

**PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS QUE REGEIX LA
CONTRACTACIÓ DEL SUBMINISTRAMENT, INSTAL·LACIÓ I POSADA EN
PRODUCCIÓ D'EQUIPAMENTS DE DISTRIBUCIÓ DE CLAU QUÀNTICA**

Expedient núm.: CTTI-2026-36



**Finançat per
la Unió Europea**

1.	OBJECTE	4
2.	DESCRIPCIÓ DE LES PRESTACIONS DE LES FASES	5
2.1.	Fase Pla de migració	5
2.2.	Fase Execució crítica.....	6
2.3.	Fase Desplegament.....	7
2.4.	Fase Anàlisi de les dades	8
3.	CARACTERÍSTIQUES DELS EQUIPS A SUBMINISTRAR	9
3.1.	Equipaments QKD (CV-QKD i QRNG).....	9
3.1.1.	Compatibilitat i integració.....	9
3.1.2.	Rendiment i funcionalitat.....	10
3.1.3.	Format físic i instal·lació	11
3.1.4.	Comunicació i canals.....	11
3.1.5.	Gestió, control i monitoratge	12
3.1.6.	Seguretat.....	13
3.1.7.	Certificació i normatives.....	13
3.2.	Equipaments KMS	14
3.2.1.	Compatibilitat i protocols.....	14
3.2.2.	Capacitats i gestió de claus	15
3.2.3.	Seguretat i supervisió	16
3.3.	Garanties esteses i servei de manteniment	17
4.	CONDICIONS D'EXECUCIÓ DEL SERVEI	19
4.1.	Estructura organitzativa	19
4.1.1.	Funcions dels perfils	19
4.1.2.	Idoneïtat dels perfils.....	21
4.1.3.	Dimensionament organitzatiu	25
4.1.4.	Clàusula de seguretat.....	25
5.	FASES DE LA PRESTACIÓ DEL SERVEI	29
5.1.	Fase Pla de migració	29
5.2.	Fase Execució crítica.....	29
5.3.	Fase Desplegament.....	30
5.4.	Fase Anàlisi de les dades	30
5.5.	Pla de devolució del servei	30
6.	ACORDS DE NIVELL DE SERVEI (ANS).....	33
6.1.	Objectiu	33
6.2.	Característiques dels indicadors	33
6.3.	Grau de l'indicador.....	34
6.4.	Càlcul dels indicadors.....	34
6.4.1.	Fórmula de càlcul del grau.....	35
6.4.2.	Exemple de càlcul.....	35
6.5.	Relació d'ANS	36
7.	MODEL DE GOVERNANÇA.....	37
7.1.	Objectiu	37



7.2.	Abast	37
7.3.	Model de relació	37
7.3.1.	Nivells del model de relació	38
7.3.1.1.	Nivell Estratègic	38
7.3.1.2.	Nivell Tàctic	38
7.3.1.3.	Nivell Operatiu	38
7.3.2.	Òrgans de Gestió (Comitès)	39
7.3.2.1.	Comitè Estratègic	39
7.3.2.2.	Comitè Executiu	40
7.3.2.3.	Comitè Operatiu	41
7.3.2.4.	Comitè Operatiu de Seguretat	42
7.3.3.	Estructura de responsabilitats	43
7.3.3.1.	Responsable de compte	43
7.3.3.2.	Responsables de serveis	44
7.3.3.3.	Responsable de seguretat (RSP)	44



1. OBJECTE

L'objecte de la present licitació és el subministrament, instal·lació i posada en producció d'equipaments de distribució de clau quàntica (QKD), amb sistema de gestió de claus (KMS) i generador quàntic de nombres aleatoris (QRNG), integrat a la xarxa de connectivitat de la Generalitat de Catalunya.

En concret, l'objecte del contracte inclou les fases següents:

- Fase 1. Pla de migració: Elaboració d'un pla per migrar, d'una xarxa òptica complexa, a una xarxa òptica amb seguretat post-quàntica. Categorització i priorització de nodes, definició de requeriments
- Fase 2. Execució crítica: Subministrament, instal·lació, configuració i posada en producció dels equipaments a seus i segments crítics (als nodes previstos a la fase inicial), creant un bloc de comunicacions encriptat quànticament.
- Fase 3. Desplegament: Desplegament i ampliació de l'anterior bloc de comunicacions encriptat als nodes restants previstos. Inclou, com en el punt anterior, el subministrament i instal·lació física d'equips, configuració i posada en producció.
- Fase 4. Anàlisi de les dades: Observació, anàlisi de dades i formació, que inclou principalment: avaluació de comportament, monitoratge, tràfic i extracció de conclusions.



2. DESCRIPCIÓ DE LES PRESTACIONS DE LES FASES

L'abast d'aquesta licitació contempla els següents serveis i subministraments a realitzar a cada fase:

- Fase Pla de migració
- Fase Execució crítica (subministraments i instal·lació de la fase inicial)
- Fase Desplegament
- Fase Anàlisi de les dades

2.1. Fase Pla de migració

Aquesta fase consisteix en l'elaboració d'un pla per migrar l'actual xarxa òptica a una xarxa òptica amb seguretat post-quàntica, així com l'anàlisi, categorització i priorització dels nodes quàntics, definició de requeriments.

Aquest pla ha d'incloure, al menys:

- Definició concreta dels objectius:
 - o Categorització de nodes. Identificació de distàncies entre nodes, punts crítics, segments relacionals entre ells i tipus de tràfic per tal de garantir que la informació quàntica viatgi sense interrupcions.
 - o Ubicació de nodes. Definició de l'abast geogràfic concret, a Barcelona i la seva àrea metropolitana, per tal d'obtenir resultats pràctics en xarxes reals.
 - o Establiment de criteris de priorització de nodes i seus. Es requereix nodes connectats amb fibra òptica, amb pèrdues que no superin el lílindar màxim.
 - o Anàlisi i definició de requeriments. Anàlisi i definició de disponibilitat d'espais i altres requeriments. Els nodes de xarxa disposen de sales tècniques aptes per incloure-hi els equipaments requerits.
 - o Valoració de conclusions. Valoració de viabilitat de la intervenció. Entrega d'un lliurable final que reculli les conclusions sobre l'abast del desplegament d'equipaments quàntics.
- Descripció de la topologia.
- Requisits previs.
- Disseny final de la nova arquitectura.
- Descripció de les dues següents fases (fase d'execució crítica i fase desplegament):
 - o Nodes de xarxa i seus implicades.
 - o Equipament a desplegar a cada node de xarxa o seu.
 - o Planificació detallada, amb dates i descripció de les actuacions.
 - o Plans de reversibilitat (rollback) per cada fase.
- Definició de proves i validació



- Entre les proves a realitzar, caldrà la prova d'integració per cada node QKD i KMS: Verificació de la generació, transmissió, recepció i ús correcte de les claus amb els equips de xarxa del node. El proveïdor haurà de certificar-ne el resultat, validat pels tècnics del CTTI.
- Avaluació de riscos i mesures de mitigació.
- Descripció del cronograma i recursos associats.
- Es definirà i acordarà amb el CTTI el contingut, i la periodicitat, dels informes operatius i executius, per al seguiment i control de les tasques i fases del contracte. El CTTI es reserva el dret de modificar els informes establerts, sol·licitar nous informes periòdics o ad-hoc, i introduir canvis en qualsevol moment de la vigència del contracte segons les necessitats del servei.
- Accés per part de qui determini el CTTI a una eina de seguiment de projecte. Actualitzada com a mínim de forma diària, per tal de garantir un control continuat i alineat amb els requeriments establerts a cada fase.

Gestió dels accessos dels tècnics als nodes i seus de la Generalitat tinguts en compte en el pla incloent la generació i actualització de la documentació necessària de PRL a l'eina de control de PRL / CAE.

2.2. Fase Execució crítica

Subministrament i instal·lació d'equipament a quatre (4) dels dotze nodes previstos en el pla de migració

Es pot tractar, per exemple, del segment entre dos centres de processament de dades, l'àmbit de l'àrea metropolitana adjacent i els principals edificis dins del segment, creant així un bloc de comunicacions encriptat quànticament.

Subministrament i instal·lació física d'equips, ajustament de les configuracions i posada en producció. Aquesta prova inicial ha de permetre detectar possibles errors de planificació i obtenir primeres dades d'anàlisi.

L'objectiu és integrar i validar la interconnexió de tots els equips necessaris en un entorn de laboratori, per elevar la maduresa de la tecnologia a un TRL8 (sistema complet i certificat, amb tecnologia acabada, testada i validada formalment per ser operativa i segura).

Això s'aconseguirà duent a terme les primeres proves i posada en marxa de la tecnologia garantint la interoperabilitat per al seu posterior desplegament als nodes en producció.

Durant aquesta fase, és fonamental que els fabricants de KMS, QKD i Generalitat col·laborin de manera estreta per garantir que la solució integral compleixi amb tots els requisits identificats per al desplegament en entorns de producció.

Aquesta etapa permetrà definir amb precisió els casos d'ús, les aplicacions i els serveis disponibles, així com els aspectes operatius essencials, com ara la gestió i monitorització integrada de la solució.

Les activitats mínimes a realitzar seran:

- Subministrament dels equips necessaris pels primers nodes.
- Desplegament inicial dels equips. Instal·lació física dels equips dels dos primers nodes i configuració bàsica per la posada en marxa dels mateixos. Un d'aquests



dos nodes haurà de correspondre obligatòriament al node ubicat a l'entorn de laboratori, que haurà de quedar plenament operatiu des del desplegament inicial.

- Calibratge i pas a producció. Ajustament de les configuracions dels nous equips i dels equips existents per garantir la comunicació entre extrems i la correcta encriptació.
- Escalat del tercer node. Desplegament dels equips del tercer node i avaluació de l'impacte al complicar l'arquitectura de dos a tres nodes i posada en producció.
- Escalat a la resta de nodes. Desplegament de la resta de nodes i seus fins a completar els quatre d'aquesta fase. Avaluació de com es comporta aquesta arquitectura més complexa. Posada en producció.
- En el cas que el CTTI decideixi posar en producció algun dels nodes desplegats durant aquesta fase, el licitador haurà d'efectuar el traspàs tècnic corresponent a l'equip designat pel CTTI, incloent la documentació, la configuració i qualsevol altre element necessari per a la seva correcta operació.
- El monitoratge dels equips posats en marxa s'haurà d'integrar amb el monitoratge del centre de control.
- Gestió del manteniment i garantia dels productes amb l'objectiu de garantir la disponibilitat dels equips posats en producció.

2.3. Fase Desplegament

Desplegament i ampliació del bloc de comunicacions encriptat quànticament als 8 nodes restants per tal d'obtenir una xarxa òptica protegida en un volum que permeti aconseguir conclusions vàlides pel que fa a instal·lació real, instal·lació operativa, integració en xarxa real, operació i manteniment reals, mètriques d'impacte real, retards, eficiència i consums.

Assegurant la integració i validació de la interconnexió de tots els equips necessaris elevant la maduresa de la tecnologia, al menys, a un TRL8 (sistema complet i certificat, amb tecnologia acabada, testada i validada formalment per ser operativa i segura).

Les activitats a realitzar, com a mínim, seran:

- Subministrament dels equips. Subministrament dels equips necessaris pels nodes d'aquesta actuació.
- Escalat a quatre nodes més. Desplegament de quatre nodes addicional en base a l'experiència de desplegament dels anteriors i avaluació de possibles increments temporals. Avaluació del comportament d'aquesta nova arquitectura, la qual tancaria l'anell metropolità. Posada en producció.
- Escalat final. Desplegament dels darrers quatre nodes i seus. Avaluació del comportament d'aquesta nova arquitectura, amb diverses seus desplegades connectades als nodes i a l'anell. Posada en producció.
- Manteniment de l'entorn de laboratori operatiu i en execució. L'entorn de laboratori haurà de mantenir-se actiu i plenament operatiu durant tota la vigència del contracte, amb capacitat per dur a terme tant proves internes com proves obertes amb tercers, segons les necessitats del CTTI. Finalitzat el contracte, el laboratori no podrà ser desmuntat ni retirat, i haurà de quedar com a



infraestructura permanent del CTTI, a disposició per a futures proves, validacions i activitats de desenvolupament relacionades.

- En el cas que el CTTI decideixi posar en producció algun dels nodes desplegats durant aquesta fase, el licitador haurà d'efectuar el traspàs tècnic corresponent a l'equip designat pel CTTI, incloent la documentació, la configuració i qualsevol altre element necessari per a la seva correcta operació.

2.4. Fase Anàlisi de les dades

Observació i anàlisi de les dades en operació real durant un període de temps que permeti extraure conclusions relacionades amb el producte evolucionat al mercat.

Les activitats principals necessàries per dur a terme l'actuació seran:

- Anàlisi de dades del tràfic entre els dos primers nodes. Avaluació del comportament del tràfic entre els dos primers nodes encriptats.
- Anàlisi de dades del tràfic entre els quatre primers nodes. Avaluació del comportament i del tràfic entre els quatre primers nodes encriptats i l'impacte de la complexitat de la nova arquitectura.
- Anàlisi de dades del tràfic dins de l'anell metropolità. Avaluació del comportament i del tràfic dins dels nodes de l'anell metropolità encriptats i l'impacte de la complexitat de la nova arquitectura.
- Anàlisi de la xarxa completa. Avaluació del comportament i del tràfic entre l'anell metropolità i les seues connectades, distingint topologies i peculiaritats dels senyals transmesos.
- Elaboració i lliurament del document que reculli, de manera estructurada i amb detall, les dades d'observació, els anàlisis realitzats i les conclusions derivades en aquesta fase.
- Formació i transferència de coneixement dels aspectes fonamentals d'operació descrita a l'apartat 5.5 Pla de devolució del servei d'aquest PPT.



3. CARACTERÍSTIQUES DELS EQUIPS A SUBMINISTRAR

3.1. Equipaments QKD (CV-QKD i QRNG)

Els sistemes de distribució quàntica de claus basats en variables contínues (CV-QKD) permeten la generació i transmissió segura de claus criptogràfiques mitjançant propietats quàntiques de la llum, com ara l'amplitud i la fase de camps electromagnètics coherents. Aquestes comunicacions es basen en parelles d'equips formats per un emissor i un receptor, que interactuen a través d'un canal òptic quantificat. Aquestes propietats permeten detectar qualsevol intercepció o manipulació de la comunicació, d'acord amb principis fonamentals de la mecànica quàntica, com el teorema de no-clonació i el col·lapse de l'estat quàntic.

Els equipaments subministrats hauran d'incloure tant mòduls emissors com receptors, necessaris per establir connexions completes entre nodes de la xarxa. Els equips han d'estar dissenyats per operar en entorns pràctics i reals, i ser compatibles amb la infraestructura de xarxa definida en aquest projecte.

A més, els equips han d'incorporar un mòdul de generació d'aleatorietat quàntica (QRNG) com a font d'alta entropia per a la generació o inicialització de claus. Aquest subsistema proporciona nombres aleatoris genuïns, no predictibles, garantits per fenòmens quàntics físicament verificables, i forma part integrant del sistema conjunt de QKD i KMS. La seva presència és necessària per assegurar nivells avançats de seguretat criptogràfica en entorns integrats.

3.1.1. Compatibilitat i integració

Tecnologia de modulació:

El sistema haurà de basar-se en CV-QKD amb esquema Prepare-and-Measure, i implementar protocols de modulació gaussiana d'estats coherents (GMCS).

Els equips QKD han de complir amb els requisits següents per garantir la seva integració en entorns reals i heterogenis:

- Compatibilitat òptica:
 - o Els equips hauran de garantir també la coexistència del canal quàntic amb dades en banda C estàndard (1530–1565 nm), assegurant la interoperabilitat i la qualitat del servei en escenaris mixtos.
 - o Suport per transmissió conjunta de canals quàntic i clàssic sobre una única fibra òptica, amb l'ús de tècniques de multiplexació WDM sense degradació significativa de rendiment.
- Interoperabilitat amb infraestructures de xarxa:
 - o Compatibilitat amb sistemes DWDM i CWDM, especificant les longituds d'ona exactes compatibles.
 - o Capacitat per personalitzar la longitud d'ona del canal quàntic.
 - o Els equips hauran de permetre la co-propagació amb almenys 4 canals DWDM de servei de client, sense degradació significativa del rendiment del sistema QKD.



- Compliment dels estàndards ETSI GS QKD 004 i 014, així com ITU-T Y.3800.
- Suport per interfícies de gestió estàndard, com SNMP i HTTP.
- Capacitat d'operació en escenaris punt-a-multipunt (P2MP).
- Flexibilitat i manteniment:
 - Possibilitat de substituir independentment qualsevol dels dispositius (emissor o receptor) sense requerir la substitució de tota la parella.
 - No s'acceptaran sistemes vinculats per parelles fixes de fàbrica que obliguin a la renovació completa del sistema en cas de fallada parcial.
- Integració amb sistemes de gestió de claus (KMS):
 - Connexió directa o indirecta amb el KMS mitjançant APIs compatibles (REST, JSON-RPC, KMIP).
 - Suport per protocols de lliurament de claus compatibles amb ETSI GS QKD 004 i 014.
- Seguretat i coherència tecnològica:
 - Garantia de compatibilitat criptogràfica i de seguretat entre dispositius d'una mateixa sèrie, model o família tecnològica del fabricant.

3.1.2. Rendiment i funcionalitat

Els sistemes hauran de complir els següents requisits mínims pel que fa al rendiment, fiabilitat i capacitat operativa:

- Rendiment criptogràfic i de transmissió
 - Pèrdua òptica màxima tolerada: mínim 10 dB.
 - Pressupost en potència: màxim de -10 dBm (10mW) .
 - Taxa mínima de generació neta de claus simètriques:
 - ≥ 1 kbps per parella emissor/receptor en condicions d'enllaç estàndard (10 dB).
 - ≥ 25 bps per servei amb sol·licitud del KMS cada 10 s.
 - ≥ 500 bps en escenaris multiusuari i condicions de xarxa màximes previstes (16 dB).

Nota: la taxa de generació de claus s'haurà d'expressar també en termes de claus AES generades per hora per parella de nodes, indicant explícitament el pressupost en potència corresponent. El sistema haurà d'assolir, com a mínim, 7.000 claus AES/hora @ 10 dB, i fins a 10.000 claus AES/hora @ 16 dB en condicions òptimes.

- Fiabilitat, autonomia i seguretat operativa



- El sistema ha de:
 - Funcionar de manera autònoma i contínua, sense dependències externes crítiques.
 - Permetre configuració com a font primària o secundària (redundant) d'entropia.
 - Disposar de mecanismes de contingència en cas de fallada de la font quàntica (bloqueig de flux, alertes, etc.); queda prohibit generar dades sintètiques de forma automàtica.
- Operativitat i gestió
 - Suport per:
 - Regeneració automàtica de claus i recuperació automàtica davant errors o interrupcions.
 - Actualització remota i segura del firmware.
 - S'ha de lliurar documentació tècnica completa i manuals operatius en català.
- Escalabilitat futura
 - Capacitat per evolucionar cap a entorns amb:
 - Integració de tecnologies post-quàntiques híbrides.
 - Suport a arquitectures SDN/NFV i escenaris de càrrega elevada.

3.1.3. Format físic i instal·lació

L'equip ha de tenir format rack de 19", amb una fondària màxima de 600 mm i una alçada màxima de 2U per unitat principal. Es podrà admetre 1U addicional per a equip auxiliar justificat (ex. alimentació, supervisió, etc.).

Ha de ser compatible amb la instal·lació en armaris estàndard de telecomunicacions.

3.1.4. Comunicació i canals

Els equips QKD han de complir els requisits següents pel que fa a la comunicació i transmissió de senyals:

- Canal clàssic de comunicació
 - Ha d'utilitzar connectivitat TCP/IP estàndard sobre interfícies RJ45 o SFP/SFP+ compatibles.
 - Ha de ser compatible amb la transmissió conjunta de dades convencionals (canals mixtos), sense interferències.
- Canal de sincronització



- La sincronització s'ha d'integrar en el canal de dades, sense requerir canals físics independents.
- Tolerància i robustesa de transmissió
 - El sistema ha de suportar enllaços amb un pressupost total de pèrdues òptiques ≥ 18 dB, assegurant operativitat en escenaris amb infraestructura variable o ampliable.
 - Ha de tolerar potències injectades > 5 dBm procedents de canals clàssics adjacents, sense degradació de la funcionalitat quàntica.

3.1.5. Gestió, control i monitoratge

Els equips han de disposar de funcionalitats avançades de supervisió i gestió operativa, incloent-hi:

- Control remot i gestió segura a través de protocols i interfícies estàndard com:
 - SSH, SNMPv3, REST API, o Netconf/YANG.
- Monitoratge en temps real de paràmetres crítics com:
 - Pèrdues òptiques, soroll, potència de senyal rebuda, entre d'altres.
 - Valors específics de distribució de claus quàntiques, incloent la Secure Key Rate (SKR), i l'Excess Noise, d'acord amb els protocols CV-QKD implementat.
- Registre complet d'activitat (logs) amb capacitat d'exportació d'auditories per a seguiment i traçabilitat dels esdeveniments del sistema.
 - Els dispositius i components hauran d'exportar els seus registres de forma contínua cap a la plataforma de recollida del CTTI i de l'Agència de Ciberseguretat per a la seva anàlisi i correlació.
- El sistema haurà d'incloure també un sistema d'alertes específic sobre el rendiment i l'estat del maquinari, incorporant com a mínim el consum de CPU, la latència en la distribució de claus, i les condicions ambientals de temperatura i humitat.
- La solució s'haurà d'integrar amb les eines de monitoratge i observabilitat del CTTI.
- Els equips hauran d'incloure com a mínim les següents interfícies físiques:
 - 1 port quàntic dedicat a la transmissió del canal quàntic.



- 1 port Ethernet per connexió de gestió i transmissió clàssica.
- 1 port de consola per configuració directa local (ex.: RS232, USB o similar).

3.1.6. Seguretat

Els equips han d'incorporar mesures avançades per garantir la integritat, confidencialitat i robustesa del sistema:

- Protecció contra atacs de canal lateral coneguts, incloent manipulacions del local oscillator i atacs basats en mesures.
- Les claus generades han de ser aleatòries i incondicionalment segures, conforme als models de seguretat reconeguts per organismes internacionals.
- Requisits específics de protecció física i supervisió:
 - Mecanismes de detecció automàtica de fallades o manipulacions (self-check, watchdogs, etc.).
 - Registre de fallades amb notificacions immediates per SNMP, API o consola local.
- El sistema QKD haurà de garantir que el valor del paràmetre de seguretat ϵ sigui menor o igual a 10^{-9} , d'acord amb les pràctiques habituals i els estàndards internacionals en QKD.

3.1.7. Certificació i normatives

Els equips han de complir amb els requisits següents per garantir la qualitat i la seguretat de la font d'entropia:

- Disposar de certificació o validació per tercers independents, basada en:
 - Tests estadístics estandarditzats reconeguts, com NIST SP 800-90B, DieHarder, TestU01 o equivalents.
 - Preferentment, certificació Common Criteria o acreditació per agències oficials com ANSSI, NIST, CCN o similars.



3.2. Equipaments KMS

Subsistema encarregat de la generació, distribució, emmagatzematge, rotació, recuperació i revocació de claus criptogràfiques en un entorn segur. Actua com a component central de la infraestructura de gestió de claus, facilitant la integració de serveis de xifrat i signatura digital, tant en entorns clàssics com en sistemes amb suport per tecnologies de distribució de claus quàntiques (QKD).

3.2.1. Compatibilitat i protocols

- El KMS haurà de ser plenament compatible amb sistemes QKD basats en protocols de distribució quàntica, incloent:
 - o CV-QKD (Continuous Variable)
 - o DV-QKD de variable discreta (compatibilitat híbrida futura)
- Haurà d'incorporar funcionalitats operatives específiques, com:
 - o Quantum-safe Key Relay entre nodes, amb implementació dels estàndards ETSI GS QKD 015, que garanteixi la distribució i retransmissió segura de claus en entorns híbrids clàssics i quàntics, i que incorpori un mecanisme explícit de gestió i execució del relay (per exemple, establiment de canals segurs autènticats i protocols de retransmissió verificables).
 - o Font d'entropia interna basada en QRNG, amb disponibilitat de mecanismes de generació alternatius (fallback) que assegurin la continuïtat del servei en cas de fallada de la font principal.
 - o Compliment dels estàndards de seguretat FIPS 140-2 o FIPS 140-3, o bé certificació Common Criteria EAL2+ per als mòduls criptogràfics interns (HSM).
 - o Ruteig redundant de claus i emmagatzematge segur.
 - o Alta disponibilitat (HA) a nivell de node QKD.
- Integració amb el pla de control de QKD per via d'interfícies estàndard:
 - o ETSI GS QKD 014 (tots els mètodes), incloent-hi SKIP, per interfícies API/KMI
 - o Altres estàndards com ETSI GS QKD 004
 - o Suport per QKD Network Layer (QNL) per topologia multipunt
- Compliment dels protocols de gestió de claus més habituals:
 - o PKCS#11, i compatibilitat amb arquitectures HSM
 - o El KMS haurà d'estar basat en un sistema operatiu Unix o similar, que garanteixi estabilitat, seguretat i compatibilitat amb entorns de xarxa i gestió de claus



- El KMS haurà de ser interoperable amb:
 - o Equips QKD de múltiples fabricants (estàndards ETSI/ITU)
 - o Sistemes criptogràfics clàssics (TLS/IPsec), i solucions híbrides post-quàntiques
- El sistema haurà de permetre també:
 - o Suport de múltiples mòduls QKD en un mateix node, amb capacitat per gestionar en concurrència un mínim de 5 mòduls QKD i 5 instàncies de KMS de manera simultània.
 - o Hibridació de claus PQC/QKD
- El KMS haurà de suportar mecanismes d'establiment de claus simètriques (SKE) i permetre la combinació criptogràfica de claus obtingudes mitjançant SKE, protocols QKD i un o més algorismes de Criptografia Post-Quàntica (PQC), facilitant la implementació d'agilitat criptogràfica i estratègies de defensa en profunditat davant amenaces presents i futures.

3.2.2. Capacitats i gestió de claus

- Capacitat per distribuir claus generades a través de QKD cap a múltiples destinataris de manera segura, escalable i traçable.
- Capacitat per distribuir, gestionar i lliurar claus simètriques de diferent naturalesa criptogràfica (clàssica, PQC i QKD), d'acord amb les polítiques definides i independentment del mecanisme de generació o establiment.
- Suport per:
 - o Clau unicast, multicast i broadcast
 - o Clau per servei, per sessió i per dispositiu
- Capacitat per operar tant en mode P2P com en topologia en estrella, hub&spoke o malla..
- Integració amb sistemes d'identitat i control d'accés:
 - o LDAP, RADIUS, SAML o protocols OAuth2/OpenID Connect
- Possibilitat de definir polítiques de control d'accés basades en rols (RBAC)
- Suport per autenticació mútua entre entitats (MFA, certificats digitals, etc.)
- Les interfícies del KMS hauran de protegir-se mitjançant HTTPS sobre TLS 1.3 (RFC 8446), amb autenticació mútua basada en certificats X.509, d'acord amb els requisits de l'estàndard ETSI GS QKD 014.
- Sistema de còpia de seguretat automàtica i restauració segura, amb xifrat de les claus en repòs i en trànsit.



- Les còpies s'han de poder realitzar:
 - o Localment, en dispositiu físic (ex. HSM secundari)
 - o Remotament, amb canals segurs (VPN, TLS 1.3)
- Les claus en backup han de disposar de protecció per hardware (HSM i mòduls TPM) o bé d'un sistema equivalent de protecció criptogràfica.
- El sistema haurà de garantir un cicle de vida complet de les claus (generació, distribució, ús, rotació, revocació i destrucció), que sigui segur i configurable segons les polítiques del CTTI i els estàndards internacionals.

3.2.3. Seguretat i supervisió

- Els sistemes KMS han d'estar protegits contra:
 - o Accés físic no autoritzat (anti-tampering, carcassa blindada si és HW)
 - o Atacs lògics (DoS, side-channel, atac per injecció de comandes)
- Han d'incloure:
 - o Monitoratge d'integritat i mecanismes de verificació (ex. checksums, firmware signatures)
 - o Suport per logging criptogràficament signat
- Registre complet d'activitats i accessos amb:
 - o Logs detallats d'operacions de generació, distribució i ús de claus
 - o Possibilitat d'integració amb sistemes SIEM (Security Information and Event Management)
- Interfície de gestió amb monitoratge en temps real dels següents paràmetres:
 - o Estat de nodes, transaccions de clau, errors i esdeveniments de seguretat
 - o Paràmetres específics de claus: Secure Key Rate (SKR), Effective Secure Key Rate (ESKR), nombre de claus emmagatzemades i nombre de claus consumides
 - o Suport per monitoratge mitjançant SNMP (Simple Network Management Protocol), per integració amb sistemes de supervisió de xarxa.
 - o El sistema haurà de disposar també d'una interfície gràfica d'administració basada en WebUI, accessible de manera segura mitjançant navegador, que permeti la gestió i monitoratge de totes les funcionalitats del KMS.
- Requeriments mínims de connectivitat física:



- 3 ports Ethernet per connexions de xarxa i un port de consola per gestió directa
- El KMS haurà de permetre la segmentació lògica o física del tràfic entre els canals de gestió, entrega de claus, recollida de claus i comunicació amb altres KMS, per garantir l'aïllament i la seguretat de cada flux.

3.3. Garanties esteses i servei de manteniment

Els equipaments subministrats hauran de complir els requisits amb relació a les seves garanties esteses, així com el seu servei de manteniment:

Garanties esteses

- Els equips (maquinari, programari i llicenciaments) hauran de disposar de garantia estesa del fabricant durant un mínim de cinc (5) anys a partir de la data d'acceptació definitiva del subministrament.
- L'adjudicatari haurà d'activar les garanties esteses dels fabricants, a nom del CTTI, en el moment en què els equips es posin en producció.
- Les garanties esteses hauran de cobrir tot el suport tècnic necessari pel correcte funcionament de la solució i la incorporació de noves funcionalitats, així com la substitució d'equipaments defectuosos in situ sense cap cost addicional per al CTTI
- L'adjudicatari serà responsable de la gestió integral de les garanties esteses amb els fabricants i de la interlocució amb el CTTI i/o amb els proveïdors que aquest designi.
- El CTTI podrà autoritzar altres gestors perquè, durant la vigència del contracte o posteriorment, puguin gestionar directament amb els fabricants les garanties esteses (recanvis, suport, etc.).

Servei de manteniment

- L'adjudicatari haurà de prestar servei de manteniment integral de tot el maquinari, programari i llicenciament subministrat, des de l'acceptació definitiva fins a la finalització del contracte.
- El servei inclourà intervencions remotes i in situ, segons sigui necessari.
- Les activitats mínimes incloses seran:
 - Suport tècnic (correu electrònic, telèfon, reunions telemàtiques o presencials, eines internes CTTI).
 - Interlocució amb els fabricants i gestió de garanties esteses.



- Anàlisi i implementació de noves funcionalitats.
- Actualitzacions de firmware i software (pla de versions).
- Revisions i actuacions preventives (pla de manteniment preventiu).
- Actuacions correctives: reparació o substitució de qualsevol element defectuós.
- Intervencions programades i d'urgència, d'acord amb el procediment de gestió de canvis del CTTI.
- Generació d'informes periòdics del servei de manteniment.
- Temps de resposta i resolució:
 - Les actuacions correctives i d'urgència hauran d'executar-se i resoldre la incidència o problema en un termini màxim de 24 hores laborables des de la notificació.
 - En cas de fallada greu o irreparable, caldrà proporcionar un equip de substitució equivalent o superior en un termini màxim de 7 dies naturals.
- Nivells de suport:
 - Nivell 1 (L1): Atenció inicial i resolució d'incidències en primera instància. Atenció i resolució d'incidències, peticions i gestió proactiva d'alertes del sistema de monitoratge.
 - Nivell 2 (L2): Suport tècnic avançat. Intervencions in situ i substitució de maquinari. Escalatge al nivell 3 quan sigui necessari.
 - Nivell 3 (L3): Suport tècnic del fabricant per a incidències crítiques o de màxima complexitat, així com noves evolucions
- L'adjudicatari haurà de facilitar els fulls de ruta dels fabricants amb relació a actualitzacions tecnològiques i suport evolutiu de maquinari, programari i llicenciamment, com a mínim, semestralment o bé en el moment en què hi hagi algun canvi rellevant.



4. CONDICIONS D'EXECUCIÓ DEL SERVEI

4.1. Estructura organitzativa

Dins d'aquest capítol es defineixen els perfils que han de formar l'estructura organitzativa que proposi el licitador, així com de forma il·lustrativa les principals funcions, que no úniques, que han de desenvolupar.

Els recursos humans assignats per l'adjudicatari han de tenir la qualificació necessària per a poder garantir amb èxit la implantació del projecte 'Encriptació Quàntica Generalitat de Catalunya'.

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

Composició dels punts per facilitar la comprensió de les necessitats demandes:

- Funcions del perfil: Inclou el detall de les responsabilitats que hauran d'assumir els perfils segons les funcions assignades.
- Idoneïtat dels perfils: Inclou les característiques acadèmiques i experiència professional que haurà de complir cada perfil.
- Proposta tècnica i organitzativa: Inclou el detall dels perfils de l'equip tècnic que el licitador consideri més adequat per a la implantació del projecte 'Encriptació Quàntica Generalitat de Catalunya'.

4.1.1. Funcions dels perfils

Les funcions mínimes que hauran d'assumir aquests perfils per a la correcta implantació de la solució són les següents:

- **Responsable de compte**: Aquest perfil correspondrà al responsable màxim (del contracte) de l'adjudicatari enfront del CTTI, vetllant per que aquest es compleixi.

Principalment és el responsable màxim dels àmbits econòmic, contractuals, organització i estratègia de prestació del servei.

- **Cap de projecte**: Serà la persona encarregada de planificar, dirigir, supervisar i coordinar totes les activitats relacionades amb els projectes, serveis i subministraments associats, incloent l'anàlisi i gestió de desviacions d'abast, costos i terminis. Gestionarà els recursos assignats, el seguiment de riscos i canvis, i la coordinació amb altres proveïdors o tercers involucrats.

Realitzarà funcions de direcció, planificació estratègica, control i supervisió tant de l'execució tècnica com de l'equip humà implicat en la implementació i operació dels sistemes de comunicació quàntica, garantint el compliment dels requisits funcionals, de qualitat i de seguretat establerts.



Serà la persona que haurà d'assegurar l'èxit del servei i els projectes dels que serà responsable, certificant la correcta execució dels mateixos així com el compliment dels requeriments i objectius marcats pel client i que hauran de cobrir tot un seguit de necessitats.

- **Arquitecte:** Perfil responsable del disseny de l'arquitectura global de la xarxa, integrant tant els elements clàssics de comunicació com els dispositius i protocols de comunicació quàntica. La seva funció serà assegurar la coherència tècnica, la compatibilitat entre sistemes i la seguretat en tot el disseny, tenint en compte els requisits específics de la tecnologia QKD (Continuous Variables – CV-QKD) i sistemes de gestió de claus (KMS). Referent tecnològic de les activitats d'arquitectura i solucions tecnològiques en l'àmbit dels serveis objecte d'aquesta licitació.

El personal amb les funcions d'arquitecte haurà de tenir com a principals tasques / responsabilitats:

- Validar el disseny (a nivell tecnològic) que permeti cobrir totes i cadascuna de les necessitats que vagin apareixent.
 - Aportar, proposar i desenvolupar les millores a nivell d'arquitectura.
 - Conjuntament amb el responsable tècnic, encarregat de donar cobertura a la necessitat de funcions avançades, com a Serveis professionals de tercer nivell en el Suport a disseny de solucions tecnològiques i altres que consideri el CTTI.
- **Administradors de xarxes i comunicació quàntica:** Responsables de totes les tasques d'administració, procediments i revisió (optimització) de la xarxa (equipament físic, virtual o al cloud), incloent totes les tasques necessàries per l'execució dels serveis definits per a un administrador de xarxa i seguretat.
- **Operadors de xarxa i seguretat:** Aquest perfil correspon a tècnics responsables de tasques d'administració bàsica, operació i monitoratge en temps real de la infraestructura de xarxes de comunicacions i serveis de seguretat associats. Seran responsables de la supervisió d'elements de xarxa i de comunicació quàntica, la gestió d'incidències de primer nivell, alarmes i notificacions d'errors, l'escalat i l'actualització de l'estat dels serveis i sistemes, així com el registre i documentació d'operacions i esdeveniments.
- **Enginyer/a de seguretat i criptografia:** Perfil encarregat de garantir que la infraestructura desplegada compleix els requeriments de seguretat en tot el cicle de vida del sistema, especialment pel que fa a la protecció de la informació, la integració del sistema de distribució de claus quàntiques (QKD) amb el sistema de gestió de claus (KMS), i la interoperabilitat amb sistemes clàssics de xifrat.
- **Coordinador/a d'integració i proves:** Perfil responsable de dissenyar, planificar i supervisar la realització de proves de sistema, incloent proves de rendiment, interoperabilitat, estabilitat i seguretat en les fases de desplegament



i validació de la nova infraestructura. Coordinarà els diferents actors tècnics implicats i serà responsable de validar la correcta integració dels sistemes de comunicació quàntica amb la resta de la xarxa.

- **Serveis professionals de tercer nivell:** Aquest perfil actuarà en col·laboració amb l'equip tècnic del client i serà l'enllaç amb el suport de nivell màxim del fabricant. La seva participació serà crítica en fases de posada en producció, resolució d'incidències de màxima complexitat i manteniment evolutiu.

Encarregat de donar cobertura a totes les fases per a la implantació de la solució. Aquests recursos estaran a disposició del CTTI per a poder ésser utilitzats principalment en les següents casuístiques:

- Suport a disseny de solucions tecnològiques.
- Certificació del disseny proposat.
- Auditoria del desplegament de la solució.
- Agilitzar la interlocució interna del fabricant.
- Participació en el procés de preparació i migració de les dades a la nova solució.
- Suport als canvis que consideri el CTTI.
- Resolució de les incidències

Aquests perfils descrits equivalen als següents de l'informe justificatiu:

Perfil	Perfil equivalent
Responsable de compte	Arquitecte
Cap de projecte	Cap de projecte
Arquitecte	Arquitecte
Administradors de xarxes i comunicació quàntica	Administrador
Operadors de xarxa i seguretat	Operador
Enginyer de seguretat i criptografia	Administrador
Coordinador d'integració i proves	Administrador

4.1.2. Idoneïtat dels perfils

A continuació es detallen els perfils principals amb les característiques mínimes que hauran de tenir, tot i que també haurà d'incloure les funcions descrites a l'apartat 3.1.1 Funcions dels perfils segons correspongui tal i com està detallat a la 3.1.3 Estructura Organitzativa:



- **Responsable de compte:**

La persona assignada haurà de disposar, com a mínim, d'una titulació universitària superior (preferentment en Enginyeria, Ciències o Tecnologies de la Informació) o, alternativament, acreditar una experiència mínima de 5 anys en la gestió i coordinació de serveis o projectes TIC d'elevada complexitat, preferentment en entorns del sector públic.

Caldrà acreditar experiència específica en la relació amb clients institucionals i en la coordinació transversal amb equips tècnics, així com en la gestió d'incidències, riscos i comunicació amb múltiples actors.

La comunicació fluïda, la proactivitat, la capacitat de negociació, la flexibilitat i l'adaptabilitat són competències fonamentals per aquest perfil.

- **Cap de projecte:**

- Titulació mínima: Grau o llicenciatura d'àmbit tecnològic, preferentment en Enginyeria de Telecomunicacions, Enginyeria Informàtica o titulacions afins.
- Experiència mínima: Almenys 5 anys d'experiència acreditada en la direcció de projectes complexos en l'àmbit de les xarxes de telecomunicacions, especialment en entorns amb tecnologies òptiques, requisits de seguretat elevada, o sistemes d'alt rendiment i disponibilitat..

- **Arquitecte:**

- Experiència mínima: 5 anys en el disseny d'arquitectures de xarxes complexes, preferentment en entorns crítics o de seguretat elevada, amb almenys 2 anys en la integració de solucions de comunicació quàntica o participació directa en pilots o projectes amb aquesta tecnologia.
- Coneixements específics requerits:
 - Disseny d'arquitectures de xarxa per a solucions híbrides clàssiques/quàntiques.
 - Coneixement de fabricants i solucions de comunicació quàntica.
 - Coneixement de protocols de distribució de claus quàntiques (QKD), CV-QKD, i gestió criptogràfica associada (KMS).
- Certificacions mínimes o equivalents:
 - Cisco Certified Design Professional (CCDP) o NSE 7 de Fortinet, com a demostració d'habilitats en disseny i seguretat de xarxa



- **Administradors de xarxes i comunicació quàntica:**

- Experiència mínima: 3 anys en administració de xarxes de comunicacions d'alta disponibilitat i rendiment, preferentment en entorns públics o crítics, i participació (encara que sigui parcial) en projectes relacionats amb la comunicació quàntica.
- Coneixements requerits:
 - Protocols de routing: IS-IS, OSPF, RIP, EIGRP, BGP per IPv4 i IPv6.
 - Serveis de nivell 2: Ethernet Virtual Circuits (EVC, QinQ, 802.1ad, EFP), classificació de VLANs, IEEE Bridging, 802.1s MST, 802.1w RSTP, MST Access Gateway.
 - Configuració, diagnosi i desplegament bàsic de sistemes de comunicació quàntica.
 - Coneixement dels requisits d'interoperabilitat amb dispositius QKD i compatibilitat amb KMS.
- Certificacions mínimes:
 - Cisco Certified Network Professional (CCNP Routing & Switching), o equivalent com NSE 3 de Fortinet.

- **Operadors de xarxa i seguretat:**

- Titulació mínima: Formació professional de grau mitjà o superior en informàtica, telecomunicacions o equivalent.
- Experiència mínima: 2 anys en tasques d'operació i monitoratge de xarxes de comunicacions i sistemes de seguretat en entorns operatius reals..

- **Enginyer/a de seguretat i criptografia:**

- Titulació mínima: Grau o llicenciatura en Enginyeria Informàtica, de Telecomunicacions, Matemàtiques o similar.
- Experiència mínima: 3 anys en projectes de seguretat de xarxa i criptografia.
- Coneixements requerits:
 - Protocols criptogràfics (TLS, IPsec, VPNs, etc.).



- Sistemes de gestió de claus (KMS, HSM).
- Coneixement de criptografia post-quàntica i de protocols de distribució de claus quàntiques (QKD).
- Normatives i bones pràctiques (ISO/IEC 27001, CCN-STIC, etc.).

- **Coordinador/a d'integració i proves:**

- Titulació mínima: Grau en Enginyeria o equivalent.
- Experiència mínima: 4 anys en projectes TIC complexos amb proves d'integració de sistemes.
- Coneixements requerits:
 - Metodologies de test (Test Plans, Use Cases, Acceptance Criteria...).
 - Coneixement d'eines de monitoratge i simulació de xarxa.
 - Coneixement de protocols de xarxa i, preferentment, de sistemes QKD/KMS.

- **Serveis professionals de tercer nivell:**

Aquest perfil correspon al d'un tècnic o enginyer d'alt nivell, especialitzat en els sistemes i equips subministrats, amb capacitat per intervenir en tasques de diagnosi, resolució d'incidències greus, optimització avançada i integració personalitzada de solucions, tant en l'àmbit de la xarxa com de la comunicació quàntica.

- Requisits:
 - Certificació de nivell màxim disponible per part dels fabricants dels sistemes que s'ofereixen (ex: Cisco CCIE, Fortinet NSE 8, etc.) o, en el cas de solucions de comunicació quàntica, acreditació directa i formal de formació, capacitació o col·laboració oficial amb el fabricant de la tecnologia QKD o KMS proposada.
 - Experiència demostrada en el desplegament o suport expert de solucions equivalents en entorns operatius.
- Obligacions del licitador:
 - Indicar clarament en la proposta els recursos que s'assignaran a aquest servei.



- Aportar CV, certificacions i referències de projectes previs similars amb solucions de comunicació quàntica o xarxes d'alta seguretat.
- Garantir disponibilitat en casos de suport crític i compatibilitat idiomàtica amb l'equip del client.

4.1.3. Dimensionament organitzatiu

A títol orientatiu, es presenta a continuació la composició mínima de l'equip, que podrà participar en totes les fases o només en alguna d'elles:

Classificació perfils	Funcions Perfil	Recurrent
Responsable de Compte	Responsable de Compte	1
Cap de projecte	Cap de projecte	1
Arquitecte de xarxa i comunicació quàntica	Arquitecte	1
Administrador de xarxes i comunicació quàntica	Administrador	2
Operador de xarxa i seguretat	Operador	2
Enginyer/a de seguretat i criptografia	Expert en criptografia, KMS i protocols	1
Coordinador/a d'integració i proves	Coordinador de test i validació funcional	1
Serveis professionals de tercer nivell	Tècnics amb màxima certificació / suport expert	1

L'adjudicatari haurà de proporcionar serveis professionals de tercers amb un mínim de 100 hores durant el contracte.

Donada la ràpida evolució de la tecnologia aquest perfils es poden canviar per perfils equivalents necessaris, sempre prèvia validació del CTTI.

Qualsevol canvi en aquests recursos assignats al servei haurà de ser comunicat prèviament al CTTI, que haurà de donar el seu vist i plau, sense el qual no es podrà portar a terme el canvi i per tant l'adjudicatari haurà de buscar una alternativa.

En cas de substitució d'algun altre component de l'equip presentat, el substitut haurà de tenir una idoneïtat equivalent o superior a la presentada en l'oferta.

4.1.4 Clàusula de seguretat

Confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arran de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 5 anys, o el que s'especifiqui en el contracte, des que es va tenir coneixement de la informació, excepte en relació a les dades personals a les què accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera



indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

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

L'empresa adjudicatària ha de posar en coneixement 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.

Conformitat amb l'Esquema Nacional de Seguretat

De conformitat amb l'article 2 del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (d'ara endavant, ENS o RD 311/2022), l'adjudicatari ha d'estar en condicions de poder evidenciar la conformitat amb l'ENS dels sistemes d'informació en què se sustentin els serveis objecte del contracte (subministrament, posada en marxa i manteniment), requerint-se que presenti el Certificat de Conformitat amb l'ENS en categoria **MITJANA**, o superior, dels sistemes que intervinguin en la prestació dels serveis indicats abans de l'inici de la prestació.

L'adjudicatari haurà de mantenir la conformitat vigent durant tot el cicle de vida del contracte. La pèrdua o retirada temporal de la conformitat s'haurà de comunicar de manera immediata i sense dilació indeguda al CTTI, que haurà de considerar l'impacte en el contracte d'aquesta circumstància.

La renovació de la conformitat durant la vigència del contracte es notificarà immediatament, incloent-hi el procés d'adaptació del sistema d'informació al Reial decret 311/2022.

Addicionalment, l'adjudicatari, haurà de notificar a l'inici de la prestació la identitat i dades de contacte de la persona que assumirà la responsabilitat de Punt o Persona de Contacte (POC), segons el que disposa l'article 13.5 del Reial decret 311/2022, així com la declaració en què consti l'acceptació de la designació i de les funcions específiques. Si durant l'execució del contracte es produeix un canvi en la persona de contacte, s'haurà de notificar de manera immediata al CTTI, abans que finalitzi la responsabilitat assumida, presentant formalment la declaració i les dades efectives de la nova persona de contacte.

En el cas que existeixi subcontractació, l'empresa adjudicatària ha d'estendre aquestes exigències a la cadena de subministrament, garantint que les empreses subcontractades compleixin amb l'ENS en la categoria requerida.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte haurà de conèixer i complir el Marc Normatiu de Ciberseguretat de la Generalitat de Catalunya: <https://portal.ciberseguretat.cat> i seguir les directrius o instruccions del CTTI i/o de l'Agència de Ciberseguretat de Catalunya.



Formació del personal

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

Adquisició de productes de seguretat

Atès que els productes a subministrar formaran part de l'arquitectura de seguretat dels sistemes de comunicacions de la Generalitat de Catalunya, als quals els correspon la categoria ALTA de l'ENS, l'adjudicatari ha de complir amb la mesura *op.pl.5 Components Certificats* de l'annex II de l'ENS.

D'acord amb la mesura *op.pl.5*, s'utilitzarà el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC)** del CCN, per seleccionar els productes o serveis subministrats per un tercer que formin part de l'arquitectura de seguretat del sistema. **En cas que no existeixin productes o serveis al CPSTIC que implementin les funcionalitats requerides, s'utilitzaran productes certificats d'acord amb allò descrit a l'article 19 de l'ENS.**

En cas que el producte estigui certificat, l'adjudicatari haurà de presentar amb detall totes les característiques dels productes o serveis i la referència de la família on s'hagi enquadrat, la categoria acreditada, la data d'inclusió i la data de revisió de validesa de l'acreditació. El mitjà pel qual s'acrediti la seguretat del producte s'haurà de mantenir en vigor i actualitzat durant tota la vigència dels drets d'ús dels actius al CTTI. Qualsevol canvi en la vigència de l'acreditació haurà de ser comunicat sense demora.

De manera alternativa, i basant-se en el principi de proporcionalitat i neutralitat tecnològica, l'arquitectura i infraestructura emprada en el sistema d'informació afectat, i considerant els riscos, els proveïdors podran presentar altres certificacions de seguretat en què es detallin les funcions de seguretat (com per exemple, la certificació emesa per l'Esquema Europeu de Certificació de Ciberseguretat o qualsevol altre que sigui aprovat per la Comissió Europea en virtut de l'article 49 del Reglament (UE) 2019/881 relatiu a l'ENISA o la certificació de la ciberseguretat de les tecnologies de la informació i la comunicació).

En defecte de certificació, l'adjudicatari haurà d'acreditar mitjançant una declaració d'aplicabilitat que el producte o servei disposa de requeriments de seguretat equivalents als exigits pel CPSTIC en relació a la família de productes corresponent al seu producte i que es poden consultar a la Guia CCN-STIC 140 "Taxonomía de referencia para productos de seguridad TIC".

En un màxim de 6 mesos des de l'inici del contracte, l'adjudicatari haurà d'incloure el seu producte al CPSTIC.



Verificació del compliment

El CTTI i/o l'Agència de Ciberseguretat de Catalunya, amb mitjans propis o de tercers, podrà auditar la correcta execució dels serveis objecte del contracte, en el moment i periodicitat que s'estimi convenient. 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.

Incidents de seguretat

El POC haurà de notificar al CTTI i al Catalonia-CERT de l'Agència de Ciberseguretat de Catalunya qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat, en els terminis i per les vies que determini o els procediments establerts.

L'empresa adjudicatària del contracte haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents i al CTTI. En cas que sigui necessari, l'empresa adjudicatària haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part del CTTI i/o per l'Agència de Ciberseguretat de Catalunya per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.



5. FASES DE LA PRESTACIÓ DEL SERVEI

5.1. Fase Pla de migració

Aquesta fase inclou la definició i concreció del pla de desplegament que definirà els passos a seguir, així com la temporalitat de cadascú d'aquests. Inclourà els següents punts:

- Definició concreta dels objectius de la solució
- Descripció de la topologia
- Requisits previs
- Disseny final de la nova arquitectura
- Descripció de les dues fases del desplegament
- Proves i validació
- Avaluació de riscos i mesures de mitigació
- Descripció del cronograma i recursos associats

La durada d'aquesta fase serà de quatre (4) mesos, a comptar des de la data d'inici de contracte.

5.2. Fase Execució crítica

Subministrament i instal·lació d'equipament a les seus i segments crítics identificats dels dotze nodes previstos, així com a l'entorn del laboratori.

Les activitats mínimes a realitzar seran:

- Subministrament dels equips. Subministrament dels equips necessaris pels primers nodes.
- Desplegament inicial dels equips. Instal·lació física dels equips dels dos primers nodes i configuració bàsica per la posada en marxa dels mateixos.
- Calibratge i pas a producció. Ajustament de les configuracions dels nous equips i dels equips existents per garantir la comunicació entre extrems i la correcta encriptació.
- Escalat del tercer node. Desplegament dels equips del tercer node i avaluació de l'impacte al complicar l'arquitectura de dos a tres nodes i posada en producció.
- Escalat a la resta de nodes. Desplegament de la resta de nodes i seus fins a completar els quatre d'aquesta fase. Avaluació de com es comporta aquesta arquitectura més complexa. Posada en producció.
- Recollida de dades necessàries per analitzar a la fase 'observació i anàlisi de dades'.

La durada d'aquesta fase serà de setze (16) mesos, a comptar des de la data de validació del pla de migració per part del CTTI.



5.3. Fase Desplegament

Desplegament i ampliació del bloc de comunicacions encriptat quànticament als 8 nodes restants. Les activitats a realitzar, com a mínim, seran:

- Subministrament dels equips. Subministrament dels equips necessaris pels nodes d'aquesta actuació.
- Escalat a quatre nodes més. Desplegament de quatre nodes addicional en base a l'experiència de desplegament dels anteriors i avaluació de possibles increments temporals. Avaluació del comportament d'aquesta nova arquitectura, la qual tancaria l'anell metropolità. Posada en producció.
- Escalat final. Desplegament dels darrers quatre nodes i seus. Avaluació del comportament d'aquesta nova arquitectura, amb diverses seus desplegades connectades als node i a l'anell. Posada en producció.
- Manteniment de l'entorn de laboratori operatiu i en execució.

La durada d'aquesta fase serà de tretze (13) mesos, a comptar des de la data de certificació de la posada en marxa dels nodes assignats en a la fase d'execució crítica, i la validació explícita per part del CTTI.

5.4. Fase Anàlisi de les dades

Observació i anàlisi de les dades en operació real durant un període de temps que permeti extraure conclusions relacionades amb el producte evolucionat al mercat.

La durada d'aquesta fase serà de vint-i-quatre (24) mesos, a comptar des de la data de certificació de la posada en marxa dels primers nodes QKD i KMS assignats a la fase d'execució crítica, i la validació explícita per part del CTTI.

5.5. Pla de devolució del servei

El licitador inclourà 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.

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.

Així mateix, es deixarà constància expressa que l'adjudicació d'aquest contracte no confereix cap dret de propietat intel·lectual o industrial a favor de l'empresa adjudicatària sobre cap dels elements esmentats, ni sobre els resultats, configuracions, dissenys, desenvolupaments o coneixement generat.



Tots els drets pertanyen exclusivament al CTTI, i l'ús d'aquests materials per part de l'empresa adjudicatària quedarà limitat estrictament a l'àmbit d'execució del contracte. Un cop finalitzada la relació contractual, l'empresa no podrà fer-ne cap ús posterior sense autorització expressa i per escrit.

El Pla de devolució haurà de complir, com a mínim, els següents principis i continguts:

- El termini d'execució serà de entre 2 i 4 mesos abans de la finalització del contracte ja sigui per haver exhaurit el termini o per cancel·lació anticipada. El CTTI es reserva el dret de poder reduir el termini d'execució segons consideri necessari.
- Inclourà la metodologia de transferència de coneixement dels aspectes fonamentals d'operació i, com a mínim:

- Proporcionar, a qui determini el CTTI, dels mitjans necessaris per a la formació dels professionals de l'àmbit relacionat amb l'objecte contractual.

Aquesta formació haurà de tenir un mínim de 2 sessions de 8 hores cadascuna o equivalent, i cobrirà els següents elements:

- Formació en els equips, serveis, funcionalitats, operació i eines implantades, aplicables al disseny escollit. Altres funcionalitats dels equips i serveis.
- Aspectes rellevants dels procediments del fabricant: roadmap, consultes tècniques, cicle de vida dels productes, contractes de manteniments, etc.
- Manuals d'usuari del servei amb informació detallada de les prestacions i funcionalitats.
- Documentació de processos, base de dades de coneixement, etc.
- Disponibilitat contínua via web.

Tota la formació i documentació necessària serà proporcionada, almenys, en idioma català.

- L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat per l'adjudicatari o la Generalitat de Catalunya en la provisió del servei.
 - La formació pràctica tutelada, en la qual el personal designat pel CTTI realitzi els treballs propis de cada procés o funcionalitat tutelats pel personal de l'adjudicatari.
- L'adjudicatari haurà d'oferir el maquinari i els equips informàtics, adscrits de forma exclusiva als serveis objecte del contracte, al CTTI o a terceres parts anomenades per aquest. La valoració dels equips es realitzarà per un tercer utilitzant el criteri de "preu de mercat" o, si no és possible, sostraint al seu preu



de compra el cost de l'amortització sense valor residual. El CTTI, o terceres parts anomenades per aquest, podrà realitzar la compra de tots o part dels equips.

- El CTTI podrà subscriure un contracte de llicència d'ús sobre els sistemes de l'adjudicatari que fossin necessaris per assegurar la continuïtat del servei.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència al CTTI, o a terceres parts anomenades per aquest, de serveis subcontractats, garanties o contractes de manteniment existents fins al moment de la terminació en els mateixos termes pactats amb els adjudicataris d'aquests.
- L'adjudicatari haurà d'oferir un Pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, el CTTI i/o altres adjudicataris.
- Durant el període de devolució del servei, l'adjudicatari ha de complir els Acords de Nivell de Servei. El Pla de devolució no ha de causar cap discontinuïtat en el servei.
- El CTTI no assumirà una dedicació significativa de recursos propis o de la Generalitat de Catalunya en les activitats de devolució.
- L'adjudicatari haurà de garantir que es disposa de la documentació actualitzada de la gestió del servei (base de dades de coneixement) a transferir.
- Abans de l'inici de la fase de devolució, l'adjudicatari ha de garantir, pels sistemes d'informació d'importància Alta, que la documentació base es troba actualitzada. Es considera documentació base la que es troba indicada com a grau de necessitat imprescindible a:

https://qualitat.solucions.gencat.cat/guies/transicio/lliurables_transicio_devolucio/

Li correspon a l'adjudicatari del contracte liderar i assegurar la qualitat i transparència del procés de devolució del servei.

La devolució del servei per part de l'adjudicatari sortint inclou dues fases:

- **Prestació en devolució:** durant l'execució del Pla de devolució l'adjudicatari sortint ha d'assegurar la continuïtat del servei amb el compliment dels ANS establerts per a cadascun dels serveis i totes les responsabilitats per a la seva correcta execució, tal i com s'especifica en el present plec. L'adjudicatari sortint és ple responsable del servei.
- **Devolució del servei:** alhora que l'adjudicatari sortint continua prestant el servei sota les condicions expressades en el present plec, haurà d'assegurar un correcte traspàs de la informació i dels serveis a qui determini el CTTI.



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'adjudicatari i el CTTI per prestar els serveis requerits de forma satisfactòria a la Generalitat de Catalunya. El CTTI farà el seguiment de la qualitat del servei i avaluarà periòdicament el servei prestat per l'adjudicatari.

El CTTI pretén obtenir un nivell de servei d'alta qualitat, així com un grau de satisfacció elevat per part dels usuaris, basat en:

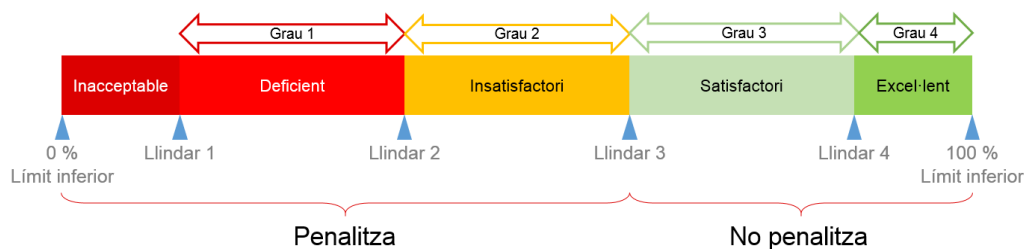
- L'establiment d'indicadors de servei, de manera que el CTTI pugui realitzar una avaluació objectiva del servei i els seus lliurables, i que l'adjudicatari tingui una base per a la correcció de les eventuais deficiències en la prestació, i per a la millora dels seus processos i organització.
- L'establiment 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.

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: Projecte, reporting, entre d'altres.
- **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 s'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:





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

6.3. Grau de l'indicador

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

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

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.

6.4. Càlcul dels indicadors

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

	Llíndar Grau 1	Llíndar Grau 2	Llíndar Grau 3	Llíndar Grau 4
<i>Indicador de mesura</i>	Valor 1	Valor 2	Valor 3	Valor 4

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 Líndar Grau 1 < valor Líndar Grau 4).
 - Si el valor és inferior al líndar 1, el grau serà 1.
 - Si el valor és igual o superior al líndar 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).
 - o Si el valor és superior al llindar 1, el grau serà 1.
 - o Si el valor és igual o inferior al llindar 4, el grau serà 4.
 - o En la resta de casos s'aplicarà la fórmula de càlcul del grau.

6.4.1. Fórmula de càlcul del grau

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

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

- 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.

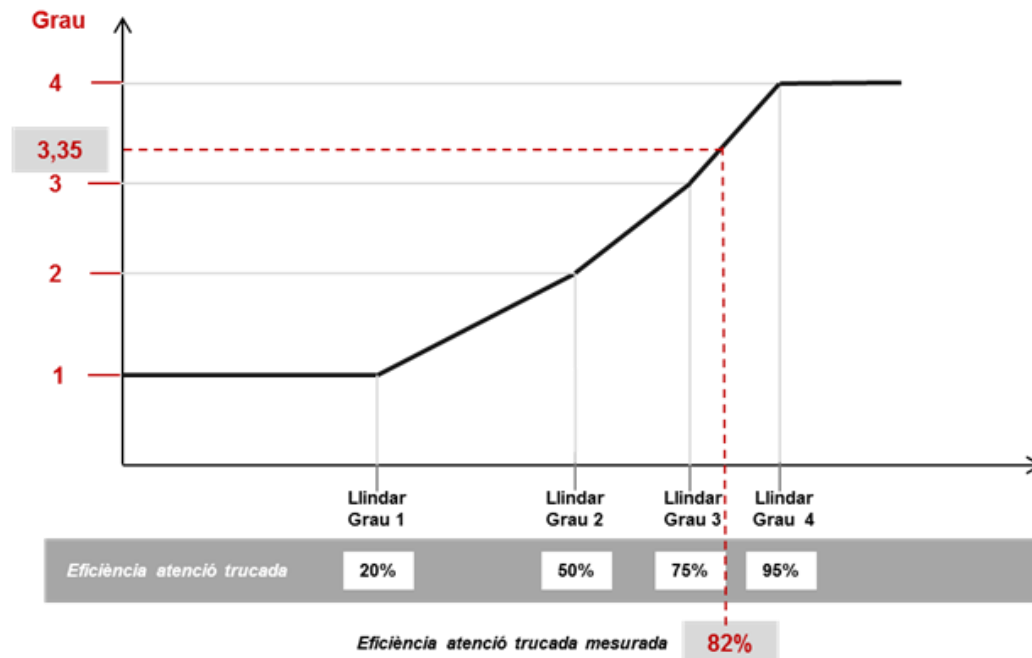
6.4.2. Exemple de càlcul

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%



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



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

6.5. Relació d'ANS

Al fitxer annex "ANS_EnQGenCat_v.01.xlsx" es troben els indicadors 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'ha explicat anteriorment.



7. MODEL DE GOVERNANÇA

7.1. Objectiu

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.

En concret aquest model pretén assolir els següents objectius estratègics principals:

- **Qualitat:** Garantir la qualitat en la prestació de serveis i la satisfacció dels usuaris, segons les necessitats dels diferents departaments i entitats de la Generalitat.
- **Eficiència:** Optimitzar l'ús dels recursos gràcies a la cerca d'eficiències, sinergies i optimització.
- **Innovació:** Transformar i innovar a l'administració d'acord amb l'estratègia transversal de les TIC de la Generalitat i de cada un dels departaments i entitats.
- **Seguretat:** Garantir que tots els serveis TIC prestats incorporen les mesures de seguretat necessàries d'acord a les directrius de l'Agència de Ciberseguretat de Catalunya i els equips estan preparats per fer front a possibles incidents de ciberseguretat.
- **Coneixement:** Generar coneixement a partir de la informació gestionada amb les TIC, per donar resposta a les necessitats i a la presa de decisions en l'àmbit del negoci dels departaments i entitats.

7.2. Abast

El model de prestació de serveis TIC 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.

7.3. Model de relació

El model de relació defineix les funcions i responsabilitats del proveïdor i del CTTI en un marc d'actuació comú, per assegurar el compliment de les obligacions de cadascuna de les parts. És un marc de relació que permet acordar el contingut i nivell de la prestació dels serveis, així com el seguiment de la prestació real en els aspectes estratègics, contractuals, tàctics i operatius.



L'adjudicatari pot ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb el CTTI, així com els mecanismes de control propis de cada servei i funció transversal. L'equip de treball dels proveïdors haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les tasques assignades.

El model de relació es sustenta en una estructura de competències i funcions que recauen sobre un esquelet de responsables del proveïdor, els quals es relacionaran amb el CTTI en base a 3 nivells (estratègic, tàctic i operatiu).

El proveïdor assignarà al CTTI els responsables que sostindran el Model de Relació. L'equip de responsables haurà de disposar igualment del dimensionament, la formació i els mitjans adequats per desenvolupar les funcions i responsabilitats assignades.

7.3.1. Nivells del model de relació

Els nivells funcionals del model de relació són el nivell estratègic, el tàctic (visió de negoci i visió tecnològica) i l'operatiu.

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

7.3.1.1. Nivell Estratègic

A nivell estratègic, el CTTI i els proveïdors tindran un intercanvi d'experiències i visions sobre l'estat de l'art dels serveis i les tendències d'evolució tecnològica d'aquests.

Els assistents per part de l'adjudicatari als comitès d'aquest nivell hauran de tenir capacitat decisòria sobre els compromisos de serveis.

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

7.3.1.2. Nivell Tàctic

En aquest nivell es farà un seguiment exhaustiu de l'execució dels serveis tecnològics i de negoci i dels contractes i s'eleva al nivell estratègic aquells aspectes que puguin originar la modificació del contracte.

7.3.1.3. 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.



7.3.2. Òrgans de Gestió (Comitès)

A continuació es descriuen la composició dels diferents comitès entre el CTTI i el proveïdor, 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.

El licitador haurà de fer explícita l'estructura i funcionament dels Comitès de relació i coordinació que siguin precisos per mantenir una interlocució permanent amb els actors involucrats en el procés.

Si així ho estimés convenient, el CTTI podrà exigir 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 de nivell tàctic, podrà formar-se un equip de treball de caràcter temporal amb objectius específics acordats prèviament.

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

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, el proveïdor haurà d'incorporar als diferents comitès les persones responsables de cada àmbit d'execució en funció dels temes específics a tractar en el comitè.

7.3.2.1. Comitè Estratègic

Format pel responsable de l'empresa adjudicatària i els representants que el CTTI determini, els assistents per part del proveïdor a aquest comitè hauran de tenir capacitat decisòria sobre els compromisos de serveis.

Títol	
Comitè Estratègic	
Participants mínims	Objectius / Temes
CTTI	Marcar les directrius estratègiques del contracte.
Direcció CTTI	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.
Responsable del contracte (si escau)	
Altres assistents (si escau)	
Generalitat	



Responsable Agència de Ciberseguretat (si escau)	Traslladar les directius estratègiques al nivell inferior.
Proveïdor	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.
Responsable de compte	Fer seguiment del model econòmic.
Responsable de serveis	Revisió i estat de situació dels aspectes més rellevants de seguretat (riscos, incidents del període, projectes en curs).
Responsables dels àmbits d'execució específics. (si escau)	Revisar i proposar les penalitzacions per incompliment del servei i escalar-les a l'òrgan de contractació.
	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.
	Eleva a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.
Entrades	
Informes i quadres de comandament del contracte.	Acta (signada digitalment entre les parts)
Actes comitès executius.	Decisions preses
Decisions a prendre.	Propostes a l'Òrgan de Contractació
Sortides	
Periodicitat	
- Anual o a petició del CTTI.	

7.3.2.2. Comitè Executiu

Format pel responsable de compte i de serveis, així com els representants que el CTTI determini.

Títol	
Comitè Executiu	
Participants mínims	Objectius / Temes
CTTI	Marcar les directrius tàctiques del contracte.
Responsable del seguiment del contracte	Realitzar el seguiment del conjunt d'activitats desenvolupades en el període, orientat especialment a l'assoliment dels objectius i eficiències plantejades pel proveïdor.
Responsable del servei	
Altres assistents (si escau)	



Generalitat	Revisió i estat de situació dels aspectes més rellevants de seguretat (riscos, incidents del període, projectes en curs).		
Responsable Agència de Ciberseguretat (si escau)	Informar i proposar al comitè estratègic les possibles modificacions del contracte que s'hagin de dur a terme.		
Proveïdor	Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord als acords de nivells de servei definits.		
Responsable de compte	Revisar i proposar les penalitzacions per incompliment del servei i escalar-les al comitè estratègic.		
Responsables de serveis	Acordar els quadres de comandament del contracte.		
Responsables dels àmbits d'execució específics (si escau)	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.		
	Desenvolupar propostes d'innovació en línia amb l'estratègia transversal del CTTI.		
Entrades		Sortides	
- Informes i quadres de comandament de seguiment del servei.		- Acta (signada digitalment entre les parts).	
- Actes comitès operatius .		- Decisions preses.	
- Actes comitès operatius de seguretat.		- Propostes al comitè estratègic	
- Decisions a prendre.			
Periodicitat			
- Semestral o a petició del CTTI.			

7.3.2.3. Comitè Operatiu

La periodicitat d'aquest comitè es preveu que sigui mensual, però aquest termini es podrà modificar d'acord amb les necessitats del servei.

Títol	
Comitè Operatiu	
Participants mínims	Objectius / Temes
CTTI	Realitzar el seguiment i control global de l'operació i provisió dels serveis d'acord als ANS.
Responsable de servei	Planificar, prioritzar i revisar les iniciatives en curs.



Responsable del seguiment del contracte (si escau)	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.
Altres assistents (si escau)	
Proveïdor	
Responsables de serveis	
Responsables operatius del servei	
Entrades	
Informes operatius de seguiment del servei.	Acta (signada digitalment entre les parts)
Anàlisi i propostes de millora.	Propostes al comitè executiu.
Decisions a prendre.	Nous procediments operatius.
Periodicitat	
Trimestral o a petició del CTTI.	

7.3.2.4. Comitè Operatiu de Seguretat

Aquest comitè operatiu transversal de seguretat tindrà una periodicitat quadrimestral, però aquest termini es podrà modificar d'acord amb les necessitats del servei.

Títol	
Comitè Operatiu de Seguretat	
Participants	Objectius / Temes
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).
Responsable de serveis	
Responsable del seguiment del contracte (si escau)	
Altres assistents (si escau)	
Generalitat	
Responsable risc tecnològic de seguretat de l'Agència de Ciberseguretat	
Proveïdor	
Responsable de seguretat del proveïdor (RSP)	



Altres personal operatiu	Seguiment de l'estat de seguretat dels projectes en curs: evolutius, correctius, etc. Escalat de problemes Tractament de les problemàtiques específiques
Entrades	Sortides
Informes d'estat de la seguretat. Anàlisi i propostes de millora. Decisions a prendre.	Acta (signada digitalment entre les parts) - Propostes al comitè executiu
Periodicitat	
- Semestral o a petició del CTTI.	

7.3.3. Estructura de responsabilitats

En aquest apartat s'indiquen els rols que participaran en els diferents comitès amb les funcions i responsabilitats específiques pels serveis objecte d'aquesta licitació.

L'empresa licitadora haurà de presentar un esquema organitzatiu correctament dimensionat que asseguri la cobertura del servei requerit.

Tot seguit s'identifiquen els rols responsables del proveïdor per a l'assegurament del compliment de les condicions d'execució.

7.3.3.1. Responsable de compte

Aquesta figura és única per proveïdor. És la figura de referència per tots els contractes entre el CTTI i el proveïdor i el darrer responsable de la prestació del conjunt de serveis i projectes del proveïdor. El responsable de compte ha de tindre capacitat decisòria sobre el servei, especialment en el cas de les UTE's. Aquesta figura es mantindrà durant tota la vida del contracte o contractes entre el CTTI i el proveïdor, 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 el proveïdor. 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.

Entre les seves responsabilitats es destaquen:

Consolidar i aportar al CTTI les informacions tant objectives com subjectives; valorades (informació fiable i de qualitat i analitzada d'acord amb el coneixement del model) que permetin la presa de decisions operatives i estratègiques al llarg de la vida del contracte.

Ser l'interlocutor principal amb el CTTI en matèria jurídica-legal per a tots els serveis/contractes prestats pel proveïdor. Serà el responsable de la formalització de les interpretacions realitzades respecte als contractes vigents, quan aquestes impliquin modificacions contractals.



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 el proveïdor.

Ser el responsable que el proveïdor 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.

7.3.3.2. Responsables de serveis

El proveïdor assignarà un responsable per cadascun dels serveis prestats tenint en compte els eixos del model de relació. Per tal de garantir l'assoliment de l'objectiu del model de disposar d'un servei totalment alineat a les necessitats dels diferents departaments i entitats, en el cas que el servei requereixi incorporar l'eix de relació d'àmbit departamental del model de relació, el proveïdor haurà d'assignar un responsable de servei específicament a cada departament o entitat al que presti servei. Haurà també d'assignar un responsable del servei des de la perspectiva transversal d'aquest. Les seves principals responsabilitats són:

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.

Assegurar la bona col·laboració entre els diferents proveïdors amb qui s'han de relacionar per tal de millorar el servei de negoci final.

7.3.3.3. Responsable de seguretat (RSP)

Aquest responsable és únic per proveïdor, i és la figura de referència pel que fa a ciberseguretat per tots els contractes entre el CTTI i el proveïdor. Ha de liderar i garantir que els serveis prestats pel proveïdor assoleixen els requeriments de seguretat sol·licitats. Serà responsable de:

Actuar com a enllaç entre el proveïdor i els diferents agents implicats (CTTI, Agència de Ciberseguretat, oficina QA de ciberseguretat) quan es tractin temes de seguretat.



Garantir, liderar i impulsar el compliment del marc normatiu de seguretat de la Generalitat de Catalunya dins la seva organització, assegurant la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives, i jurídiques); així com les directrius en matèria de seguretat definides per l'Agència de Ciberseguretat.

Coordinar reunions de seguiment periòdiques amb CTTI i l'Agència de Ciberseguretat per informar del grau d'adequació dels serveis al model de seguretat de la Generalitat de Catalunya, identificar-ne els riscos més rellevants i proposar plans d'acció per la seva mitigació.

Que tot el personal de l'empresa que prestarà serveis al CTTI i la Generalitat, passi per un pla de conscienciació i formació en matèria de seguretat, focalitzant-se en el marc normatiu de la Generalitat i els procediments de seguretat que li siguin d'aplicació.

Assegurar la informació regular al CTTI, Oficina QA de ciberseguretat i a l'Agència de Ciberseguretat segons els terminis marcats, de tot el relacionat amb la seguretat (incidents, mesures correctores, riscos, nous projectes, iniciatives, etc.).

Assegurar que tot el personal del proveïdor que hagi de tractar dades o sistemes de tractament de dades de nivell sensible o superior signin un Acord de Confidencialitat Individual. El CTTI i l'Agència de Ciberseguretat podran auditar aquest aspecte.

Coordinació operativa amb l'equip de resposta a incidents i amb el SOC de l'Agència de Ciberseguretat davant incidents o possibles amenaces de ciberseguretat (lliurament d'evidències per la gestió i investigació d'incidents de seguretat, suport per l'aplicació ràpida de mesures de protecció i contenció davant amenaces o ciberincidents, disposar d'informació vinculada al dispositiu, etc.).

Utilitzar el Portal de Seguretat de forma regular per fer el seguiment de tota la informació vinculada a la seguretat dels actius de la Generalitat de Catalunya.

Garantir i liderar dins la seva organització la correcta implantació dels plans de continuïtat i disponibilitat acordats amb el CTTI i l'Agència de Ciberseguretat.

Garantir l'execució de proves de recuperació de desastres dels serveis objecte del contracte, de forma coordinada amb el CTTI i l'Agència de Ciberseguretat.

Coordinar tot l'àmbit formatiu en ciberseguretat, tant les sessions formatives que s'impartiran conjuntament amb l'Agència de Ciberseguretat, com les tasques de conscienciació/formació que els tècnics hauran de traslladar als usuaris finals (recomanacions, píndoles, vídeos formatius, etc.).

Garantir l'execució de proves de recuperació de còpies de seguretat per validar-ne la correcta execució.

Assegurar la informació regular segons els terminis marcats, del relacionat amb la Continuïtat i Disponibilitat (incidents, mesures correctores, riscos, nous projectes, iniciatives, etc.).

Facilitar els indicadors que es considerin oportuns per garantir els nivells de seguretat que estableixi l'Agència de Ciberseguretat i CTTI.



