat de negociació i gestió estratègica.

- **Responsable de servei (TAM):** Es designarà un Technical Account Manager exclusiu per al tenant de la Generalitat de Catalunya amb una dedicació del 100%.
  - **Rol principal:** Garantir la correcta prestació del servei en el dia a dia, assegurant el compliment dels ANS, els requisits de sobirania i la millora contínua.
  - **Responsabilitats clau:**

- Punt de contacte operatiu amb el CTTI (Responsables de Servei, Centre de Control i altres àmbits).
- Definirà i validarà l'arquitectura del tenant, assegurant la correcta configuració dels serveis cloud computing i el compliment dels requisits de sobirania, seguretat i interoperabilitat establerts pel plec.
- Revisar plantejaments d'arquitectura a petició de CTTI
- La gestió i seguiment diari del servei, així com la resolució de conflictes i redimensionament temporal o permanent d'aquest.
- Manteniment del registre de l'evolució del servei per a posteriorment poder elaborar els informes de servei i justificar el compliment dels ANS.
- Seguiment i control dels recursos assignats als serveis.
- Analitzar qualsevol desviació i situacions de gravetat dins la qualitat, terminis o abast del servei.
- A nivell transversal, realitzar el control de costos, l'estimació d'esforços i el seu seguiment.
- A nivell transversal, analitzar les modificacions en abast i cost del servei que es puguin derivar i interpretar aquestes modificacions respecte dels contractes vigents. En cas que no impliquin una modificació contractual, ser el garant de formalitzar i implementar internament a la seva organització els acords presos.
- Gestionar processos definits pel CTTI: incidències, canvis, peticions, problemes, coneixement, etc.
- Establirà les polítiques de govern del tenant, incloent etiquetatge, gestió de subscripcions, control de costos i traçabilitat, vetllant pel compliment normatiu (GDPR, ENS)
- Responsable dels informes de servei, procediments, instruccions operatives i guies multi-proveïdor.
- El TAM haurà d'elaborar informes tant operatius com d'incidents, seguiment SLA i memòries de complerts normatius periòdiques. Proporcionarà també informes executius sobre ús, seguretat i suggeriments de millora, assegurant una comunicació clara amb CTTI.
- Gestionar els riscos i assegurar l'optimització del servei.
- Responsable de reportar els incidents segons NIS2 (garantint notificacions en 24h/72h/1m) i de preparar la documentació requerida per a auditoria d'ENS

  - **Perfil:** Coneixement tècnic-operatiu, capacitat de coordinació multi-proveïdor, orientació a resultats i millora contínua.

- **Responsable de seguretat** (RSP)
  - **Rol principal:** El **RSP** és la figura de governança i interlocució estratègica respecte els temes de seguretat, amb el CTTI i l'Agència de Ciberseguretat de Catalunya. Figura estratègica i operativa que actua com a **punt de contacte únic en matèria de seguretat** entre el proveïdor i la Generalitat. Ha de garantir

el **compliment normatiu**, la supervisió dels controls de seguretat i la gestió integral dels incidents durant tota la vigència del contracte.

- **Responsabilitats clau:**
  - Representarà el POC (point of contact) del proveïdor de cara al compliment de les normatives.
  - Canalitzar i supervisar el **compliment dels requisits de seguretat** establerts al plec i en el Marc Normatiu de la Generalitat.
  - **Notificar** qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació o serveis de la Generalitat, en els terminis i per les vies que determini el CTTI, l'Agència de Ciberseguretat de Catalunya o els procediments establerts en el Marc Normatiu de la Generalitat de Catalunya d'acord amb l'ENS i la Guia Nacional de Gestió i Notificació de Ciberincidents.
  - Coordinar la **gestió d'incidents** amb el CTTI i l'Agència de Ciberseguretat: identificació, contenció, erradicació, recuperació i recopilació d'evidències.
  - Garantir l'**accés a informació crítica** (logs, traces, telemetria) per auditories i investigacions.
  - Supervisar l'adequació contínua dels controls davant noves amenaces o canvis normatius.
  - Garantir una disponibilitat **24x7** de l'operació de la seguretat dels serveis objecte del contracte.
  - Mantenir un **pla de resposta immediata** validat pel CTTI i l'Agència de Ciberseguretat.
- **Perfil:** Alta especialització en seguretat, gestió incidents, coneixement avançat de la normativa de seguretat, visió estratègica, capacitat de lideratge.

- **Arquitecte de solucions**
  - **Rol principal:** Assessorar en l'estratègia tecnològica i donar suport als projectes per garantir solucions òptimes.
  - **Responsabilitats clau:**
    - Definir arquitectures tècniques alineades amb les necessitats del CTTI i les bones pràctiques del sector.
    - Donar suport en la fase de disseny i implementació de projectes, assegurant escalabilitat, seguretat i eficiència.
    - Col·laborar amb el TAM per anticipar necessitats i amb el Responsable de compte per garantir coherència amb l'estratègia global.
  - **Perfil**: Alta especialització tècnica, visió estratègica, capacitat d'integració entre tecnologia i negoci.

El tàndem d'arquitecte de solucions i TAM són els encarregats de traslladar novetats sobre el full de ruta del núvol públic sobirà que siguin aprofitables pels serveis que ja hi estan en funcionament, o bé pels projectes futurs que hi vindran.

Puntualment, i sense que es considerin rols estructurals del servei licitat, per a necessitats concretes de projectes o evolució del servei, CTTI podrà demanar a través del TAM, perfils especialistes en diferents matèries, destacant

- **Especialista de seguretat**: Per donar suport en totes les tasques de seguretat del núvol públic sobirà, assegurant el compliment normatiu i proposant millores d'optimització, alineat amb les polítiques definides per l'Agència de Ciberseguretat de Catalunya. En el moment de definir i muntar la landing zone serà un perfil clau.
- **Especialista de networking:** Per donar suport en la definició, configuració i optimització de la infraestructura de xarxa del núvol públic sobirà per garantir rendiment i disponibilitat. En el moment de definir i muntar la landing zone serà un perfil clau. Dissenyarà i supervisarà la segmentació de xarxa, els mecanismes de protecció (xifrat, IAM, zero-trust) i la configuració de passarel·les segures, assegurant la conformitat amb ENS, NIS2 i els requisits de sobirania.
- **Especialista de IA:** Per donar assessorament i suport en l'ús de serveis del núvol públic sobirà relacionats amb tecnologies d'intel·ligència artificial, ja sigui per millorar processos i serveis o bé infusionar IA als serveis que s'hi allotgin.
- **Enginyer DevOps:** Per donar suport a la implementació de processos d'automatització mitjançant Infrastructure as Code (IaC) i pipelines de lliurament continu, garantint la integració de controls DevSecOps i la coherència amb les polítiques corporatives i normatives aplicables.

4.2 Localització Física

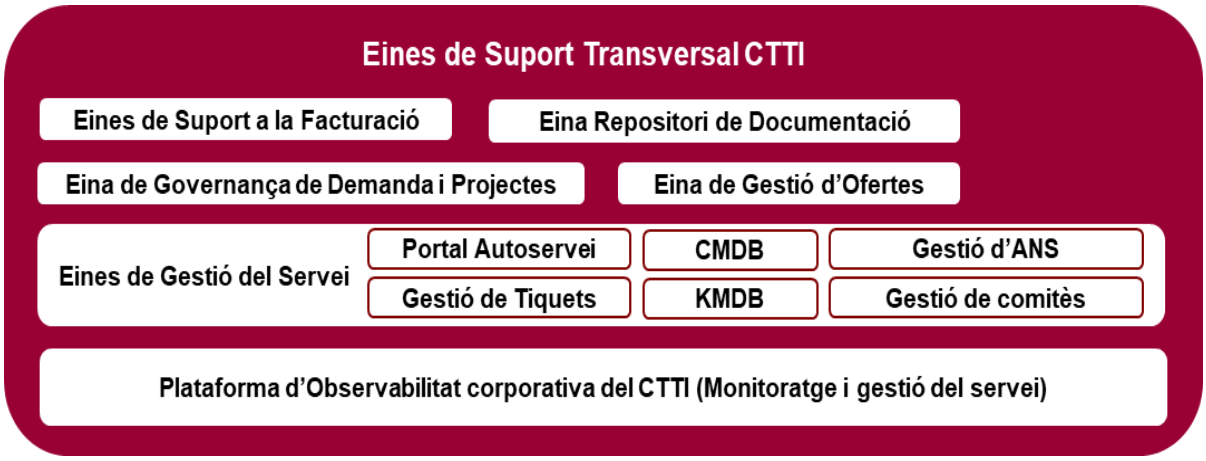
Els professionals que formin part del servei estaran ubicats en les instal·lacions pròpies de l'empresa homologada.

De manera excepcional, en casos d'incidències crítiques o per necessitats especials del servei, el CTTI podrà requerir l'assistència presencial de perfils específics de l'empresa homologada en alguna o algunes ubicacions designades pel propi CTTI.

4.3 Eines

4.3.1 Eines de Governança del Servei del CTTI

Els processos de governança dels serveis TIC se suporten en un conjunt d'eines que l'empresa homologada haurà d'utilitzar i mantenir actualitzades. Aquestes eines seran determinades i/o proporcionades pel CTTI, sent les principals:



Il·lustració: Mapa complet d'eines principals transversals del CTTI

Concretament, l'empresa homologada haurà d'utilitzar les següents eines:

4.3.1.1 Eines de Gestió del Servei

Actualment el CTTI disposa de diverses eines que donen suport als processos de governança dels serveis. A continuació es detallen les eines de les quals disposa el CTTI per a la gestió i operació del servei:

- **Eina de gestió del compliment dels acords de nivell de servei:** El CTTI disposa d'una eina per enregistrar els indicadors de servei, agregar-ne la informació, calcular el nivell d'acompliment en base als acords de nivell de servei establert i calcular la penalització associada si escau.

  Aquesta eina és el referent per fer el seguiment del compliment dels acords de nivell de servei establerts amb l'empresa homologada, en cas que la informació no vingui automàticament d'altres eines del CTTI l'empresa homologada serà responsable de proveir-la en el format que el CTTI determini.

- **Eina de gestió de comitès de crisi i notificacions d'alertes:** El CTTI disposa d'una eina per a la gestió de les notificacions d'alertes de la plataforma corporativa d'observabilitat i també dels comitès de crisi, anomenada SOSTIC.
  Aquesta eina és d'ús obligatori per a les dues tipologia de gestions i l'empresa homologada ha de garantir el seu coneixement i el procés de subscripció en tot moment.

4.3.1.2 Eines de Suport a la Facturació

El CTTI disposa de dues eines vinculades al procés de facturació i validació del servei rebut:

- **Eina de conciliació:** sistema d'informació que fa la conciliació dels elements de despesa rebuts pels proveïdors amb relació a l'inventari a la CMDB, les tarifes i altres regles de facturació establertes. Aquesta eina permet la consulta de costos per part de CTTI i proveïdors i la imputació d'aquests costos cap als seus clients.

- **Eina de gestió d'albarans:** portal que permet validar el servei efectivament rebut i que permet als proveïdors iniciar el procés de facturació dels serveis entregats al CTTI. L'empresa homologada podrà consultar l'estat de validació del servei entregat i, un cop validat pel CTTI, recuperar el codi d'albarà que haurà de constar a la factura.

4.3.1.3 Eina de Governança de Demanda i Projectes

El CTTI disposa d'eines per gestionar la demanda de projectes i fer el control i seguiment dels projectes.

L'empresa homologada haurà d'utilitzar aquesta eina conjuntament amb el CTTI per dur a terme les tasques relacionades amb els processos i procediments relatius a les peticions de servei del contracte següents:

- Control i gestió de la cartera de projectes.
- Presentació i acceptació de propostes.
- Formalització de la comanda.
- Planificació i acceptació de fites de facturació.
- Control i seguiment dels projectes.

El grau de control i seguiment dels projectes s'estipularà en funció de la criticitat del projecte per al negoci i del que estableixi la metodologia del CTTI.

L'empresa homologada podrà realitzar el seguiment detallat dels projectes en les seves pròpies eines, assegurant que la informació requerida s'actualitza sobre les eines del CTTI.

4.4 Processos, activitats i documentació associada a la gestió de serveis

La finalitat de la gestió de serveis és controlar i vetllar que els serveis estiguin disponibles, accessibles, mantinguts, actualitzats, informats, difosos als diferents actors implicats i que compleixin els objectius de qualitat del CTTI.

Els processos del CTTI estan definits i aprovats per la Direcció i publicats per l'acompliment de tots els actors implicats.

Aquests processos es suporten, majoritàriament, en una única eina de gestió a fi d'agilitzar, documentar i controlar qualsevol esdeveniment, incidència, problema, error conegut o dada, necessària per a cada servei i donar la millor resposta possible davant de qualsevol petició. Aquesta eina és propietat del CTTI i és qui en determina l'ús. Podrà ser utilitzada pel SAU, CTTI i qualsevol empresa homologada de serveis que intervingui en els gestió dels processos relacionats de serveis.

Tota la informació, vinculada a cada element dels processos detallats a continuació, ha de poder ser consultada per qualsevol agent que participi en aquest procés (Usuaris, SAU, CTTI, Centre de Control, proveïdors o altres agents). Com a mínim són els següents:

4.4.1 Gestió de la Disponibilitat, Capacitat i Continuïtat

La gestió de la disponibilitat, capacitat i continuïtat són tres dels eixos de l'observabilitat, on la disponibilitat del sistema fa esment a què els serveis del núvol públic sobirà estan en funcionament i prestant el servei de manera efectiva, mentre que en la capacitat és important el dimensionament per satisfer la demanda del servei requerit, fent esment que una falta de capacitat pot derivar a curt o mig termini a una incidència de disponibilitat del núvol.

La funció de la gestió de la capacitat haurà de ser liderada per l'empresa homologada, que ha d'optimitzar la gestió de recursos i preveure l'evolució del consum, notificant amb anticipació suficient les situacions on es pugui produir manca de recursos o be recursos excedents.

És responsabilitat de l'empresa homologada la gestió de la disponibilitat, capacitat i continuïtat del núvol públic sobirà així com del seu dimensionament inicial. A partir del dimensionament inicial dels serveis, aquests evolucionen i serà necessari que l'empresa homologada analitzi i entengui l'impacte de càrrega dels recursos i/o infraestructures de la demanda del negoci actual i com aquest evolucionarà o es comportarà al llarg del temps.

4.4.2 Conciliació, Acceptació del Servei i Facturació

El CTTI té establerts procediments de conciliació dels costos, d'acceptació del servei rebut i facturació. L'empresa homologada ha de seguir aquests procediments i utilitzar les eines que el CTTI té implementades.

Les despeses que es puguin derivar de l'adaptació dels sistemes d'informació de l'empresa homologada als formats que sol·liciti el CTTI seran al seu càrrec. També serà la responsable de donar suport tècnic al CTTI en qualsevol dubte relacionat amb els elements facturats i els formats d'elements de cost i facturació.

A alt nivell i amb dates aproximades, un cicle de facturació es subdivideix en els següents passos:

- Recepció dels fitxers de cost i càrrega a les eines de CTTI (de l'1 al 5 de cada mes).
- Conciliació de costos rebuts i identificació de serveis no inventariats (costos que no s'acceptaran) i termini perquè el proveïdor ho solucioni (fins al 10 de cada mes).
- Procés de repercussió de costos a client i publicació d'informes (fins al 20 de cada mes).
- Acceptació del servei rebut mitjançant l'aprovació de l'albarà o albarans de proveïdor (dia 20 de cada mes).
- Emissió de la factura de proveïdor cap a CTTI (a partir del 20 de cada mes).
- Publicació i revisió de discrepàncies (a partir del 20 de cada mes).

4.4.2.1 Recepció de Costos dels Serveis

L'empresa homologada haurà de lliurar al CTTI un detall dels costos dels serveis prestats mitjançant un fitxer tipus csv en el format que el CTTI té establert. Addicionalment haurà de fer les actuacions tècniques necessàries per integrar amb la periodicitat que s'estipuli, els costos en l'eina de FinOps de CTTI.

Aquest detall de costos contindrà la informació necessària per poder-se correlacionar amb l'inventari i els elements de cost imputables a recursos individuals, independentment de la solució tècnica sobre la qual se suporti el servei. Els costos hauran d'estar alineats amb el procés de provisió del servei (dades identificatives dels elements, data d'alta, data de baixa, etc.).

Les incorporacions d'elements de cost que impliquin una nova tipificació en el fitxer de costos hauran de ser notificades al CTTI, amb una anticipació mínima de trenta (30) dies naturals a la implantació dels serveis.

El CTTI podrà realitzar canvis en el format del fitxer durant l'execució del contracte per adaptar-lo a altres serveis o elements de cost, i l'empresa homologada els haurà d'aplicar en un termini màxim de dos mesos.

4.4.2.2 Conciliació de Costos Rebuts

El CTTI realitzarà la conciliació de les dades rebudes requerint suport per part de l'empresa homologada si fos necessari. En cas de discrepàncies o incongruències en la facturació, durant el procés de conciliació aquestes seran tractades de forma conjunta entre el CTTI i l'empresa homologada.

Si la responsabilitat de la discrepància recau sobre l'empresa homologada, a més del retorn del valor de la discrepància el CTTI podrà sol·licitar a l'empresa homologada que assumeixi el cost de gestió que ha suposat per al CTTI el tractament de dita discrepància.

En termes generals les regles de conciliació implantades analitzen els punts següents :

- Que les tarifes siguin correctes: imports correctes, tarifa vigent, aplicació de franges tarifàries segons volumetria, entre d'altres.
- Que l'inventari sigui correcte: el servei existeix i està actiu a inventari, les volumetries facturades i inventariades coincideixen, entre d'altres.
- Que es compleixi la lògica de facturació: no hi ha duplicats, no hi ha càrrecs incompatibles, entre d'altres.

4.4.2.3 Acceptació del Servei Rebut

El procés de facturació considera, previ a l'enviament de la factura al CTTI, una conformitat de la prestació del servei a través d'un document o albarà, seguint els procediments, eines i els estàndards del CTTI.

El CTTI validarà només el cost que es pugui confirmar com a servei prestat.

4.4.2.4 Facturació dels Serveis Rebuts

La factura finalment emesa per l'empresa homologada indicarà el codi d'albarà de validació i estarà desglossada pels diferents grups d'elements o serveis tecnològics que la componen. La factura s'emetrà segons l'establert al pla de facturació detallat al plec administratiu.

El CTTI podrà canviar, durant la vigència del contracte, el model de facturació actual a un model d'auto-factura.

4.5 Gestió de la Seguretat

En matèria de seguretat de la informació, l'empresa homologada ha de garantir el compliment dels requeriments establerts a la clàusula *3.1.6 Requeriments de sobirania de seguretat i compliment* d'aquest plec.

L'empresa homologada serà el responsable de la gestió de la seguretat dels serveis objecte d'aquesta licitació i dels corresponents basats que se'n derivin.

Atès que la seguretat és un aspecte essencial del servei objecte del contracte, l'empresa homologada haurà de portar a terme totes les actuacions necessàries de prevenció, detecció, protecció, resposta i recuperació per garantir uns elevats nivells de seguretat dels serveis.

Per aquestes actuacions, i donada la naturalesa canviant de les amenaces i l'evolució tecnològica, l'empresa homologada mantindrà un procés de millora contínua i adequarà els controls de seguretat durant l'execució del servei, d'acord amb l'ENS i les directrius vigents del CTTI o de l'Agència de Ciberseguretat. Així mateix, re-avaluarà els controls davant canvis significatius, incidents rellevants o noves exigències i aportarà les evidències que li siguin requerides, sense cost addicional.

Respecte la subcontractació de béns i serveis, l'empresa homologada haurà d'analitzar i mitigar riscos derivats de la cadena de subministrament, aplicant les mesures de contingència necessàries i garantint el mateix nivell de compliment en tota la cadena.

El CTTI i l'Agència de Ciberseguretat de Catalunya i els organismes competents podran auditar la correcta execució dels processos (qualitat i seguretat) per aquest fet, l'adjudicatari garantirà l'accés total als documents que es sol·licitin i eines relacionats, prestarà assistència sense cost addicional, i executarà el pla d'acció acordat en forma i termini.

Per tot l'anterior, s'establiran els mecanismes de coordinació necessaris amb CTTI i l'Agència de ciberseguretat.

Efectes del no compliment dels requeriments de seguretat

Qualsevol incompliment que afecti els requisits de seguretat de la clàusula 3.1.6 d'aquest plec (incloent llindars d'anàlisi, traçabilitat, identitat, comunicacions, excepcions no gestionades, auditories, observabilitat, PRD/backups, etc) es considerarà un defecte en la prestació del servei.

L'adjudicatari procedirà a corregir el defecte dins del termini de 5 dies, sense cost addicional per al CTTI, i n'aportarà les evidències. Els incompliments comportaran les penalitats previstes a l'ANS.

En sistemes de categoria ALTA, el CTTI podrà suspendre temporalment la prestació de serveis o la operació del sistema fins a la seva adequada esmena o mitigació (art. 31.6 ENS), sense perjudici d'altres mesures que corresponguin d'acord amb l'ENS, la política de Ciberseguretat de la Generalitat de Catalunya, aquests plecs o qualsevol altra normativa aplicable i vigent.

Els incompliments que afectin dades personals es regiran pel disposat a la normativa aplicable en matèria de protecció de dades (RGDP i LOPDGG).

Deure de Confidencialitat

El personal de l'empresa homologada ha de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat té caràcter indefinit i subsistirà inclús després d'haver cessat la seva relació laboral amb el Contractista.

L'empresa homologada ha de comunicar aquesta obligació de confidencialitat al seu personal i ha de controlar el seu compliment.

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

4.6 Gestió ambiental i sostenibilitat

La consecució de polítiques públiques ambientals i socials és clau per l'assoliment d'un desenvolupament sostenible.

Per tant, en matèria de restriccions a la utilització de determinades substàncies perilloses i sobre la gestió dels residus dels productes elèctrics i electrònics, seran d'aplicació la Llei 22/2011, de 28 de juliol, de residus i sòls contaminats, el Reial Decret 219/2013, de 22 de març, sobre restriccions a la utilització de determinades substàncies perilloses en aparells elèctrics i electrònics, i el Reial Decret 110/2015, de 20 de febrer, sobre residus d'aparells.

L'empresa homologada haurà de vetllar per l'excel·lència en la prestació del servei tenint en compte la sostenibilitat ambiental de les activitats en la prestació dels serveis i obres objecte d'aquest contracte, aplicant polítiques de millora i sostenibilitat contínua en tot el cicle de vida mitjançant el seguiment, validació i verificació de la implantació de les mesures que duguin a reduir l'impacte ambiental, per exemple garantint la retirada i reciclatge de tot aquell material que es doni de baixa o s'hagi de substituir.

Per tot l'equipament electrònic necessari per a la prestació del servei, l'empresa homologada haurà de garantir que els equips acompleixin amb la regulació RoHS (Restriction of Hazarous Substances), es a dir, que els equips estan fabricats i són lliures de materials perillosos com són el plom, mercuri, cadmi, cromo VI (també conegut com cromo hexavalent), PBB i PBDE. L'empresa homologada també haurà de garantir que els equips electrònics per a la prestació del servei, acompleixen amb estàndards d'eficiència energètica per aquest tipus d'equipament com és l'energy star, o equivalent.

L'empresa homologada haurà d'elaborar, mantenir i executar un "Pla de Sostenibilitat Ambiental", per el servei o grups de serveis a validar per part del CTTI que haurà d'incloure, els aspectes següents:

- Informe anual del control de les emissions de gasos d'efecte hivernacle (GEH) en la prestació del servei, fonamentat en calculadora d'emissions de GEH de l'Oficina Catalana del Canvi Climàtic.

- Informe anual de l'impacte en l'aplicació de la norma ISO 14001 o EMAS a la seva organització.

4.7 Seguiment contractual

A continuació es detallen les principals obligacions contractuals que haurà de complir l'empresa homologada:

Periodicitat	Descripció
Abans de la formalització del contracte	Declaració responsable sobre la ubicació dels dos CPD
Abans de la formalització del contracte	Informe sobre l'aplicació de les mesures de conciliació
En 10 dies des de la formalització	Pla de mesures de conciliació corresponsable del temps laboral, familiar i personal en relació a les persones ocupades en l'execució del contracte
En el primer mes de contracte	Pla de treball (Pla Director) per desplegar tots els serveis descrits en el plec.
Mensual	Comitè Operatiu
Bimensual	Comitè Tàctic
Semestral	Comitè Estratègic
Semestral	Informe de l'estat en què es trobin les subcontractacions i de les mètriques de qualitat que efectuïn sobre les empreses subcontractades
Anual	Informe de seguiment del servei d'acord amb l'apartat de seguretat
Anual	Formació o transferència de coneixement als professionals del CTTI (mínim 5 sessions de 8 hores cadascuna o equivalent)
Anual	Pla de Sostenibilitat Ambiental

Taula Quadre resum principals obligacions contractuals

5 FASES DE LA PRESTACIÓ DEL SERVEI

L'empresa homologada executarà la prestació del servei d'acord al pla acordat que tingui en compte les característiques i fases específiques que es detallen a continuació:

5.1 Fase de Constitució del Servei

Aquesta fase inclou totes les tasques necessàries per a la prestació dels primers serveis de cloud computing que se sol·licitin en el primer basat.

L'objectiu d'aquesta fase és la preparació de tota la infraestructura per disposar de tot el catàleg de serveis de cloud computing i desplegar les primeres solucions TIC.

La duració d'aquesta fase serà d'un màxim de dotze (12) mesos, a comptar des de l'inici del contracte de la primera comanda realitzada, i fins la posada en marxa dels primers serveis de cloud computing sobre la nova regió.

Durant aquest període el CTTI es reserva el dret d'iniciar la fase de prestació del servei utilitzant els serveis de la regió europea addicional de núvol públic sobirà.

Com a part de la fase de constitució del servei, l'empresa homologada haurà de seguir el procés de Preparar el Servei de CTTI per assegurar que els equips que gestionen l'operació i explotació dels serveis disposen de tota la informació necessària per poder realitzar-la amb la qualitat esperada.

És imprescindible que totes les tasques del procés estiguin finalitzades per poder activar el servei als usuaris finals.

Un cop finalitzada la constitució de la regió de núvol públic sobirà, l'empresa homologada haurà de demostrar el compliment de tots els requisits del servei, en especial l'assoliment del grau de sobirania SEAL-3. El CTTI establirà un comitè específic d'avaluació d'aquest compliment.

5.2 Fase de Prestació del Servei

Aquesta fase engloba l'execució de tots els serveis definits a l'objecte, tal i com es descriu a l'apartat 3. *Descripció dels serveis.*

Aquesta fase tindrà una durada que abastarà des de la posada en marxa dels primers serveis fins a la finalització del contracte.

5.3 Fase de Devolució del Servei

Aquesta fase té com a objectiu garantir la millor transferència d'informació, documentació, activitats de traspàs de coneixement i qualsevol operativa que es derivés del contracte, al CTTI o a qui el CTTI determini.

El licitador inclourà en la seva proposta un Pla de Devolució del servei detallat que descrigui les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts en relació amb la devolució i que inclogui els termes i condicions en què es realitzarà aquesta

reversió. A més, caldrà posar a disposició del proveïdor entrant la documentació, contactes i tot el que sigui necessari per assegurar la transferència òptima del coneixement sense afectar la prestació del servei de la Generalitat.

En cas de cessament o finalització del contracte, el proveïdor estarà obligat a tornar el control dels serveis objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb els de prestació del servei, sense cost addicional per al CTTI.

El termini d'execució de la fase de devolució serà de dotze (12) mesos des de la notificació oficial d'expiració o cancel·lació, total o parcial del servei, durant els que l'empresa homologada haurà de posar en pràctica el Pla de Devolució descrit a la seva oferta alineat als requisits aquí detallats. El CTTI es reserva el dret de poder reduir el termini d'execució segons consideri necessari.

Durant el període de la devolució del servei, l'empresa homologada ha de complir els acords de nivell de servei (ANS). El pla de devolució no haurà de causar cap discontinuïtat en el servei o en la seva qualitat, així com cap pèrdua de la normativa associada a la sobirania. En el període de la devolució del servei l'empresa homologada només facturarà els serveis que estigui operant, els quals s'aniran reduint fins al final de la devolució.

El CTTI podrà subscriure un contracte de llicència d'ús sobre els sistemes de l'empresa homologada que fossin necessaris per a assegurar la continuïtat del servei.

Les etapes del procés de devolució seran les següents:

a) <u>Notificació formal i planificació inicial</u>
   - CTTI notificarà amb un mínim de 12 mesos la finalització del contracte
   - Es revisaran les clàusules contractuals del servei
   - L'adjudicatari realitzarà una definició detallada del pla de devolució que contingui com a mínim:
     - La metodologia de transferència de coneixement dels aspectes fonamentals d'operacions i projectes en curs
     - La definició de responsabilitats i la gestió de la resolució de problemes entre la nova empresa homologada, el CTTI i/o altres empreses.
     - El nivell de suport tècnic que s'oferirà durant tot el procés, incloent punts de contacte, resposta a incidències i disponibilitat d'experts per resoldre dubtes o problemes.
     - Compromís de compliment legal i de seguretat: El pla de devolució ha d'assegurar el compliment de la normativa de protecció de dades (per exemple, RGPD) i altres regulacions aplicables associades a la sobirania.

b) <u>Inventari final de serveis i artefactes gestionats per l'adjudicatari</u>
   - Detall dels serveis desplegats
   - Volumetria d'emmagatzematge consumit
   - Configuració detallada dels tenants o subscripcions
   - Relació d'identitats amb drets d'accés
   - Certificats, secrets i claus
   - Configuració de connectivitat
   - Automatitzacions i polítiques d'estalvi declarades

c) <u>Pla de formació al nou adjudicatari</u>

- Processos de gestió del tenant
- Processos de gestió definits adhoc durant el servei
- Accés a la informació, la documentació i altre material utilitzat pel proveïdor actual en la provisió del servei per la Generalitat de Catalunya.

d) Transició progressiva al nou adjudicatari
   - Coordinació per evitar interrupcions de servei
   - Opcions de coexistència del servei anterior i el nou durant la fase de devolució

e) Eliminació segura de dades de gestió del servei del proveïdor actual
   - Procediment certificat d'esborrat segur de la informació requerida segons polítiques de sobirania i normatives europees.

f) Tancament administratiu
   - Revisió de facturació pendent
   - Revisió de penalitzacions pendents
   - Emissió de l'acte d'acceptació de la fase de devolució i la finalització del contracte

6 ACORDS DE NIVELL DE SERVEI (ANS)

6.1 Objectiu

Es descriu el model d'Acord de Nivell de Servei (en endavant ANS), que defineix els indicadors i els nivells de servei exigits, i estableix una base objectiva i mesurable que reflecteixi el compromís entre l'empresa homologada i el CTTI per prestar els serveis requerits de forma satisfactòria.

El CTTI pretén obtenir un nivell de servei d'alta qualitat, així com un grau de satisfacció elevat, fonamentat en:

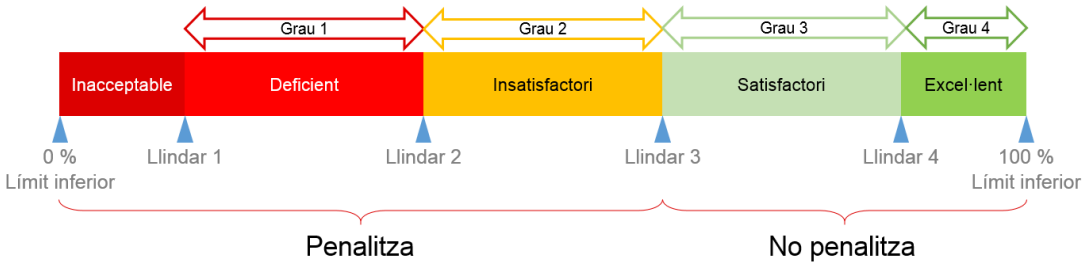
- L'establiment d'indicadors de servei, de manera que el CTTI pugui realitzar una avaluació objectiva del servei i els seus lliurables, i que l'empresa homologada tingui una base per a la correcció de les eventuals deficiències en la prestació, i per a la millora dels seus processos i organització.
- L'establiment d'un model de penalitzacions que relacioni el nivell de prestació del servei amb la seva facturació.
- L'establiment d'indicadors que permetin mesurar el grau de satisfacció percebuda pels usuaris del servei.

A "l'Annex ANS" del present plec es troben els indicadors de servei definits pels serveis descrits en aquest document. Els indicadors que hi consten s'aplicaran en el càlcul de les penalitzacions per incompliment del llindar mínim requerit com s'explica a continuació.

6.2 Característiques dels Indicadors

Els indicadors tindran les següents característiques:

- **Codi**. Identificador únic de l'indicador.
- **Nom**. Defineix l'objecte de mesura de l'indicador.
- **Descripció**. Descripció de l'indicador i el seu objectiu. S'inclouen les restriccions necessàries per dur a terme el càlcul del valor de l'indicador (per exemple, restriccions horàries, tipificació dels incidents, etc.).
- **Categoria**. Agrupa diferents ANS d'un mateix tipus. Per exemple: Consultes, Gestió de Peticions, Gestió d'incidències, Gestió d'Inventari.
- **Fórmula d'obtenció/eina**. Fórmula a aplicar pel càlcul del valor de l'indicador de mesura, identificant les variables que intervenen al càlcul (mètriques) i, si escau, la referència a l'eina que permet l'automatització i extracció de les dades.
- **Periodicitat**. Freqüència de mesura del valor de l'indicador.
- **Llindars de grau per a la definició dels trams**. Valors que defineixen el grau de compliment del nivell de servei exigit. Per a cada indicador es definiran 4 llindars de grau. En funció de la banda en què es trobi l'indicador presentarà els valors següents:



Il·lustració: Llindars de grau per indicadors

- **Penalització màxima (PPMax).** Determina el valor màxim al qual pot arribar la penalització en el cas d'incompliment del llindar objectiu definit.

6.2.1 Grau d'Indicadors

El grau de l'indicador pot prendre els valors següents:

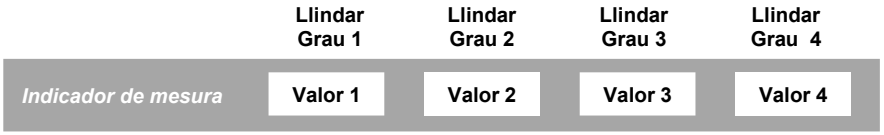
Grau	Valor
1	Deficient o Inacceptable
2	Insatisfactori
3	Satisfactori
4	Excel·lent

Taula: Valors del grau de l'indicador

El grau 4 serà el nivell objectiu, mentre que el grau 3 serà el nivell d'acompliment mínim per considerar que l'indicador és satisfactori.

6.3 Càlcul dels Indicadors

Per tot indicador s'estableixen 4 llindars que defineixen els trams lineals que han de permetre l'obtenció del grau associat.



Il·lustració: Indicadors de mesura i llindar

Pel valor mesurat per un indicador (valor indicador), s'haurà de cercar entre quins llindars es troba i aplicar el següent procediment, tenint en compte si els valors definits pels llindars (Valor 1 – Valor 4) són creixents o decreixents:

- Per valors de llindars creixents (valor Llindar Grau 1 < valor Llindar Grau 4).
- Per valors de llindars creixents (valor Llindar Grau 1 < valor Llindar Grau 4).
- Si el valor és inferior al llindar 1, el grau serà 1.
- Si el valor és igual o superior al llindar 4, el grau serà 4.
- En la resta de casos s'aplicarà la fórmula de càlcul del grau.

- Per valors de llindars decreixents (valor Llindar Grau 1 > valor Llindar Grau 4).
- Si el valor és superior al llindar 1, el grau serà 1.
- Si el valor és igual o inferior al llindar 4, el grau serà 4.
- En la resta de casos s'aplicarà la fórmula de càlcul del grau.

6.3.1 Fórmula de Càlcul del Grau

$$Grau = \frac{(Valor\ indicador - Valor\ llindar\ inferior)}{(\text{Valor llindar superior } - \text{Valor llindar inferior})} + Grau\ corresponent\ al\ llindar\ inferior$$

En aplicar la fórmula de càlcul del grau, cal tenir en compte les consideracions següents:

- Quan dos o més llindars prenen el mateix valor, el valor del "Grau corresponent al llindar inferior" correspon al del llindar coincident superior.

Per exemple, quan el Llindar Grau 1 i el Llindar Grau 2 prenen el mateix valor, el "Grau corresponent al llindar inferior" correspon al del Llindar Grau 2, és a dir, pren valor 2.

- Quan el valor mesurat per un indicador (valor indicador) coincideix amb algun dels valors definits pels llindars (Valor 1, Valor 2, Valor 3), es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident. Quan dos o més llindars prenen el mateix valor, es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident superior.

Per exemple, suposant els següents valors de llindars: Llindar Grau 1 i el Llindar Grau 2 prenen el mateix valor, 20%, Llindar Grau 3 pren valor 75% i Llindar Grau 4 pren valor 95%; quan el valor mesurat per l'indicador pren valor 20%, el "Valor llindar inferior" pren valor 20%, el "Valor llindar superior" pren valor 75% i el "Grau corresponent al llindar inferior" pren valor 2.

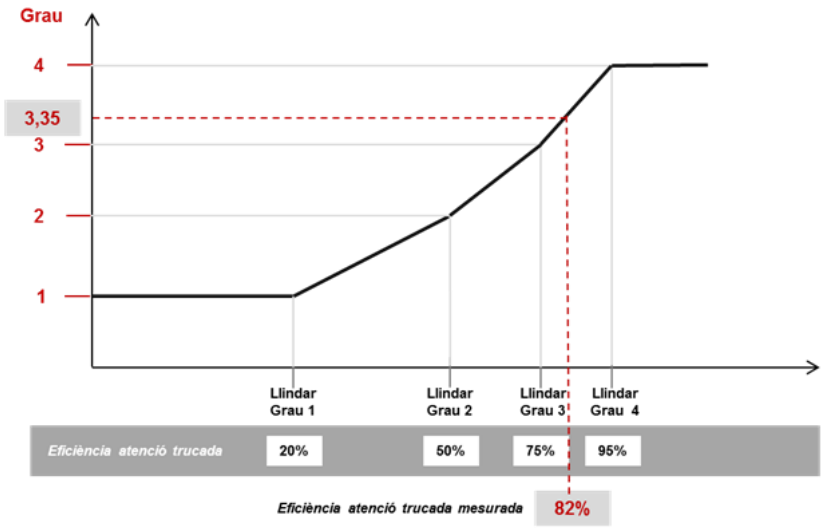
6.3.2 Exemple de Càlcul

Suposem que tenim l'indicador "Eficiència atenció trucada" que pot prendre valors percentuals entre 0% i 100% i que el valor objectiu és 95%. Si s'han definit els següents llindars:

Llindar Grau	Valor de l'indicador
1	20%
2	50%
3	75%
4	95%

Taula: Exemple de valor de l'indicador i llindar

Si el valor mesurat en un període per l'indicador "Eficiència atenció trucada" ha estat 82%, el grau calculat és: ((82-75)/(95-75))+3=3,35.



Il·lustració: Exemple valor de grau calculat

Aquest model és dinàmic, ja que permet adaptar-se en el temps a nous nivells objectius i nivells mínims, sense variar els graus possibles.

6.4 Relació d'ANS

L'empresa homologada serà la responsable de portar la informació necessària perquè es pugui valorar el grau de compliment dels indicadors indicats.

També podrà presentar una proposta de nous indicadors addicionals per a la revisió, actualització i millora dels esmentats indicadors, i un procés per al monitoratge continu dels seus indicadors que es pot trobar la relació a l'Annex ANS.

6.5 Fonts d'informació per a l'obtenció dels nivells de servei

El CTTI emprarà el sistema d'informació CONTIC (Control d'acord de nivell de servei TIC) per al càlcul, anàlisi i emmagatzemament d'indicadors de servei i de procés. Tot i que a l'inici del servei el sistema d'informació CONTIC no sigui capaç de calcular tots els indicadors definits, s'aniran incorporant progressivament al seu catàleg. El proveïdor haurà de proveir els indicadors que estiguin sota la seva responsabilitat a través de les interfícies habilitades.

Principalment l'origen de les dades utilitzat per al càlcul dels indicadors seran les eines de gestió dels tiquets i monitoratge del CTTI. Per aquells indicadors que el CTTI no sigui capaç d'obtenir de manera autònoma, serà responsabilitat de l'empresa homologada calcular-los i reportar-los amb la periodicitat establerta i el detall i format que requereixi el CTTI, podent arribar a nivell d'instància de servei o de tiquet.

El CTTI utilitzarà els indicadors de servei per realitzar els càlculs de compliment dels ANS i per generar els informes corresponents.

6.6 Modificacions dels indicadors i nivells de servei

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei, el CTTI conjuntament amb l'homologat consensuaran i planificaran la seva modificació.

Algunes de les causes que poden comportar aquestes modificacions són, entre d'altres, les variacions d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, les innovacions i les millores del servei.

6.7 Aplicacions dels acords de nivell de servei

Els Acords de Nivell de Servei definits per a cada servei seran d'obligat compliment al llarg del contracte, excepte que per causes de força major o circumstàncies excepcionals, i de mutu acord, es podrà decidir la no obligatorietat del compliment d'alguns ANS.

6.8 Pla de millora en el cas d'incompliment reiterat dels ANS

En cas d'incompliment reiterat dels Acords de Nivell de Servei, durant un període de 3 mesos consecutius o 3 mesos alternats en un període de 6 mesos, el proveïdor estarà obligat a presentar un pla de millora del servei amb l'objectiu d'assolir el compliment dels ANS. S'entén com a incompliment dels ANS que un 25% o més dels indicadors de mesura relacionats a Annex ANS estiguin per sota del llindar 3.

El pla de millora s'haurà de presentar en un termini de 2 setmanes a partir que es compleixi la condició anterior i, un cop validat pel CTTI, s'executarà amb els mitjans propis de l'empresa homologada, sense que aquesta pugui repercutir-ne el cost ni dedicar els recursos del servei de forma significativa.

El pla de millora haurà de permetre el compliment dels ANS en un termini màxim de 2 mesos

7 MODEL DE GOVERNANÇA

El model de prestació de serveis TIC de CTTI està definit com un escenari multi proveïdor amb externalització de serveis tecnològics. El responsable de l'estratègia i el Govern TIC és el CTTI i el model de governança estableix el model de relació entre els diferents actors implicats; Generalitat, CTTI, i proveïdors. Així, doncs, aquest model de relació estableix les activitats, entrades i sortides dels diferents comitès que el configuren, així com els mecanismes de seguiment per assegurar que la governança es duu a terme de la manera més eficaç i eficient possible. En definitiva el model de governança TIC de la Generalitat de Catalunya té com a objectiu gestionar de manera eficient i eficaç els recursos TIC disponibles, per tal de garantir el millor servei que doni resposta a necessitats estratègiques, de seguretat i operatives dels departaments i entitats.

Amb aquest objectiu es planteja un model de relació amb tres nivells de governança, i diferents comitès de seguiment o òrgans de gestió.

7.1 Model de relació

El model de relació es basa en establir els comitès i el seu funcionament, per assegurar el compliment dels requeriments de les condicions d'execució dels serveis descrites en aquest plec. Aquests comitès tindran també com a funció executar els mecanismes per ajustar aquestes condicions d'acord amb l'evolució de les necessitats de servei.

A continuació es concreta el model de relació i estructura de comitès que s'implementarà per la governança específica dels serveis objecte d'aquesta licitació i que s'emmarquen en el model de governança general.

Els nivells funcionals del model de relació són el nivell estratègic, el tàctic i l'operatiu.

Tant l'empresa homologada com el CTTI es comprometen a què les decisions preses en un nivell flueixin al nivell posterior o anterior.

7.1.1 Nivell Estratègic

A nivell estratègic, el nivell executiu del CTTI i l'empresa homologada tindran un intercanvi d'experiències i visions sobre l'estat de l'art dels serveis i les tendències d'evolució tecnològica d'aquests, defineix objectius, pren decisions d'alt nivell i gestió de riscos majors. Els assistents per part de l'empresa homologada als comitès d'aquest nivell hauran de tenir capacitat decisòria sobre els compromisos de serveis.

El nivell estratègic, des de la perspectiva de l'empresa homologada, és el nivell màxim de seguiment del contracte i la prestació del servei. Des d'aquest nivell, s'elevarà a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.

7.1.2 Nivell Tàctic

En aquest nivell es farà un seguiment exhaustiu de l'execució dels serveis dels contractes basats i s'elevarà al nivell estratègic aquells aspectes que puguin originar la modificació del contracte. Defineix l'evolució del servei des de diverses perspectives transversals (arquitectura, seguretat, compliment, etc.) convertint les necessitats i exigències de sobirania i regulació en controls tècnics i polítiques a aplicar sobre el servei. També exerceix funcions de validació i aprovació dels canvis significatius

7.1.3 Nivell Operatiu

Aquest nivell té com a objectiu l'operació diària del servei segons els procediments desenvolupats i tractar les problemàtiques específiques que afectin el servei prestat. Supervisa i dirigeix la prestació del servei, gestionant incidents, els ANS, els canvis, la facturació del servei i en general qualsevol activitat relacionada amb la operació del servei.

7.2 Òrgans de Gestió (Comitès)

A continuació es descriuen la composició dels diferents comitès entre el CTTI i l'empresa homologada, així com altres actors de la Generalitat, i el seu funcionament, per assegurar el compliment dels requeriments de les condicions d'execució dels serveis descrites en aquest plec. Aquests comitès tindran també com a funció executar els mecanismes per ajustar aquestes condicions d'acord amb l'evolució de les necessitats de servei.

En aquest apartat es descriuen tant els òrgans de gestió de l'Acord Marc com els dels contractes basats.

L'empresa homologada haurà de fer explícita l'estructura i funcionament dels Comitès de relació i coordinació sense incorporar els comitès estratègics que siguin precisos per mantenir una interlocució permanent amb els actors involucrats en el procés.

Si així ho estimés convenient, el CTTI podrà incorporar canvis en la freqüència de celebració de les reunions, així com sol·licitar reunions extraordinàries de seguiment.

De forma extraordinària i, sota la supervisió del comitè executiu del basat, podrà formar-se un equip de treball de caràcter temporal amb objectius específics acordats prèviament.

A continuació es descriuen els diferents comitès identificats anteriorment amb la següent estructura a títol enunciatiu, sens perjudici que al llarg de l'execució del servei es puguin ajustar les característiques de cada comitè (Participants, Objectius, Entrades, Sortides, etc.).

En aquest sentit, l'empresa homologada haurà d'incorporar als diferents comitès les persones responsables de cada àmbit d'execució en funció dels temes específics a tractar en el comitè.

Tant l'empresa homologada com el CTTI es comprometran a què les decisions preses en un nivell flueixin al nivell posterior o anterior.

7.2.1 Comitè Estratègic Acord Marc

Format pel responsable de l'empresa homologada i els representants que el CTTI determini, els assistents per part de l'empresa homologada a aquest comitè hauran de tenir capacitat executiva sobre els compromisos de servei. Aquest comitè es farà conjunt per a tots els contractes basats de l'Acord Marc adjudicats, i que es constituirà a partir de la primera adjudicació d'un contracte basat a una empresa homologada.

<table>
<tr><th colspan="2">Títol</th></tr>
<tr><td colspan="2">Comitè Estratègic Acord Marc</td></tr>
<tr><th>Participants mínims</th><th>Objectius / Temes</th></tr>
<tr><td>CTTI
- Direcció CTTI
- Responsable del contracte de l'AM
- Responsable dels contractes basats.
- Altres assistents (si escau)
Generalitat
- Responsable Agència de Ciberseguretat (si escau)
Proveïdor
- Responsable de compte
- Responsable de serveis
- Responsables dels àmbits d'execució específics. (si escau)</td><td>- Marcar les directrius estratègiques de l'AM.
- Realitzar el seguiment del conjunt d'activitats desenvolupades en el període, orientat especialment a l'assoliment dels objectius i eficiències plantejades pel proveïdor.
- Planificar, prioritzar i revisar les iniciatives en curs.
- Traslladar les directius estratègiques al nivell inferior.
- Mantenir una actitud proactiva en tots els aspectes de la relació, interessant-se pel compliment dels ANS i impulsant, dintre de la seva organització, qualsevol mesura de la qual en pugui resultar una millora continua de la qualitat global del servei.
- Fer seguiment del model econòmic.
- Revisió i estat de situació dels aspectes més rellevants de seguretat (riscos, incidents del període, projectes en curs).
- Revisar i proposar les penalitzacions per incompliment del servei i escalar-les a l'òrgan de contractació.
- Traslladar les directrius tàctiques als contractes basats.
- Planificar, prioritzar i revisar les activitats amb impacte transversal.
- Fer el seguiment de les obligacions contractuals.
- Desenvolupament de propostes d'innovació en línia amb l'estratègia transversal del CTTI.
- Elevar a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.</td></tr>
<tr><th>Entrades</th><th>Sortides</th></tr>
<tr><td>- Informes i quadres de comandament dels contractes basats.</td><td>- Acta (signada digitalment entre les parts)
- Decisions preses</td></tr>
</table>

- Actes comitès executius dels contractes basats. - Decisions a prendre.	- Propostes a l'Òrgan de Contractació
Periodicitat	
- Anual o a petició del CTTI.	

Taula Descripció del comitè estratègic

7.2.2 Comitè Tàctic Acord Marc

Format pel responsable de compte i de serveis, així com els representants que el CTTI determini. Aquest comitè es farà conjunt per a tots els basats de l'Acord Marc adjudicats.

Títol	
Comitè Executiu Contractes Basats	
Participants mínims	**Objectius / Temes**
CTTI - Responsable del contracte basat - Responsable del servei - Responsable del contracte de l'AM (si escau) - Altres assistents (si escau) Generalitat - Responsable Agència de Ciberseguretat Proveïdor - Responsable de compte - Responsables de serveis - Responsables dels àmbits d'execució específics (si escau)	- Marcar les directrius tàctiques del contracte basat. - Realitzar el seguiment del conjunt d'activitats desenvolupades en el període, orientat especialment a l'assoliment dels objectius i eficiències plantejades pel proveïdor. - Revisió i estat de situació dels aspectes més rellevants de seguretat (riscos, incidents del període, projectes en curs). - Informar i proposar al responsable del contracte de l'AM de les possibles modificacions del contracte basat que s'hagin de dur a terme. - Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord als acords de nivells de servei definits. - Revisar i proposar les penalitzacions per incompliment del servei i escalar-les al responsable del contracte de l'AM. - Acordar els quadres de comandament del contracte basat. - Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord amb els acords de nivells de servei definits. - Traslladar les directrius tàctiques al nivell operatiu. - Planificar, prioritzar i revisar les activitats. - Fer el seguiment de les obligacions contractuals i del model econòmic del contracte basat. - Desenvolupar propostes d'innovació en línia amb l'estratègia transversal del CTTI.

	- Realitzar el seguiment de l'operació i governança de la seguretat per part del proveïdor:
	  ○ Grau d'adequació al model de seguretat que ha d'implementar el proveïdor perquè s'adeqüi al model de Ciberseguretat.
	  ○ Eficiència en la gestió de vulnerabilitats dels serveis, fent focus en les vulnerabilitats crítiques.
	  ○ Excepcions de seguretat: volum, criticitat, controls compensatoris a aplicar, etc.
	  ○ Incidents de seguretat del període. Revisió i gestió de millores associades.
	  ○ Nivells de Servei de Seguretat del proveïdor (ANS).
	  ○ Seguiment de l'estat de seguretat dels projectes en curs: evolutius, correctius, etc.
	- Escalat de problemes
	- Tractament de les problemàtiques específiques

Entrades	**Sortides**
- Informes i quadres de comandament de seguiment del servei. - Actes comitès operatius dels contractes basats. - Actes comitès operatius de seguretat dels contractes basats. - Decisions a prendre.	- Acta (signada digitalment entre les parts). - Decisions preses. - Propostes al responsable de contracte de l'AM
Periodicitat	
- Semestral o a petició del CTTI.	

Taula Descripció del comitè executiu

7.2.3 Comitè Operatiu

Aquest comitè operatiu transversal es farà per cadascun dels contractes basats adjudicats. La periodicitat d'aquest comitè es preveu que sigui mensual, però aquest termini es podrà modificar d'acord amb les necessitats del servei.

<table>
<tr><th colspan="2">Títol</th></tr>
<tr><td colspan="2">Comitè Operatiu Transversal Contracte Basats</td></tr>
<tr><th>Participants mínims</th><th>Objectius / Temes</th></tr>
<tr><td>CTTI
- Responsable de servei
- Responsable contracte basat (si escau)
- Altres assistents (si escau)
Proveïdor
- Responsables de serveis
- Responsables operatius del servei</td><td>- Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord als ANS.
- Planificar, prioritzar i revisar les iniciatives en curs.
- Realitzar el seguiment de l'operació diària del servei, i verificar la correcta gestió de peticions, canvis, problemes i incidents.
- Desenvolupar i mantenir els procediments operatius necessaris per al correcte funcionament del serveis.
- Anàlisi de peticions i/o situacions de canvi en els serveis.
- Escalat de possibles millores detectades en el servei.
- Tractament de les problemàtiques específiques.
- Desenvolupament de propostes d'innovació en línia amb l'estratègia i necessitat de negoci del departament o entitat.</td></tr>
<tr><th>Entrades</th><th>Sortides</th></tr>
<tr><td>- Informes operatius de seguiment del servei.
- Anàlisi i propostes de millora.
- Decisions a prendre.</td><td>- Acta (signada digitalment entre les parts).
- Propostes al comitè executiu del contracte basat.
- Nous procediments operatius.</td></tr>
<tr><th colspan="2">Periodicitat</th></tr>
<tr><td colspan="2">- Trimestral o a petició del CTTI.</td></tr>
</table>

Taula Descripció del comitè operatiu

8 ANNEXOS

8.1 Annex ANS

ANNEX ANS_Núvol Públic Sobirà.xlsx