Consorci Sanitari Integral

SERVEI DE SUPORT A LES OPERACIONS I ADMINISTRACIÓ DELS SISTEMES I BAAS/DRAAS DEL CONSORCI SANITARI INTEGRAL

EXPEDIENT CSI-2027-22

CatSalut Servei Català de la Salut

Generalitat de Catalunya
Departament de Salut

Índex

1 Introducció 6
1.1 Glossari de termes 6
2 Model de servei 7
2.1 Model operatiu general i govern del servei 7
2.1.1 Principis generals del model operatiu 7
2.1.2 Estructura del govern del servei 7
2.1.3 Rols i responsabilitats de l'adjudicatari 8
2.1.4 Model de prestació i horaris de servei 8
2.1.5 Matriu de responsabilitats (RACI) del govern del servei 9
2.2 Eines de gestió, monitorització i tiqueting 9
2.2.1 Principis generals sobre l'ús d'eines 9
2.2.2 Eina de gestió del serveis 10
2.2.3 Eina de gestió de la configuració (CMDB) 10
2.2.4 Eines de gestió del coneixement 11
2.3 Procediments de gestió de incidències, canvis i peticions de servei 11
2.3.1 Marc metodològic (ITIL) 11
2.3.2 Gestió d'incidències 11
2.3.3 Gestió dels problemes 13
2.3.4 Gestió del canvi 13
2.3.5 Gestió de peticions de servei 15
2.4 Reporting 15
2.4.1 Principis generals 15
2.4.2 Informes periòdics de servei 15
2.4.3 Reporting d'incompliments 17
2.5 Capacitat tècnica a demanda - Marc general 17
2.5.1 Naturalesa i finalitat 17
2.5.2 Preu hora i factors de conversió 17
2.5.3 Activació i autorització 18
2.5.4 Registre de consum 18
2.5.5 Informe de consum i validació prèvia a la facturació 18
2.6 Seguretat transversal 19
2.6.1 Marc de seguretat 19

2.6.2 Gestió d'accessos i identitats 19
2.6.3 Gestió de vulnerabilitats i pegats de seguretat 20
2.6.4 Gestió d'esdeveniments de seguretat 21
2.7 Gestió de la documentació tècnica i base del coneixement 21
2.7.1 Tipus de documents 22
2.7.2 Repositori documental 23
2.7.3 Obligacions documentals en la transició i finalització del contracte 23
2.8 Catàleg de KPIs operatius 23
2.8.1 Definició de KPIs 24
3 Lot 1: Operació i administració de sistemes 27
3.1 Descripció del servei 27
3.1.1 Objecte del lot 27
3.1.2 Abast del servei 27
3.1.3 Límits del servei i relació amb d'altres lots 28
3.1.4 Model de prestació i presència física 29
3.1.5 Horari i model de cobertura 31
3.1.6 Capacitat tècnica a demanda 31
3.2 Model de guàrdies 32
3.2.1 Nivells de guàrdia 32
3.2.2 Horari de les guàrdies 33
3.2.3 Composició del pool de tècnics 33
3.2.4 Escalat al Nivell 3 34
3.2.5 Registre i documentació 34
3.3 Inventari i descripció de l'entorn 34
3.3.1 Consideracions generals 34
3.3.2 Infraestructura de servidors 35
3.3.3 Plataforma de virtualització 35
3.3.4 Sistemes d'emmagatzematge 35
3.3.5 Xarxa i seguretat 36
3.3.6 Software base 36
3.3.7 Ubicació dels *datacenters* i sales tècniques 37
3.3.8 Volum operatiu de referència 37
3.4 Monitorització i gestió d'alertes 38

3.4.1 Plataforma de monitorització 38
3.4.2 Gestió d'alertes 40
3.5 Requeriments funcionals del servei de nivell 2 43
3.5.1 Àmbit de resolució N2 43
3.5.2 Procés de gestió d'incidències 44
3.5.3 Gestió de peticions de servei 45
3.5.4 Gestió de tasques de sistemes 45
3.6 Requeriments funcionals del servei de nivell 3 47
3.6.1 Descripció i abast del servei N3 47
3.6.2 Tecnologies i plataformes en abast del N3 47
3.6.3 Serveis exclosos de l'abast del N3 d'aquest lot 49
3.6.4 Model d'escalat N2 - N3 50
3.6.5 Suport a tasques derivades de projectes 51
3.7 Perfils professionals 51
3.7.1 Consideracions generals 51
3.7.2 Perfils requerits 52
3.7.3 Compatibilitat de perfils 54
3.7.4 Estabilitat i canvis en l'equip assignat 54
3.7.5 Formació i actualització de coneixements 55
3.8 Pla d'auditoria i manteniment preventiu dels sistemes 55
3.8.1 Contingut mínim del pla 55
3.8.2 Planificació i periodicitat 56
3.8.3 Informe d'auditoria i plans d'acció 56
3.9 Equipament de treball del personal assignat 57
3.9.1 Equips informàtics 57
3.9.2 Dispositiu mòbil per a guàrdies 57
3.9.3 Responsabilitat sobre l'equipament 57
4 Lot 2: Backup as a Service 58
4.1 Descripció del servei 58
4.1.1 Objecte del lot 58
4.1.2 Abast del servei 58
4.1.3 Model de prestació i horari 60
4.2 Inventari i volumetria del servei 60

4.2.1 Entorn de backup actual (BaaS) 60
4.2.2 Volumetria requerida per al servei BaaS 61
4.2.3 Volumetria requerida per al servei DRaaS 61
4.3 Requeriments funcionals del servei 61
4.3.1 BaaS – Backup as a Service 61
4.3.2 DRaaS – Disaster Recovery as a Service 64
4.4 Requeriments tècnics del servei 65
4.5 Operació i monitorització del servei 68
4.5.1 Tasques operatives diàries 68
4.5.2 Monitorització del servei 68
4.6 Perfils professionals 68
4.7 Pla de formació 69
4.8 Seguretat 70
4.8.1 Obligacions específiques de seguretat 70
5 Lot 3: Administració de infraestructura SAP 72
5.1 Descripció del servei 72
5.1.1 Objecte del lot 72
5.1.2 Abast del servei 72
5.1.3 Model de prestació i horari 73
5.2 Requeriments funcionals del servei 73
5.2.1 Guàrdia localitzable 73
5.2.2 Check mensual 74
5.2.3 Responsable del servei (*Service Manager*) 75
5.2.4 Activitats no incloses al servei base 75
5.3 Capacitat tècnica a demanda 75
5.3.1 Volum i condicions 76
5.4 Perfils professionals 76
6 Lot 4: Administració plataforma CITRIX 78
6.1 Descripció del servei 78
6.1.1 Objecte del lot 78
6.1.2 Abast del servei 78
6.1.3 Model de prestació i horari 79
6.2 Infraestructura i volumetria del servei 80

6.2.1 Consideracions generals 80
6.2.2 Plataforma Citrix Virtual Apps and Desktops (CVAD) 81
6.2.3 Citrix StoreFront i workspace 81
6.2.4 Citrix NetScaler ADC 82
6.2.5 Mecanismes d'aprovisionament (MCS/PVS) 82
6.2.6 Gestió de perfils d'usuaris 82
6.2.7 Volumetria del servei 82
6.3 Requeriments funcionals del servei N3 83
6.3.1 Marc general 83
6.3.2 Àmbit de responsabilitat de la plataforma CVAD 83
6.3.3 Àmbit de responsabilitat de la plataforma NetScaler ADC 84
6.4 Perfils professionals 84
6.4.1 Compatibilitat de perfils 86
6.5 Capacitat tècnica a demanda 86

1 Introducció

Aquest document detalla els requeriments tècnics específics del plec de prescripcions tècniques de 'Serveis de suport a les operacions, administració dels sistemes i BaaS del Consorci Sanitari Integral' (en endavant CSI).

1.1 Glossari de termes

Termes generals del servei

Terme	Definició
RTE	Requeriments tècnics específics. Document que descriu els requeriments particulars dels serveis objectes d'aquesta licitació
PPT	Plec de prescripcions tècniques. Document que estableix les condicions generals, SLAs, ubicacions i marc general de prestació del servei.
Licitador	Empresa que presenta oferta en resposta al present procediment de contractació.
Adjudicatari	Empresa a la qui s'adjudica un o diversos lots del contracte.
Període de transició	Fase inicial del contracte destinada del traspàs de coneixement i assumpció del servei per part de l'adjudicatari.
KPI	*Key performance indicator*. Indicador clau de rendiment per mesurar el compliment operatiu del servei.
SLA	*Service Level Agreement.* Acord de nivell de servei que estableix els compromisos de qualitat i disponibilitat pactats.
RACI	Matriu d'assignació de responsabilitats.
CMDB	*Configuration management database.* Base de dades de gestió de la configuració amb l'inventari i relacions entre els elements de infraestructura.
DTSD	*Direcció de tecnologia i Salut Digital*. Departament de sistemes d'informació del Consorci Sanitari Integral.
CSI	*Consorci Sanitari Integral.*

2 Model de servei

2.1 Model operatiu general i govern del servei

2.1.1 Principis generals del model operatiu

Els serveis objecte de la present licitació s'han de prestar sota un model de serveis gestionats, en el qual l'adjudicatari assumeix la responsabilitat integral de l'operació, administració i manteniment dels sistemes i plataformes que s'inclouen en cada lot, d'acord amb els nivells de servei establerts en el PPT i els requisits específics recollits en el present document.

El model operatiu ha de basar-se en els principis següents:

- **Orientació a resultats:** L'adjudicatari és responsable del resultat del servei i no únicament de l'execució de tasques. La prestació s'avaluarà mitjançant els KPIs i SLAs definits per a cada lot.
- **Gestió proactiva:** L'adjudicatari ha d'anticipar-se a les incidències i degradacions del servei mitjançant la monitorització contínua, la gestió de la capacitat i el manteniment preventiu, sense esperar que sigui el CSI qui detecti les anomalies.
- **Millora contínua:** L'adjudicatari ha de proposar de manera periòdica mesures d'optimització tècnica i operativa que aportin valor al servei, documentant-les i presentant-les en els comitès de seguiment establerts.
- **Transparència i traçabilitat:** Tota activitat realitzada sobre els sistemes en abast ha de quedar registrada en l'eina de gestió corporativa, amb el nivell de detall suficient per garantir l'auditabilitat de les operacions.
- **Seguretat per disseny:** Qualsevol actuació sobre els sistemes ha de respectar les polítiques de seguretat del CSI i incorporar els principis de mínim privilegi, segregació de funcions i traçabilitat d'accessos.

2.1.2 Estructura del govern del servei

L'adjudicatari ha d'establir una estructura de govern formal que garanteixi una interlocució clara, àgil i estructurada amb el CSI. Aquesta estructura ha de contemplar, com a mínim, els nivells següents:

Comitè de Direcció

- **Periodicitat:** Trimestral.
- **Participants:** Responsable de servei de l'adjudicatari (Service Manager) i representants de la direcció TI del CSI.
- **Contingut:** Revisió del compliment global del contracte, evolució dels KPIs agregats, iniciatives de millora, gestió d'escalats d'incidents o peticions no resoltes i planificació a mitjà termini.

Comitè de seguiment operatiu

- **Periodicitat:** Mensual.
- **Participants:** Responsable tècnic de cada lot i referent TI del CSI.

- **Contingut:** Revisió detallada dels KPIs per lot, anàlisi d'incidències rellevants del període, seguiment del pla de canvis, estat d'accions obertes i presentació de l'informe mensual de servei.

Reunió Operativa del servei

- **Periodicitat:** Setmanal o quinzenal, segons les necessitats de cada lot.
- **Participants:** Tècnics responsables de l'adjudicatari i referents tècnics del CSI.
- **Contingut:** Seguiment d'incidències en curs, planificació de canvis de la setmana, coordinació d'actuacions i resolució d'impediments operatius del dia a dia.

2.1.3 Rols i responsabilitats de l'adjudicatari

L'adjudicatari ha de designar, com a mínim, els rols funcionals següents per a la gestió global del contracte:

Rol	Responsabilitat principal
Service Manager	Interlocutor de nivell estratègic. Responsable global del compliment contractual, escalats i relació amb la direcció del CSI.
Responsable tècnic	Interlocutor tècnic per a cada lot adjudicat. Coordina l'equip tècnic i respon del compliment dels KPIs del lot.
Responsable de qualitat i reporting	Elabora els informes de servei, supervisa el compliment dels SLAs i gestiona el quadre de comandament.

Tots els rols anteriors han de ser coberts per persones identificades i comunicades formalment al CSI. Qualsevol canvi en les persones assignades a aquests rols ha de ser notificat amb un mínim de 15 dies naturals d'antelació, excepte en casos de força major. Aquests perfils poden ser compatibles entre si, pel que una persona pot cobrir un o diversos rols.

2.1.4 Model de prestació i horaris de servei

L'adjudicatari ha de garantir la cobertura del servei d'acord amb les franges horàries definides per a cada nivell de criticitat. Com a criteri general per als serveis objecte d'aquest RTE, s'estableix el model de cobertura següent, que podrà ser precisat per a cada lot en els capítols corresponents:

Modalitat	Descripció
Horari estès	Cobertura de dilluns a divendres en horari de 07:30 a 17:00h (hora peninsular), dies laborables. Aplicable a tasques d'administració i operació.

Guàrdia localitzable	Disponibilitat de tècnic de guàrdia fora de l'horari estès, amb temps de resposta definit al PPT, per a l'atenció d'incidències greus. Aplicable a la gestió d'incidències crítiques i a tots els sistemes classificats com a crítics. Caldrà garantir la continuïtat i disponibilitat dels serveis en un entorn crític 24x7.

L'adjudicatari ha de garantir en tot moment la continuïtat del servei, evitant dependències crítiques en persones individuals (*single point of failure* humà), i ha de disposar de procediments documentats de cobertura davant d'absències, baixes o vacances del personal assignat.

2.1.5 Matriu de responsabilitats (RACI) del govern del servei

Activitat	CSI	Adj. Lot 1	Adj. Lot 2	Adj. Lot 3	Adj. Lot 4
Convocar Comitè de Direcció	R	I	I	I	I
Elaborar continguts i KPIs per al comitè de direcció	C	R	R	R	R
Convocar Comitè de Seguiment Operatiu	R	I	I	I	I
Elaborar informe mensual de servei	I	R	R	R	R
Validar i acceptar informe mensual	A/R	C	C	C	C
Mesurar i certificar KPIs i SLAs del lot	A	R	R	R	R
Elaborar informe desviació SLA	C	R	R	R	R
Aprovar pla d'acció corrector per desviació	A/R	C	C	C	C
Fer seguiment de les accions obertes dels comitès	A	R	R	R	R
Mantenir quadre de comandament operatiu	C	R	R	R	R

Llegenda de la matriu:

- **R (Responsable)**: Qui executa la tasca materialment.
- **A (Accountable)**: Qui té la responsabilitat última de l'èxit de la tasca (només un per fila).
- **C (Consultat)**: Qui aporta coneixement o protocols (com el Licitant facilitant la KB al N1 i N2).
- **I (Informat)**: Qui rep notificacions sobre l'estat de la incidència.

2.2 Eines de gestió, monitorització i tiqueting

2.2.1 Principis generals sobre l'ús d'eines

L'adjudicatari ha de disposar de les eines tecnològiques necessàries per garantir una gestió integral, traçable i auditada de tots els serveis inclosos en el contracte. L'ús d'aquestes eines no és opcional, constitueix un requisit mínim de prestació del servei.

S'estableixen els següents principis generals següents respecte a les eines de gestió:

- **Integració amb els sistemes corporatius:** Sempre que sigui tècnicament viable, les eines de l'adjudicatari han d'integrar-se amb les plataformes corporatives de l'organització (eina de tiqueting, CMDB, monitorització, etc.), evitant la creació de silos d'informació independents.
- **Propietat de les dades:** Totes les dades generades en el context de la prestació del servei (tiquets, alertes, registres, informes, inventaris) són propietat del CSI. L'adjudicatari ha de garantir la seva exportació i lliurament en formats estàndard en qualsevol moment que sigui requerit, i en qualsevol cas a la finalització del contracte.
- **Accés per part del CSI:** El CSI ha de disposar en tot moment d'accés en mode consulta a totes les eines utilitzades en la prestació del servei, sense restriccions ni necessitat de mediació per part de l'adjudicatari.
- **Disponibilitat de les eines:** Les plataformes de gestió i monitorització han de tenir una disponibilitat mínima equivalent a la dels serveis que supervisen. Una fallada en les eines de gestió no eximeix l'adjudicatari del compliment dels seus compromisos de servei.
- **Confidencialitat de les dades:** Garantir que si s'accedeix a dades mediques caldrà complir amb els requeriments de les clàusules de confidencialitat del contracte.

2.2.2 Eina de gestió del serveis

El sistema de tiqueting per al seguiment de les peticions serà el sistema emprat internament pel CSI, actualment Atlassian Jira Cloud.

Es facilitarà una formació bàsica en l'ús de l'eina i es prepararà per tal de que l'adjudicatari rebi e-mails de la mateixa a l'adreça de correu requerida. L'adjudicatari haurà d'operar prioritàriament sobre aquesta plataforma. Si l'adjudicatari proposa l'ús d'una eina pròpia, haurà de justificar-ne les capacitats i garantir la integració bidireccional amb els sistemes corporatius, sense cost addicional per al CSI i en cap cas afecti en el compliment dels SLA definits en els present plec tècnic.

2.2.3 Eina de gestió de la configuració (CMDB)

L'adjudicatari ha de mantenir actualitzada la informació dels elements de configuració (CIs) dels sistemes en abast a l'eina CMDB corporativa del CSI, actualment JIRA Assets.

- **Completesa:** Tots els sistemes, components i serveis en abast han d'estar representats com a CIs, amb els seus atributs tècnics i les seves relacions de dependència.
- **Actualització:** Qualsevol canvi sobre la infraestructura ha de reflectir-se en la CMDB en un termini màxim de **48 hores** des de la seva implantació.

2.2.4 Eines de gestió del coneixement

L'adjudicatari ha de mantenir una base de coneixement actualitzada que doni suport a l'operació del servei i faciliti la transferència de coneixement en cas de canvi de proveïdor. Aquesta base de coneixement ha d'incloure, com a mínim:

- **Runbooks i procediments operatius:** Procediments documentats per a les tasques habituals d'operació i per a la resposta davant d'incidències conegudes.
- **Procediments d'escalat:** Arbre de decisió i contactes per a l'escalat d'incidències per tipus i severitat.
- **Registre de problemes coneguts** (*Known Error Database, KEDB*):* Repositori d'errors coneguts amb els seus *workarounds* documentats.
- **Documentació tècnica d'arquitectura:** Diagrames i documentació actualitzada de l'arquitectura dels sistemes en abast.

Tota la documentació ha d'estar emmagatzemada en una plataforma accessible per al CSI, en formats estàndard i no propietaris, i ha de mantenir-se actualitzada com a part integrant de la prestació del servei.

2.3 Procediments de gestió de incidències, canvis i peticions de servei

2.3.1 Marc metodològic (ITIL)

El departament de tecnologia i salut digital (DTSD) aplica les bones pràctiques d'**ITIL (*Information Technology Infrastructure Library*)** com a marc de referència per a la gestió dels seus serveis TI. En conseqüència, tots els adjudicataris han d'operar sota aquesta mateixa metodologia, garantint una alineació plena amb els processos, la terminologia i els fluxos de treball establerts per ITIL en la seva versió vigent.

A aquests efectes, l'adjudicatari haurà d'acreditar en la seva oferta el coneixement i l'aplicació efectiva d'ITIL mitjançant:

- **Certificació organitzativa:** L'empresa licitadora ha de demostrar experiència en la prestació de serveis gestionats sota marc ITIL.
- **Certificació individual:** Els perfils clau assignats al contracte han de disposar, com a mínim, de certificació ITIL Foundation. Es valorarà positivament la disposició de certificacions de nivell superior (ITIL Practitioner, ITIL Managing Professional o ITIL Strategic Leader).
- **Documentació de processos:** L'adjudicatari ha de lliurar, durant el període de transició, la documentació dels seus processos interns adaptada al marc ITIL i alineada amb els procediments del CSI.

2.3.2 Gestió d'incidències

El procés de gestió d'incidències té com a objectiu restaurar la normalitat del servei en el menor temps possible, minimitzant l'impacte sobre CSI i els seus usuaris.

Classificació i priorització

Totes les incidències han de ser classificades en funció de dos paràmetres:

- **Impacte:** Abast de l'afectació sobre els usuaris, processos de negoci o sistemes crítics.
- **Urgència:** Velocitat amb la qual la incidència requereix resolució per evitar una degradació major.

La combinació d'ambdós paràmetres determina la **prioritat** de la incidència, d'acord amb la matriu següent:

	Urgència alta	**Urgència mitjana**	**Urgència baixa**
Impacte alt	P1 – Crític	P2 – Alt	P3 – Mig
Impacte mitjà	P2 – Alt	P3 – Mig	P4 – Baix
Impacte baix	P3 – Mig	P4 – Baix	P4 - Baix

Els temps de resposta i resolució associats a cada prioritat es defineixen en el PPT. No obstant això, a efectes operatius, l'adjudicatari ha de garantir els procediments d'actuació següents per a cada nivell:

Prioritat	**Actuació requerida**
P1 – Crític	Activació immediata de l'equip de resolució. Notificació al CSI en un màxim de 15 minuts des de la detecció. Actualitzacions d'estat cada 30 minuts fins a la resolució. Convocatòria de comitè tècnic si la resolució supera 1 hora.
P2 – Alt	Assignació prioritària a tècnic especialista. Notificació al CSI en un màxim de 30 minuts. Actualitzacions d'estat cada 2 hores.
P3 – Mig	Gestió dins del flux operatiu normal. Notificació i actualitzacions d'acord amb els terminis definits al PPT.
P4 – Baix	Gestió planificada. Resolució dins del termini acordat sense requeriment de notificació immediata.

Cicle de vida de la incidència

El cicle de vida de tota incidència ha de seguir, com a mínim, les fases següents d'acord amb el marc ITIL:

1. **Identificació i registre**: Tota incidència, independentment del canal de detecció (alerta automàtica, notificació d'usuari, detecció proactiva), ha de ser registrada immediatament en l'eina de tiqueting amb tots els camps obligatoris emplenats.
2. **Classificació i priorització**: Assignació de la categoria, impacte, urgència i prioritat d'acord amb la matriu definida.
3. **Diagnosi i investigació**: Anàlisi tècnica per part del nivell de suport corresponent (N2 o N3 segons el lot).

4. **Resolució i restabliment del servei**: Aplicació de la solució o workaround que restableixi el servei en el menor temps possible.
5. **Tancament i validació**: Confirmació de la resolució per part de CSI i tancament formal del tiquet amb documentació de la solució aplicada.
6. **Revisió post-incident (P1 i P2)**: Per a incidències crítiques o d'alta prioritat, s'ha de realitzar un informe Post-Incident Review (PIR) en un termini màxim de 5 dies hàbils des del tancament, que inclogui la cronologia de l'incident, les accions realitzades i les mesures preventives proposades.

2.3.3 Gestió dels problemes

La gestió de problemes té com a objectiu identificar les causes arrel de les incidències recurrents o d'alt impacte, reduir la probabilitat de la seva reaparició i minimitzar el seu impacte en cas que es produeixin.

Identificació i registre de problemes

L'adjudicatari ha d'obrir un registre de problema en els casos següents:

- Qualsevol incidència de prioritat P1, un cop resolta.
- Qualsevol incidència de prioritat P2 que es repeteixi més de dues vegades en un període de 30 dies.
- Qualsevol situació en la qual l'adjudicatari detecti un patró de recurrència que, al seu criteri tècnic, justifiqui la investigació de la causa arrel amb independència de la prioritat de les incidències associades.

Investigació i resolució

Per a cada registre de problema obert, l'adjudicatari ha de:

- Realitzar una anàlisi de causa arrel, documentant el procés i les conclusions en el registre de problema.
- Proposar i implementar, amb l'aprovació del CSI, les accions correctores necessàries per eliminar o mitigar la causa arrel identificada.
- Documentar un workaround en la KEDB per a tots els errors coneguts mentre la solució definitiva no estigui disponible, de manera que el personal de suport pugui reduir l'impacte de futures recurrències sense necessitat d'escalada.

2.3.4 Gestió del canvi

El procés de gestió del canvi té com a objectiu assegurar que qualsevol modificació sobre els sistemes i serveis en abast es realitza de manera planificada, controlada, documentada i amb el mínim risc possible per a la continuïtat del servei. L'adjudicatari no gestionarà els canvis directament, ja que serà el propi equip de la DTSD qui farà aquestes tasques i atomitzarà i transformarà les tasques responsabilitat de l'adjudicatari en peticions de servei i tasques de sistemes. L'equip d'operacions podrà en qualsevol cas fer propostes de canvis i canvis d'emergència, però la gestió del cicle de vida a partir d'aquell moment no estarà dintre de les seves responsabilitats.

Com a referència, es descriu la metodologia que segueix el CSI per a la gestió de canvis.

Tipologia de canvis

D'acord amb el marc ITIL, tots els canvis es classifiquen en les categories següents:

Tipus de canvi	Descripció	Circuit d'aprobació
Canvi estàndard	Canvi preautoritzat, de baix risc, ben documentat i amb procediment conegut.	Registre informatiu. Sense aprovació prèvia requerida.
Canvi normal	Canvi planificat que requereix avaluació i aprovació formal. Pot ser de baixa, mitjana o alta complexitat.	Aprovació del CAB. Termini mínim de presentació: 5 dies hàbils abans de la implementació.
Canvi d'emergència	Canvi que ha de ser implementat de manera urgent per resoldre o prevenir una incidència crítica.	Aprovació del CAB d'emergència (eCAB).

Requeriments del procés de gestió del canvi

Per a qualsevol canvi normal, l'adjudicatari ha de lliurar una RFC (*Request for Change*) que inclogui com a mínim:

- Descripció detallada del canvi i justificació tècnica.
- Requeriments de capacitat d'infraestructura.
- Sistemes i serveis afectats, amb indicació de l'impacte previst.
- Pla d'implementació pas a pas, amb estimació de la finestra de canvi requerida.
- Anàlisi de riscos i mesures de mitigació.
- Pla de marxa enrere: Procediment detallat per revertir el canvi en cas que es produeixi una incidència durant la seva implementació. Tota RFC sense pla de marxa enrere documentat serà rebutjada.
- Criteris d'èxit i validació post-implementació.
- Responsable tècnic de l'execució del canvi.

Comitè d'aprovació de canvis

L'adjudicatari pot participar activament en el CAB de CSI, revisant les RFCs en els terminis establerts i aportant tota la informació tècnica necessària per a la seva avaluació. Les reunions del CAB tindran la periodicitat definida per CSI, amb caràcter mínim setmanal.

Finestres de manteniment

Les tasques derivades de la gestió del canvi hauran de respectar les finestres de manteniment definides pel CSI per a la implementació de canvis sobre els sistemes en producció. Qualsevol tasca que requereixi una actuació fora de la finestra de

manteniment establerta haurà de ser justificat i aprovat explícitament per la direcció corresponent al servei (assistencial o no).

2.3.5 Gestió de peticions de servei

Les peticions de servei han de ser gestionades de manera independent de les incidències, a través del catàleg de serveis disponible en l'eina de tiqueting. L'adjudicatari ha de mantenir actualitzat el catàleg de peticions associat als serveis de cada lot, incloent-hi per a cadascuna:

- Descripció del servei i condicions d'elegibilitat.
- Informació requerida per a la tramitació.
- Temps d'execució estàndard (OLA).
- Fluxos d'aprovació requerits, si escau.

2.4 Reporting

2.4.1 Principis generals

L'adjudicatari ha de proporcionar al CSI una visió clara, completa i periòdica del rendiment dels serveis prestats, mitjançant un model de reporting estructurat que permeti avaluar el compliment dels compromisos contractuals, identificar tendències i donar suport a la presa de decisions.

El model de reporting ha de regir-se pels principis següents:

- **Objectivitat i traçabilitat:** Totes les dades reportades han de provenir directament de les eines de gestió i monitorització, evitant qualsevol manipulació manual que pugui comprometre la seva fiabilitat. El CSI s'ha de poder remetre a les fonts originals per contrastar qualsevol dada reportada.
- **Puntualitat:** Els informes han de ser lliurats en els terminis establerts, sense que l'adjudicatari pugui al·legar manca d'informació per justificar retards.
- **Orientació a la millora:** El reporting no ha de limitar-se a la constatació de dades, sinó que ha d'incloure l'anàlisi de les desviacions detectades, les seves causes i les mesures correctores o preventives proposades per l'adjudicatari.
- **Adaptabilitat:** El model de reporting ha de poder adaptar-se a les necessitats canviants de CSI. L'adjudicatari ha d'incorporar modificacions raonables en el contingut o el format dels informes sense cost addicional, sempre que es sol·licitin amb un preavís mínim d'un mes.

2.4.2 Informes periòdics de servei

L'adjudicatari ha de lliurar els informes periòdics següents, en format electrònic i en els canals definits pel CSI:

Informe mensual de servei

- Destinataris: Responsables tècnics i de direcció de CSI.
- Termini de lliurament: Abans del 5è dia hàbil del mes següent al que es reporta.

- Contingut mínim:
    - Resum executiu del mes, amb valoració global del servei.
    - Quadre de KPIs per lot, amb comparativa respecte al mes anterior i a l'acumulat anual.
    - Compliment dels SLAs definits al PPT, amb indicació explícita de les desviacions produïdes i el seu impacte econòmic si escau (penalitzacions).
    - Anàlisi detallada del volum d'incidències: distribució per prioritat, categoria, lot i tendència mensual.
    - Incidències P1 i P2 del mes: cronologia, causa, resolució i accions preventives.
    - Estat del catàleg de problemes oberts i tancats durant el mes.
    - Resum d'activitat de canvis: nombre de canvis per tipus, èxits, fallades i canvis revertits.
    - Estat de la capacitat dels sistemes principals en abast, amb tendències i previsions.
    - Pla d'accions de millora del mes següent, amb responsable i termini.
    - Estat de les accions acordades en el comitè anterior.

Informe trimestral de servei

- Destinataris: Direcció TI de CSI i Service Manager de l'adjudicatari.
- Termini de lliurament: Abans del 10è dia hàbil del mes següent al trimestre que es reporta.
- Contingut mínim:
    - Anàlisi acumulada dels KPIs i SLAs del trimestre, amb comparativa interanual si el contracte ho permet.
    - Evolució de les tendències d'incidències, problemes i canvis.
    - Avaluació del grau de maduresa operativa del servei i pla de millora.
    - Propostes d'optimització tècnica i operativa per al proper trimestre.
    - Estat del pla de formació i certificació de l'equip assignat.
    - Novetats tecnològiques rellevants per als serveis en abast (actualitzacions de fabricant, fi de suport, noves versions, etc.).

2.4.3 Reporting d'incompliments

Quan es produeixi un incompliment d'un SLA o KPI definit, l'adjudicatari ha d'activar un procediment de gestió de desviacions que inclogui:

1. **Notificació immediata**: Comunicació al CSI en el moment en què es detecti que un indicador se situa en risc d'incompliment, sense esperar al tancament del període de mesura.
2. **Informe de desviació**: Lliurament d'un informe específic en un termini màxim de 3 dies hàbils des de la constatació de l'incompliment, que inclogui la causa de la desviació, l'impacte produït i el pla d'acció correctora amb terminis.
3. **Seguiment de la correcció**: Inclusió de l'estat de les accions correctores en els informes periòdics fins a la seva resolució definitiva.
4. **Informe de tancament**: Un cop resolta la desviació, lliurament d'un informe de tancament que acrediti la normalització de l'indicador i les mesures preventives implantades per evitar la seva recurrència.

L'existència d'un procediment de gestió de desviacions actiu no eximeix l'adjudicatari de les penalitzacions econòmiques que puguin derivar-se dels incompliments, d'acord amb el règim sancionador establert al PPT.

2.5 Capacitat tècnica a demanda - Marc general

2.5.1 Naturalesa i finalitat

La capacitat tècnica a demanda és l'instrument mitjançant el qual el CSI pot disposar de capacitat tècnica de l'adjudicatari per a actuacions no incloses en el servei base de cada lot. La seva activació és discrecional per part del CSI i respon a necessitats puntuals, evolutives o no previstes que requereixen una dedicació específica i formalitzada.

La capacitat tècnica a demanda té caràcter **variable**: únicament es facturaran les hores efectivament consumides i validades pel CSI d'acord amb el procediment establert en el present apartat. El volum màxim definit per a cada lot constitueix un sostre pressupostari, no un compromís de consum ni una obligació de pagament per part del CSI. Les hores no consumides dins d'una anualitat no generen cap dret de compensació econòmica a favor de l'adjudicatari.

2.5.2 Preu hora i factors de conversió

Cada lot en abast determinarà el preu unitari per hora en horari d'oficina que el licitador ha d'incloure en la seva oferta econòmica. Aquest preu hora base és la unitat de referència sobre la qual s'apliquen els factors de conversió i equivalència establerts per a cada franja horària, modalitat de prestació o perfil professional, d'acord amb la taula específica de cada lot.

Les hores consumides en franges horàries o modalitats subjectes a factor de conversió es comptabilitzaran en el registre de consum com a hores base equivalents, resultants d'aplicar el factor corresponent a les hores reals d'execució. La facturació es calcularà

sobre les hores base equivalents acumulades al període, multiplicades pel preu unitari hora ofert. Els coeficients multiplicadors emplenats pel licitador no són objecte de valoració econòmica independent, però sí que vinculen contractualment l'adjudicatari, i podran ser objecte de valoració dins els criteris subjectius del lot corresponent.

2.5.3 Activació i autorització

Tota actuació amb càrrec a la capacitat tècnica a demanda requereix l'aprovació prèvia del CSI:

- **Actuacions planificades**: L'adjudicatari ha de presentar una estimació de les hores necessàries amb un mínim de 5 dies hàbils d'antelació respecte a la data d'execució prevista. L'aprovació ha de ser formalitzada pel responsable tècnic del lot al CSI abans de l'inici de l'actuació.
- **Actuacions urgents derivades d'incidències o problemes**: l'aprovació pot ser verbal en el moment de l'escalat, però ha de ser ratificada en el tiquet corresponent en un termini màxim de 24 hores.

Cap actuació amb càrrec a la capacitat tècnica a demanda podrà ser facturada si no disposa de l'aprovació corresponent.

2.5.4 Registre de consum

L'adjudicatari ha de mantenir en tot moment un registre actualitzat del consum de la capacitat tècnica a demanda, accessible per al CSI sota demanda. Per a cada actuació executada, el registre ha d'incloure com a mínim:

- Data, hora d'inici i hora de finalització de l'actuació.
- Descripció de l'actuació realitzada i referència al tiquet associat.
- Professional que ha executat l'actuació.
- Franja horària d'execució i factor de conversió aplicat.
- Hores reals d'execució i hores base equivalents resultants.
- Saldo d'hores base disponibles actualitzat.

2.5.5 Informe de consum i validació prèvia a la facturació

Amb una antelació mínima de 5 dies hàbils respecte a la data de tancament de cada període de facturació mensual, l'adjudicatari ha de lliurar al CSI un informe de consum de la capacitat tècnica a demanda que reculli la totalitat de les actuacions executades durant el mes, d'acord amb el contingut del registre definit a l'apartat anterior.

El responsable tècnic del lot al CSI disposa d'un termini de 3 dies hàbils des de la recepció de l'informe per procedir a la seva validació o per comunicar discrepàncies motivades a l'adjudicatari. La validació formal del CSI és condició necessària i prèvia a l'emissió de qualsevol factura corresponent a la part variable del contracte. En cas de discrepàncies, ambdues parts han de resoldre-les en el termini abans del tancament del cicle de facturació.

Un cop validat l'informe, el CSI emetrà la comanda de la part variable corresponent al consum del període, que servirà de base per a la facturació per part de l'adjudicatari.

2.6 Seguretat transversal

2.6.1 Marc de seguretat

La seguretat dels sistemes i de la informació gestionada en el marc del present contracte és una responsabilitat compartida entre el CSI i l'adjudicatari, si bé la custòdia i el compliment de les polítiques de seguretat corporatives recauen en tot moment sobre el CSI. L'adjudicatari ha d'actuar en tot moment com a garant de la seguretat en les operacions que realitzi sobre els sistemes en abast, i ha d'incorporar els principis de seguretat com un element intrínsec a la prestació del servei, no com un complement opcional.

El model de seguretat transversal aplicable a tots els lots es fonamenta en els principis següents:

- **Mínim privilegi:** Cap usuari, compte de servei o procés automatitzat no ha de disposar de més permisos dels estrictament necessaris per a l'execució de les seves funcions. L'adjudicatari ha de revisar periòdicament els privilegis assignats i eliminar qualsevol accés sobrant o obsolet.
- **Segregació de funcions:** Les tasques d'administració, operació i auditoria han de recaure en perfils diferenciats, evitant que una mateixa persona pugui realitzar i validar les seves pròpies actuacions sense supervisió.
- **Traçabilitat total:** Qualsevol accés o actuació realitzada sobre els sistemes en abast ha de quedar registrada de manera que sigui possible reconstruir qui ha fet què, quan i des d'on, amb un nivell de detall suficient per donar suport a investigacions forenses si fos necessari.
- **Seguretat per defecte:** Qualsevol nou sistema, component o configuració incorporada al servei ha de partir d'un estat segur com a punt de partida, requerint una justificació explícita per a qualsevol obertura o excepció a les polítiques de seguretat.
- **Defensa en profunditat:** La seguretat s'ha d'implementar en múltiples capes, de manera que la fallada d'un control de seguretat no comprometi la totalitat del sistema.
- **Confidencialitat de les dades:** Garantir que si s'accedeix a dades mediques caldrà complir amb els requeriments de les clàusules de confidencialitat del contracte.

2.6.2 Gestió d'accessos i identitats

Provisió i gestió de comptes

L'adjudicatari ha de sotmetre's al model de gestió d'accessos i identitats definit pel CSI, que inclou com a mínim els requisits següents:

- Tots els comptes d'accés als sistemes en abast han de ser aprovats formalment pel CSI abans de la seva creació, independentment del nivell de privilegis associat.

- L'adjudicatari ha de mantenir en tot moment un registre actualitzat de tots els comptes associats a la prestació del servei, incloent-hi comptes personals, comptes de servei i comptes compartits, amb indicació del responsable, la data de creació i la justificació del nivell d'accés atorgat.
- Queda expressament prohibit l'ús de comptes genèrics o compartits per a tasques d'administració. Tota actuació administrativa ha de realitzar-se amb comptes personals i nominatius, plenament traçables.

Cicle de vida dels accessos

Fase	Requeriment
Alta	Sol·licitud formal aprovada pel CSI. Compte creat d'acord amb la política de nomenclatura corporativa.
Revisió periòdica	Revisió trimestral de tots els comptes actius, amb validació explícita per part del CSI dels accessos que han de mantenir-se.
Modificació	Qualsevol canvi en els privilegis d'un compte ha de seguir el mateix circuit d'aprovació que l'alta.
Baixa	En cas de baixa o canvi de rol d'un tècnic de l'adjudicatari, el compte associat ha de ser deshabilitat en un termini màxim de 30 minuts des de la comunicació. L'adjudicatari ha de notificar proactivament al CSI qualsevol canvi de personal que afecti accessos actius.

Autenticació

Tots els accessos administratius als sistemes en abast han de requerir **autenticació multifactor (MFA)**, especialment per a accessos remots i per a comptes amb privilegis elevats.

L'accés remot als sistemes en abast ha de realitzar-se exclusivament a través dels canals segurs definits pel CSI (ZTNA / CITRIX, VPN corporativa), quedant expressament prohibit qualsevol accés directe des de xarxes externes sense passar pels controls establerts.

2.6.3 Gestió de vulnerabilitats i pegats de seguretat

L'adjudicatari ha de mantenir un procés actiu de gestió de vulnerabilitats sobre tots els sistemes en abast del seu lot, que inclogui:

- Revisió vulnerabilitats publicades: Revisió constant de la publicació dels CVE de la infraestructura que gestiona. Els resultats han de ser lliurats al CSI i han de ser la base per a la planificació d'aplicació dels pegats.
- Classificació i priorització: Les vulnerabilitats detectades han de ser classificades d'acord amb el seu nivell de criticitat, i prioritzades per a la seva correcció en funció del risc que representin per als sistemes del CSI.
- Terminis de correcció: L'adjudicatari ha de respectar els terminis màxims de correcció de vulnerabilitats següents, excepte justificació documentada i acceptada pel CSI:

Criticitat	Termini màxim de correcció
Crítica	72 hores des de la detecció o publicació del CVE.
Alta	7 dies naturals
Mitjana	30 dies naturals
Baixa	Proper cicle de parxeig planificat

- Excepcions: En els casos en què l'aplicació d'un pegat no sigui possible dins del termini establert (incompatibilitat tècnica, risc operatiu, dependència de fabricant), l'adjudicatari ha de documentar la justificació i, en la mesura del possible, implementar mesures compensatòries.
- Mantenir al dia les eines d'aplicació de pegats del CSI així com proposar millores en l'arquitectura dels sistemes crítics per tal de garantir que els pegats es puguin fer en calent sense afectació en els serveis corporatius de CSI.

2.6.4 Gestió d'esdeveniments de seguretat

L'adjudicatari ha de notificar al CSI preferentment de manera immediata, i en tot cas, en un termini màxim de 2 hores, qualsevol esdeveniment de seguretat detectat que pugui afectar la confidencialitat, integritat o disponibilitat dels sistemes o de la informació gestionada.

Davant d'un incident de seguretat confirmat, l'adjudicatari ha de col·laborar activament amb l'equip de seguretat del CSI, aportant tots els registres, evidències i informació tècnica necessaris per a la seva investigació i contenció.

L'adjudicatari ha de disposar d'un procediment documentat de resposta a incidents de seguretat, alineat amb el marc de gestió d'incidents del CSI, que ha de ser lliurat durant el període de transició.

2.7 Gestió de la documentació tècnica i base del coneixement

La documentació tècnica és un actiu estratègic del CSI i constitueix un element essencial per garantir la continuïtat del servei, la transferència de coneixement i la independència del CSI respecte a l'adjudicatari. Per aquest motiu, la generació, el manteniment i l'actualització de la documentació tècnica no és una activitat opcional ni complementària, sinó un requisit inherent a la prestació del servei, el compliment del qual serà avaluat de manera periòdica.

Els principis que regeixen la gestió documental en el marc d'aquest contracte són:

- **Propietat del CSI:** Tota la documentació generada en el context de la prestació del servei és propietat exclusiva del CSI, independentment de qui l'hagi elaborat. L'adjudicatari no pot retenir, restringir ni condicionar l'accés a cap document en cap circumstància.
- **Actualització com a part del servei:** La documentació ha de reflectir en tot moment l'estat real dels sistemes i dels procediments. Qualsevol canvi sobre la infraestructura o els processos operatius ha de comportar l'actualització de la

documentació afectada com a part integrant de la seva implementació, no com una tasca posterior i diferida.

- **Formats estàndard i no propietaris:** Tota la documentació ha de ser lliurada i mantinguda en formats oberts i estàndard que garanteixin la seva accessibilitat sense dependència d'eines específiques de l'adjudicatari.
- **Organització de la documentació:** La documentació s'organitzarà als gestors documentals per part del personal del CSI, amb una estructura de carpetes i un sistema de nomenclatura definits, i serà accessible per als perfils autoritzats del CSI en tot moment, sense necessitat d'intermediació per cap part.
- **Control de versions:** Tota la documentació estarà sotmesa a un sistema de control de versions que permeti identificar la versió vigent, l'autor de cada revisió, la data de modificació i un resum dels canvis efectuats.

2.7.1 Tipus de documents

L'adjudicatari ha de mantenir actualitzat, com a mínim, el corpus documental següent, organitzat per tipologia.

Documentació d'arquitectura i infraestructura

- Diagrames d'arquitectura: Representació actualitzada de l'arquitectura dels sistemes en abast de cada lot, incloent-hi les dependències entre components, la segmentació de xarxa, els fluxos de comunicació i la integració amb sistemes externs. Els diagrames han de mantenir-se en un format editable, no únicament com a imatge estàtica.
- Inventari de sistemes: Inventari complet i actualitzat de tots els sistemes en abast, amb els atributs tècnics rellevants de cada element.
- Documentació de configuració: Configuracions rellevants dels sistemes crítics, amb el nivell de detall suficient per permetre la seva reconstrucció en cas de desastre o en el context d'un canvi de proveïdor

Documentació operativa

- Runbooks operatius: Procediments pas a pas per a les tasques d'operació habituals de cada lot, incloent-hi l'arrencada i parada de sistemes, la gestió de processos de fons, les tasques de manteniment preventiu i les comprovacions periòdiques de l'estat del servei.
- Procediments d'escalat: Document que defineix l'arbre de decisió per a l'escalat d'incidències per tipus, severitat i lot, amb els contactes actualitzats de cada nivell d'escalat.
- Procediments de gestió d'alertes: Documentació de la resposta esperada davant de cada tipus d'alerta de monitorització, incloent-hi el diagnòstic inicial, les accions de primer nivell i els criteris per a l'escalat.

Documentació de gestió i seguiment

- Plans de servei per lot: Document que descriu el model operatiu específic de cada lot, l'estructura de l'equip assignat, les eines utilitzades, els processos aplicables i els compromisos de servei.
- Informes de servei: D'acord amb el que s'estableix al punt 2.4 del present document.
- Actes de reunions de govern: Registre de les decisions, acords i accions derivats de cada reunió dels comitès establerts al punt 2.1.

2.7.2 Repositori documental

Tota la documentació ha de centralitzar-se en el repositori corporatiu del CSI, accessible per als perfils autoritzats de les dues parts: Atlassian Confluence Cloud.

2.7.3 Obligacions documentals en la transició i finalització del contracte

A l'inici del contracte - Període de transició

Durant el període de transició, l'adjudicatari entrant ha de rebre i revisar tota la documentació existent, identificar les llacunes documentals i elaborar un pla de documentació que estableixi els terminis per cobrir els dèficits detectats. Aquest pla ha de ser aprovat pel CSI i el seu compliment serà un dels criteris d'avaluació del període de transició.

Durant la vigència del contracte

L'estat de la documentació serà revisat en el marc dels comitès de seguiment mensuals, on l'adjudicatari ha de reportar els documents creats, actualitzats i pendents d'actualització durant el mes, i justificar qualsevol desviació respecte al pla de documentació vigent.

A la finalització del contracte

En el moment de la finalització del contracte, ja sigui per venciment o per qualsevol altra causa, l'adjudicatari ha de garantir:

- Lliurament al CSI de la totalitat de la documentació tècnica en la seva versió més actualitzada, en els formats estàndard acordats.
- Verificació conjunta amb el CSI de la completesa i actualitat de la documentació lliurada.
- Col·laboració activa en la transferència de coneixement a l'adjudicatari entrant durant el període de transició sortint, incloent-hi sessions de traspàs presencials per a cada lot si el CSI així ho requereix.
- Destrucció certificada de qualsevol còpia de la documentació del CSI que hagi quedat en els sistemes de l'adjudicatari sortint.

2.8 Catàleg de KPIs operatius

El present catàleg defineix els indicadors clau de rendiment (KPIs) transversals aplicables a la totalitat dels lots objecte del present contracte. Aquests indicadors constitueixen el mecanisme objectiu i homogeni de mesura del rendiment operatiu del servei, i són la base sobre la qual s'avalua el compliment dels compromisos

contractuals, s'apliquen les penalitzacions establertes i es prenen decisions de govern en els comitès definits.

El model de KPIs es regeix pels principis següents:

- **Automatització de la mesura:** Tots els KPIs han de ser calculats de manera automàtica a partir de les dades extretes directament de les eines de gestió i monitorització corporatives, sense intervenció manual que pugui comprometre la seva objectivitat. L'adjudicatari ha de garantir que les seves eines generen les dades necessàries per al càlcul de la totalitat dels indicadors aquí definits.
- **Disponibilitat de les dades brutes:** El CSI ha de tenir accés en tot moment a les dades brutes que sustenten el càlcul de cada KPI, sota sol·licitud a l'adjudicatari.
- **Període de mesura:** Excepte indicació contrària, tots els KPIs es calculen amb periodicitat mensual i es reporten a l'informe mensual de servei. Els indicadors marcats com a operatius en temps real han de ser accessibles de manera contínua a través del quadre de comandament operatiu.
- **Valors llindar:** Per a cada KPI s'estableixen tres nivells de referència: el valor objectiu que representa el nivell de qualitat esperat en condicions normals de servei, el valor de mínim acceptable per sota del qual s'activen les penalitzacions, i el valor de risc que, sense activar penalitzacions directes, obliga l'adjudicatari a presentar un pla d'acció correctora en el termini de 3 dies hàbils.
- **Evolució dels indicadors:** El catàleg de KPIs pot ser revisat i ampliat de mutu acord entre el CSI i l'adjudicatari en el marc dels comitès de seguiment, sense que la incorporació de nous indicadors pugui suposar cap cost addicional per al CSI.

2.8.1 Definició de KPIs

KPI-01 - Compliment del temps de resposta

Atribut	Descripció
Descripció	Percentatge d'incidències en les quals el temps de resposta ha estat igual o inferior al temps màxim contractat, per prioritat i nivell de criticitat del servei
Fórmula	Incidències amb temps de resposta ≤ SLA / Total incidències del període × 100
Unitat	Percentatge (%)
Font de dades	Eina de tiqueting corporativa
Periodicitat	Mensual
Valor objectiu	≥ 98% per a totes les prioritats

Valor de risc	Entre 95% i 97,9%
Valor mínim acceptable	95% (per sota s'activen penalitzacions secció 7.5 del PPT)

KPI-02 – Compliment del temps de resolució

Atribut	**Descripció**
Descripció	Percentatge d'incidències en les quals el temps de resolució ha estat igual o inferior al temps màxim contractat, per prioritat i nivell de criticitat del servei
Fórmula	Incidències resoltes dins del SLA / Total incidències del període × 100
Unitat	Percentatge (%)
Font de dades	Eina de tiqueting corporativa
Periodicitat	Mensual
Valor objectiu	≥ 97% per a P3 i P4 / ≥ 99% per a P1 i P2
Valor de risc	Entre 95% i 96,9% (P3/P4) / Entre 95% i 98,9% (P1/P2)
Valor mínim acceptable	95% per a totes les prioritats

KPI-03 – Taxa de reobertura d'incidències

Atribut	**Descripció**
Descripció	Percentatge d'incidències que han estat reobertes després del seu tancament per no haver estat resoltes de manera efectiva
Fórmula	Incidències reobertes en el mes / Total incidències tancades en el mes × 100
Unitat	Percentatge (%)
Font de dades	Eina de tiqueting corporativa
Periodicitat	Mensual
Valor objectiu	≤ 3%
Valor de risc	Entre 3% i 5%

Valor mínim acceptable	≤ 5% (per sobre obliga a presentar pla d'acció correctora)
Nota	Una incidència reoberta dins dels 5 dies hàbils posteriors al tancament computa com a reobertura del tiquet original, no com a nova incidència

3 Lot 1: Operació i administració de sistemes (N2/N3)

3.1 Descripció del servei

3.1.1 Objecte del lot

El Lot 1 té per objecte la prestació del servei de gestió i administració dels sistemes TI del CSI, estructurat en dos nivells de servei complementaris i indissociables:

- **Operacions de Sistemes - Nivell 2 (N2)**: Servei d'operació contínua dels sistemes, orientat a la supervisió, el manteniment de la disponibilitat i la resolució d'incidències operatives en el marc dels processos i procediments establerts.
- **Administració de Sistemes - Nivell 3 (N3)**: Servei d'administració avançada dels sistemes, orientat a la gestió del cicle de vida i la resolució de problemes complexos que requereixen un coneixement profund de les plataformes gestionades.

Ambdós nivells han de ser prestats de manera integrada per l'adjudicatari del Lot 1, garantint una cobertura contínua i sense interrupcions en la cadena d'escalat entre N2 i N3, i assegurant en tot moment la coordinació amb els adjudicataris dels lots 2, 3 i 4 en els aspectes que afecten la infraestructura de base que sustenta les seves plataformes específiques.

3.1.2 Abast del servei

El servei de Lot 1 abasta la totalitat dels sistemes d'infraestructura TI del CSI, amb independència de la tecnologia de virtualització, el sistema operatiu o la ubicació física dels mateixos. A títol orientatiu, i sense caràcter limitatiu, l'abast inclou les categories de sistemes següents:

Categoria	Descripció
Servidors físics	Servidors en rack ubicats als centres de processament de dades del CSI, incloent-hi la gestió dels seus sistemes d'administració remota.
Servidors virtuals	Hipervisors i màquines virtuals allotjades sobre les plataformes d'hipervisor del CSI (Nutanix AHV), incloent-hi la gestió de la capa de virtualització.
Sistemes operatius	Administració dels sistemes operatius instal·lats sobre els servidors en abast, tant en entorns Windows Server com Linux (RedHat, SUSE, Ubuntu o altres distribucions en ús al CSI)
Capa de middleware i software base	Gestió del programari de base instal·lat sobre els sistemes (servidors web, servidors d'aplicacions, agents de monitorització, agents de backup, etc.), en coordinació amb els adjudicataris dels lots corresponents quan escaigui.
BBDD	Operació i administració de bases de dades SQL Server i PostgreSQL.

Sistemes d'emmagatzematge	Operació dels sistemes d'emmagatzematge associats als servidors en abast, incloent-hi la gestió de volums, snapshots i polítiques de tiering.
Infraestructura de backup	Operació del servei de backup dels sistemes en abast en coordinació amb l'adjudicatari del Lot 2, limitada a la part operativa (verificació d'execució, gestió d'alertes de backup, sol·licituds de restauració), quedant l'administració de la plataforma CommVault sota la responsabilitat del Lot 2.
Gestió de la plataforma de monitorització	Administració, manteniment i evolució de la plataforma de monitorització centralitzada, d'acord amb el que s'estableix al punt 3.4.1 del present document.

3.1.3 Límits del servei i relació amb d'altres lots

El Lot 1 actua com a capa de servei d'infraestructura transversal sobre la qual es recolzen els serveis específics dels lots 2, 3 i 4. Per aquest motiu, és fonamental que les responsabilitats entre lots estiguin clarament delimitades per evitar llacunes de cobertura o duplicitats operatives. Els límits principals s'estableixen de la manera següent:

Àmbit	Lot 1	Lot relacionat
Infraestructura dels sistemes SAP	Sistema operatiu, emmagatzematge i virtualització dels servidors de la plataforma SAP.	Lot 3 assumeix la capa d'arquitectura, SAP Basis i superior.
Infraestructura de la plataforma CITRIX	Sistema operatiu i virtualització dels servidors Citrix. Operativa diària de la plataforma.	Lot 4 assumeix la capa d'aplicació i configuració Citrix nivell 3.
Infraestructura de backup	Sistema operatiu i virtualització dels servidors onprem. Verificació operativa de l'execució dels jobs i gestió d'alertes de primer nivell.	Lot 2 assumeix l'administració de la plataforma CommVault i la definició de polítiques.
Monitorització	Administració de la plataforma de monitorització i cobertura de tots els sistemes dels quatre lots.	Els lots 2, 3 i 4 han de col·laborar en la definició dels checks específics de les seves plataformes.

L'adjudicatari del Lot 1 ha d'establir procediments de coordinació formals amb els adjudicataris dels lots 2, 3 i 4, que han de quedar documentats durant el període de transició i ser aprovats pel CSI. En cas de discrepància sobre la responsabilitat d'una actuació concreta, el CSI actuarà com a àrbitre i la seva decisió serà vinculant.

3.1.4 Model de prestació i presència física

El servei del Lot 1 s'ha de prestar sota un model de prestació híbrid, que combina el treball en remot per a les tasques d'operació i administració susceptibles de ser executades a distància, amb la presència física obligatòria a les instal·lacions del CSI per a les actuacions que així ho requereixin, així com per garantir una interlocució àgil i un coneixement profund de l'entorn.

Amb independència del model de prestació en cada moment, l'adjudicatari ha de garantir un mínim de 3 FTE (Full Time Equivalent) dedicats al servei amb un alt grau de coneixement de l'entorn del CSI. Aquests recursos han de tenir una dedicació real i efectiva al present contracte, suficient per absorbir la càrrega operativa, cobrir les franges horàries de servei establertes i garantir la continuïtat del coneixement de l'entorn durant tota la vigència del contracte. L'adjudicatari ha de justificar en la seva oferta que el dimensionament proposat garanteix el compliment d'aquest mínim en totes les situacions, incloent-hi períodes de vacances, baixes i absències del personal assignat.

Presència mínima obligatòria

L'adjudicatari ha de garantir la presència física d'un mínim d'un (1) tècnic a les instal·lacions del CSI durant tots els dies laborables, en horari a convenir amb el CSI durant el període de transició. Aquesta presència ha de cobrir, com a mínim, la franja horària central del dia laboral i ha de ser suficient per atendre les necessitats d'interlocució tècnica, les actuacions que requereixin accés físic als sistemes i la coordinació amb els equips interns del CSI.

Respecte a la persona assignada a la presència física, s'estableixen les condicions següents:

- No és requisit que sigui sempre la mateixa persona, però tots els tècnics que exerceixin aquesta funció han de formar part de l'equip assignat al contracte, tenir un coneixement suficient de l'entorn del CSI i haver estat identificats i comunicats formalment al CSI.
- L'adjudicatari ha de garantir en tot moment que la persona present a les instal·lacions té el nivell tècnic i les credencials d'accés adequades per atendre les situacions que puguin sorgir durant la seva jornada de presència.
- L'adjudicatari ha de disposar d'un calendari de presència mensual, lliurat al CSI abans del primer dia hàbil de cada mes, que identifiqui la persona assignada a cada dia i garanteixi la cobertura contínua sense buits.

Ubicacions de prestació del servei

El servei s'ha de prestar des de les ubicacions següents:

Modalitat	Ubicació	Aplicació
Presència física	Instal·lacions del CSI: Oficina de la DTSD, CPDs i altres ubicacions corporatives	Mínim 1 tècnic tots els dies laborables, en horari a convenir. Actuacions que

		requereixin accés físic als sistemes en qualsevol moment.
Remot	Instal·lacions de l'adjudicatari, teletreball o equivalent	Resta de tasques d'operació i administració susceptibles de ser executades a distància, inclosa la cobertura de guàrdia 24x7 fora de l'horari de presència

L'adjudicatari ha de garantir que els tècnics en modalitat remota disposen de les eines, els accessos i la connectivitat necessaris per operar amb plena efectivitat, sense que la modalitat de treball en remot pugui ser al·legada com a causa de demora o limitació en la resposta davant d'incidències.

Actuacions que requereixen presència física

A títol orientatiu, i sense caràcter limitatiu, requereixen presència física a les instal·lacions del CSI les actuacions següents:

- Intervencions sobre maquinari físic (substitució de components, connexió de cablejat, manipulació de dispositius d'emmagatzematge, etc.).
- Actuacions de recuperació davant de fallades que impedeixin l'accés remot als sistemes.
- Instal·lació o substitució de servidors físics o components d'infraestructura.
- Accés a consoles físiques de servidors o dispositius sense gestió remota disponible.
- Qualsevol actuació sobre sistemes o zones del CPD que, per motius de seguretat, no permetin l'accés remot.
- Reunions tècniques o de coordinació que el CSI requereixi presencialment.

En els casos en què es requereixi presència física fora de l'horari de presència habitual (cap de setmana, festius o fora de la franja horària acordada), l'adjudicatari ha de garantir la disponibilitat d'un tècnic per desplaçar-se a les instal·lacions del CSI en un termini màxim de 1 hora des de la sol·licitud, sense que això comporti cap cost addicional per al CSI sempre que es tracti d'una incidència crítica.

Condicions d'accés a les instal·lacions

El personal de l'adjudicatari que hagi d'accedir físicament a les instal·lacions del CSI haurà de complir les condicions d'accés establertes per la política de seguretat física corporativa del CSI, que seran comunicades durant el període de transició. En particular:

- Tot el personal haurà d'estar identificat i acreditat per al CSI prèviament al seu primer accés a les instal·lacions.

- L'adjudicatari haurà de notificar al CSI qualsevol incorporació o baixa de personal amb accés físic, en els terminis establerts al punt 2 del present document.

3.1.5 Horari i model de cobertura

El servei del lot 1 ha de prestar-se sota el model de cobertura següent:

Modalitat	Descripció
Horari estès (07:30 – 17:00, L-V)	Operacions N2: gestió d'incidències, execució de peticions de servei i suport operatiu general en dies laborables.
24x7x365	Operacions N2: monitorització, gestió d'alertes i atenció d'incidències crítiques i d'alta prioritat. Escalat a guàrdies fora d'horari estès.
Guàrdia localitzable	Disponibilitat de tècnic de guàrdia fora de l'horari estès per a l'atenció d'incidències crítiques que requereixin intervenció administrativa avançada, amb un temps de resposta màxim de 30 minuts des de la notificació

L'adjudicatari ha de garantir en tot moment la cobertura del servei sense dependències en persones individuals, disposant de procediments documentats per assegurar la continuïtat davant d'absències, baixes o vacances del personal assignat.

3.1.6 Capacitat tècnica a demanda

Es defineix una capacitat tècnica a demanda per al Lot 1 destinada principalment a donar cobertura a les intervencions programades que, per la seva naturalesa o pel seu impacte potencial sobre els sistemes en producció, no poden ser executades durant l'horari habitual de servei. A títol orientatiu, i sense caràcter limitatiu, constitueixen exemples d'ús habitual d'aquesta capacitat tècnica les actuacions següents:

- Actualitzacions de firmware i BIOS de servidors físics.
- Aplicació de pedaços de sistema operatiu sobre sistemes crítics que requereixen finestra nocturna o de cap de setmana.
- Migracions i moviments de màquines virtuals amb impacte sobre el servei.
- Canvis d'infraestructura de risc elevat que requereixen finestra de manteniment ampliada.
- Actuacions de manteniment preventiu planificades fora de l'horari de producció.
- Qualsevol altra actuació programada que el CSI requereixi executar fora de l'horari habitual de servei.

Volum

El volum mínim de la capacitat tècnica a demanda és de **200 hores efectives anuals**. La capacitat tècnica a demanda és un requisit obligatori del present lot: les ofertes

que no incloguin la capacitat tècnica a demanda en les condicions establertes en el present apartat seran excloses del procés de licitació.

Condicions d'ús

Intervencions programades

Les actuacions programades que requereixin l'ús de la capacitat tècnica a demanda han de ser sol·licitades pel CSI amb un mínim de 5 dies hàbils d'antelació respecte a la data d'execució prevista, per permetre la planificació adequada dels recursos.

Tota intervenció programada ha de disposar de la seva corresponent petició aprovada abans de l'inici de la seva execució, independentment que es tracti d'una actuació inclosa en el catàleg de canvis estàndard o que requereixi tramitació com a canvi normal.

Incidències i problemes greus

En el cas d'incidències greus que requereixin una intervenció urgent fora de l'horari habitual de servei i que no estiguin cobertes pel model de guàrdia definit, les hores de la capacitat tècnica poden ser consumides les 24 hores del dia, 7 dies a la setmana.

Taula d'equivalència

S'haurà de contemplar l'equivalència entre els diferents horaris de servei dins d'una taula, ja que la capacitat tècnica a demanda es podrà emprar en qualsevol horari, tant diürn, com nocturn com festiu, així com si les hores son presencials o remotes, seguint el model de la taula següent:

	Multiplicador de capacitat tècnica a demanda			
	Remot		Presencial	
Tipus de perfil	Nocturn	Festiu	Nocturn	Festiu
Operador N2				
Administrador				

3.2 Model de guàrdies

El CSI disposa d'un model de guàrdia estructurat en tres nivells per a la cobertura de les incidències que es produeixen fora de l'horari de servei habitual. Cada nivell té un àmbit de responsabilitat clarament definit i les incidències han de progressar seqüencialment a través dels nivells en ordre ascendent quan l'escalat sigui necessària, sense que cap nivell pugui ser saltat o activat de manera independent sense haver esgotat prèviament les possibilitats de resolució del nivell anterior, excepte en els casos en què la naturalesa de la incidència requereixi una actuació immediata de nivell superior degudament justificada.

3.2.1 Nivells de guàrdia

Nivell 1 - Guàrdia de Service Desk

El primer nivell de guàrdia és cobert pels tècnics del servei de Service Desk del CSI. Constitueix el punt d'entrada únic per a totes les incidències que es produeixin durant l'horari de guàrdia, independentment de la seva naturalesa o gravetat. El nivell 1 és responsable de la recepció, el registre i la classificació inicial de la incidència, i de l'activació del nivell 2 quan la resolució superi el seu àmbit de competència. Aquest nivell és intern al CSI i queda fora de l'abast del present lot.

Nivell 2 - Guàrdia d'Operacions de Sistemes

El segon nivell de guàrdia és cobert per un pool de tècnics d'operacions i constitueix l'objecte del present lot en l'àmbit de les guàrdies. Rep les escalades del nivell 1 i és responsable de la diagnosi i la resolució de les incidències operatives que no hagin pogut ser resoltes en el primer nivell, d'acord amb les tecnologies i les responsabilitats definides al present document.

La cobertura d'aquest nivell ha de ser prestada per l'adjudicatari mitjançant un pool rotatiu de tècnics en modalitat de guàrdia localitzable, de manera que en tot moment hi hagi un tècnic disponible per atendre les escalades del nivell 1 dins dels temps de resposta establerts.

Nivell 3 - Guàrdia d'Administració Avançada

El tercer nivell de guàrdia és cobert pels administradors de sistemes interns del CSI, que disposen del coneixement més avançat de l'entorn i de la capacitat de decisió i autorització necessàries per a actuacions de major calat sobre els sistemes crítics. Aquest nivell s'activa quan la resolució de la incidència requereix actuacions que excedeixen l'àmbit de competència o de responsabilitat del nivell 2, com ara el reinici de sistemes crítics de negoci, la presa de decisions sobre l'arquitectura o l'escalat a fabricants externs. Aquest nivell és intern al CSI i queda fora de l'abast del present lot.

3.2.2 Horari de les guàrdies

Franja	Dies	Horari
Guàrdia dia laborable	Dilluns a divendres laborables	Des de les 17:00h fins a les 07:30 del dia següent
Guàrdia en caps de setmana i festius	Dissabte, diumenge i festius	24 hores

Durant la franja horària no coberta per la guàrdia en dies laborables, el servei es presta en modalitat de servei diürn d'acord amb els horaris i el model de cobertura definits al punt 3.1 del present document.

3.2.3 Composició del pool de tècnics

El pool de tècnics assignats a la guàrdia ha d'estar identificat i comunicat formalment al CSI, amb el calendari de guàrdies actualitzat mensualment.

Tots els tècnics del pool han de tenir un nivell de coneixement de l'entorn del CSI suficient per atendre les incidències habituals de guàrdia de manera autònoma.

L'adjudicatari ha de disposar d'un procediment documentat de substitució del tècnic de guàrdia en cas d'impossibilitat sobrevinguda, garantint la cobertura sense interrupcions i notificant al CSI qualsevol canvi en la composició de la guàrdia activa.

3.2.4 Escalat al Nivell 3

Quan la resolució d'una incidència requereixi l'activació del Nivell 3, el tècnic de guàrdia de Nivell 2 ha de:

- Haver esgotat els procediments documentats disponibles per al tipus d'incidència en qüestió o haver determinat que la resolució requereix una actuació altament especialitzada que correspon al Nivell 3 (reinici de sistema crític, contacte amb fabricant extern, decisions d'arquitectura, etc.).
- Notificar al Nivell 1 la necessitat d'escalat al Nivell 3, aportant tota la informació recollida durant la diagnosi per facilitar la presa de decisió i l'actuació del Nivell 3 sense demora ni pèrdua de context.
- Romandre disponible i actiu durant la resolució per part del Nivell 3, donant suport tècnic operatiu a les actuacions que siguin necessàries i mantenint el registre del tiquet actualitzat fins al tancament de la incidència.
- En el cas que la incidència necessiti d'un expert en la tecnologia, serà responsabilitat de l'adjudicatari aconseguir aquest recurs durant la incidència i iniciar les accions per a la seva resolució.
- En cas de que fos necessari, l'adjudicatari també s'encarregarà d'escalar directament el cas al fabricant de la solució o bé indirectament a traves d'un proveïdor. També s'encarregarà de fer el seguiment exhaustiu fins que es resolgui la incidència.

3.2.5 Registre i documentació

Tota incidència atesa durant la guàrdia ha de quedar registrada en l'eina de tiqueting en el moment de la seva recepció, independentment de l'hora en què es produeixi. El registre ha d'incloure com a mínim l'hora de notificació del Nivell 1, l'hora d'acusament de recepció del Nivell 2, les accions realitzades i el resultat obtingut. En cas d'escalat al Nivell 3 o fabricant, ha de quedar constància de l'hora d'activació i la justificació de l'escalat.

3.3 Inventari i descripció de l'entorn

3.3.1 Consideracions generals

La informació recollida en el present apartat descriu l'entorn tecnològic actual sobre el qual s'ha de prestar el servei del Lot 1, i constitueix la referència de partida per al dimensionament de l'equip, la planificació de la transició i l'elaboració de les ofertes per part dels licitadors. Les xifres indicades tenen caràcter orientatiu i poden existir variacions raonables derivades de l'evolució natural del parc de sistemes durant el procés de licitació. L'adjudicatari no podrà al·legar desconeixement de l'entorn com a causa d'un dimensionament inadequat de la seva oferta.

Durant el període de transició, l'adjudicatari realitzarà un inventari complet i validat de la totalitat dels sistemes en abast, que constituirà la línia de base oficial del contracte i serà gestionat al repositori documental com a document viu.

3.3.2 Infraestructura de servidors

Servidors físics

El CSI disposa d'un parc de 25 servidors físics en abast del present lot, distribuïts entre els centres de processament de dades descrits a l'apartat 3.2.5. Els fabricants i models principals presents en el parc són Fujitsu PRIMEFLEX XF3070 M3.

Màquines virtuals

Sobre la infraestructura de virtualització descrita a continuació, el CSI opera un total de 397 màquines virtuals en abast del present lot.

Distribució per sistema operatiu

La distribució del parc de servidors (físics i virtuals) per sistema operatiu és la següent:

Sistema operatiu	Versió	Nombre de sistemes
Windows server	2025	5
Windows server	2022	126
Windows server	2019	79
Windows server	altres	41
SUSE Linux Enterprise Server	15SP7	20
SUSE Linux Enterprise Server	15SP5	8
Debian Linux	-	9
CentOS	-	7
Ubuntu	-	7
Oracle Linux	-	3
Nutanix	-	51
Appliance	-	41

3.3.3 Plataforma de virtualització

La infraestructura de virtualització del CSI es basa en Nutanix AHV en la seva versió AOS 7.3.1.4, i està formada per un total de 23 hosts físics agrupats en 7 clústers. La gestió centralitzada es realitza mitjançant Prism Central en la darrera versió a dia de publicació del present document.

3.3.4 Sistemes d'emmagatzematge

El CSI disposa dels sistemes d'emmagatzematge següents:

Tipus	Fabricant	Capacitat total	Observacions
NAS	Huawei OceanStore	490TiB	Dels quals 100TiB en clúster
NAS	Nutanix Files	33TiB	En clúster

3.3.5 Xarxa i seguretat

El CSI disposa de diferents elements de xarxa, com ara switchos per a la connectivitat, Firewalls per a la seguretat perimetral i Controladores WiFi i APs per a la connectivitat sense fils. A continuació, es detallen el model, el fabricant, el tipus de dispositiu i la quantitat existent de cadascun:

Fabricant - Model	Tipus dispositiu	Quantitat
Aruba 2930F	Switch Accés	50
Aruba 6200F	Switch Accés	5
HP 5412zl	Switch Accés	25
HP 2620	Switch Accés	10
HP 2530	Switch Accés	7
HP 2610	Switch Accés	31
HP 2520	Switch Accés	1
HP 2510	Switch Accés	7
Aruba CX 8325	Switch CORE	2
Aruba 6300M	Switch CORE	2
Aruba CX 8360	Switch CORE	4
Aruba 3810M	Switch CORE	2
Cisco Nexus 9000	Switch Data Center	4
FortiGate 1800F	Firewall	2
FortiGate 80F	Firewall	4
FortiGate 40F	Firewall	12
Aruba 7210	Controladora WiFi	2
Aruba MM-VA-1K	Mobility Conductor (Virtual)	2
HPE Aruba Networking AP-303	Punt d'accés (Campus AP)	158
HPE Aruba Networking AP-303H	Punt d'accés (Campus AP)	1
HPE Aruba Networking AP-305	Punt d'accés (Campus AP)	98
HPE Aruba Networking AP-315	Punt d'accés (Campus AP)	191
HPE Aruba Networking AP-345	Punt d'accés (Campus AP)	5
HPE Aruba Networking AP-503H	Punt d'accés (Campus AP)	8
HPE Aruba Networking AP-505	Punt d'accés (Campus AP)	21
HPE Aruba Networking AP-515	Punt d'accés (Campus AP)	50

3.3.6 Software base

Els servidors en abast del Lot 1 allotgen, entre d'altres, el software de base i middleware següent, la gestió operativa del qual recau sobre l'adjudicatari del present lot:

Software	Versió	Nombre d'instàncies	Observacions
Apache Tomcat	9.0.111 i altres	8	

Oracle	19c i 11.2.0.3	9	
SQL Server	2022, 2019 i altres	47	112 instàncies
MAXDB		2	
MySQL		14	
PostgreSQL		9	

3.3.7 Ubicació dels *datacenters* i sales tècniques

Els sistemes en abast del Lot 1 es troben ubicats en els centres de processament de dades (CPD) següents:

CPD	Ubicació	Sistemes en abast
HSJD	Sant Joan Despí	364 + 16 Físics
HGH	L'Hospitalet de Llobregat	12 + 2 Físics
HDM	Barcelona	10 + 2 Físics
ABS Collblanc	Collblanc	Només infraestructura de xarxa
ABS Torrassa	Torrassa	3 + 1 Físics
CAE Sant Feliu	Sant Feliu de Llobregat	4 + 1 Físics
CAE Cornellà	Cornellà de Llobregat	4 + 1 Físics
Residència Collblanc Companys Social	Collblanc	Només infraestructura de xarxa
Residència Francisco Padilla	L'Hospitalet de Llobregat	Només infraestructura de xarxa

3.3.8 Volum operatiu de referència

A continuació s'indica el volum operatiu mensual de referència, obtingut a partir de les dades del servei predecessor, amb l'objectiu de facilitar el dimensionament de l'equip per part dels licitadors:

Indicador	Volum mensual aproximat
Incidències	30
Incidències greus	3
Peticions de servei	100
Tasques de sistemes	30

L'eina de tiqueting corporativa actualment en ús al CSI és Jira Service Management (Cloud), i constituirà la plataforma de referència per a la gestió de tots els serveis objecte del present contracte.

3.4 Monitorització i gestió d'alertes

3.4.1 Plataforma de monitorització

El CSI disposa actualment d'una plataforma de monitorització centralitzada basada en **Centreon**, mitjançant la qual es supervisen la totalitat dels sistemes i serveis en abast dels quatre lots objecte de la present licitació. Aquesta plataforma cobreix la monitorització d'infraestructura de servidors, sistemes operatius, serveis de xarxa i processos i serveis, i constitueix l'eina de referència per a la detecció d'alertes i la gestió proactiva del servei.

No obstant això, la instal·lació actual de Centreon es troba en una **versió obsoleta**, sense suport actiu del fabricant, amb limitacions funcionals rellevants per a les necessitats operatives actuals i amb un deute tècnic acumulat que compromet la fiabilitat i l'escalabilitat de la plataforma. Per aquest motiu, la renovació o substitució de la plataforma de monitorització és una de les necessitats identificades en el marc d'aquesta licitació.

Abast de la monitorització requerida

Amb independència de la solució tècnica proposada, la plataforma de monitorització ha de cobrir la totalitat dels sistemes monitoritzats a l'actualitat, incloent-hi com a mínim:

- Disponibilitat i rendiment de servidors físics i virtuals (CPU, memòria, disc, xarxa).
- Estat dels sistemes operatius (serveis del sistema, processos crítics, espai en disc, logs d'error).
- Infraestructura de xarxa associada als sistemes en abast (latència, pèrdua de paquets, estat d'interfícies).
- Sistemes d'emmagatzematge (ocupació, rendiment I/O, estat de les unitats).
- Disponibilitat de serveis i endpoints aplicatius.
- Estat d'execució de processos batch i planificació de tasques, amb alertes davant de jobs fallits, retardats o amb comportament anòmal.
- Monitorització específica de les plataformes tecnològiques dels lots 2, 3 i 4 (CommVault, SAP i Citrix/NetScaler), detallada en els capítols corresponents.

Opcions de proposta tècnica

L'adjudicatari haurà de presentar en la seva oferta una proposta tècnica justificada per a la plataforma de monitorització, optant per una de les dues alternatives següents:

Opció A - Manteniment i actualització de Centreon

L'adjudicatari proposa mantenir Centreon com a plataforma de monitorització, executant una actualització integral que la posi al dia respecte a la versió suportada actual pel fabricant. En aquest cas, l'oferta ha d'incloure obligatòriament:

- Pla d'actualització detallat amb fases, terminis i riscos identificats.
- Versió objectiu proposada i roadmap d'actualitzacions futures.
- Justificació tècnica de la idoneïtat de Centreon per cobrir tots els requisits de monitorització del present contracte.
- Relació de les millores funcionals que s'obtindran respecte a la situació actual.

Opció B - Substitució per una nova plataforma de monitorització

L'adjudicatari proposa substituir Centreon per una plataforma de monitorització alternativa. En aquest cas, l'oferta ha d'incloure obligatòriament:

- Identificació i descripció de la nova plataforma proposada.
- Justificació tècnica i comparativa respecte a Centreon, demostrant que la nova solució cobreix la totalitat dels requisits definits en el present apartat.
- Pla de migració detallat que garanteixi la continuïtat del servei de monitorització durant el procés de transició, sense degradació de la cobertura ni dels temps de detecció d'alertes.
- Inventari de checks i configuracions actuals de Centreon que hauran de ser migrats a la nova plataforma.
- Acreditació de l'experiència de l'adjudicatari en la implantació i gestió de la plataforma proposada.
- Aquesta solució podrà ser onprem, com la plataforma actual, o al cloud gestionat per l'adjudicatari.

Requeriments tècnics comuns a ambdues opcions

Amb independència de l'opció escollida, la plataforma resultant ha de complir els requisits tècnics mínims següents:

Requisit	Descripció
Alerting automatitzat	Generació automàtica d'alertes amb classificació per severitat i notificació als canals definits (correu, missatgeria corporativa i/o integració amb l'eina de tiqueting).
Correlació d'esdeveniments	Capacitat per correlacionar múltiples alertes i reduir el soroll operatiu, identificant l'alerta arrel.
Retenció de mètriques	Les mètriques de rendiment han de retenir-se un mínim de **12 mesos** per permetre l'anàlisi de tendències i la gestió de la capacitat.
Panells en temps real	Disponibilitat de *dashboards* operatius accessibles per al CSI sense intermediació de l'adjudicatari.

Integració amb tiqueting	Creació automàtica de tiquets en l'eina de gestió de serveis davant d'alertes de severitat definida.
Escalabilitat	La plataforma ha de ser capaç d'incorporar nous sistemes sense degradació del servei de monitorització.
Alta disponibilitat	La pròpia infraestructura de monitorització ha de disposar de redundància suficient per evitar punts únics de fallada.
Accés per part del CSI	El CSI ha de disposar en tot moment d'accés en mode consulta a la plataforma, sense restriccions ni necessitat de mediació.
Propietat de les dades	Tota la configuració, checks, mètriques i historial d'alertes són propietat del CSI i han de poder exportar-se en formats estàndard en qualsevol moment.

Terminis d'implantació

Independentment de l'opció escollida, l'adjudicatari ha de garantir que la plataforma de monitorització es troba **operativa i amb cobertura equivalent o superior a l'actual** abans de la finalització del període de transició, tal com es defineix al capítol 7 del present document. Durant el procés d'actualització o migració, no es podrà produir en cap cas una reducció de la cobertura de monitorització existent.

3.4.2 Gestió d'alertes

La gestió d'alertes constitueix un element crític del servei d'operacions, ja que representa el mecanisme principal de detecció proactiva d'anomalies i el punt de partida del procés d'atenció i resolució d'incidències. L'adjudicatari ha de disposar d'un procediment formal i documentat de gestió d'alertes que garanteixi que cap alerta generada per la plataforma de monitorització quedi sense atenció, classificació i resposta en els terminis establerts.

El model de gestió d'alertes ha de basar-se en els principis següents:

- Cobertura total: Totes les alertes generades per la plataforma de monitorització han de ser ateses, independentment de l'hora, el dia o el nivell de criticitat. L'existència d'un volum elevat d'alertes no pot ser al·legada com a causa de manca d'atenció sobre alertes individuals.
- Temps de resposta garantit: Cada nivell de severitat d'alerta té associat un temps màxim de resposta que l'adjudicatari ha de respectar i que serà mesurat de manera automatitzada a partir dels registres de la plataforma de monitorització i de l'eina de tiqueting.
- Reducció del soroll: L'adjudicatari ha de treballar activament per reduir el volum d'alertes falses o de baixa utilitat, mantenint la plataforma de monitorització ajustada i evitant la dessensibilització de l'equip d'operacions davant d'alertes recurrents sense impacte real.

- Millora contínua: L'adjudicatari ha de revisar periòdicament el catàleg d'alertes, proposen ajustos de llindars, noves cobertures i eliminació d'alertes obsoletes, i presentar aquestes propostes en els comitès de seguiment operatiu.

Classificació de les alertes per severitat

Severitat	Definició	Temps de resposta	Acció requerida
Crític	Fallada o degradació greu d'un sistema o servei amb impacte directe sobre la disponibilitat o el rendiment dels serveis assistencials.	10 minuts	Obertura de tiquet prioritat crítica. Notificació immediata al tècnic de guàrdia i al CSI. Inici de diagnosi sense demora.
Alt	Situació anòmala amb potencial d'evolucionar cap a una fallada crítica si no s'atén, o amb impacte limitat sobre el servei.	30 minuts	Obertura automàtica de tiquet prioritat alta. Notificació al tècnic responsable. Inici de diagnosi i aplicació de mesures preventives.
Mitjà	Degradació lleu o avís de tendència negativa que no impacta de manera immediata sobre el servei però que requereix atenció.	4 hores	Obertura de tiquet. Anàlisi i planificació d'accions correctores dins de l'horari operatiu habitual.
Baix / Informatiu	Avís de caràcter informatiu o alerta de llindar preventiu que no requereix actuació immediata.	8 hores	Registre i revisió durant la jornada operativa. Agrupació en informes periòdics d'estat.

Procediment de gestió d'alertes

El flux de gestió d'alertes ha de seguir el procediment següent per a totes les alertes de severitat Crític i Alt, i de manera simplificada per a les de severitat Mitjà i Baix:

<u>Detecció i notificació</u>

- La plataforma de monitorització genera l'alerta i la notifica de manera automàtica als canals definits (correu electrònic, missatgeria corporativa, SMS per a alertes crítiques) i als perfils assignats en funció de la severitat i el tipus de sistema afectat.
- Els canals de notificació i els perfils destinataris han de ser configurats i mantinguts actualitzats per l'adjudicatari, i han de reflectir en tot moment l'estructura real de l'equip de guàrdia.
- Per a alertes de severitat Crític, s'ha de garantir una notificació per doble canal (p.ex. correu + SMS o trucada automàtica) per assegurar la recepció per part del tècnic de guàrdia.

Acusament de recepció (acknowledgement)

- El tècnic receptor ha d'acusar recepció de l'alerta en la plataforma de monitorització dins del temps de resposta establert per a cada severitat, registrant la seva identitat i l'hora d'acusament.
- L'acusament de recepció implica la responsabilitat explícita del tècnic sobre el seguiment i la resolució de l'alerta o la seva escalat si no és de la seva competència.

Diagnosi inicial i correlació

- El tècnic ha de realitzar una diagnosi inicial per determinar la naturalesa i l'abast de l'alerta, incloent-hi la correlació amb altres alertes actives per identificar si es tracta d'una alerta arrel o d'un símptoma secundari d'un problema de major abast.
- En cas que la correlació indiqui que múltiples alertes responen a una mateixa causa, s'ha de gestionar com una única incidència agrupada, evitant la duplicació de tiquets i esforços.

Obertura de tiquet i classificació

- Tota alerta de severitat Crític, Alt o Mitjà ha de generar un tiquet en l'eina de gestió de serveis, amb la prioritat corresponent i amb la informació tècnica inicial disponible.
- Per a alertes de severitat Baix o Informatiu, el registre pot ser agrupat en un tiquet diari o setmanal de seguiment, sempre que no evidenciïn una tendència negativa que requereixi atenció individualitzada.
- Idealment, la creació del tiquet ha serà automàtica per a alertes de severitat Crític i Alt, sense dependència de l'acció manual del tècnic.

Resolució o escalat

- El tècnic ha d'aplicar el procediment documentat corresponent al tipus d'alerta (*runbook*) per intentar la resolució en el menor temps possible.
- En cas que la resolució no sigui possible en el temps establert o requereixi intervenció de N3, s'ha de procedir a l'escalat formal d'acord amb el procediment definit al punt 2.3.2 del present document.
- Si l'alerta deriva en una incidència que no pot ser resolta de manera immediata, s'ha d'aplicar un *workaround* que restableixi el servei mentre es treballa en la solució definitiva, documentant-lo en el tiquet corresponent.

Tancament i documentació

- Una alerta es considera tancada quan la condició que la va originar ha desaparegut de manera verificada i el servei afectat ha recuperat el seu funcionament normal.
- El tancament ha de quedar registrat en la plataforma de monitorització i en el tiquet associat, incloent-hi la causa identificada i les accions realitzades.
- Per a alertes crítiques, el tancament ha de ser notificat explícitament al CSI, indicant la causa, la durada de l'afectació i les mesures preventives adoptades.

Revisió i optimització de les alertes

L'adjudicatari ha de dur a terme una revisió periòdica del catàleg d'alertes per garantir la seva eficàcia i rellevància. Aquesta revisió ha de tenir una periodicitat mínima trimestral i ha d'incloure:

- Anàlisi del volum d'alertes per tipus, severitat i sistema, identificant les alertes de major freqüència i menor valor operatiu.
- Proposta d'ajustos de llindars per reduir falsos positius sense comprometre la detecció real d'anomalies.
- Identificació de mancances de cobertura i proposta de nous checks de monitorització.
- Revisió de les alertes marcades com a acknowledged de manera recurrent sense derivar en accions correctores, que poden ser indicatives d'un problema crònic no resolt o d'un llindar mal configurat.

Els resultats d'aquesta revisió han de ser presentats al CSI en el marc del comitè de seguiment trimestral, i les propostes d'ajust han de ser aprovades pel CSI abans de la seva implantació.

3.5 Requeriments funcionals del servei de nivell 2

3.5.1 Àmbit de resolució N2

L'equip N2 és responsable de la resolució de les incidències operatives habituals sobre els sistemes en abast. A títol orientatiu, i sense caràcter limitatiu, l'àmbit de resolució N2 inclou:

Àmbit	Exemples d'incidències N2
Sistemes operatius	Reinici de serveis del sistema, gestió de processos descontrolats, alliberament d'espai en disc, anàlisi de logs d'error, recuperació d'accessos locals bloquejats.
Disponibilitat de serveis	Reinici de serveis i aplicacions caigudes, verificació i recuperació de serveis de xarxa, comprovació i restabliment de connectivitat entre sistemes.
Rendiment	Identificació i actuació sobre processos que consumeixen recursos de manera anòmala, aplicació de mesures pal·liatives davant de saturació de CPU, memòria o disc.

Emmagatzematge	Ampliació de volums, gestió d'alertes d'ocupació, verificació de l'estat de les unitats i escalat davant de fallades de maquinari.
Backup	Verificació de l'execució dels jobs de backup, gestió d'alertes de fallada i coordinació amb el Lot 2 per a la resolució d'incidències en la plataforma CommVault.
Accessos i autenticació	Resolució d'incidències d'accés a sistemes, interns o proveïdors, en coordinació amb els equips de seguretat del CSI, desbloqueig de comptes de servei.

3.5.2 Procés de gestió d'incidències

Recepció i verificació

Les incidències arriben al N2 per dues vies principals: escalat manual a partir d'alertes observades a la plataforma de monitorització o escalat manual des del N1 a través de l'eina de tiqueting. En qualsevol cas, el tècnic N2 ha de verificar que la incidència no és un duplicat d'una altra en curs i ha de confirmar la prioritat assignada, ajustant-la si la diagnosi inicial revela un impacte diferent.

Diagnosi i resolució

El tècnic N2 ha d'iniciar la diagnosi aplicant en primer lloc els runbooks operatius disponibles. Si la incidència no correspon a cap patró documentat o el runbook no resulta efectiu, ha de documentar les accions realitzades i els resultats obtinguts per facilitar la continuïtat per part d'altres tècnics o del nivell N3.

El tiquet ha de mantenir-se actualitzat amb el progrés de la resolució amb la freqüència mínima següent:

Prioritat	Freqüència mínima d'actualització
Crític	30' o canvi rellevant a l'estat
Alt	2h o canvi rellevant a l'estat
Mig	4h o canvi rellevant a l'estat
Baix	Canvi rellevant

Aplicació de workarounds

Quan la resolució definitiva no sigui possible dins dels temps establerts, el tècnic N2 ha d'aplicar un workaround que permeti restablir el servei de manera temporal, documentant-lo en el tiquet i obrint si escau un registre de problema per a la recerca de la solució definitiva. L'aplicació d'un workaround no implica el tancament de la incidència.

Escalat a N3

L'escalat d'una incidència del N2 al N3 ha de produir-se quan concorri alguna de les circumstàncies següents:

- La resolució requereix actuacions d'administració avançada que excedeixen l'àmbit de competència del N2.

- S'ha superat el 50% del temps de resolució establert sense haver resolt la incidència ni aplicat un workaround efectiu.
- La diagnosi indica que la causa arrel pot tenir un impacte més ampli que requereix una anàlisi aprofundida de nivell N3.
- El tècnic N2 ha esgotat els procediments documentats disponibles sense obtenir resultats.

Tota escalat ha de realitzar-se amb el traspàs complet de la informació recollida durant la diagnosi N2. El tècnic N2 roman com a responsable del tiquet fins al seu tancament, fent el seguiment de la resolució per part del N3 i actuant com a punt de contacte amb el CSI durant tot el procés.

Coordinació amb els adjudicataris d'altres lots i serveis gestionats N3

L'equip N2 del Lot 1 actua com a punt de coordinació operativa en els casos en què una incidència afecti sistemes o serveis que depenen de capes tecnològiques gestionades per lots i serveis diferents. En cas d'incidència que afecti la infraestructura de base gestionada pel Lot 1 i les plataformes superiors gestionades per altres serveis, l'adjudicatari del Lot 1 ha d'actuar com a coordinador tècnic de la resolució. Les incidències de coordinació entre lots han de quedar registrades en un tiquet únic, amb la participació documentada de cada lot implicat.

3.5.3 Gestió de peticions de servei

L'equip N2 és responsable de l'execució de les peticions de servei assignades al Lot 1, d'acord amb el catàleg de serveis definit i mantingut per l'adjudicatari en coordinació amb el CSI. Totes les peticions han de ser gestionades a través de l'eina de tiqueting corporativa, respectant els temps d'execució definits per a cada tipologia.

L'adjudicatari ha de mantenir el catàleg de peticions de servei actualitzat, incloent per a cada petició la descripció, la informació requerida per a la seva tramitació, el temps d'execució estàndard i els fluxos d'aprovació aplicables. Qualsevol nova tipologia de petició ha de ser proposada al CSI per a la seva validació abans d'incorporar-se al catàleg.

3.5.4 Gestió de tasques de sistemes

Descripció del model

El servei N2 incorpora un àmbit de treball específic per a l'execució de tasques de sistemes, un model operatiu que permet al CSI integrar el treball tècnic derivat de projectes TI en el flux operatiu de l'equip d'operacions, sense que aquest formi part dels processos de gestió de projectes ni assumeixi responsabilitats de cap de projecte o anàlisi funcional.

El model funciona de la manera següent:

- Els projectes TI del CSI generen tasques tècniques sobre els sistemes en abast que per la seva naturalesa poden ser executades per l'equip N2 sense requerir coneixement del context global del projecte.

- Aquestes tasques són atomitzades prèviament pels integrats dels equips de projecte, és a dir, descompostes en unitats de treball mínimes, autònomes i completament documentades, fins a un nivell de granularitat equivalent al d'una petició de servei estàndard.
- Un cop atomitzades, les tasques es registren en l'eina de tiqueting com a tasques de sistemes pendents d'aprovació
- Setmanalment es reuneix l'equip dels projectes amb el responsable tècnic del servei per aprovar les tasques que es consideren que poden entrar en el següent període i s'assignen a l'equip N2 per a la seva execució planificada, habitualment amb una periodicitat setmanal.
- L'equip N2 executa la tasca tal com està documentada i reporta el resultat, sense necessitat de participar en reunions de projecte ni de conèixer les dependències o l'estat global de la iniciativa de la qual deriva.

Cicle de vida d'una tasca de sistemes

1. Definició: El responsable de la tasca de projecte descompon les tasques tècniques en unitats d'execució autònomes. Cada tasca resultant ha de ser autocontinguda i executable sense dependència d'informació externa no inclosa en la seva pròpia documentació.
2. Documentació i registre: Cada tasca de sistemes ha de quedar registrada en l'eina de tiqueting amb el tipus Tasca de sistemes, que ha d'incloure com a mínim:
    - Descripció detallada de la tasca.
    - Sistemes afectats i credencials o accessos necessaris.
    - Procediment d'execució pas a pas o enllaç a la documentació depenent.
    - Criteri d'èxit i validació post-execució.
    - Pla de marxa enrere en cas d'error durant l'execució.
    - Finestra d'execució prevista i dependències amb altres tasques, si n'hi ha.
    - Responsable de la validació del resultat.
3. Planificació setmanal: Les tasques de sistemes preparades s'incorporen a la cua de tasques de sistemes de l'equip N2, que es revisa i consensua amb el CSI amb periodicitat setmanal. La planificació ha de tenir en compte la càrrega operativa de l'equip, garantint que l'execució de tasques de projecte no compromet la capacitat de resposta davant d'incidències.
4. Execució i registre: El tècnic N2 executa la tasca d'acord amb el procediment documentat, registrant en el tiquet el resultat de cada pas i qualsevol desviació respecte al procediment previst. En cas que durant l'execució es detecti qualsevol circumstància no prevista que pugui comprometre el resultat o la seguretat dels sistemes, el tècnic ha d'aturar l'execució i notificar-ho al responsable de la tasca de projecte abans de continuar.
5. Validació i tancament: El tancament del tiquet requereix la confirmació explícita de la persona designada com a responsable de validació en la documentació de la tasca.

Gestió de la càrrega i prioritats

La coexistència de les tasques de sistemes amb la càrrega operativa habitual ha de gestionar-se sota els criteris següents:

- L'atenció a incidències té prioritat absoluta sobre l'execució de qualsevol tasca de sistemes planificada, sense excepció.
- Les tasques de sistemes s'han d'executar preferentment durant les franges horàries de menor activitat d'incidències, d'acord amb els patrons de càrrega operativa identificats.
- En cas que durant l'execució d'una tasca es produeixi una incidència que requereixi l'atenció del tècnic assignat, la tasca ha de ser suspesa de manera ordenada i represa posteriorment, documentant en el tiquet l'estat en el qual ha quedat l'execució.
- Si el volum de tasques de sistemes en un període determinat és susceptible de comprometre la capacitat operativa de l'equip N2, l'adjudicatari ho ha de comunicar proactivament al CSI per tal de replanificar les tasques o revisar el dimensionament del servei.
- Setmanalment a la reunió de planificació es traslladarà al CSI l'estat de les tasques planificades, indicant les executades, les pendents i qualsevol desviació respecte a la planificació, amb la seva justificació.

3.6 Requeriments funcionals del servei de nivell 3

3.6.1 Descripció i abast del servei N3

El servei d'Administració de Sistemes de Nivell 3 (N3) constitueix el nivell d'expertesa tècnica màxima del Lot 1, i té com a objecte principal la resolució de les incidències i peticions de servei que, per la seva complexitat tècnica, excedeixen la capacitat de resolució de l'equip d'operacions de Nivell 2 (N2).

El servei N3 actua, per tant, com a receptor de les escalades del N2, assumint la resolució de les situacions que requereixen un coneixement avançat de les plataformes i tecnologies en abast. La relació entre ambdós nivells ha de caracteritzar-se per la màxima integració i fluïdesa operativa: l'escalat d'una incidència o petició al N3 no ha de representar en cap cas una demora en la seva resolució ni una pèrdua de coneixement sobre l'estat de la situació per part del CSI. Des de la perspectiva del CSI, els nivells N2 i N3 han de comportar-se com un únic equip integrat, amb una interlocució única i una traçabilitat completa i ininterrompuda al llarg de tot el cicle de vida de qualsevol incidència o petició, independentment del nivell que en tingui la responsabilitat de resolució en cada moment.

3.6.2 Tecnologies i plataformes en abast del N3

L'abast del servei N3 del present lot es limita a les tecnologies i plataformes següents, sobre les quals l'adjudicatari ha d'acreditar coneixement avançat i capacitat de resolució autònoma:

Sistemes operatius

Tecnologia	Abast
Linux	Administració avançada de les distribucions presents en l'entorn del CSI (Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Ubuntu Server i altres distribucions en ús). Inclou la resolució de problemes complexos de sistema, gestió avançada de processos, diagnosi de rendiment, gestió del kernel, actualització de pegats de seguretat i resolució d'incidències que requereixin intervenció a nivell de sistema operatiu.
Windows Server	Administració avançada de totes les versions de Windows Server en ús al CSI. Inclou la resolució de problemes complexos de sistema, gestió avançada de rols i serveis, diagnosi de rendiment, actualització de pegats i resolució d'incidències que requereixin intervenció a nivell de sistema operatiu.

Bases de dades

Tecnologia	Abast
SQL Server	Administració avançada de les instàncies SQL Server en abast del Lot 1. Inclou la resolució d'incidències complexes de motor de base de dades, optimització de consultes i rendiment, gestió d'alta disponibilitat (Always On, mirroring), tasques de manteniment, actualització de pegats i administració de backups i recuperació, i gestió de la seguretat a nivell de base de dades.
PostgreSQL	Administració avançada de les instàncies PostgreSQL en abast del Lot 1. Inclou la resolució d'incidències complexes, optimització del rendiment, gestió de la replicació, tasques de manteniment, actualització de pegats i administració de backups i recuperació, i gestió de la seguretat.

Programari de base i serveis de directori

Tecnologia	Abast
Active directory	Administració avançada del servei de directori corporatiu. Inclou la resolució d'incidències complexes de replicació, gestió de la topologia de sites i serveis, administració avançada de GPOs, diagnosi de problemes d'autenticació i autorització, i gestió del cicle de vida dels controladors de domini.
DNS	Administració avançada del servei DNS corporatiu. Inclou la resolució d'incidències complexes de resolució de noms, gestió de zones i registres, i diagnosi de problemes de resolució.
DHCP	Administració avançada del servei DHCP corporatiu. Inclou la gestió d'àmbits i reserves, resolució d'incidències complexes d'assignació d'adreces i coordinació amb l'equip de xarxa (gestionat per un servei N3 independent).
Exchange	Administració avançada de la plataforma de correu Exchange on-premises hibridat amb M365. Inclou la resolució

	d'incidències complexes de flux de correu, gestió de bases de dades de bústies, administració de connectors i polítiques de transport, actualització de pegats i diagnosi de problemes de rendiment i disponibilitat.
WSUS	Administració de la plataforma de gestió d'actualitzacions Windows Server Update Services. Inclou la gestió de l'aprovació i distribució de pedaços, la resolució d'incidències de sincronització i distribució, i la coordinació amb el pla de pegats definit al present document.

SaaS

Tecnologia	Abast
M365	Administració avançada dels serveis Microsoft 365 en ús al CSI. Inclou la resolució d'incidències complexes de servei, gestió avançada de llicències i usuaris, administració de polítiques de seguretat i compliment, i coordinació amb el suport de Microsoft quan la resolució requereixi intervenció del fabricant.

Plataforma de monitorització

Tecnologia	Abast
Plataforma de monitorització	Administració, manteniment i evolució de la plataforma de monitorització centralitzada en abast del Lot 1, ja sigui Centreon actualitzat o la nova plataforma proposada per l'adjudicatari d'acord amb el que s'estableix al punt 3.4.1. Inclou la gestió de la configuració de la plataforma, la incorporació de nous sistemes i checks, l'actualització de versions i la resolució d'incidències sobre la pròpia eina de monitorització.

3.6.3 Serveis exclosos de l'abast del N3 d'aquest lot

El CSI disposa de serveis gestionats de Nivell 3 independents per a les plataformes i àmbits tecnològics següents, els quals queden expressament exclosos de l'abast del servei N3 del present lot:

Àmbit	Observacions
Networking	Disposarà de servei N3 gestionat independent. L'adjudicatari del Lot 1 ha de coordinar-se amb aquest servei quan les incidències o peticions tinguin dependències amb la capa de xarxa, però no assumirà cap responsabilitat de resolució sobre aquesta plataforma.
Ciberseguretat	Disposarà de servei N3 gestionat independent. L'adjudicatari del Lot 1 ha de col·laborar amb l'equip de ciberseguretat en els termes definits al punt 2.6 del present document, però no assumirà responsabilitats pròpies d'aquest àmbit.
SAP	Cobert íntegrament pel Lot 3 del present expedient.

Citrix / Netscaler	Cobert íntegrament pel Lot 4 del present expedient.
Telefonia IP	Disposarà de servei N3 gestionat independent. Queda fora de l'abast N3 del present lot.
Virtualització / Hipervisor	Disposarà de servei N3 gestionat independent. Queda fora de l'abast N3 del present lot.

L'adjudicatari del Lot 1 ha d'establir mecanismes de coordinació formals amb els equips N3 responsables dels àmbits exclosos, per garantir una resposta conjunta àgil en les situacions en què una incidència o petició tingui dependències entre la infraestructura de base gestionada per aquest lot i qualsevol de les plataformes excloses.

3.6.4 Model d'escalat N2 - N3

Principis del model d'escalat

La frontera operativa entre el N2 i el N3 ha de ser, en la mesura del possible, invisible per al CSI. L'escalat d'una incidència o petició al N3 no ha de comportar en cap cas una demora en la resposta ni una pèrdua de context o de coneixement sobre la situació per part del CSI. L'adjudicatari ha de garantir que, independentment del nivell intern que tingui la responsabilitat de resolució en cada moment, el CSI disposa en tot moment d'una interlocució única, consistent i actualitzada sobre l'estat de qualsevol incidència o petició.

A aquests efectes, l'adjudicatari ha d'establir mecanismes interns que garanteixin:

- La transferència completa del context en el moment de l'escalat, de manera que el tècnic N3 receptor disposi de tota la informació recollida durant la diagnosi N2 i no hagi de repetir passos ni sol·licitar al CSI informació ja proporcionada.
- La continuïtat de la comunicació amb el CSI sense interrupcions durant el procés d'escalat, de manera que el canvi de nivell intern no sigui perceptible des de l'exterior.
- La traçabilitat íntegra de totes les accions realitzades per ambdós nivells en el mateix tiquet, sense fragmentació de la informació entre sistemes o registres diferents.

Criteris d'escalat al N3

L'escalat d'una incidència o petició del N2 al N3 ha de produir-se quan concorri alguna de les circumstàncies següents:

- La resolució requereix coneixement avançat o privilegis d'accés sobre alguna de les tecnologies definides al punt 3.3 que excedeixen l'àmbit de competència de l'equip N2.
- S'ha superat el 50% del temps de resolució establert per a la prioritat de la incidència sense haver-la resolt ni aplicat un workaround efectiu.

- La diagnosi inicial indica que la causa probable de la incidència requereix una investigació de profunditat que excedeix la capacitat operativa del N2.
- El tècnic N2 ha esgotat els procediments documentats disponibles sense obtenir resultats satisfactoris.

Responsabilitat del tiquet durant l'escalat

Durant el procés d'escalat, la responsabilitat formal del tiquet roman en el tècnic N2 que va iniciar l'escalat, qui actua com a punt de contacte principal amb el CSI i vetlla per la correcta actualització del tiquet i la comunicació de l'estat al CSI. El tècnic N3 assumeix la responsabilitat tècnica de la resolució però no es converteix en l'interlocutor principal amb el CSI, tret que la naturalesa tècnica de la incidència requereixi una comunicació directa i especialitzada que així ho justifiqui.

3.6.5 Suport a tasques derivades de projectes

El servei N3 del present lot no proporciona suport directe a projectes TI del CSI. La gestió i l'execució dels projectes TI es realitza a través dels proveïdors contractats específicament per a cada iniciativa, que disposen del coneixement funcional i tècnic necessari per a la seva execució.

No obstant això, en el context del model de tasques de sistemes descrit al punt 3, pot donar-se la circumstància que una tasca derivada d'un projecte, un cop atomitzada i assignada a l'equip N2 per a la seva execució, reveli durant la seva execució una complexitat tècnica que excedeixi el coneixement de l'equip N2 sobre alguna de les tecnologies en abast del N3. En aquest cas, la tasca podrà ser escalat al N3 seguint el mateix circuit d'escalat definit al punt 3.6.4, amb les particularitats següents:

- L'escalat ha de ser avaluada i autoritzada pel Responsable Tècnic del Lot abans de la seva formalització, per garantir que la complexitat tècnica justifica la intervenció del N3 i no respon a una manca de documentació o atomització adequada de la tasca.
- En cas que l'escalat reveli que la tasca no ha estat suficientment atomitzada o documentada per a la seva execució en N2, el Responsable Tècnic del Lot ho ha de comunicar al responsable de la tasca del projecte perquè procedeixi a la seva redefinició, sense que l'equip N3 hagi d'assumir el coneixement contextual del projecte.
- En cap cas el servei N3 no assumirà tasques de disseny, arquitectura o gestió de projectes que corresponguin al proveïdor de projectes contractat.

3.7 Perfils professionals

3.7.1 Consideracions generals

L'adjudicatari ha de disposar d'un equip humà suficientment dimensionat per garantir la prestació del servei en les condicions establertes en el present document, cobrint la totalitat de les franges horàries requerides, les tecnologies en abast i les modalitats de presència física i remota definides al punt 3.1.

El dimensionament de l'equip és responsabilitat de l'adjudicatari, qui ha de justificar en la seva oferta que el nombre de persones i els perfils proposats són adequats per absorbir la càrrega operativa de referència, garantir els temps de resposta i resolució establerts i mantenir la qualitat del servei durant tot el període contractual, incloent-hi les situacions de vacances, baixes i absències del personal.

Els perfils definits en el present apartat constitueixen els requisits mínims que l'adjudicatari ha de cobrir. L'adjudicatari pot proposar en la seva oferta una estructura d'equip ampliada, sempre mantenint els perfils mínims exigits i que justifiqui adequadament el compliment de tots els requisits del servei descrits.

En cap cas el CSI assumirà responsabilitat sobre el dimensionament de l'equip proposat per l'adjudicatari. Un dimensionament insuficient que resulti en incompliments de servei serà responsabilitat exclusiva de l'adjudicatari i no podrà ser al·legat com a causa de força major ni com a justificació de desviacions en els KPIs i SLAs contractuals.

3.7.2 Perfils requerits

Responsable del servei (Service Manager)

Atribut	Descripció
Funció	Interlocutor estratègic de l'adjudicatari davant del CSI. Responsable global del compliment contractual, la qualitat del servei i la relació amb la direcció TI del CSI.
Dedicació	Parcial. Ha d'estar disponible per al CSI en horari laborable i ser localitzable fora d'aquest horari per a situacions d'escalat de direcció.
Dependència	Pot ser un perfil compartit amb altres contractes de l'adjudicatari, sempre que es garanteixi la dedicació i la disponibilitat requerides.
Experiència Mínima	Mínim 5 anys d'experiència en gestió de serveis TI gestionats de complexitat similar.
Certificacions Requerides	ISO20000 o ITIL Managing Professional o ITIL Foundation amb experiència demostrable equivalent
Certificacions Valorades	PMP, PRINCE2 o equivalent en gestió de projectes i serveis

Responsable tècnic del lot

Atribut	Descripció
Funció	Interlocutor tècnic principal de l'adjudicatari davant del CSI per al Lot 1. Responsable de la coordinació de l'equip tècnic, el compliment dels KPIs del lot i la supervisió de la qualitat operativa. Participa en els comitès de seguiment operatius i actua com a responsable de l'escalat tècnica interna.

Dedicació	Dedicació exclusiva al present contracte. Ha d'estar disponible en horari laborable i ser localitzable fora d'aquest per a situacions d'escalat tècnica d'alt impacte.
Dependència	No pot ser un perfil compartit amb altres contractes.
Experiència Mínima	Mínim 5 anys d'experiència en administració de sistemes i gestió de serveis TI gestionats, dels quals almenys 2 anys en rol de responsabilitat tècnica d'equip.
Certificacions Requerides	ISO20000 o ITIL Foundation i certificació tècnica avançada en almenys dues de les tecnologies principals en abast del lot.
Coneixements tècnics	Coneixement avançat de la totalitat de les tecnologies en abast del lot. Capacitat per donar suport tècnic als equips N2 i N3 en situacions complexes

Tècnic d'operacions N2

Atribut	**Descripció**
Funció	Operació diària dels sistemes en abast: gestió d'alertes, atenció i resolució d'incidències de segon nivell, execució de peticions de servei, supervisió de processos batch i execució de tasques de sistemes planificades.
Dedicació	Dedicació al present contracte. L'adjudicatari ha de dimensionar el nombre de tècnics N2 necessaris per garantir la cobertura 24x7 i la presència física mínima establerta al punt 3.1, tenint en compte els torns, les guàrdies i les cobertures per absències.
Experiència Mínima	Mínim 1 any d'experiència en operació de sistemes TI en entorns de complexitat similar.
Certificacions Requerides	ISO2000 o ITIL Foundation. Coneixement funcional de les tecnologies en abast del lot adequat al nivell N2.
Coneixements tècnics	Sistemes operatius Linux i Windows Server a nivell operatiu. Coneixement funcional dels serveis de directori, DNS, DHCP i WSUS. Gestió d'alertes en plataformes de monitorització. Ús de plataformes de tiqueting ITSM.

Administrador N3

Atribut	**Descripció**
Funció	Resolució de les incidències i peticions escalades des del N2 sobre les tecnologies requerides a l'abast del present lot.

Dedicació	Dedicació al present contracte. Fora de l'horari estès, en modalitat de guàrdia localitzable per a la cobertura de les escalades crítiques.
Experiència Mínima	Mínim 4 anys d'experiència en administració avançada de sistemes TI.
Certificacions Requerides	Dintre del pool d'administradors s'han de cobrir les certificacions: Certificació avançada en sistemes operatius Linux (RHCE o equivalent) i/o Windows Server (AZ-800 o equivalent). Certificació oficial Microsoft en Active Directory i serveis associats (AZ-800 o equivalent vigent). Certificació oficial Microsoft en Exchange i/o Microsoft 365 (MS-203, MS-102 o equivalent vigent). Certificació oficial Microsoft en SQL Server (DP-300 o equivalent vigent). Acreditació d'experiència avançada en PostgreSQL mitjançant referències o certificació equivalent reconeguda.

3.7.3 Compatibilitat de perfils

L'adjudicatari pot proposar en la seva oferta una estructura en la qual un mateix tècnic cobreixi més d'un dels perfils N3 definits als apartats anteriors, sempre que pugui acreditar el nivell de coneixement i les certificacions requerides per a cadascun dels perfils que es proposa combinar, i que el dimensionament global de l'equip garanteixi els temps de resposta i cobertura establerts sense degradació de la qualitat del servei.

En cap cas un mateix tècnic podrà combinar la funció de Responsable Tècnic del Lot (Perfil 2) amb la de tècnic N2 (Perfil 3) ni amb cap dels perfils N3 (Perfils 4, 5 i 6) en el mateix torn de cobertura, per garantir la disponibilitat del Responsable Tècnic per a les funcions de coordinació i interlocució amb el CSI.

3.7.4 Estabilitat i canvis en l'equip assignat

La qualitat del servei depèn en gran mesura de l'estabilitat de l'equip assignat i del coneixement acumulat sobre l'entorn del CSI. Per aquest motiu, s'estableixen les condicions següents respecte als canvis en el personal assignat al contracte:

- Qualsevol substitució dels perfils Service Manager i/o Responsable Tècnic del Lot ha de ser comunicada al CSI amb un mínim de 30 dies naturals d'antelació, aportant el perfil del substitut proposat per a la seva validació prèvia. El CSI es reserva el dret de rebutjar un perfil substitut que no compleixi els requisits mínims establerts, sense que això suposi cap cost addicional per al CSI.
- Les substitucions dels perfils tècnics N2 i N3 han de ser comunicades al CSI amb un mínim de 15 dies naturals d'antelació, excepte en casos de força major degudament justificats.
- En tots els casos de substitució, l'adjudicatari ha de garantir un període de solapament entre el tècnic sortint i el tècnic entrant, de durada suficient per garantir la transferència completa del coneixement de l'entorn, sense cost addicional per al CSI.

3.7.5 Formació i actualització de coneixements

L'adjudicatari ha de garantir la formació contínua de l'equip assignat per mantenir el coneixement actualitzat sobre les tecnologies en abast i les bones pràctiques del sector. A aquests efectes:

- Ha de presentar en la seva oferta un pla de formació inicial per al període de transició, que garanteixi que tot el personal assignat disposa del coneixement necessari sobre l'entorn específic del CSI abans de l'inici de la fase operativa.
- Ha de presentar anualment al CSI un pla de formació i certificació per a l'any en curs, incloent-hi les formacions previstes, les certificacions a renovar o obtenir i el personal beneficiari.
- Davant de canvis tecnològics significatius en l'entorn del CSI (actualitzacions de plataformes, incorporació de noves tecnologies, etc.), l'adjudicatari ha de garantir la formació del personal afectat en un termini raonable previ a la posada en marxa dels canvis, sense que el procés de formació pugui afectar la qualitat del servei.

3.8 Pla d'auditoria i manteniment preventiu dels sistemes

L'adjudicatari ha de disposar d'un pla d'auditoria tècnica periòdica que cobreixi la totalitat dels sistemes i tecnologies en abast del Lot 1, orientat a la detecció proactiva de deficiències de configuració, desviacions respecte a les bones pràctiques del sector, mancances de seguretat, oportunitats de millora i necessitats de parxeig no cobertes pel pla de pegats habitual.

Aquest pla constitueix un dels instruments principals de la gestió proactiva del servei i ha de permetre al CSI disposar d'una visió periòdica i estructurada de l'estat real dels seus sistemes, més enllà de la gestió reactiva d'incidències i de les comprovacions operatives diàries.

L'adjudicatari ha de presentar en la seva oferta una proposta detallada del pla d'auditoria, que serà valorada com a criteri tècnic d'adjudicació. El pla ha de reflectir el coneixement de l'adjudicatari sobre les tecnologies en abast i la seva capacitat per aportar valor proactiu al servei, més enllà del compliment dels requisits operatius mínims.

3.8.1 Contingut mínim del pla

El pla d'auditoria proposat per l'adjudicatari ha de cobrir, com a mínim, els àmbits d'anàlisi següents per a cadascuna de les tecnologies en abast:

- Configuració i compliment de bones pràctiques: Verificació que la configuració dels sistemes s'ajusta a les guies de referència del fabricant i a les bones pràctiques reconegudes del sector per a cada tecnologia.
- Seguretat i bastionat: Revisió del compliment de les línies de base de seguretat definides, identificació de configuracions insegures, comptes o permisos excessius, serveis innecessaris actius i qualsevol desviació respecte a la política de seguretat del CSI.

- Pegats i cicle de vida: Verificació de l'estat d'actualització dels sistemes, identificació de pedaços pendents d'aplicar i components propers al seu End of Life o End of Support no recollits en el pla de pegats habitual.
- Proposta de millores en l'arquitectura que permetin fer les actualitzacions en calent sense downtime i garantint l'afectació mínima als serveis corporatius.
- Rendiment i capacitat: Anàlisi de les tendències de consum de recursos, identificació de colls d'ampolla i propostes d'optimització per millorar el rendiment o anticipar necessitats de creixement.
- Resiliència i alta disponibilitat: Revisió de la configuració dels mecanismes de redundància i alta disponibilitat, identificació de punts únics de fallada (single points of failure) i verificació que els procediments de recuperació estan actualitzats i son efectius.
- Documentació i CMDB: Verificació de la coherència entre la configuració real dels sistemes i la documentació tècnica i la CMDB, identificant les desviacions i proposant les actualitzacions necessàries.

3.8.2 Planificació i periodicitat

El pla d'auditoria ha d'organitzar-se en cicles anuals, distribuint les auditories al llarg de l'any per tecnologia de manera que es garanteixi una cobertura completa de tots els sistemes en abast dins de cada cicle. L'adjudicatari ha de proposar en la seva oferta la planificació detallada del cicle anual, indicant per a cada tecnologia la periodicitat proposada i la justificació tècnica de la mateixa.

3.8.3 Informe d'auditoria i plans d'acció

Els resultats de cada auditoria han de quedar documentats en un informe tècnic d'auditoria lliurat al CSI en un termini màxim de 10 dies hàbils des de la finalització de l'auditoria. L'informe ha d'incloure, com a mínim:

- Abast i data de l'auditoria realitzada.
- Metodologia i eines emprades.
- Resum executiu amb la valoració global de l'estat dels sistemes auditats.
- Relació detallada de les trobades (findings), classificades per severitat.
- Pla d'accions correctores: Per a cada trobada de severitat Crítica, Alta i Mitjana, l'informe ha d'incloure una proposta d'acció correctora amb la descripció tècnica de la solució recomanada, l'estimació d'esforç necessari i el termini proposat per a la seva implementació.
- Comparativa amb l'auditoria anterior del mateix àmbit (a partir del segon cicle), indicant les trobades resoltes, les pendents i les noves detectades.

El pla d'accions correctores derivat de cada auditoria ha de ser revisat i aprovat pel CSI, i el seu seguiment ha de ser incorporat a l'ordre del dia del comitè de seguiment operatiu mensual fins a la resolució de la totalitat de les trobades de severitat Crítica i Alta.

3.9 Equipament de treball del personal assignat

L'adjudicatari ha de proporcionar, al seu càrrec, la totalitat dels equips de treball necessaris per al personal assignat a la prestació del servei. Aquesta obligació inclou tots els tècnics assignats al contracte, independentment de la seva modalitat de prestació (presencial o en remot) i del rol que exerceixin.

3.9.1 Equips informàtics

L'adjudicatari ha de dotar cada tècnic assignat al servei d'un equip informàtic portàtil, atès que el model de prestació és híbrid i es requereix que el personal pugui operar amb plena efectivitat tant des de les instal·lacions del CSI com des de la modalitat de treball en remot, sense restriccions derivades de les característiques del maquinari.

Els equips han de complir, com a mínim, els requisits tècnics necessaris per garantir el funcionament fluid de totes les eines de gestió, monitorització, tiqueting i accés remot utilitzades en la prestació del servei. L'adjudicatari és responsable del seu manteniment, actualització i substitució en cas d'avaria, sense que cap d'aquests conceptes pugui afectar la continuïtat del servei.

3.9.2 Dispositiu mòbil per a guàrdies

L'adjudicatari ha de proporcionar un telèfon mòbil corporatiu a cadascun dels tècnics que formin part del pool de guàrdia de Nivell 2. Aquest dispositiu constitueix el canal principal de contacte durant les franges horàries de guàrdia i ha de garantir la localització del tècnic en tot moment durant la seva franja de cobertura. Es requereix un número de telèfon únic per contactar amb el servei de guàrdies, pel que s'haurà d'implementar la funcionalitat de centraleta virtual o equivalent.

L'adjudicatari és responsable de posar a disposició del CSI, en tot moment, els números de contacte actius dels tècnics de guàrdia, i de garantir que aquests dispositius es troben operatius i amb cobertura suficient durant tota la franja horària de guàrdia.

3.9.3 Responsabilitat sobre l'equipament

La propietat, el manteniment i la gestió de la totalitat dels equips descrits en el present apartat recauen exclusivament sobre l'adjudicatari. El CSI no assumeix cap responsabilitat sobre l'equipament de treball del personal de l'adjudicatari, ni en termes de provisió, manteniment, assegurança ni substitució. En cas de finalització del contracte o de canvi de personal assignat, l'adjudicatari ha de garantir que el nou personal disposa de l'equipament necessari des del primer moment de la seva incorporació al servei, sense que el procés de provisió d'equips pugui afectar en cap cas la continuïtat o la qualitat del servei. Els equips s'aprovisionaran amb els requeriments de seguretat i polítiques d'identitat i accés del CSI.

4 Lot 2: Backup as a Service i Disaster Recovery as a Service

4.1 Descripció del servei

4.1.1 Objecte del lot

El Lot 2 té per objecte la prestació d'un servei de backup com a servei compost per dos sub-serveis complementaris i indissociables de protecció de dades:

- **Backup as a Service (BaaS)**: Servei integral de còpia de seguretat mitjançant el qual l'adjudicatari ha d'aportar la seva pròpia solució de protecció de dades - incloent-hi el maquinari, el programari, la infraestructura d'emmagatzematge, les llicències i les eines de gestió necessàries - per donar cobertura de còpia de seguretat a la totalitat dels sistemes i dades en abast, tant en la seva component local com en la component remota de llarga retenció (LTR).
- **Disaster Recovery as a Service (DRaaS)**: Servei de recuperació davant de desastres basat en la replicació de les màquines virtuals designades pel CSI cap a un entorn de virtualització aliè i independent del CSI, totalment preparat per a la seva posada en marxa en cas d'activació del pla de recuperació davant de desastres, amb un RPO màxim de 24 hores i un RTO màxim de 4 hores.

Ambdós sub-serveis han de ser gestionats de manera integrada per l'adjudicatari, compartint consola de gestió i monitorització, i han de garantir en tot moment la integració directa amb la plataforma CommVault Simpana actualment en ús al CSI.

L'adjudicatari és responsable de la implantació, l'operació, el manteniment, l'actualització i l'evolució de la totalitat de la solució durant tota la vigència del contracte. Cap d'aquests conceptes pot representar un cost addicional per al CSI més enllà del que s'estableixi en les condicions econòmiques de l'oferta, a excepció de les ampliacions de capacitat expressament previstes en el present document. En particular, la posada en marxa del servei DRaaS no ha de suposar cap cost addicional per increment de llicenciaments de la plataforma de protecció del CSI.

4.1.2 Abast del servei

La solució ha de suportar la totalitat de les plataformes que CommVault Simpana és capaç de protegir en el moment de l'inici del contracte, així com les tecnologies que pugui suportar en el futur en cas que el CSI realitzi canvis de versió o de plataforma. En aquest cas, l'adjudicatari ha d'assumir dins el servei les instal·lacions i configuracions necessàries per garantir la continuïtat de la protecció, sempre que les noves plataformes restin suportades per CommVault Simpana.

La solució BaaS ha de donar cobertura de còpia de seguretat, com a mínim, als elements següents:

Tipologia	Descripció
Sistemes operatius de servidors virtuals	Còpia de seguretat a nivell de sistema operatiu de la totalitat dels servidors virtuals en abast, garantint la recuperabilitat completa del sistema en cas de fallada.

Servidors de fitxers	Còpia de seguretat de la totalitat dels volums i carpetes compartides dels servidors de fitxers del CSI, amb granularitat de recuperació a nivell de fitxer individual.
Servidors físics	Còpia de seguretat de servidors físics en abast, en entorns mixtos físics i virtuals.
Aplicacions corporatives i bases de dades	Còpia de seguretat consistent de les aplicacions corporatives en abast i les seves bases de dades associades, garantint la integritat de les dades en el moment de la còpia mitjançant els mecanismes d'integració adequats per a cada plataforma (agents, snapshots aplicatius, scripts, VSS, etc.).
Nous serveis	Qualsevol nou servei o sistema que el CSI posi en marxa durant la vigència del contracte ha de ser incorporat a la solució en un termini màxim de 15 dies des de la sol·licitud, sense cost addicional fins als límits de capacitat contractats.

La solució DRaaS ha de cobrir la replicació i la recuperació davant de desastres de les màquines virtuals designades pel CSI, d'acord amb els requisits mínims següents:

Àmbit	**Descripció**
Rèplica de màquines virtuals	Totalitat de les màquines virtuals designades pel CSI com a objecte del pla de recuperació davant de desastres, d'acord amb el llistat que serà definit durant el període de transició i que podrà ser actualitzat durant la vigència del contracte.
Entorn de virtualització de destí	Clúster de virtualització aliè i totalment independent del CSI, prèviament configurat per a la seva integració directa per al punt d'activació de la rèplica. L'entorn pot basar-se en tecnologia d'hipervisor VMware o Nutanix. No es contempla la sobresubscripció de memòria ni de CPU: la plataforma ha d'estar totalment disponible en recursos per al CSI. Capacitat mínima d'emmagatzematge: 10TB + 100TB en repositori (dins o fora de la infraestructura específica) per realitzar proves.
Datacenter destí	El datacenter on s'emmagatzemen les còpies i les rèpliques ha de ser de Tier III i estar certificat segons l'ENS de tipus mitjà
Comunicacions	Totes les comunicacions necessàries per a l'operativitat del servei DRaaS han d'estar configurades i a càrrec de l'adjudicatari, mitjançant una línia de comunicacions dedicada proposada per l'adjudicatari. La transmissió de les dades ha de ser deduplicada, comprimida i xifrada, i no ha d'implicar l'establiment d'una VPN entre el CSI i el datacenter de l'adjudicatari.

4.1.3 Model de prestació i horari

Es requereix durant la durada del contracte, un servei integral d'administració, gestió, explotació i suport davant d'incidències tant en la plataforma existent com en la proposada en paral·lel del propi sistema de còpies de seguretat i dels elements que ho composen (maquinari, comunicacions, programari) per a donar un servei de suport integral a CSI, resoldre consultes d'operació i administració.

Aquest servei s'haurà de donar, com a mínim en horari laboral de 8 a 18h.

Monitorització 24x7x365	Supervisió contínua de l'execució dels jobs de backup i les rèpliques DRaaS, amb generació d'alertes davant de qualsevol fallada o anomalia. Atenció d'incidències crítiques les 24 hores del dia, 7 dies a la setmana, 365 dies l'any.
Servei d'administració i suport	Atenció personalitzada en el centre de gestió del proveïdor de dilluns a divendres en horari de 10 hores. Administració de la plataforma, gestió de polítiques, execució de restauracions, configuració de nous jobs i atenció de peticions de servei.
Suport fora d'horari	Fora de l'horari personalitzat 10x5, l'adjudicatari ha d'oferir el suport necessari per garantir la prestació del servei en les condicions establertes.
Execució del DR	Execució dels procediments de Disaster Recovery en cas que sigui necessari, les 24 hores del dia, 7 dies a la setmana, 365 dies l'any.

L'adjudicatari podrà efectuar les evolucions tecnològiques que consideri necessàries en el conjunt de la solució de còpies de seguretat, si escauen i així ho considera, sempre acordant amb CSI el moment idoni per fer-ho per tal de minimitzar l'impacte.

Les peticions de suport tècnic només podran ser sol·licitades pel personal del Departament TIC del CSI o les persones designades a aquests efectes.

4.2 Inventari i volumetria del servei

La informació recollida en el present apartat descriu la volumetria actual de l'entorn de backup del CSI i constitueix la referència de partida per al dimensionament de la solució per part dels licitadors. Les xifres indicades són caràcter orientatiu, podent existir variacions raonables derivades de l'evolució natural del parc de sistemes durant el procés de licitació. Es preveu un creixement anual aproximat del 10% durant la durada del contracte, que l'adjudicatari ha de considerar en el dimensionament de la seva proposta.

4.2.1 Entorn de backup actual (BaaS)

L'entorn actual de backup del CSI presenta les característiques principals següents:

Plataforma de backup	CommVault Simpana
Dades del frontal de backup	114TB en total

Màquines virtuals	55TB
Filesystems i aplicacions	59TB

La plataforma de backup objecte del nou servei ha d'estar basada en una arquitectura CommVault amb, com a mínim, un CommServe, dos MediaAgents locals i un MediaAgent remot.

4.2.2 Volumetria requerida per al servei BaaS

Concepte	Capacitat requerida
Màquines virtuals a protegir	400VM
Emmagatzematge del repositori principal (CPD CSI)	300TB
Emmagatzematge del repositori secundari (CPD adjudicatari)	450TB

L'emmagatzematge local de 300 TB ha d'estar basat en una cabina amb connexió 10/25 Gb mitjançant tecnologia DAC, amb capacitat per separar la gestió del dispositiu i la presentació dels volums de dades en segments de xarxa diferenciats (VLAN de gestió i VLAN d'emmagatzematge independents). Tota la infraestructura externa ha d'estar en alta disponibilitat dins el datacenter de l'adjudicatari, des de les comunicacions externes fins a l'entorn de processament.

4.2.3 Volumetria requerida per al servei DRaaS

Concepte	Capacitat requerida
Màquines virtuals a replicar	25VM
Emmagatzematge SSD del repositori de l'appliance	10TB
Memoria RAM de l'appliance	512GB
Capacitat de processador	2CPU de 16 nuclis
Emmagatzematge disponible per restore i proves (dins o fora de l'appliance)	100TB
Retenció mínima del catàleg de rèpliques	30 dies

4.3 Requeriments funcionals del servei

4.3.1 BaaS – Backup as a Service

L'adjudicatari haurà d'aportar el seu propi sistema i infraestructura de còpies de seguretat en modalitat de Backup as a Service (BaaS) en tots aquells elements subjectes de l'abast d'aquest plec tècnic a la infraestructura actual. És a dir, haurà d'aportar el seu propi maquinari i programari necessari per a implementar el subsistema de backup allà on calgui, oferint una consola de gestió, definició, planificació, execució – manual i automàtica – i recuperació de les còpies de seguretat de les dades, com de la totalitat dels sistemes operatius servidors corporatius virtuals, servidors de fitxes, i aplicacions, així com fer-se càrrec del manteniment, actualitzacions i evolucions necessàries de tot el maquinari i programari cobert sota el servei durant la durada de contracte de serveis que s'estableixi en aquesta licitació.

Dins del servei de còpia de seguretat l'adjudicatari haurà de realitzar les tasques pròpies de l'operació diària d'un sistema de còpies de seguretat com son:

- Monitorització dels jobs de còpia de seguretat de la nit anterior
- Correcció d'errors i rellançament de tasques
- Configuració de nous treballs de còpia de seguretat per als nous serveis que vagi creant el CSI.
- Informes diaris i setmanals del resultat de les còpies de seguretat
- Garantir el rendiment adequat per que les copies es facin en el mínim temps possible i de forma optimitzada.
- Garantir el bon dimensionament del llicenciament dels backups per poder suportar el creixement vegetatiu futur de les dades sense costos addicionals.
- Auditar periòdicament els sistemes per garantir que es fa backup de totes les dades sense excepcions.

La solució ha de garantir que almenys una còpia de les dades resideixi fora de les instal·lacions corporatives on resideixen físicament les dades originals.

La solució proposada, tant local com remota, haurà d'oferir la integració directa amb l'eina actual de Backup Commvault Simpana.

Qualsevol ampliació no prevista en el servei i el seu cost serà mesurada d'acord amb els costos d'ampliació d'espai contractat i especificats a l'oferta.

Requeriments mínims de la còpia de seguretat

Les polítiques de còpies de seguretat ja existents s'hauran de preservar menys en cas de proposta de millora per part del licitador, tant en cobertura, programació i finestra, per tal d'aconseguir una finestra en el dia, tant la còpia local com la còpia remota auxiliar.

La retenció establerta per al servei de còpies de seguretat local serà mínimament de:

- 15 dies incrementals i Fulls
- 45 dies fulls setmanals
- 365 dies fulls mensuals

Per la retenció estesa LTR a la còpia remota auxiliar haurà de contemplar:

- 15 dies incrementals i Fulls
- 45 dies fulls setmanals
- 365 dies fulls mensuals
- Fulls anuals il·limitats

Aquestes còpies han de poder-se efectuar sense requerir cap aturada dels sistemes operatius en producció.

L'espai d' emmagatzematge ofert en la còpia estesa LTR, ha de ser adaptat a l'ús que requerirà CSI, com a mínim les mides i còpies definides en l'annex tecnològic a protegir, actualment estimat en una ocupació mínima de 64TB un cop processades les dades amb els sistemes de compressió, de-duplicació o d'altres que el sistema aporti. S'haurà d'incloure dins el servei el creixement d'aquesta ocupació de la còpia de llarga retenció fins com a mínim 100Tb.

També es requereix que el sistema local contemplat en forma IaaS com el propi contracte de serveis defineixin la possibilitat de contractar un increment d'espai d'emmagatzematge de còpies de seguretat respecte a l'ofert inicialment, per tal de facilitar l'adaptació del sistema de còpies de seguretat a nous futurs projectes que CSI així com els creixements vegetatius del mateix en especial respecte a les retencions il·limitades anuals, que es pugui dur a terme i que requereixin la salvaguarda de dades no previstes en aquest moment.

El sistema, tant local (del que l'adjudicatari haurà d'assumir el creixement en espai) com el del aprovisionat externament per a la còpia auxiliar estesa del LTR, ha de permetre, per tant, la contractació d'un increment de l'espai per a còpies de seguretat. El licitador haurà d'especificar en la documentació de l'oferta el cost de l'increment d'aquest emmagatzematge en forma de cost mensual per TB.

El Servei haurà d'oferir integració i suport en les còpies de seguretat en tota la plataforma de CSI que es troba detallada a l'annex tecnològic d'aquest plec tècnic.

Caldrà donar suport a qualsevol plataforma que Commvault Simpana sigui capaç de protegir així com les tecnologies que suporti en un futur en el cas que CSI realitzi canvis de versió o plataforma que empra la corporació per tal d'assegurar la continuïtat dels serveis. En aquest cas l'adjudicatari assumirà dins el servei les instal·lacions i configuracions necessàries per a garantir la còpia de seguretat del programari renovat sempre que resti suportat per Commvault Simpana.

El Servei haurà d'oferir una consola d'administració per la plataforma que permeti al personal tècnic de CSI, la revisió, definició i explotació.

La consola d'administració ha de permetre definir la ubicació en la recuperació i permetre una autonomia total en cas de restauració en qualsevol moment horari, i en tal cas si s'escau haurà d'existir un suport si la restauració no pot ser executada per a donar suport en la restauració.

El sistema productiu de backup haurà de permetre la recuperació de les dades en un entorn aïllat diferent a l'entorn d'explotació, de tal manera que es pugui restaurar l'objecte del NAS o de qualsevol dels agents contemplats actualment, en qualsevol plataforma on es pugui validar la integritat i totalitat dels objectes/dades recuperats, ja sigui per un incident concret o bé simplement a fi i efecte de validar la correctesa de les còpies emmagatzemades. Per "validar" s'entén el següent:

- Garantir que a partir de les còpies es poden recuperar els sistemes originals amb correcte funcionament i amb dades "exactes" que es pretén recuperar.
- Garantir que les pròpies proves de recuperació i validació de les còpies no afectaran als sistemes en producció.

La plataforma en paral·lel, ha de permetre que CSI pugui monitoritzar l'estat de l'execució dels treballs de backup, així com la revisió dels resultats i errors obtinguts en els treballs ja finalitzats o cancel·lats. Preferiblement, la consola haurà de permetre també llançar notificacions (p. Exemple mitjançant correu electrònic) per notificar canvis d'estat, alertes o errors en aquests treballs.

Manteniment del llicenciament i suport

El servei de backup haurà d'incloure el manteniment de les llicències i subscripcions necessàries al llarg de la vigència del contracte. També haurà d'incloure el suport de fabricant per tal de tenir accés a noves versions del programari, així com la possibilitat d'escalar casos de suport en cas que sigui necessari. L'adjudicatari serà l'encarregat d'obrir i gestionar aquests casos amb fabricant, fent d'interlocutor entre el fabricant i CSI. En el cas que les necessitats de còpia de seguretat del CSI canviïn durant la durada del contracte (per exemple, migració de dades a Office 365), l'adjudicatari adaptarà aquestes llicències a les noves necessitats, intentant minimitzar qualsevol sobre cost que pugui esdevenir.

4.3.2 DRaaS – Disaster Recovery as a Service

Les operacions han de basar-se en la replicació de les màquines virtuals designades pel CSI que han d'estar disponibles per a la seva posada en marxa en cas d'activació del pla de recuperació davant de desastres.

S'han de conservar diverses còpies que, a més de servir com a còpia de seguretat, han de tenir la possibilitat de ser replicades cap a un entorn de virtualització aliè a CSI, quedant preparades per a la seva posada en marxa. L'entorn de virtualització pot recolzar-se en tecnologia d'hipervisor dels fabricants Vmware o Nutanix, però ha de tractar-se d'un clúster aliè a CSI i totalment independent, així com prèviament configurat per a la seva integració directa per al punt d'activació de la rèplica. En cas de necessitat d'activació d'aquest entorn de virtualització extern, es podrà accedir de forma remota.

Les comunicacions necessàries per a la operativitat del servei han d'estar configurades i a càrrec del proveïdor del servei. Per altra banda, es podrà optar pel disseny d'un pla que permeti, dins del RTO establert, disposar de la plataforma de virtualització instal·lada i funcionant a la seu designada del CSI en un temps inferior a 4 hores des del moment de l'avís.

Requeriments mínims del servei

- Integració de la gestió i monitorització de la solució des de la consola de gestió i protecció de l'entorn.

- Disposar de dos orígens per realitzar aquestes rèpliques, en cas de fallida d'alguna d'elles per assegurar el destí de les dades, dels quals com a mínim un ha de ser aliè a CSI.
- Com a mínim un d'aquests orígens ha de ser immutable.
- Històric d'almenys 30 dies de retenció de les rèpliques.
- El Datacenter en què estiguin emmagatzemades les còpies, així com la rèplica, ha de ser de Tier III i certificat segons l'ENS tipus mitjà.
- No es contempla la sobre subscripció de memòria ni de CPU, ja que la plataforma ha d'estar totalment disponible en recursos per a CSI.
- El sistema no pot interferir amb les eines de còpia de seguretat ni amb la finestra actual de còpia de seguretat.
- La transmissió de les dades ha de ser deduplicada, comprimida i xifrada i no implicarà una VPN entre el Consorci i el datacenter del licitador.
- Capacitat de, com a mínim, 10 TB per a l'emmagatzematge de les rèpliques.
- Emmagatzematge disponible en cas de desastre per a fer restore i proves de concepte (dins o fóra de l'appliance) de 100TB.
- Plataforma de virtualització en destí amb suficient capacitat de computació i emmagatzematge per assumir el funcionament de totes les MV replicades.
- Capacitat de restauració i validació automàtiques des de qualsevol dels orígens indistintament.
- La posada en marxa del servei no ha de suposar cap cost addicional per l'increment de llicenciaments de la plataforma de protecció de CSI.
- Ús d'una línia de comunicacions dedicada proposada pel licitador.
- RPO de màxim 24 hores.
- RTO de màxim 4 hores.
- Serveis gestionats de la solució plantejada, a nivell operatiu i d'administració.
- Serveis professionals necessaris per a la instal·lació, activació i transport del servei.
- Validació diària del correcte funcionament de les còpies de seguretat.

4.4 Requeriments tècnics del servei

Per al disseny de la proposta d'una solució de backup es requereix que el primer joc de còpies de seguretat a disc es realitzi al datacenter del CSI en un emmagatzematge aprovisionat pel licitador i en un segon joc a un entorn al datacenter de l'adjudicatari.

La solució proposada haurà de tenir la capacitat de realitzar còpies de seguretat de les plataformes de virtualització de servidors dels fabricants Nutanix i Vmware, així com la capacitat de fer cross hypervisor restore entre els dos fabricants.

Aquestes pròpies plataformes estaran a disposició de l'adjudicatari per a instal·lar la infraestructura necessària per a donar el servei requerit de backup descrit en el present plec de prescripcions en format d'appliance / servidor virtual.

Totes les còpies de seguretat, tant les principals com les secundàries, hauran d'estar definides com a immutables i amb mecanismes de protecció contra ransomware.

El backup es realitzarà a un emmagatzematge aportat per l'adjudicatari tant en local com al cloud propi. Aquestes còpies hauran de ser emmagatzemades en dispositius amb característiques air-gapped i immutables al datacenter de l'adjudicatari.

La solució proposada ha de ser administrada, gestionada i mantinguda pel licitador.

Totes les actualitzacions de la plataforma han d'anar incloses dins del servei durant tota la vigència del contracte.

En el cas de substituir l'actual plataforma de backup, l'adjudicatari serà responsable de l'explotació de la mateixa mentre duri el procés de retenció de les dades.

Còpia local

Servei IaaS amb una estructura NAS local d'emmagatzematge adient per a mantenir les còpies ubicades al CPD del CSI.

La proposta ha d'incloure, com a requeriments mínims, la següent infraestructura:

- Cabina d'emmagatzematge amb 300 TB usables com a espai "landing zone" de les còpies de seguretat. Caldrà que disposi connexió 10/25Gb mitjançant tecnologia DAC.
- Característiques de seguretat de la connexió amb l'entorn de backup amb capacitat per a separar la gestió del dispositiu i la presentació dels volums de dades en segments de xarxa diferents.

Còpia externa

Per a la ubicació d'un CPD fora del CSI, es requereix que aquest compleixi les especificacions de com a mínim TIER 3 i la seva ubicació ha d'estar dins del territori Espanyol. L'incompliment d'aquest requisit, així com tots els que es consideren com a mínims, serà causa d'exclusió del procediment. Per part del licitador es donarà la informació rellevant a la propietat del maquinari, accés físic a l'entorn així com l'accés lògic a la dada. La qual haurà de ser identificada no només en ubicació sinó també el model de protecció de la mateixa i el model de comunicació entre CSI i els dos emmagatzematges externs.

La solució garanteix que almenys una còpia de les dades resideixi fora de les instal·lacions corporatives on resideixen físicament les dades originals. El Datacenter

extern resideix a territori nacional, amb la certificació TIER III és una plataforma gestionada al 100% per l'equip tècnic del proveïdor actual. No es contemplen repositoris a clouds públics degut a la criticitat i la protecció de la dada.

Tota la infraestructura en alta disponibilitat dins el datacenter de l'adjudicatari des de les comunicacions externes fins a l'entorn de processament, incloent el programari requerit per a un correcte funcionament i protecció de l'entorn.

Tot el hardware i software necessari per a donar el servei de BaaS es regirà per una subscripció vigent durant el període que duri el contracte.

La connectivitat entre la cabina ubicada al Datacenter del CSI i el Datacenter destí es realitzarà sense necessitats de muntar cap connexió VPN / IPSEC. Es farà servir una línia de comunicació exclusiva per aquest servei, a càrrec de l'adjudicatari.

Model d'immutabilitat en quant a les còpies offline amb tecnologia air gapped.

Segmentació en VLAN's diferents per a emmagatzematge i per a gestió.

Capacitat per a realitzar una restauració en el destí off-site de màquines virtuals en el datacenter de destí per a proves DR, o casos especials amb accés exclusiu mitjançant VPN.

La infraestructura utilitzada per al servei de còpia de seguretat haurà de ser propietat de l'adjudicatari, no sent vàlides propostes amb servidors a clouds públics.

Les còpies remotes hauran d'estar ubicades en un Datacenter on la distància des del CSI sigui inferior a 50km. Aquest data centre disposarà de categoria tipus Tier III amb certificació ENS grau mitjà, per part del Datacenter i del licitador.

Infraestructura DRaaS

L'entorn de virtualització de destí ha de complir els requisits següents:

- Requeriments tècnics mínims descrits a la volumetria del servei
- Clúster aliè i totalment independent del CSI, prèviament configurat i integrat per a l'activació directa de la rèplica.
- Tecnologia d'hipervisor VMware o Nutanix, a elecció de l'adjudicatari.
- Sense sobre subscripció de memòria ni de CPU: tots els recursos han d'estar totalment disponibles per al CSI en tot moment, sense compartir-los amb altres clients.
- Capacitat de computació i emmagatzematge suficient per assumir el funcionament de la totalitat de les màquines virtuals replicades en cas d'activació.
- Capacitat mínima d'emmagatzematge per a restore i proves de 100 TB.

4.5 Operació i monitorització del servei

4.5.1 Tasques operatives diàries

L'adjudicatari ha de realitzar, com a mínim, les tasques operatives diàries següents sobre la plataforma de backup:

- Revisió d'informes diaris i verificació que tots els backups programats s'han executat correctament, tant al repositori local com al repositori remot.
- Revisió de la llista de programació i còpies auxiliars, verificant que les programacions s'han llançat i completat correctament i documentant els resultats.
- Revisió i resolució de les còpies fallides i rellançament dels jobs que compleixin aquest criteri.
- Revisió de les retencions de les dades allotjades offline, incloent-hi la revisió de l'eina de Data Aging i la verificació del purgat dels treballs caducats.
- Supervisió del rendiment de la deduplicació (DDB), incloent-hi els paràmetres de temps de cua i ingestió dels darrers 3 dies.
- Reconstrucció de la base de dades de deduplicació si es detecten problemes.
- Revisió i resolució de possibles mancances d'espai als MediaAgents.
- Verificació de la securització dels components CORE de l'entorn, amb especial focus en la protecció antiransomware dels MediaAgents.
- Verificació de l'estat dels pedaços i actualitzacions del sistema operatiu dels components de la plataforma.
- Atenció de sol·licituds de restauració requerides pel CSI.

4.5.2 Monitorització del servei

La monitorització del servei s'ha de realitzar les 24 hores del dia, 365 dies l'any, i ha de cobrir la disponibilitat i l'operativitat de la totalitat dels elements de la plataforma. La monitorització pot realitzar-se des del centre de serveis gestionats de l'adjudicatari, sempre que el CSI disposi de visibilitat de la plataforma de gestió en mode lectura en tot moment, sense necessitat d'intermediació.

Els protocols d'actuació i els llindars dels nivells d'alerta per a cadascun dels elements de la plataforma s'han de pactar entre l'adjudicatari i el CSI abans de l'inici del servei, i han de quedar documentats en el manual de procediments del servei.

La comunicació de les incidències originades des del servei de monitorització i la seva resolució s'ha de notificar al CSI per correu electrònic i, en cas de no disponibilitat de la plataforma de correu, per via telefònica.

4.6 Perfils professionals

Responsable del servei (Service Manager)

Atribut	Descripció
Funció	Interlocutor únic de l'adjudicatari davant del CSI per a tots els aspectes de gestió del servei (operació, supervisió i seguiment). Responsable del

	compliment contractual i de la relació amb el Departament TIC del CSI.
Dedicació	Parcial. Disponible en horari laborable i localitzable fora d'aquest per a situacions d'escalat.
Experiència Mínima	Mínim 5 anys d'experiència en gestió de serveis TI gestionats de complexitat similar.

Tècnic especialista en Backup i DRaaS

Atribut	**Descripció**
Funció	Administració, operació i manteniment de la plataforma CommVault i de la solució DRaaS. Responsable de les tasques operatives diàries, la gestió de polítiques, l'atenció de restauracions i la coordinació de les proves de recuperació.
Dedicació	Dedicació al present contracte. L'adjudicatari ha de dimensionar el nombre de tècnics necessaris per garantir la cobertura i les tasques operatives diàries.
Experiència Mínima	Mínim 3 anys d'experiència en administració de plataformes CommVault en entorns de complexitat similar.

4.7 Pla de formació

L'adjudicatari és responsable de formar al personal del Departament TIC del CSI en les noves tecnologies i plataformes implantades en el marc del present lot, garantint un coneixement suficient sobre les seves característiques, funcionament i processos operatius que requereixin la participació del personal del CSI.

La formació ha de realitzar-se abans de la posada en marxa dels serveis, en els horaris, grups i format convinguts amb el CSI, i ha de cobrir com a mínim els àmbits següents:

- Funcionament i ús de la consola de gestió centralitzada per a la revisió, definició i explotació del servei de backup i de la solució DRaaS.
- Procediments operatius de monitorització i gestió accessibles des de les eines posades a disposició del CSI.
- Procediments d'activació del pla de recuperació davant de desastres i validació de les rèpliques.
- Processos de sol·licitud de restauració i seguiment del seu estat.

L'adjudicatari ha de presentar en la seva oferta un pla de formació detallat que inclogui, com a mínim: sessions previstes, perfils i nombre de participants, metodologia, calendari, continguts i durada estimada. El pla de formació ha de ser aprovat pel CSI, que és l'encarregat d'establir les directrius per al disseny del pla definitiu i de coordinar-ne l'execució.

Addicionalment, davant de qualsevol canvi tecnològic significatiu en la plataforma durant la vigència del contracte (actualitzacions de versió, incorporació de noves funcionalitats, canvis en els procediments operatius, etc.), l'adjudicatari ha de garantir la formació del personal del CSI afectat en un termini raonable previ a la posada en marxa dels canvis, sense que el procés de formació pugui afectar la qualitat del servei.

4.8 Seguretat

Les obligacions de seguretat del present lot complementen i especifiquen, en el context particular del servei BaaS i DRaaS, els requisits transversals de seguretat establerts al punt 2.6 del present document. Atesa la naturalesa crítica del servei — que implica la custòdia, la transmissió i l'emmagatzematge de la totalitat de les dades i sistemes del CSI — l'adjudicatari ha de mantenir el màxim nivell de diligència en matèria de seguretat en totes les operacions realitzades en el marc del present lot.

4.8.1 Obligacions específiques de seguretat

L'adjudicatari ha de garantir la seguretat, la disponibilitat, la confidencialitat i la integritat de la informació gestionada en el marc del present lot mitjançant el compliment, com a mínim, de les obligacions següents:

Compliment normatiu i polítiques de seguretat

- Complir en tot moment amb els estàndards i les polítiques de seguretat del CSI, que seran comunicades durant el període de transició i podran ser actualitzades durant la vigència del contracte.
- Garantir la confidencialitat, la integritat i la disponibilitat de la totalitat de la informació emmagatzemada en el marc del servei, tant en les còpies locals com en les còpies remotes.
- Informar al CSI sobre la seva política de seguretat corporativa, així com sobre la seva implementació i seguiment per part de la seva organització, en el moment de l'inici del servei i davant de qualsevol canvi rellevant.

Protecció de les dades i les comunicacions

- Garantir que tota la informació transmesa pel CSI no és emmagatzemada, duplicada ni interceptada de manera no autoritzada en cap punt de la xarxa o la infraestructura de l'adjudicatari.
- Garantir el xifratge de les dades en repòs i en trànsit en la totalitat dels components de la solució, tant en el repositori local com en el repositori remot i en les comunicacions de replicació DRaaS.
- Garantir la immutabilitat de totes les còpies i rèpliques, amb mecanismes de protecció contra ransomware i modificacions no autoritzades, independents entre ells i independents del maquinari emprat.
- Garantir les característiques air-gapped de l'emmagatzematge remot, evitant qualsevol connexió directa accessible des de l'exterior que pugui comprometre la integritat de les còpies.

Control d'accés i traçabilitat

- Garantir l'accés a qualsevol element de la infraestructura del servei mitjançant un control d'accés lògic estricte, restringit als usuaris autoritzats i d'acord amb els principis de mínim privilegi i segregació de funcions establerts al punt 2.6.2 del present document.
- Garantir l'aplicació estricta de les normes de seguretat per part de la totalitat del personal de l'adjudicatari amb accés als sistemes o a les dades del CSI.
- Executar totes les operacions de servei seguint procediments escrits que contemplin les normes de seguretat aplicables.

Gestió proactiva de la seguretat

- Informar per escrit al CSI tan aviat com es detectin riscos reals o potencials de seguretat en la xarxa o en l'equipament relacionat amb el servei, en un termini màxim de 2 hores des de la detecció, d'acord amb el que s'estableix al punt 2

5 Lot 3: Administració de infraestructura SAP Basis

5.1 Descripció del servei

5.1.1 Objecte del lot

El Lot 3 té per objecte la prestació del servei de gestió i administració avançada de Nivell 3 de la plataforma SAP del CSI, incloent-hi la totalitat dels components SAP en abast i les bases de dades Oracle i MAXDB que els sustenten.

El servei s'estructura en dos elements complementaris i indissociables:

- Servei base: Cobreix la totalitat de les tasques recurrents i previsibles necessàries per garantir la correcta operació, el manteniment i el govern de la plataforma SAP, incloses en la tarifa mensual del servei.
- Capacitat tècnica a demanda: Cobreix les accions per situacions sobrevingudes, no previstes o de volum variable que, per la seva naturalesa, no poden ser assumides dins del servei base sense distorsionar-ne el dimensionament, incloent-hi la resolució d'incidències complexes, problemes, peticions de servei i canvis.

Aquest model substitueix el model de borsa d'hores global del contracte predecessor, amb l'objectiu de millorar la previsibilitat econòmica del servei i incrementar la transparència operativa.

5.1.2 Abast del servei

El servei cobreix la totalitat dels components de la plataforma SAP del CSI i les seves bases de dades associades. A títol de referència, i sense caràcter limitatiu, els sistemes en abast en el moment de la publicació de la present licitació són els següents:

Component	Descripció
SAP HIS	Sistema de gestió hospitalària (Hospital Information System). Component crític per a l'operativa assistencial del CSI.
SAP R3/ECC	Sistema ERP.
SAP PI	Plataforma d'integració i orquestració de processos per a l'intercanvi de missatges entre sistemes.
SAP Web Dispatcher	Component de balanceig i enrutament de peticions web als sistemes SAP.
Bases de dades Oracle	Bases de dades Oracle que sustenten la totalitat dels sistemes SAP en abast, incloent-hi la seva administració avançada, l'optimització del rendiment i la gestió de la seva alta disponibilitat
SAP Content Server	Repositori d'emmagatzematge per la gestió i accés de documentació digitalitzada.
SAP Router	Servei de proxy per comunicació dels sistemes SAP amb l'exterior.

La arquitectura SAP del CSI inclou, per a cadascun dels sistemes en abast, els entorns de Desenvolupament (DEV), Qualitat (QAS) i Producció (PRD), la gestió dels quals queda inclosa en el present lot en la seva totalitat.

Queda expressament exclosa de l'abast del present lot la gestió de la infraestructura de base sobre la qual s'executen els sistemes SAP (màquines virtuals sobre plataforma Nutanix, update de kernel del sistema operatiu, emmagatzematge i xarxa), que és responsabilitat del Lot 1. L'adjudicatari del Lot 3 ha d'establir procediments de coordinació formals amb l'adjudicatari del Lot 1 per a les actuacions que requereixin intervenció a ambdues capes.

5.1.3 Model de prestació i horari

El servei es prestarà en modalitat predominantment remota, atesa la naturalesa de les plataformes gestionades. L'adjudicatari ha de disposar en tot moment dels accessos, les eines i la connectivitat necessaris per operar amb plena efectivitat des de qualsevol ubicació, garantint que la modalitat remota no suposa cap limitació en els temps de resposta ni en la qualitat del servei, especialment durant la cobertura de guàrdia.

En casos excepcionals degudament justificats que requereixin presència física a les instal·lacions del CSI, l'adjudicatari ha de garantir la disponibilitat d'un tècnic per desplaçar-se en un termini acordat amb el CSI.

Modalitat	Aplicació
Horari estès	Prestació del servei base: operació diària, gestió d'incidències, peticions de servei i canvis planificats.
Guàrdia localitzable 24x7	Cobertura ininterrompuda per a la resolució d'incidències crítiques i greus fora de l'horari estès, integrada en el model de tres nivells definit al present document. L'adjudicatari del Lot 3 actua com a N3 especialitzat en plataforma SAP, rebent els escalats del servei de guàrdies del CSI quan la resolució requereix coneixement avançat de la plataforma.

5.2 Requeriments funcionals del servei

El servei base comprèn les activitats de caràcter fix, recurrent i previsible que l'adjudicatari ha de prestar de manera continuada durant tota la vigència del contracte, incloses en la tarifa mensual del servei i independents del consum de la capacitat tècnica a demanda.

5.2.1 Guàrdia localitzable

L'adjudicatari ha de garantir la cobertura de guàrdia de Nivell 3 SAP Basis fora de l'horari d'oficina descrit al present document, integrada en el model de tres nivells del

CSI en el qual l'adjudicatari actua com a N3 especialitzat en plataforma SAP, rebent els escalats del N2 quan la resolució requereix coneixement avançat de la plataforma.

La guàrdia ha de ser coberta per un tècnic SAP Basis localitzable en tot moment durant la seva franja de cobertura, amb els temps de resposta següents des de la notificació del N2:

Prioritat	Temps màxim de resposta
Crítica	15 minuts
Alta	30 minuts

La cobertura de la guàrdia, incloent-hi la disponibilitat del tècnic i el temps de resposta inicial, forma part del servei base i no computa sobre les hores de la capacitat tècnica a demanda. No obstant això, les hores de dedicació efectiva a la resolució de les incidències ateses durant la guàrdia sí que computen sobre la capacitat tècnica a demanda, aplicant el multiplicador corresponent a la franja horària d'actuació d'acord amb la taula definida al punt 5.3.

5.2.2 Check mensual

L'adjudicatari ha de realitzar una revisió tècnica mensual de la totalitat dels sistemes SAP en abast, amb l'objectiu d'avaluar proactivament l'estat de salut de la plataforma, identificar riscos i proposar accions preventives abans que es converteixin en incidències.

El check mensual ha de cobrir, com a mínim, els àmbits següents:

- Estat general dels sistemes SAP del landscape (DEV, QAS, PRD): disponibilitat, rendiment, consum de recursos i espai.
- Revisió dels logs del sistema i dels dumps ABAP acumulats durant el mes, identificant patrons recurrents que puguin indicar problemes latents.
- Estat de l'execució dels jobs crítics planificats i identificació d'anomalies en la planificació de tasques.
- Estat de les bases de dades Oracle i MAXDB: espai, rendiment, alertes actives i estat dels backups.
- Estat del sistema de transport (TMS): transports pendents, errors acumulats i estat del landscape.
- Estat de la plataforma SAP PI/PO: cues de missatges, errors recurrents i rendiment de la integració.
- Estat del Web Dispatcher: disponibilitat, rendiment i configuració.
- Revisió del compliment del pla de pegats de seguretat i l'estat del cicle de vida dels components.

Els resultats del check mensual han de quedar documentats en un informe tècnic mensual lliurat al CSI, incloent-hi les anomalies detectades, les accions preventives proposades, evolutius així com el seu grau de prioritat. Aquest informe constitueix la base per a la planificació de les actuacions del mes següent amb càrrec a la capacitat tècnica a demanda.

El temps de dedicació al check mensual i a l'elaboració de l'informe corresponent forma part del servei base i no computa sobre la capacitat tècnica a demanda.

5.2.3 Responsable del servei (*Service Manager*)

L'adjudicatari ha de designar un Responsable de Servei com a interlocutor únic davant del CSI per a tots els aspectes de gestió del contracte. La dedicació del Responsable de Servei a les tasques pròpies de la gestió del servei forma part del servei base i no computa sobre la capacitat tècnica a demanda.

Les tasques incloses en el servei base com a part del rol de Responsable de Servei són:

- Participació en els comitès de seguiment establerts al punt 2.1 del present document (operatiu mensual i estratègic trimestral).
- Elaboració i lliurament dels informes periòdics de servei definits al punt 2.4, incloent-hi el seguiment dels KPIs, l'estat de les accions obertes i el consum de la capacitat tècnica a demanda.
- Gestió de la relació amb el proveïdor de llicències de SAP per a les tasques administratives associades al suport OSS (obertura i seguiment de missatges, gestió de notes i descàrrega de pedaços), sense perjudici que el temps tècnic de resolució d'aquests missatges pugui computar sobre la capacitat tècnica a demanda quan escaigui.
- Coordinació amb els adjudicataris d'altres lots i amb els serveis gestionats externs en els aspectes relacionats amb la plataforma SAP.

5.2.4 Activitats no incloses al servei base

Queden expressament excloses del servei base, i per tant computaran sobre hores de la capacitat tècnica a demanda, la totalitat de les actuacions tècniques sobre la plataforma SAP que no formin part dels elements descrits als punts anteriors, incloent-hi sense caràcter limitatiu:

- Resolució d'incidències de qualsevol prioritat i complexitat.
- Gestió i resolució de problemes.
- Atenció i execució de peticions de servei.
- Implementació de canvis sobre la plataforma.
- Aplicació de Support Packages, notes SAP i pedaços.
- Refrescs de sistemes, còpies de mandant i qualsevol altra actuació de manteniment evolutiu.
- Suport a projectes o iniciatives del CSI.
- Resolució tècnica de missatges OSS amb SAP en coordinació amb el proveïdor de llicències.

5.3 Capacitat tècnica a demanda

La capacitat tècnica a demanda és l'instrument mitjançant el qual el CSI consumeix els serveis tècnics de l'adjudicatari per a la totalitat de les actuacions no incloses en el servei base. Tota actuació tècnica sobre la plataforma SAP que no formi part explícita

del servei base ha de ser tramitada i executada amb càrrec a la capacitat tècnica a demanda.

5.3.1 Volum i condicions

El volum mínim de la capacitat tècnica a demanda és de **200 hores** base anuals. Les hores no consumides no són acumulables al període següent ni són objecte de compensació econòmica.

L'oferta econòmica del licitador ha d'incloure un preu base anual per a la totalitat d'hores les hores en horari d'oficina, sobre el qual s'aplicaran els multiplicadors de consum corresponents a la franja horària d'execució d'acord amb la taula d'equivalència següent:

Franja horària	Multiplicador
Horari d'oficina	x 1,0
Fora d'horari d'oficina	x 1,5
Diumenges i festius	x 1,75

5.4 Perfils professionals

Responsable del servei (Service Manager)

Atribut	Descripció
Funció	Interlocutor estratègic de l'adjudicatari davant del CSI. Responsable global del compliment contractual, la qualitat del servei, la relació amb la direcció TI del CSI.
Dedicació	Parcial. Disponible en horari laborable i localitzable fora d'aquest per a situacions d'escalat.
Experiència Mínima	Mínim 5 anys d'experiència en gestió de serveis TI gestionats de complexitat similar.

Tècnic especialista N3 SAP BASIS

És el perfil tècnic central del lot i ha de tenir un coneixement profund de la totalitat dels components SAP en abast i de les bases de dades Oracle i MAXDB associades.

Atribut	Descripció
Funció	Responsable de l'execució de les tasques del servei base (operació diària, checks, manteniment preventiu, parxeig) i de la resolució de les incidències, problemes, peticions de servei i canvis escalats, tant en horari de servei com en la cobertura de guàrdia.
Dedicació	L'adjudicatari ha de dimensionar el nombre de tècnics SAP Basis necessaris per garantir la cobertura del servei base en horari estès, la guàrdia

	localitzable 24x7 i la disponibilitat de recursos per a les actuacions de capacitat tècnica a demanda.
Experiència Mínima	Mínim 4 anys d'experiència en administració avançada de sistemes SAP Basis en entorns de producció crítics, incloent-hi experiència demostrable en administració de bases de dades Oracle en entorns SAP.
Certificacions requerides	• C_DBADM - SAP Certified Associate - Database Administrator - SAP HANA. • C_TADM - SAP Certified Technology Consultant – SAP S/4HANA System Administration • E_S4CON - SAP Certified Technology Specialist - SAP S/4HANA Conversion and SAP System Upgrade

6 Lot 4: Administració plataforma CITRIX CVAD i NetScaler ADC

6.1 Descripció del servei

6.1.1 Objecte del lot

El Lot 4 té per objecte la prestació del servei de gestió i administració avançada de Nivell 3 (N3) de la plataforma de virtualització d'aplicacions i escriptoris del CSI, basada en Citrix Virtual Apps and Desktops (CVAD) — que inclou els components XenApp i XenDesktop — i de la plataforma de lliurament d'aplicacions Citrix NetScaler ADC, tant en la seva component interna com en la seva component perimetral.

El servei té per objecte la resolució de les incidències, els problemes i les peticions de servei sobre les plataformes en abast que, per la seva complexitat tècnica, excedeixen la capacitat de resolució dels nivells de suport previs (N1 i N2), d'acord amb el model de guàrdies i escalat definit al present document. L'adjudicatari actua, per tant, com a nivell d'expertesa tècnica màxima sobre les plataformes Citrix del CSI, assumint la responsabilitat de la seva administració avançada, el manteniment del seu cicle de vida i la garantia de la seva estabilitat, disponibilitat i rendiment.

El servei s'emmarca en el model de serveis gestionats del CSI i ha d'operar de manera integrada i coordinada amb els adjudicataris dels lots 1 i 2, així com amb els serveis gestionats independents de Networking i Ciberseguretat.

6.1.2 Abast del servei

El servei de Lot 4 abasta les plataformes i components tecnològics següents:

Citrix Virtual Apps and Desktops

Component	Descripció
XenApp (Citrix Virtual Apps)	Plataforma de publicació i lliurament d'aplicacions virtuals als usuaris finals del CSI, incloent-hi la gestió dels servidors de sessions, les polítiques de publicació i el cicle de vida de les aplicacions publicades.
XenDesktop (Citrix Virtual Desktops)	Plataforma de lliurament d'escriptoris virtuals als usuaris finals del CSI, incloent-hi la gestió dels catàlegs de màquines, els grups de lliurament i les polítiques d'assignació.
Delivery Controllers	Administració avançada dels controladors de lliurament CVAD, incloent-hi la gestió de la base de dades del site, la configuració de les polítiques Citrix i la resolució d'incidències sobre el nucli de la plataforma.
Citrix StoreFront	Administració del servei d'accés i autenticació dels usuaris a les aplicacions i escriptoris publicats, incloent-hi la gestió dels stores, les polítiques d'autenticació i la integració amb el directori actiu.
Mecanismes d'aprovisionament	Administració avançada dels mecanismes d'aprovisionament de màquines virtuals en ús a l'entorn del CSI (Machine Creation Services i/o

	Provisioning Services), incloent-hi la gestió de les imatges mestres i el seu cicle d'actualització.
Gestió de perfils d'usuari (FSLogix)	Administració de la solució de gestió de perfils d'usuari en ús a l'entorn Citrix del CSI, incloent-hi la resolució d'incidències de perfil, la gestió de les polítiques de redirecció de carpetes i l'optimització del rendiment de càrrega de perfils.
Citrix Director	Ús de la consola de monitorització i suport de Citrix per a la diagnosi i resolució d'incidències de sessió, rendiment i disponibilitat de la plataforma.

Citrix NetScaler ADC

El servei cobreix la totalitat dels dispositius NetScaler ADC desplegats en l'entorn del CSI, que operen en dos àmbits diferenciats amb funcions complementàries:

Component	Descripció
NetScaler intern (xarxa corporativa)	Dispositiu NetScaler ADC desplegat a la xarxa interna corporativa del CSI, que actua com a balancejador de càrrega per als equips (thin clients) que es connecten a la granja Citrix des de la xarxa local. Inclou l'administració de les VIPs de balanceig, les polítiques de persistència de sessió, els monitors de servei i la configuració d'alta disponibilitat.
NetScaler perimetral (DMZ)	Dispositiu NetScaler ADC desplegat a la zona desmilitaritzada (DMZ) del CSI, que proporciona accés remot segur per VPN i accés a les aplicacions publicades des de l'exterior de la xarxa corporativa. Inclou l'administració del Citrix Gateway, les polítiques d'autenticació i autorització, la gestió dels certificats SSL/TLS i les polítiques de seguretat perimetral (WAF).

6.1.3 Model de prestació i horari

El servei del Lot 4 s'ha de prestar sota un model de prestació predominantment remot, atesa la naturalesa de les plataformes gestionades, que permeten la seva administració i operació en la seva totalitat des de qualsevol ubicació amb connectivitat segura als sistemes del CSI.

L'adjudicatari ha de disposar en tot moment de les eines, els accessos i la connectivitat necessaris per operar amb plena efectivitat en modalitat remota, garantint que aquesta modalitat de prestació no suposa cap limitació en els temps de resposta ni en la qualitat de la resolució de les incidències, els problemes i les peticions de servei en abast.

No obstant el caràcter predominantment remot del servei, poden existir situacions excepcionals en les quals la presència física de l'adjudicatari a les instal·lacions del CSI

sigui necessària. A títol orientatiu, i sense caràcter limitatiu, es consideren situacions que poden justificar la presència física les següents:

- Situacions d'incident major en les quals la pèrdua d'accés remot als sistemes impedeixi la diagnosi i resolució de la incidència per via telemàtica.
- Posades en marxa o migracions de plataforma de gran abast que, per la seva complexitat o el seu risc, es consideri convenient supervisar de manera presencial.
- Reunions tècniques o de coordinació que el CSI requereixi presencialment per a la resolució d'una situació específica.

En qualsevol cas, la presència física ha de ser prèviament justificada i acordada entre l'adjudicatari i el CSI, i no pot ser imposada de manera unilateral per cap de les parts.

Atesa la diferent criticitat operativa de les dues plataformes en abast, el servei s'ha de prestar sota el model de cobertura diferenciat següent:

Plataforma	Modalitat	Descripció
Citrix CVAD (XenApp / XenDesktop)	24x7x365	Cobertura ininterrompuda tots els dies de l'any, incloent-hi caps de setmana i festiu. Inclou l'atenció i resolució d'incidències, problemes i peticions de servei sobre la plataforma CVAD que excedeixin la capacitat de resolució del N2.
NetScaler ADC (intern i perimetral)	24x7x365	Cobertura ininterrompuda tots els dies de l'any, incloent-hi caps de setmana i festius. Inclou l'atenció i resolució d'incidències crítiques sobre els dispositius NetScaler, atesa la seva funció com a punt d'accés crític tant per als usuaris interns com per als accessos externs.
Guàrdia localitzable	Fora d'horari d'oficina	Disponibilitat de tècnic de guàrdia localitzable fora de l'horari d'oficina per a la resolució d'incidències crítiques sobre la plataforma que no puguin esperar a l'inici de la jornada laborable.

6.2 Infraestructura i volumetria del servei

6.2.1 Consideracions generals

Concepte	Descripció
Centres gestionats	3 Hospitals, 3 CAPs, 3 CAEs i 2 Residències
Nombre aproximat d'usuaris totals	4.000 usuaris
Usuaris concurrents Citrix	Aproximadament 500 usuaris
Horari operatiu	Servei 24x7
Distribució de la infraestructura	Infraestructura distribuïda entre dos CPDs (principal i secundari)

Casos d'ús principals	Escriptori virtual complet (VDI) i publicació d'aplicacions corporatives
Hypervisor	Nutanix AHV
Emmagatzematge	Nutanix Distributed Storage
MFA	Microsoft MFA
Antivirus / EDR	Trend Vision One / Trend AI
Plataforma de còpia de seguretat	Commvault amb còpia al núvol
Plataforma de monitorització	Centreon i Citrix Director

6.2.2 Plataforma Citrix Virtual Apps and Desktops (CVAD)

Concepte	**Descripció**
Versió CVAD	Citrix Virtual Apps and Desktops 24.02 LTSR CU3
Model de llicenciament	Citrix Hybrid Multi-Cloud
Delivery Controllers	2
StoreFront Servers	2
SQL Server	2 servidors SQL Server 2022 en clúster Always On
Instàncies WEM	1
Servidor de llicències Citrix	1
Servidor de llicències RDS	1
Citrix Director	Desplegat de forma redundant als brokers
VDAs desplegats	Aproximadament 94 entre XenApp i XenDesktop
Tipologia d'escriptoris	No persistents
Sistemes operatius VDAs	Windows Server 2022 i Windows 11
Catàlegs	13
Delivery Groups	10

6.2.3 Citrix StoreFront i workspace

Concepte	**Descripció**
Servidors StoreFront	2
Versió StoreFront	24.02 LTSR CU3
Balanceig	Citrix ADC
URL d'accés	https://app.csi.cat
Workspace App Windows	Versió 25.11.10.50
Dispositius gestionats	Aproximadament 2.000 PCs Windows, 400 Thin Clients
Mètodes d'autenticació	LDAP, SAML i Azure AD
MFA / SSO	Microsoft Authenticator

6.2.4 Citrix NetScaler ADC

Concepte	Descripció
Model	Citrix ADC VPX
Firmware	NS13.1 Build 61.23
ADCs externs	2 a la DMZ
ADCs interns	2
Arquitectura	Alta disponibilitat (HA) actiu/passiu
Integració MFA	Microsoft Entra ID / Azure AD
Certificats	Certificats emesos per entitat pública certificadora
Renovació de certificats	Manual

6.2.5 Mecanismes d'aprovisionament (MCS/PVS)

Concepte	Descripció
Tecnologia d'aprovisionament	Machine Creation Services (MCS)
Golden Images	2
Golden Image XenApp	Windows Server 2022
Golden Image XenDesktop	Windows 11
Actualitzacions	Manuals
Manteniment	Mensual
Entorn de test / preproducció	Disponible
Segmentació de catàlegs	No existeixen catàlegs diferenciats per hospitals o serveis
Automatització addicional /configuracions	Scripts PowerShell / GPO's / Politiques Citrix

6.2.6 Gestió de perfils d'usuaris

Concepte	Descripció
Solució de perfils	Entorn mixt Citrix UPM i FSLogix
Emmagatzematge de perfils	Nutanix Files
Redirecció de carpetes	Desktop, Documents i Downloads

6.2.7 Volumetria del servei

La volumetria aquí mostrada es basa en les dades reals recopilades pel Consorci Sanitari Integral des de la seva eina de tiqueting. L'objectiu d'aquesta volumetria és que el licitador es pugui fer una idea de l'esforç requerit, però en cap cas es podrà fer servir aquesta volumetria com a requeriment de consum mínim o màxim

	Incidències / mes	Peticions / mes	Hores per petició
Administració plataforma Citrix	4	4	4h

6.3 Requeriments funcionals del servei N3

6.3.1 Marc general

El servei N3 del Lot 4 cobreix l'administració avançada de les plataformes Citrix CVAD i NetScaler ADC, actuant com a nivell d'expertesa tècnica màxima per a la resolució de les incidències, els problemes i les peticions de servei que excedeixen la capacitat de resolució del N2 del Lot 1.

Cal tenir en compte que el servei d'operacions del Lot 1 assumeix la gestió operativa diària de la plataforma Citrix, incloent-hi tasques com la publicació de noves imatges mestres, la gestió del cicle de vida de les aplicacions publicades, la monitorització de l'estat de les sessions i la resolució d'incidències operatives habituals. El Lot 4 actua, per tant, com a suport especialitzat d'escalat sobre aquests mateixos àmbits quan la complexitat tècnica requereix un nivell de coneixement i intervenció superiors, i com a responsable exclusiu dels àmbits que per la seva naturalesa corresponen a l'administració avançada de la plataforma.

6.3.2 Àmbit de responsabilitat de la plataforma CVAD

L'adjudicatari ha de donar cobertura N3 sobre la totalitat dels components de la plataforma CVAD en abast (XenApp, XenDesktop, Delivery Controllers, StoreFront, MCS/PVS i gestió de perfils d'usuari), assumint com a responsabilitats pròpies, entre d'altres, les següents:

- Resolució d'incidències i problemes complexos sobre qualsevol component de la plataforma CVAD que no hagin pogut ser resolts pel N2 del Lot 1, incloent-hi problemes sobre el nucli de la plataforma (Delivery Controllers, base de dades del site), errors d'aprovisionament de màquines, incidències complexes de perfil d'usuari i problemes d'autenticació i accés a nivell de plataforma.
- Administració avançada de les polítiques Citrix (HDX, sessió, accés, impressió i perfils), incloent-hi la seva creació, modificació i optimització en resposta a necessitats operatives o incidències de rendiment i experiència d'usuari. I administració del sistema WEM.
- Gestió del cicle de vida de la plataforma: planificació i execució de les actualitzacions de versió dels components CVAD, elaboració i seguiment del pla de parcheo de la plataforma en coordinació amb el Lot 1, i gestió proactiva del cicle de vida dels components per evitar situacions de End of Life sense planificació.
- Interlocució amb Cloud Software Group (Citrix) per a la resolució de casos de suport que requereixin intervenció del fabricant, actuant com a intermediari únic entre el fabricant i el CSI i mantenint el CSI informat de l'estat de qualsevol cas obert.
- Suport especialitzat al Lot 1 en les tasques operatives que, per la seva complexitat o risc, requereixin la supervisió o intervenció d'un tècnic N3, com ara actualitzacions d'imatges mestres de gran abast, canvis estructurals en els catàlegs de màquines o modificacions de polítiques d'alt impacte.
- Administració avançada dels Servidors SQL dedicats a la infraestructura.

- Administració avançada dels Servidors de llicències CITRIX i RDS.
- Administració de les GPO del directory actiu específiques de la plataforma CITRIX.

6.3.3 Àmbit de responsabilitat de la plataforma NetScaler ADC

L'adjudicatari ha de donar cobertura N3 sobre la totalitat dels dispositius NetScaler ADC en abast — el dispositiu intern de balanceig de la granja Citrix i el dispositiu perimetral de la DMZ per a accés remot i VPN — assumint com a responsabilitats pròpies, entre d'altres, les següents:

- Resolució d'incidències i problemes complexos sobre els dispositius NetScaler que no hagin pogut ser resolts pel N2 del Lot 1, incloent-hi problemes de connectivitat, comportament anòmal del balanceig, errors d'autenticació en el Gateway i incidents de seguretat sobre els dispositius perimetrals.
- Administració avançada de la configuració dels dispositius NetScaler, incloent-hi la gestió de VIPs, serveis i polítiques de balanceig intern, la configuració del Citrix Gateway per a l'accés remot extern, les polítiques d'autenticació i autorització avançades (AAA, nFactor), la gestió del WAF i la gestió del cicle de vida dels certificats SSL/TLS instal·lats.
- Gestió del cicle de vida de la plataforma: planificació i execució de les actualitzacions de firmware dels dispositius NetScaler, garantint la no afectació del servei durant el procés d'actualització mitjançant la gestió adequada de l'alta disponibilitat.
- Notificació proactiva al CSI de qualsevol patró d'atac o activitat sospitosa detectada a través dels logs del NetScaler perimetral, en un termini màxim de 2 hores des de la seva identificació, en coordinació amb l'equip de Ciberseguretat del CSI.
- Gestió del cicle de vida dels certificats SSL/TLS, amb notificació proactiva al CSI amb un mínim de 30 dies d'antelació respecte a la data de caducitat de qualsevol certificat instal·lat en els dispositius.
- Interlocució amb Cloud Software Group (Citrix) per a la resolució de casos de suport sobre la plataforma NetScaler que requereixin intervenció del fabricant.
- Gestió avançada del servei de FAS de gestió de certificats per l'autenticació federada.

6.4 Perfils professionals

El dimensionament de l'equip és responsabilitat de l'adjudicatari, qui ha de justificar en la seva oferta que el nombre de persones i els perfils proposats són adequats per absorbir la càrrega operativa de referència, garantir els temps de resposta i resolució establerts i mantenir la qualitat del servei durant tot el període contractual, incloent-hi les situacions de vacances, baixes i absències del personal.

En cap cas el CSI assumirà responsabilitat sobre el dimensionament de l'equip proposat per l'adjudicatari. Un dimensionament insuficient que resulti en

incompliments de servei serà responsabilitat exclusiva de l'adjudicatari i no podrà ser al·legat com a causa de força major ni com a justificació de desviacions en els KPIs i SLAs contractuals.

Responsable del servei (Service Manager)

Atribut	Descripció
Funció	Interlocutor únic de l'adjudicatari davant del CSI per a tots els aspectes de gestió del servei. Responsable del compliment contractual i de la relació amb el Departament TIC del CSI.
Dedicació	Parcial. Disponible en horari laborable i localitzable fora d'aquest per a situacions d'escalat.
Experiència Mínima	Mínim 5 anys d'experiència en gestió de serveis TI gestionats de complexitat similar.

Tècnic especialista N3 CITRIX CVAD

Atribut	Descripció
Funció	Resolució de les incidències, els problemes i les peticions de servei escalades sobre la plataforma Citrix CVAD (XenApp, XenDesktop, Delivery Controllers, StoreFront, i gestió de perfils d'usuari). Administració avançada de la plataforma i manteniment del seu cicle de vida.
Dedicació	Dedicació al present contracte en horari d'oficina. L'adjudicatari ha de dimensionar el nombre de tècnics CVAD necessaris per garantir la cobertura del servei i la resolució de les escalades dins dels temps de resposta establerts.
Experiència Mínima	Mínim 2 anys d'experiència en administració avançada de plataformes Citrix Virtual Apps and Desktops en entorns de producció d'envergadura similar a l'entorn del CSI.
Certificacions requerides	Citrix Certified Expert – Virtualization Citrix Certified Associate App Delivery and Security (Expert)

Tècnic especialista N3 NetScaler ADC

Atribut	Descripció
Funció	Resolució de les incidències, els problemes i les peticions de servei escalades sobre els dispositius NetScaler ADC en abast (intern i perimetral DMZ). Administració avançada de la plataforma, incloent-hi el balanceig de càrrega, el Citrix Gateway, les

	polítiques de seguretat perimetral i la gestió de certificats SSL/TLS.
Dedicació	Dedicació al present contracte en modalitat de cobertura 24x7, en modalitat de guàrdia localitzable fora de l'horari estès. L'adjudicatari ha de dimensionar el pool de tècnics NetScaler de manera que la cobertura ininterrompuda quedi garantida sense dependències en persones individuals.
Experiència Mínima	Mínim 4 anys d'experiència en administració avançada de dispositius Citrix NetScaler ADC en entorns de producció crítics, incloent-hi experiència demostrable en entorns amb component de seguretat perimetral (DMZ, Gateway, WAF).
Certificacions requerides	Citrix Certified Expert App Delivery and Security

6.4.1 Compatibilitat de perfils

L'adjudicatari pot proposar en la seva oferta una estructura en la qual un mateix tècnic cobreixi els perfils d'especialista CVAD i especialista NetScaler, sempre que pugui acreditar el nivell de coneixement i les certificacions requerides per a ambdós perfils i que el dimensionament global de l'equip garanteixi la cobertura y temps de resposta establerts per al servei.

6.5 Capacitat tècnica a demanda

Es defineix una capacitat tècnica a demanda per a evolutius en el Lot 4, destinada a donar cobertura a les actuacions d'evolució tecnològica sobre les plataformes Citrix CVAD i NetScaler ADC que, per la seva naturalesa, van més enllà del manteniment operatiu habitual inclòs en el servei i requereixen una planificació i execució específiques. A títol orientatiu, i sense caràcter limitatiu, constitueixen exemples d'ús habitual de la capacitat tècnica a demanda les actuacions següents:

- Actualitzacions de versió de la plataforma CVAD (upgrades de Delivery Controllers, VDAs, StoreFront, etc.).
- Actualitzacions de firmware i versió dels dispositius NetScaler ADC.
- Incorporació de noves funcionalitats o components a la plataforma Citrix existents.
- Migracions o reestructuracions de la plataforma que no constitueixin un projecte independent.
- Optimitzacions de configuració de calat que requereixin una dedicació significativa fora de l'operativa habitual.
- Qualsevol altra actuació evolutiva sobre les plataformes en abast que el CSI requereixi i que excedeixi el marc de les incidències, els problemes i les peticions de servei habituals.

El volum de la capacitat tècnica a demanda és de **50 hores efectives** anuals.

Les actuacions s'han de realitzar preferentment en horari no productiu (tarda, nits, caps de setmana o festius), per minimitzar l'impacte sobre els usuaris de la plataforma. L'horari d'execució ha de ser acordat amb el CSI en cada cas.

Taula d'equivalència

S'haurà de contemplar la equivalència entre els diferents horaris de servei dins d'una taula, ja que la capacitat tècnica a demanda es podrà emprar en qualsevol horari, tant diürn, com nocturn com festiu, així com si les hores son presencials o remotes, seguint el model de la taula següent:

	Multiplicador de capacitat tècnica a demanda			
	Remot		Presencial	
Tipus de perfil	Nocturn	Festiu	Nocturn	Festiu
Tècnic especialista				