

PLEC DE PRESCRICIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT D'INFRAESTRUCTURA CIBER RESILIENT D'EMMAGATZEMATGE DE DADES NO ESTRUCTURADES PER L'INSTITUT CATALÀ D'ONCOLOGIA (ICO) EXP. (CP-2024-09)

Índex

1. Objecte del contracte.....	2
2. Objectius.....	2
3. Situació actual.....	2
4. Descripció de necessitats.....	5
4.1 Sistema d'emmagatzematge de producció i ciberprotegit.....	5
4.2 Especificacions dels serveis.....	8
4.3 Servei de suport de administració.....	9
5. Termini de garantia i període de consolidació.....	11
6. Seguiment del projecte.....	12
7. Seguiment de la qualitat/penalitzacions.....	12
Les situacions extraordinàries seran avaluades i aprovades en l'àmbit del comitè de seguiment del servei.....	13
8. Descripció de la metodologia a utilitzar.....	13
9. Requeriments de seguretat.....	13
10. Lliurables del projecte.....	14
11. Contingut i estructura de l'oferta tècnica (SOBRE B).....	15



1. Objecte del contracte

L'Institut Català d'Oncologia (ICO) és una empresa pública sense ànim de lucre, creada al 1995, i adscrita al Servei Català de la Salut. La seva missió és "la de treballar per reduir l'impacte del càncer a Catalunya".

L'ICO és el primer Institut integral del Càncer de Catalunya i treballa als vessants de la recerca, prevenció i l'assistència. Segurament, dins de l'assistència els tractaments més utilitzats estan inclosos dins dels processos de la radioteràpia o els processos de la quimioteràpia.

L'objecte del present contracte és la renovació de la infraestructura d'emmagatzematge de dades no estructurades de l'ICO, optant per una solució integral que permeti ampliacions i renovacions graduals durant un període mínim de 10 anys i que compti amb mesures de protecció contra ciberamenaces,—per tant, l'adquisició de nou maquinari així com la seva instal·lació, configuració i formació del personal tècnic del ICO amb detall indicat al plec de prescripcions tècniques— fent convergir en una única infraestructura l'emmagatzematge de dades assistencials i de recerca de l'Institut Català d'Oncologia.

2. Objectius

Els objectius són els següents:

- Renovació tecnològica del maquinari d'emmagatzematge de dades no estructurades de l'ICO.
- Millora en la gestió d'un únic sistema centralitzat enlloc de múltiples sistemes, de diferents fabricants.
- Convergència de l'emmagatzematge de dades assistencial i de recerca.
- Protecció de les dades contra ciberamenaces.
- Adquisició d'una solució adequada per fer front al creixement continu de la instal·lació.
- Adquisició d'una solució adequada per fer front a la obsolescència de la pròpia solució sense provocar interrupcions en el servei.

3. Situació actual

L'actual infraestructura d'emmagatzematge de dades no estructurades del ICO està formada per múltiples equips de diferents fabricants, que s'estan quedant desactualitzats tecnològicament, sense capacitat disponible ni resiliència envers ciberamenaces. Aquests equips s'utilitzen en dos entorns diferenciats:

- Entorn Windows: Els equips es destinen a unitats de xarxa que els usuaris utilitzen des dels seus ordinadors o servidors amb Windows, i que es gestionen mitjançant polítiques del directori actiu del ICO.
- Entorn Linux, sistemes de computació d'alt rendiment (High Performance Computing, HPC): Els equips es fan servir per llegir i escriure fitxers, mitjançant el protocol NFS, des dels nodes de computació. Aquests equips



d'emmagatzematge disposen de sistemes secundaris que en fan còpies de seguretat incrementals. L'ICO disposa de dos clústers HPC que tenen un ús moderat. L'autenticació dels usuaris i gestió de grups d'usuaris és a nivell de cada clúster.

Les característiques dels sistemes d'emmagatzematge per cada entorn són els següents:

Entorn MS Windows ICO

- NAS producció:
 - o 1x NAS VNX 5200 (85 TB)
 - o 1 x NAS Synology RS2418PR (44 TB)

Entorns Linux (HPC) ICO

Cluster Recerca:

- 14 nodes de computació (total: 276 CPU)
- NAS producció:
 - o 1 x servidor Dell R740xd2, amb capacitat neta de 200TB (NFSv3), 10Gbps
 - o 1 x NAS Dell Emc2 vnx3200, amb capacitat neta de 14TB (NFSv3), 10Gbps
 - o 1 x NAS Thecus N12000 Pro, amb capacitat neta de 99TB (NFSv3), 10Gbps
- NAS backup
 - o 1 x NAS Thecus N12000, amb capacitat neta de 99TB (NFSv3), 10Gbps
 - o 1 x NAS Thecus N12000, amb capacitat neta de 90TB (NFSv3), 10Gbps
 - o 2 x NAS Thecus N12000 Pro, amb capacitat neta de 99TB (NFSv3), 10Gbps
 - o 1 x NAS Synology DS1815 (92 TB)

Cluster Assistencial:

- 5 nodes de computació (total: 128 CPU)
- NAS producció:
 - o 1 x servidor Dell R740xd2, amb capacitat neta de 200TB (NFSv3), 10Gbps
- NAS backup:
 - o 1 x servidor Dell R740xd2, amb capacitat neta de 200TB (NFSv3), 10Gbps

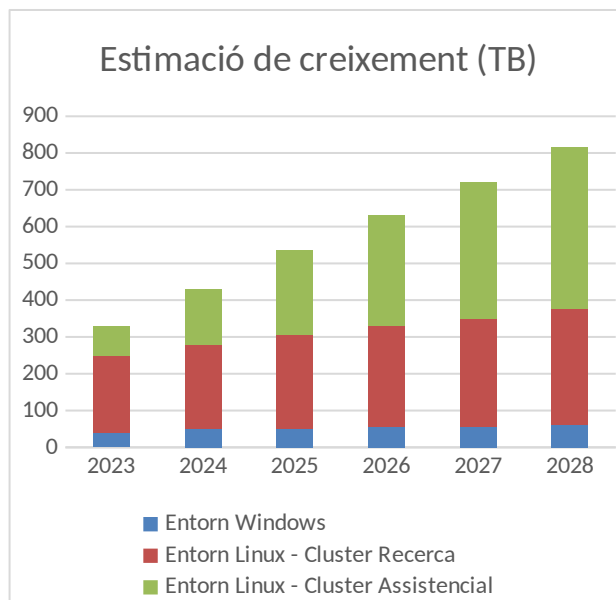
La solució proposada ha de substituir els equips de NAS de producció d'ambdós entorns, permetent al ICO retirar els equips Thecus, Synology i VNX. Els equips Dell



R740xd2, que estan actualment sota garantia, es destinaran a sistemes de salvaguarda.

La previsió de creixement de dades no estructurades (producció) és la següent, a data 31 de desembre 2023 en endavant:

NAS Producció	2023	2024	2025	2026	2027	2028
Entorn Windows	40	50	50	55	55	60
Entorn Linux - Clúster Recerca	209	230	255	275	295	315
Entorn Linux - Clúster Assistencial	80	150	230	300	370	440
Total (TB)	329	430	535	630	720	815



La solució proposada ha de permetre la convergència d'entorns Windows i Linux, mitjançant diferents protocols (SMB/CIFS, NFS, FTP, etc.), així com permetre ampliacions de capacitat d'emmagatzematge en els propers anys.

El present contracte té per objecte el subministrament i instal·lació d'una solució ciber resilient d'emmagatzematge de dades no estructurades, així com un entorn replicat ciberprotegit i un servei de suport màxim de 50 hores, d'acord amb el detall més endavant indicat:

Entorn productiu d'emmagatzematge

Codi Validació: 7ZRF0F4WL6JCHADYWD9JL7A6
Verificació: <https://ico.eadministracio.cat/>
Document signat electrònicament des de la plataforma esPublico Gestiona | Pàgina 4 de 16



Entorn ciberprotegit d'emmagatzematge
Instal·lació, configuració de la infraestructura i formació.
Suport (màxim 50 hores)

4. Descripció de necessitats. Requeriments d'obligat compliment.

Es consideren els següents requeriments com els mínims indispensables per una solució d'emmagatzematge ciber resilient per una entitat de les característiques del ICO. Tots els requeriments han de formar part de la solució, i en cap cas, s'acceptaran característiques previstes en la fulla de ruta del producte o en fase de desenvolupament i/o proves.

4.1 Sistema d'emmagatzematge de producció i ciberprotegit

La solució a contractar ha de contemplar l'aportació de la infraestructura necessària per a una solució integral d'emmagatzematge de dades no estructurades amb protecció contra ciberamenaces.

Aquesta solució ha de contemplar mecanismes de replicació cap a un entorn ciberprotegit, aïllat de la xarxa de l'Institut Català d'Oncologia. L'entorn ciberprotegit només ha de connectar-se a l'entorn de producció només el temps necessari per a fer la sincronització de dades.

En concret, i com a mínim, es demana l'adquisició dels següents articles:

- Els nodes/servidors que componen la solució d'emmagatzematge. Es considera un node, a un maquinari amb la seva memòria RAM, CPU, interfaces de xarxa i emmagatzematge en disc (control·ladors i discs), que té la capacitat de còmput per processar i administrar l'emmagatzematge, i no comparteix elements d'emmagatzematge (discs, control·ladors, etc.) amb altres nodes. D'aquesta forma l'addició de nodes fa que la solució augmenti en capacitat i prestacions.
- Llicències de la solució.
- Elements físics per instal·lació dels elements en un *rack*.
- Cables i òptiques necessàries per la intercomunicació d'elements.
- Cables d'alimentació necessaris per a la connexió de la solució, amb connectors C13/C14.
- Electròniques necessàries per a la connectivitat de la solució.
- La instal·lació i configuració inicials, el traspàs de coneixement, formació i suport per la explotació que executarà l'Institut Català d'Oncologia.

4.1.1 Requeriments tècnics i característiques

- La solució ha d'estar basada en un maquinari i programari dissenyats específicament per a aquest propòsit, i que es subministren de forma conjunta per part del fabricant.



- La solució ha de estar basada en una arquitectura NAS Scale-out real, és a dir en una arquitectura totalment distribuïda on totes les control·ladores són actives, comparteixen recursos i es reparteixen la càrrega.
- La solució ha de ser una solució de mercat amb una maduresa mínima demostrable de 5 anys, i amb una previsió de vida superior als 10 anys, que permeti adquirir nous components per a gestionar l'obsolescència dels components més antics sense pèrdua de servei.
- La solució ha de permetre afegir nodes de diferents tipologies, per permetre concentrar la millora del sistema en la capacitat o en les prestacions del sistema, per adaptar-se a les necessitats del ICO. D'aquesta forma, si les necessitats d'accés a les dades, per part dels clústers de computació de l'ICO augmenten, la solució s'ha de permetre afegir nodes que permetin millorar el rendiment del sistema.
- L'incorporació de nous nodes s'ha de fer sempre sense pèrdua de servei. El sistema ha de ser capaç d'autobalancejar, de forma automàtica i sense intervenció manual dels administradors, totes les dades entre tots els discs i control·ladores para a garantir un ús homogeni dels recursos.
- Cada node incorpora memòria RAM, CPU, interfaces de xarxa i emmagatzematge en disc (control·ladores i discs), fent que afegir nodes augmenti la capacitat i prestacions del sistema. Les CPU han d'estar basades en tecnologia x86 amb un número de cores suficients per al funcionament normal de tota la plataforma.
- Cada node incorpora una capa de discs SSD, que es poden utilitzar per metadades, extensió de memòria cache o emmagatzemar fitxers concrets.
- La solució ha de permetre la creació d'un volum únic i únic filesystem per al total de la capacitat. Aquest volum ha de poder ser expandible fins a més de 100PB. El filesystem únic s'ha de poder segmentar en recursos de xarxa, segons les necessitats.
- Les dades s'han de distribuir de forma uniforme, automàtica i en calent entre tots els nodes del sistema per a garantir un màxim aprofitament dels recursos, tant des d'un punt de vista de rendiment com de capacitat.
- El sistema ha de poder, segons polítiques, desbordar dades "fredes" cap a sistemes d'emmagatzematge d'objectes externs en el núvol, comprimint i xifrant les dades abans d'abandonar la solució, sense incorporar cap component addicional. Aquesta reubicació de les dades ha de ser transparent a l'usuari i ha de poder seguir accedint a les dades com si estiguessin físicament dins de la solució.
- La solució ha de oferir de manera nativa i simultània, fins i tot pel mateix recurs, la comunicació en múltiples protocols. Com a mínim CIFS/SMB (versions SMBv2, SMBv3, SMBv3.11), NFS (versions NFSv3, NFSv4, NFSv4.1, NFSv4.2), FTP, HTTP, S3, HDFS.
- La solució ha de permetre configurar en calent el tipus de protecció de les dades a nivell de share, export, carpeta o fitxer. Canviar el tipus de protecció no ha de ser en cap cas disruptiu.
- La solució proposada ha de tenir una capacitat inicial neta de, com a mínim, 530TB, sense tenir en compte mecanismes de reducció de dades.
- La solució inicial proposada ha de tenir una tolerància mínima respecte fallada de components de 2 discs i 1 node/control·ladora. A mesura que s'afegeixin nodes al sistema, la tolerància davant de fallada de maquinari ha d'augmentar.
- La solució proposada ha de disposar d'un mínim de 4 control·ladores, i en cas de fallada d'una d'elles, el rendiment global del sistema no pot disminuir més



del 25%. A mesura que s'afegeixin nodes al sistema, l'impacte màxim tolerable en el rendiment ha de disminuir.

- L'impacte d'una fallada de disc ha de distribuir-se entre totes les control·ladores existents amb l'objectiu de tenir el menor impacte en el rendiment del sistema.
- L'impacte de qualsevol fallada de maquinari ha de ser escalable, reduint-se a mesura que s'afegeixen nodes al sistema.
- En cas de fallada d'un component mentre es fan servir protocols NFSv3, NFSv4 o SMB3, el sistema ha de suportar un failover automàtic sense interrupció del servei.
- La solució ha de disposar d'un sistema de balanceig de càrrega per assegurar que les connexions d'equips al sistema es distribueixen de forma uniforme i automàtica entre les control·ladores, podent tenir en compte variables com el número de connexions, throughput o la CPU de cada node.
- La solució ha de poder ser actualitzada, tant el sistema operatiu com el firmware de maquinari i de discs, de forma no disruptiva, permetent als administradors tornar a l'estat anterior si és necessari.
- La solució ha de permetre la creació de snapshots a nivell de carpeta. Aquests snapshots seran de només lectura protegint l'esborrat accidental de dades.
- La solució proposada ha de tenir redundància de xarxa i d'alimentació.
- La solució ha de permetre, si es desitja, la integració d'un sistema d'antivirus a nivell de carpeta. També ha de permetre, a nivell de carpeta, bloquejar i evitar l'emmagatzematge de fitxers d'extensions concretes.
- La solució ha de permetre la gestió de la obsolescència del maquinari, permetent coexistir diferents generacions de maquinari, i permetent la retirada d'equips obsolets, sense interrupció del servei.
- La solució proposada ha de presentar un rendiment òptim per a més de 200 CPUs concurrents fent operacions de lectura i/o escriptura.
- La solució proposada ha de tenir un rendiment teòric, en throughput NFS, superior o igual a 4,5GBytes/s (100% lectura) i 3GBytes/s (100% escriptura). El rendiment ha de millorar a mesura que escali el sistema.
- La solució ha de disposar d'una interfície de gestió centralitzada per l'administració i monitoratge preventiu, eficaç, àgil i intuïtiva.
- La solució ha de permetre controlar l'ús d'emmagatzematge establint quotes per usuari, grup i/o directoris.
- La solució ha de permetre establir polítiques de qualitat de servei a nivell de protocol, usuari, recurs de xarxa o directori.
- La solució ha de poder-se integrar amb Directori Actiu, LDAP o establir ACLs de forma local.
- La solució ha de comptar amb un sistema de monitoratge que inclogui la funcionalitat d'avís automàtic al fabricant, i permetre la difusió d>alertes via SMTP i SNMP.
- La monitorització ha de ser proactiva, permetent posar en quarentena un disc abans que falli.
- La solució ha de permetre configurar la generació i enviament d'informes periòdics amb informació sobre l'estat del sistema.
- La monitorització del sistema ha de permetre identificar amb tota granularitat possible els possibles colls d'ampolla en el rendiment del sistema.
- La solució ha de poder integrar-se amb la solució actual de monitorització del ICO (Zabbix 6 LTS).
- La solució ha de disposar d'eines per a la gestió automàtica de snapshots.
- La solució ha de poder-se administrar via web, CLI o REST.



La solució proposada ha de disposar un mínim de 6 ports (SFP+) a 10Gbps per connectar amb les electròniques dels clústers de computació, així com amb la electrònica principal del ICO. La connectivitat de la solució ha de ser IPv4.

- La protecció contra ransomware de la solució ha de ser capaç de bloquejar fitxers en base a patrons de comportament dels usuaris. La solució ha de permetre bloquejar l'accés de l'usuari en qüestió i generar alertes als administradors. La solució ha de permetre la gestió de falsos positius.
- El mecanisme de protecció davant de ciberamenaces ha de permetre bloquejar l'escriptura en cas de detecció de possibles amenaces en l'entorn productiu.
- La solució ha de contemplar la replicació contra l'entorn ciberprotegit i aïllat. La connexió entre l'entorn de producció i el ciberprotegit s'ha de mantenir només durant la sincronització de les dades. En cas d'una amenaça identificada i activa en el entorn productiu, no s'ha de produir cap sincronització.
- Les llicències del programari contra ciber amenaces han d'estar dimensionades d'acord a la capacitat inicial del sistema, i s'han d'incloure dins del manteniment del fabricant.
- Tots els equips i components seran nous, sense utilització prèvia.
- La solució ha d'oferir un únic servei de suport per a incidents, així com per totes les accions proactives o reactivas contemplades en el contracte de manteniment.
- La solució, en la seva totalitat, tant de maquinari com de programari, ha d'estar lligada directament amb contractes de manteniment amb el fabricant de la solució.
- El fabricant ha de disposar de possibilitat de suport de la solució més enllà de 5 anys.

4.2 Especificacions dels serveis

Els serveis associats a la posada en marxa de la solució ciber resilient d'emmagatzematge són:

- Instal·lació física de l'equipament:
 - o Instal·lació dels entorns de producció i ciberprotegit.
 - o Interconnexió de tots els elements.
 - o Tots els components instal·lats hauran d'incorporat la darrera versió de firmware compatible amb els elements en producció que s'incorporin a l'entorn.
- Configuració inicial i validació del funcionament de l'entorn.
- Traspàs de coneixement als tècnics de l'ICO.
- Recomanacions de cara al traspàs de dades dels sistemes NAS actuals cap a la nova solució, per a implementar una prova pilot, així com l'incremental en el moment del pas a producció. El traspàs de dades el reatitzarà el personal del ICO.
- Proves de restauració des de l'entorn ciberprotegit i gestió d'alertes de possibles ciber amenaces.
- Metodologia: l'adjudicatari haurà de concretar la metodologia aplicada a l'hora de la implantació i gestió del projecte. Es requereix la figura de director de projecte per part de licitador. Aquest perfil haurà d'aportar capacitat demostrable per garantir la metodologia als serveis d'implantació.
- Planificació: abans de l'inici del projecte es presentarà el projecte detallat de la planificació, que inclourà, com a mínim, les següents fases:



- o Fase d'anàlisi.
- o Fase de disseny d'implantació i planificació.
- o Fase d'implantació.
- o Fase de proves de l'entorn de producció i ciberprotegit.
- o Fase de disseny de la migració.
- o Fase de proves de migració a producció.
- o Documentació.
- o Formació.
- Documentació: provisió de la documentació final de projecte, que haurà d'incloure els següents aspectes:
 - o Descripció general del maquinari/programari adquirits, funcionalitats. Memòria d'implantació, procediments d'instal·lació utilitzats, esquema de components i llicències, màquines que donen el servei, programari utilitzat, versions i configuració, relació amb altres serveis i memòria de les proves de la instal·lació efectuades.
 - o Manual d'explotació: processos associats, monitoratge, revisió de *logs*, treball planificats, treballs sota demanda, gestió del storage, gestió d'usuaris, gestió de snapshots, gestió de seguretat i gestió de l'entorn ciberprotegit.
 - o Contactes i suport.

4.3 Servei de suport d'administració

Es contempla al pressupost base de licitació 50 hores de suport tècnic pels següents conceptes:

- Resolució de peticions i/o incidències sol·licitades per pels tècnics del ICO.
- Tasques d'administració dels sistemes de segon i tercer nivell. Tasques d'administració per canvis no estàndards, (no habituals en el dia a dia de l'hospital). Aquestes tasques es preveu siguin molt excepcionals, però en el cas que resultin necessàries es consideren incloses en el preu de licitació:
 - o Horari de cobertura 10x5
 - o Temps d'atenció màxim de 1 hora
 - o Temps de resposta màxim de 4 hores
- Suport proactiu, que inclogui
 - o Revisió 1 cop a l'any del correcte funcionament de la solució.
 - o Generació d'un informe de valoració de la "salut" del sistema amb les recomanacions oportunes per garantir la funcionalitat de la instal·lació.

Es demanen les següents característiques per aquest servei:

- La comunicació de les peticions i incidències les faran els tècnics informàtics de l'ICO i es realitzarà mitjançant:
 - o Eina de *ticketing* per aplicació web de l'ICO o un altre proposada per l'adjudicatari.
 - o Correu electrònic.



- o En el cas de peticions i incidències urgents o reclamació d'aquestes és necessari poder contactar amb l'equip de suport per telèfon.
- Les peticions de millora o evolució del sistema es faran arribar als òrgans de seguiment per decidir sobre la seva execució.
- El suport serà preferiblement remot, però es podrà fer de forma presencial.
- El licitador pot ofertar uns nivells de resposta superiors als següents:
 - o Tipus d'horari:
 - ✓ Administratiu: De dilluns a divendres, 8.00h. a 19.00h.
 - ✓ Incidències crítiques: 7 x 24
 - o Tipus d'incidències: Les incidències es classificaran en quatre graus, segons la gravetat:
 - ✓ *Crítica*: no disponibilitat d'una funció bàsica del sistema, que impedeix dur a terme de forma correcta processos crítics del negoci i que no es poden posposar ni dur a terme d'una forma alternativa sense perjudicar l'operació.
 - ✓ *Urgent*: no disponibilitat d'una funció que afecta a múltiples usuaris i subsistemes, que, tot i ser important per a l'operació, es pot posposar o es pot dur a terme d'una forma alternativa, encara que sigui temporalment.
 - ✓ *Moderada*: no disponibilitat d'una funció que afecta a pocs usuaris, que, tot i ser important per a l'operació, es pot posposar o es pot dur a terme d'una forma alternativa, ni que sigui temporalment.
 - ✓ *Baixa*: qualsevol altra incidència.
 - o Temps de resposta i resolució:
 - ✓ T0: Temps màxim de resposta. Des que la incidència és comunicada al Help Desk, fins que un tècnic qualificat contacta amb l'usuari.
 - ✓ T1: Temps màxim de resolució. Des que la incidència és comunicada al Help Desk fins que es resol i es tanca.
- L'adjudicatari haurà de garantir els temps màxims de resposta i resolució que es reflecteixen a la taula següent:

Concepte	Paràmetres	Nivell mínim incidències
Gestió d'actuacions i accions correctives	Temps de resposta	Baixa < 2h horari adm.
		Moderada < 2h horari adm.
		Urgent < 2h horari 24x7
		Crítica < 1 hora 24x7
	Temps màxim de resolució per al 90% de les actuacions segons la prioritat establerta	Baixa < 15 dies laborables
		Moderada < 5 dies laborables
		Urgent < 3 dies laborables
		Crítica < 8 hores
	% màxim d'actuacions reobertes	< 10 %



Concepte	Paràmetres	Nivell mínim incidències
Peticions	Anàlisi de la petició i dimensionament	< 3 dies laborables (objectiu individual) / 90%
	Desviació respecte avaluació	Desviació d'execució vs. Execució < 10% /90% peticions

- El licitador proposarà un responsable tècnic com a referent del projecte.

5. Termini de garantia i període de consolidació

El termini de garantia serà com a **mínim de cinc anys** des de la data de recepció definitiva del projecte per part del centre.

L'acceptació del projecte de subministrament de la infraestructura d'emmagatzematge de dades no estructurades per l'ICO es farà un cop es compleixin les condicions següents, que es reflectiran en un acta lliurada per l'ICO:

- ✓ S'ha instal·lat i parametrizat l'equipament i està en funcionament
- ✓ S'han integrat tots els elements en el sistema de monitoratge del l'ICO i el servei d'informàtica ha donat el seu vistiplau a les mesures de rendiment
- ✓ S'ha lliurat tota la documentació requerida del projecte
- ✓ S'han fet tots els cursos/sessions de formació als usuaris
- ✓ El sistema porta dues setmanes en producció sense cap incidència crítica o urgent

El servei d'assistència es tradueix, tant a l'accés a recursos tècnics del fabricant, anàlisi i resolució d'incidències (tant remotament com presencialment, del rendiment i funcionament del sistema) com en llicència per utilitzar actualitzacions dels programaris base incorporats en la solució en tota la durada del contracte.

- Manteniment i suport directe del fabricant.
- Manteniment 24x7, temps de resposta de 4 hores, durant un mínim de 5 anys, a comptar des de la posada en producció de la instal·lació.
- Manteniment in-situ.
- Manteniment i suport preventius i reactius.
- Disponibilitat de recanvis en un màxim de 4 hores.
- Esforç continu fins a la resolució de les incidències.
- Garanties d'actualització de *drivers* i *firmware* durant el temps de vida dels productes.
- Es demanen els següents requeriments:
 - o Manteniment i suport preventius i reactius:
 - El contractista actuarà com a punt únic de contacte per a l'hospital per a tota la solució, tot i que l'hospital, si ho considera convenient, podrà accedir directament als fabricants.



- En el període contractat de manteniment de la solució, el contractista efectuarà les tasques de manteniment preventiu que la solució requereixi.
 - El manteniment podrà ser in situ en cas necessari.
 - Funcionalitat i utilització pel fabricant d'eines de diagnòstic remot.
 - El manteniment del hardware el proporcionarà directament el fabricant.
 - Les noves versions del firmware estaran a disposició de l'hospital conforme el fabricant les publiqui.
 - Capacitat d'escalar suport als fabricant sempre que sigui necessari.
 - La execució de tasques previstes per suport, garantia i estabilització no consumirà temps del servei d'administració.
- o La proposta i el preu han d'incloure el manteniment del hardware proposat per un mínim de 5 anys.

6. Seguiment del projecte

Es crearà un Comitè de Seguiment integrat per personal de l'hospital i de l'empresa adjudicatària.

Per part del licitador és imprescindible la incorporació d'un director de projecte que serà l'encarregat de la gestió del projecte, l'assoliment de les fites i la gestió de la resolució de problemes.

Aquest Comitè de Seguiment del contracte es reunirà amb una periodicitat mínima mensual per supervisar l'execució del contracte, comprovar el compliment dels nivells de servei establerts i resoldre els eventuais conflictes que puguin sorgir.

7. Seguiment de la qualitat/penalitzacions

Durant el desenvolupament dels serveis requerits, l'ICO realitzarà el seguiment dels nivells de qualitat establerts i aplicarà un sistema de mesura contínua de la qualitat, segons els estàndards vigents en cada moment. En aquesta línia podrà determinar els estàndards i eines metodològiques a emprar en cada moment.

El nivell ofert per qui resulti adjudicatari del servei, constituirà un Acord de Nivell de Servei (ANS), el compliment del qual es mesurarà en una periodicitat mensual durant tota la durada de la prestació del servei pel comitè de seguiment del projecte, i l'incompliment de l'ANS, serà motiu de penalització amb els criteris establerts a l'apartat de penalitzacions d'aquest document, i la seva reiteració de la rescissió del contracte.

El contractista estarà subjecte al següent règim de penalitzacions (no acumulables entre si com a conseqüència d'un mateix fet).



- Les demores en l'execució del projecte respecte el pla de treball pactat, de durada superior a 2 setmanes, seran motiu de penalització, amb un import del 2% del contracte per setmana de retard imputable a l'adjudicatari.
- Qualsevol situació de limitacions significatives a la disponibilitat del sistema en producció, crítica, de durada superior a un dia laborable i imputable al contractista, serà motiu de penalització amb un import de l'1% del contracte per cada dia de demora.

Com a norma general, queden excloses les penalitzacions en els indicadors quan:

- Existeixin situacions extraordinàries que portin a alteracions que desvirtuin la mitja.
- Que la raó de la desviació es degui a components que no estan sota la responsabilitat de l'adjudicatari.

L'ICO valorarà i tindrà en compte de forma positiva els compliments positius de l'adjudicatari, de forma que es podran realitzar compensacions en el cas que el grau de compliment dels ANS estigui en general per sobre del previst. En aquest cas no s'aplicarien penalitzacions.

Les situacions extraordinàries seran avaluades i aprovades en l'àmbit del comitè de seguiment del servei.

8. Descripció de la metodologia a utilitzar

Es requereix que els oferents indiquin, a la seva proposta, de forma detallada, la metodologia (sobre B) que utilitzaran per a l'execució del conjunt de serveis objecte d'aquesta contractació.

- El licitador haurà de presentar a la seva oferta la metodologia que utilitzarà per garantir l'assoliment del projecte, ha de contemplar les següents especificacions:
 - ✓ Ha de cobrir tant els aspectes relatius a la parametrització, configuració i implantació del sistema, com de seguiment i control del projecte.
 - ✓ Ha d'estar estructurada en etapes d'execució.
 - ✓ Ha d'haver estat desenvolupada basant-se en l'experiència en implantacions anàlogues.
- El licitador haurà d'incloure, a la seva oferta, el disseny, desenvolupament, planificació i impartició de la formació al departament d'informàtica de l'hospital.
- El licitador haurà d'incloure, a la seva proposta, una descripció del sistema de control i gestió de riscos que aplicarà durant el transcurs del projecte.
- Pla de manteniment preventiu.

9. Requeriments de seguretat

L'empresa adjudicatària es compromet a prendre totes les mesures tècniques i organitzatives al seu abast per garantir l'objectiu de seguretat de la informació, que es basa en els tres principis següents:



- **La confidencialitat** de la informació, assegurant que només hi accedeixen les persones que han estat autoritzades a fer-ho.
- **La integritat** de la informació, assegurant que la informació i els mètodes que la processen són exactes i complets.
- **La disponibilitat** d'aquesta informació, assegurant que els usuaris autoritzats tenen accés a aquestes dades, mòduls i aplicacions quan ho necessitin.

Igualment, es compromet a prendre les mesures que preveu la normativa en vigor en matèria de seguretat de la informació i protecció de dades de caràcter personal.

L'adjudicatari ha de complir els requisits establerts pel Reglament UE 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que respecte al tractament de dades personals i a la lliure circulació d'aquestes dades, per la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i de garantia dels drets digitals, i pel Reial Decret 1720/2007, de 21 de desembre, en tot allò que sigui d'aplicació, i tota altra norma relacionada que estigui vigent.

Accés a dades personals, o de caràcter reservat:

L'empresa adjudicatària es compromet a no accedir innecessàriament a aquelles dades a les quals tingui accés per raó de la tasca que té encomanada.

Sempre que calgui manipular dades, es treballarà amb dades de proves, simulades o fictícies. Un cop acabat el desenvolupament o prova, s'esborraran totes les dades manipulades, tant si són fictícies com reals.

En cas que sigui necessari accedir a les dades reals, l'empresa i els seus treballadors es comprometen a mantenir la confidencialitat respecte a la informació coneguda, a no alterar-ne el contingut i a no revelar, comunicar, ni posar a disposició de tercers, per cap mitjà, escrit, electrònic, verbal o per qualsevol altre procediment, cap d'aquestes dades o part d'elles, o la informació que se n'hagi pogut extreure.

L'accés a aquestes dades reals haurà de ser autoritzat pel responsable del fitxer o pel responsable de seguretat de l'hospital.

Col·laboració en les auditories periòdiques

L'empresa adjudicatària es compromet a facilitar tota la informació necessària per realitzar les auditories periòdiques que dugui a terme l'hospital, així com a aportar els coneixements i informacions que tingui a fi de millorar els aspectes relacionats amb la seguretat i la protecció de dades de caràcter personal.

Col·laboració en gestió de la ciberseguretat

L'empresa adjudicatària es compromet a aplicar els pegats necessaris per resoldre vulnerabilitats detectades per l'hospital, així com a emetre avisos en cas de detecció de vulnerabilitats en els seus productes i a col·laborar en el diagnòstic i resolució d'incidents de seguretat facilitant tota la informació necessària, així com a aportar els coneixements i informacions que tingui a fi de millorar els aspectes relacionats amb la seguretat i la protecció de dades de caràcter personal.



Mesures organitzatives

L'empresa adjudicatària informarà al Comitè de Seguiment de les mesures organitzatives i tècniques que ha pres per assegurar la confidencialitat, integritat i disponibilitat de la informació i les dades de caràcter personal propietat de l'Institut Català d'Oncologia.

10. Lliurables del projecte

En el decurs del projecte, l'empresa adjudicatària haurà de lliurar la documentació que seguidament es detalla en formats compatible amb Word, Excel, Power Point de Microsoft, i Acrobat-PDF d'Adobe, seguint la metodologia de gestió de projectes proposada:

- Planificació detallada del projecte, amb identificació de fites i punts de control.
- Actes de reunions.
- Informes de seguiment, amb identificació d'alertes i punts crítics.
- Pla de manteniment i suport.
- Pla de migració dels sistemes actuals cap a la nova solució.
- Pla de posada en funcionament.
- Pla d'actuació davant de ciberamenaces.
- Manuals d'usuari, d'instal·lació i d'operativa de funcionament.
- Guies ràpides per les opcions més comuns i la configuració de plataforma.
- Qualsevol altra documentació aplicable a aquest tipus de treball.

La documentació lliurada per l'adjudicatari haurà de ser aprovada pel personal que l'Institut Català d'Oncologia designi. Sense aquesta aprovació, no es podrà donar com a completada la fase del projecte a la qual correspongui. Els productes resultants de l'execució del contracte seran propietats de l'ICO.

11. Contingut i estructura de l'oferta tècnica (SOBRE B)

L'oferta del licitador s'ha d'estructurar amb els apartats i continguts que seguidament s'indiquen:

▪ **Resum executiu:**

Resum per a la Direcció dels continguts més significatius de la proposta de serveis, destacant-ne els recursos i les propostes de valor afegit.

▪ **Memòria tècnica:**

Memòria tècnica que inclogui cadascun dels criteris susceptibles de judici de valor indicats en el informe de necessitats.

▪ **Plantejament general del projecte i solució tècnica:**

Solució que es proposa, fent especial èmfasi en la descripció de les característiques o fluxos que es demanen a l'oferta, detallant el grau de resposta als requeriments especificats en el plec i estratègia de desplegament del projecte.



S'indicarà així mateix una descripció de la metodologia d'execució (inclou gestió de qualitat i de seguretat), de les eines que s'utilitzaran i del model de gestió del servei, indicant els òrgans i procediments de relació amb l'Institut Català d'Oncologia.

▪ **Lliurables pel pla d'execució proposat:**

Planificació del projecte amb la descripció de les fases i activitats, les entrades i sortides de cada fase previstes, i l'assignació de responsabilitats en cadascuna. El pla d'execució diferenciarà i detallarà clarament les fases següents:

- ✓ Instal·lació i configuració.
- ✓ Posada en funcionament.
- ✓ Pla de migració de les dades cap a la nova plataforma.
- ✓ Suport i garantia.

Per a cada fase, s'indicarà l'equip de treball proposat, amb la quantitat d'hores de dedicació previstes en cadascuna i per a cada perfil professional. S'haurà de ressaltar la dedicació requerida a l'Institut Català d'Oncologia en cada fase.

▪ **Model de relació i de gestió del projecte:**

Estructura i mesures proposades de seguiment i control del projecte.

▪ **Metodologia:**

Descripció de la metodologia que s'emprarà per a l'execució del projecte.

Es requereix la figura de director de projecte per part del licitador. Aquest perfil haurà d'aportar capacitació demostrable per garantir la metodologia aplicada als serveis d'implantació.

En la documentació haurà de constar un índex específic de la memòria tècnica del sobre B, amb llista de correspondències entre epígrafs i criteris d'adjudicació.

Carles Muñoz Montplet
Director de Tecnologia i Física
Institut Català d'Oncologia

