

PLEC DE PRESCRIPCIONS TÈCNIQUES

**SERVEI DE MANTENIMENT GLOBAL DEL SISTEMA INFORMÀTIC DE LA UNITAT DE
CRIBRATGE NEONATAL I SISTEMES DE SUPORT ADMINISTRATIUS COMPLEMENTARIS**

Nº EXPEDIENT: 2025-125

1.- OBJECTE DEL CONTRACTE:

L'Hospital Clínic de Barcelona (HCB) i en concret la Unitat de Cribratge Neonatal (UCN) enquadrada dins els laboratoris del Centre de Diagnòstic Biomèdic (CDB) realitza la detecció precoç de malalties metabòliques a tots els nounats de Catalunya. L'objectiu d'aquest concurs és la contractació dels serveis de manteniment integral del sistema informàtic particular utilitzat per aquesta unitat per tal de desenvolupar aquest programa, així com, dels elements de suport a la gestió administrativa utilitzats per aquesta unitat complementaris al sistema. La base del sistema i l'element crític del mateix és una aplicació software feta a mida sobre tecnologia Oracle per l'empresa Limit Quattro, S.A (en endavant Limit 4) que actualment és l'encarregada de portar a terme tots els serveis de manteniment aquí descrits. L'aplicació és coneguda com "ERP LIMIT 4 CRIBRATGE BIOQUIMIC".

De forma general, els serveis de manteniment a incloure a l'oferta per tots i cadascun dels elements implicats seran sempre en l'horari de funcionament de la UCN, és a dir, de Dilluns a Divendres, de les 8:00 hores a les 15:00 hores.

La voluntat del CDB és la contractació d'un proveïdor de serveis que sigui l'únic responsable del funcionament del sistema informàtic principal de la unitat i dels elements de suport (Veure detall dels elements a l'Annex I), essent aquest proveïdor l'encarregat de gestionar la relació i contractació amb els tercers implicats en el conjunt de sistemes.

La contractació del servei serà per 36 mesos, sense possibilitat de pròrroga.

2.- MODEL DE SERVEI

L'objectiu que el CDB persegueix amb la contractació d'aquest servei és garantir el funcionament en òptimes condicions de tots els sistemes de la UCN en l'horari de funcionament operatiu d'aquesta. Amb aquest propòsit, es busca un proveïdor que sigui capaç de respondre als problemes sorgits amb rapidesa i eficàcia per tal de garantir la qualitat del servei. Addicionalment, s'espera un coneixement profund de l'aplicació "ERP LIMIT 4 CRIBRATGE BIOQUIMIC" que permeti al proveïdor no solament la resolució reactiva de problemes, si no també proposar i executar accions de millora en aspectes clau com l'optimització de la Base de Dades.

2.1.1 Pautes per a la proposta del Model de Servei

Els proveïdors hauran de proposar un model de funcionament operatiu del servei. Aquest model haurà de complir unes pautes bàsiques/requeriments mínims descrits en aquest apartat i als que necessàriament el proveïdor que resulti adjudicatari haurà d'acreditar:

- **Model de relació amb el CDB i l'HCB:**

El proveïdor haurà de proposar uns canals de comunicació per contactar davant de qualsevol eventualitat que es produeixi en els elements a mantenir inclosos en aquest concurs (veure Annex I). Aquests canals hauran d'incloure com a mínim un email de contacte i un telèfon de contacte.

El proveïdor haurà de descriure a la seva oferta els canals de comunicació (email, telèfons, etc) que habilitarà per la notificació i seguiment d'incidències reportades des dels diferents àmbits.

- **Model de producció del servei:**

Basat en el model de relació anterior, el proveïdor haurà de descriure el model de producció proposat pel servei, descrivint en tot moment com es resoldran els següents requeriments **obligatoris**:

- Punt d'entrada de l'activitat: El proveïdor haurà de descriure el punt d'entrada o de reporting d'incidències. En aquest apartat s'ha de explicitar que pel conjunt de sistemes, el personal de l'HCB tindrà un únic punt d'interlocució per la resolució de les diferents problemàtiques (independentment de l'element que ha provocat la incidència).
- Punt de contacte únic amb tercers: El proveïdor adjudicatari haurà de convertir-se en un partner tecnològic per l'HCB a l'àmbit dels sistemes de la UCN. En aquesta funció, el proveïdor actuarà com punt únic de contacte per l'HCB pel manteniment contractat. Això comporta que el proveïdor haurà de gestionar pels seus mitjans les relacions amb tercers fabricants o distribuïdors dels elements a mantenir, sense que en cap cas això comporti un cost addicional per l'HCB més enllà del acordat en aquest concurs. Així, serà el propi proveïdor el que contracti els serveis als tercers que consideri oportuns pel desenvolupament integral dels serveis aquí descrits.
- Suport virtual/presencial: El proveïdor haurà de descriure en el model de producció per quines funcions donarà un suport remot, així com, per quines hi donarà un suport presencial. L'HCB posarà a disposició de l'adjudicatari una connexió VPN,

així com accés a tots els servidors que hi hagi de mantenir per mitjà d'aquesta connexió.

- **Model de Transició:**

Aquest apartat descriu com es realitzarà el Model de Transició entre els diferents proveïdors d'aquest servei de manteniment en cas de que es produeixi aquesta circumstància. El termini de transició total incloent totes les seves fases serà d'un total de 2 mesos.

Es defineix com:

- Proveïdor Sortint: L'empresa actual que realitza els serveis de manteniment i que no hagi aconseguit l'adjudicació del present concurs.
- Proveïdor Entrant: Adjudicatari del present concurs.

Fase de Transició d'Entrada del Servei

Es defineixen les fases de solapament entre el proveïdor Sortint i l'Entrant segons el següent calendari:

- Fase de Solapament Inicial: Traspàs de coneixements.
 - Duració màxima d' 1 mes previ al començament del present contracte.
 - En aquesta fase la responsabilitat del manteniment continua essent del Proveïdor Sortint que facturarà els seus serveis com en l'actualitat.
 - El Proveïdor Entrant destacarà a les instal·lacions de l'HCB, el personal necessari per aconseguir els coneixements necessaris.
 - Les despeses del Proveïdor Entrant van totalment al seu càrrec. No s'acceptarà cap facturació addicional per aquest concepte.
- Fase Inicial d'Execució del Contracte
 - Duració màxima del 1er mes d'inici del present contracte.
 - En aquesta fase s'inicia l'execució d'aquest contracte; l'adjudicatari tindrà plena responsabilitat sobre el servei.
 - Durant aquesta fase l'HCB podrà disposar del Proveïdor Sortint per intervenir puntualment per clarificar punts clau que no hagin quedat adequadament transferits a la Fase de Solapament inicial.
- Fase d'Execució Normalitzada

- S'inicia una vegada finalitzada la fase anterior. El Proveïdor Entrant treballa de manera autònoma i a ple rendiment.

Fase de Transició de Sortida del Servei

Es defineixen les fases entre el proveïdor adjudicatari del present expedient i el del futur una vegada acabat l'actual:

- Fase de Solapament Final: Traspàs de coneixements.
 - Durada màxima d'1 mes que coincideix amb l'últim mes de duració del present expedient.
 - En aquesta fase la responsabilitat del manteniment continua essent del Proveïdor Sortint que facturarà els seus serveis en el marc del present expedient.
 - Amb el consentiment de l'HCB, el Proveïdor Sortint donarà tota la documentació al nou proveïdor.
 - La devolució de l'aval al proveïdor adjudicatari del present contracte així com el pagament de l'últim termini de facturació estarà condicionat a una adequada transferència de coneixements i documentació en aquesta fase de Transició de Sortida.

3.- ABAST DEL SERVEI

L'abast del servei haurà de cobrir **necessàriament**:

- *Maquinari*: El servei de suport i manteniment es realitzarà sobre l'equipament de la UCN, en concret sobre els elements descrits a l'Annex I. En el cas de que hagi una renovació/actualització/canvi d'algun d'aquests elements també quedarà coberta a l'àmbit d'aquest concurs, entenent que aquestes substitucions únicament es produïren per la normal renovació dels sistemes o per reparacions. Queda dins l'abast d'aquest manteniment la resolució de qualsevol malfuncionament, avaria o incidència que es produís en els elements llistats, així com la resolució total del problema i el restabliment del servei i, addicionalment, qualsevol peça de recanvi que fos necessària per procedir al restabliment del servei.

Qualsevol altra equipament no llistat a l'Annex I queda expressament fora de l'abast d'aquest concurs.

En particular, respecte els PC's utilitzats per la UCN, el proveïdor adjudicatari només s'encarregarà del correcte funcionament d'aquests amb l'aplicació principal "ERP LIMIT 4 CRIBRATGE BIOQUIMIC" (connectivitat i funcionament) i amb la resta

d'aplicacions llistades a l'Annex I, així com del software client que fos necessari instal·lar per interaccionar amb el mencionat aplicació. Explícitament queda fora de l'abast qualsevol renovació d'aquests PC's. No obstant, sí que es responsabilitat de l'adjudicatari restablir el servei dels PC's amb l'aplicació una vegada substituït l'equip. En termes semblants s'ha d'actuar amb les impressores, no essent responsable el proveïdor adjudicatari del hardware, però sí del correcte funcionament i integració de les impressores al conjunt de sistemes.

Sí que assumirà el proveïdor el manteniment total d'altres elements hardware complementaris com l'escàner o la ensobradora, inventariats també a l'Annex I.

Respecte els Servidors, al estar englobats dins els sistemes de virtualització propis de l'HCB, les tasques de manteniment habituals (actualitzacions del SO, backup's etc) seran assumides per l'HCB, necessitant únicament del proveïdor en cas de necessitats que requereixin del coneixement funcional de l'aplicatiu o en el cas de restauració de l'aplicació en cas de fallida major.

- *Programari*: El proveïdor adjudicatari serà el responsable del manteniment de tot element de programari inventariat a l'Annex I d'aquest document.

Queda dins l'abast d'aquest manteniment la resolució de qualsevol malfuncionament, desconfiguració accidental o incidència que es produís en els elements llistats, així com la resolució total del problema i el restabliment del servei i, addicionalment, la utilització de qualsevol programari de suport que fos necessari per procedir al restabliment del servei. També quedarà cobert, en cas que fos necessari, qualsevol restauració de dades des de BackUp.

És especialment important mantenir en òptimes condicions de funcionament especialment aquelles integracions del "ERP LIMIT 4 CRIBRATGE BIOQUIMIC", tant amb analitzadors com amb programari de tercers.

El contracte de manteniment inclourà 30h anuals d'un perfil d'analista per desenvolupaments i adaptacions dels diferents elements fets a mida que componen el "ERP LIMIT 4 CRIBRATGE BIOQUIMIC". En cas que les hores no es vegin consumides totalment en un any natural, les restants, s'acumularan per l'any següent amb el mateix propòsit.

- *Nivell de Servei a complir*

El conjunt de sistemes i aplicacions inclosos en aquest concurs presten un servei crític pel funcionament de la UCN i, així doncs, per la tasca assistencial que aquesta porta a terme. El principal objectiu d'aquest concurs, i per tant de l'adjudicatari, és que els sistemes estiguin en perfecte funcionament pels usuaris de la UCN durant l'horari de treball d'aquesta (de Dilluns a Divendres de 8:00 a 15:00). La resolució d'incidències en aquest interval de temps ha de ser ràpida i efectiva no poden estar cap dels elements que componen la unitat inoperatius o funcionant de una manera inadequada causant disconfort a l'usuari final més enllà de 10 hores laborables de la UCN des del reporting de la incidència.

- *Facturació de Serveis i sancions pel incompliment del nivell de servei*

El proveïdor presentarà com oferta a aquest concurs un import pel global dels serveis inclosos a l'abast. La facturació es produirà per trimestres anticipats.

Respecte al no compliment del nivell de servei de demanat pels diferents elements aquí descrits, l'HCB podrà exigir fins a un 5% de penalització a l'import total de la factura del següent trimestre. L'import de la penalització serà establert per l'HCB i comunicat al proveïdor per procedir a l'ajustament en la facturació.

Una reiterada falta en assolir el nivell de servei aquí descrit (més de 5 incompliments en un trimestre), podrà desencadenar la ruptura del contracte de manteniment. Addicionalment, el fet de que l'HCB decideixi deixar d'utilitzar l'aplicació "ERP LIMIT 4 CRIBRATGE BIOQUIMIC" també seria motiu de cancel·lació d'aquest contracte.

4.- SEGURETAT I CONFIDENCIALITAT DE LES DADES

L'empresa adjudicatària s'ha de responsabilitzar del compliment de les mesures en seguretat que, d'acord amb el Reial Decret 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguridad (ENS), ha establert l'HCB relacionades amb els equips i/o serveis objecte del contacte. Per acreditar aquest compliment l'adjudicatari ha de presentar la documentació indicada a l'**annex II del PPT "Seguretat TI i OT"**. Els serveis corresponents requeriran aquesta documentació a l'empresa que hagi presentat la millor oferta en el tràmit de requeriment establert a l'article 150.2 de la LCSP. En cas de no complir adequadament el requeriment, o no complir amb els requeriments sol·licitats, s'aplicarà l'establert en el mateix article 150.2.

5.- MODEL DE LA OFERTA

Els proveïdors que decideixin presentar ofertes a aquest concurs i per tal de facilitar la seva avaluació, d'ajustar el contingut tècnic de la mateixa al màxim possible al format que es descriu a continuació:

1. Resum executiu de la solució oferta, resumint els punts més significatius de la proposta del servei i les prestacions addicionals ofertes (podent aquestes ser considerades o no per l'HC)
2. Descripció del Model de Servei
3. Abast del Servei
4. Pla de Qualitat
5. Recursos Humans i Tècnics
6. Referències de l'empresa en serveis similars

Barcelona,

Santiago Salvat Blanco
Cap Econòmic-Administratiu
de la Direcció de Sistemes d'Informació

ANNEX I

Equipamiento del Sistema de Gestió de la Unitat de Cribratge Neonatal i Complementaris

Productes	Descripció del Producte	Nombre de Sèrie
	BBDD ORACLE LICENSE STD EDITION ONE 10 USERS ASFU DBA Oracle Database	
	Actualitzacions i manteniment APEX.	
	ERP LIMIT4 NOU NADONS 15 USUARIS	
	SoftWare OMR Kodak Alaris Capture Pro.	
	Kodak S2070 Scanner NS	63235761
	Ensobradora tsi-4s expert 1 st + 1 catch tray field fit	21HB1895

ANNEX II
Seguretat TI i OT



**Requisits Generals de Seguretat
per a la contractació de Serveis i
Productes TI i OT
(dins del marc de l'ENS)**

Barcelona, març de 2024
Versió v1.0

Contingut

1	Introducció i objectius	12
2	Abast	12
3	Aspectes Generals de Seguretat per a Serveis	12
3.1	Requisits per a la contractació de Serveis d'Implantació d'Infraestructura i programari tant IT com OT	12
3.2	Subcontractació	13
3.3	Requisits de serveis de Desenvolupament de Programari	13
3.4	Serveis al Núvol	15
3.5	Excepcions	15
4	Aspectes Generals de Seguretat per a Productes	15
4.1	Primera Opció – “Certificació del Producte al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació”	16
4.2	Segona Opció – Certificació Internacional del Producte	16
4.3	Tercera Opció - Certificació de Conformitat amb l'Esquema Nacional de Seguridad (ENS) per part de la empresa subministradora del producte	16
4.4	Quarta Opció – Auditoria de Seguretat	16
4.5	Cinquena Opció – Declaració de Responsabilitat Legal i Qüestionari de Seguretat	17
4.6	Recordatori Documentació Tècnica exigible	21
5	Avaluació d'Impacte	21

Introducció i objectius

Aquest document té com a objectiu informar dels requisits de seguretat que haurà de complir qualsevol servei i/o producte amb característiques IT o OT que es vulgui implantar a l'organització Hospital Clínic de Barcelona en compliment dels requisits exigits per l'Esquema Nacional de Seguretat (ENS en endavant).

Abast

Establir els criteris de seguretat necessaris per a garantir que tots els serveis i productes que necessitin ser desplegats o integrats a la corporació Hospital Clínic ho faci amb un nivell òptim de seguretat i garantint en la mesura de lo possible l'acompliment normatiu vigent.

El document pretén incloure la casuística de compliment com de no compliment de la legalitat vigent, en aquest cas respecte de l'ENS, de les diferents casuístiques.

Aquest document aplica a qualsevol procés de contractació o compra de productes i serveis IT/OT. En el cas de productes, es consideraran dins de l'abast tant els sistemes de TI com l'equipament OT (IoMT, IoT).

Entenem com a productes i serveis IT/OT (IoMT) tots aquells que:

- Es connecten a la xarxa de l'hospital Clínic (LAN/WAN/WIFI)
- Requereixen de la connexió telemàtica d'un professional/servei/sistema de l'hospital per a la realitzar activitat professional de l'hospital (producte/servei extern)

En el cas de la incorporació de productes, s'han de presentar les evidències d'acord amb l'opció d'acreditació escollida i aportar la documentació necessària que ho certifiqui.

Aspectes Generals de Seguretat per a Serveis

Davant del procés de contractació i incorporació d'un servei a l'àmbit d'IT o OT cal seguir en tot moment el principi de professionalitat, segons l'article 16 de l'ENS:

- La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.
- Les organitzacions que prestin serveis a l'Hospital Clínic de Barcelona han de comptar amb professionals qualificats i amb uns nivells idonis de gestió i maduresa en els serveis prestats.
- Es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del lloc de treball.

Requisits per a la contractació de Serveis d'Implantació d'Infraestructura i programari tant IT com OT

En el cas de serveis, cal presentar Certificat de Conformitat amb l'ENS relatiu al servei que es pretén prestar amb la categoria d'acord amb la sol·licitud. Per defecte es sol·licitarà per a la provisió de serveis que sustentin les activitats principals del Clínic un certificat de nivell MITJÀ com a mínim.

Aquest requisit aplica a qualsevol implantació d'infraestructura d'IT i OT, com per exemple xarxes, emmagatzemament, servidors, dispositius de còpies de seguretat i altres elements d'infraestructura, aparells d'electromedicina o de manteniment. etc. Aplica tanmateix al desplegament d'elements de programari específics de suport a la infraestructura tecnològica o de suport a negoci.

Detall de requisits de components subministrats a la contractació de Serveis On Premise

Qualsevol component o producte subministrat dins el servei caldrà que compleixi els criteris indicats a l'apartat 4. Aspectes Generals de Seguretat per a Productes.

Adicionalment, El Clínic podrà requerir del proveïdor, a més a més del Certificat de Conformitat amb l'ENS del servei contractar, el detall de la Declaració d'Aplicabilitat i mesures utilitzades, per garantir que els components proveïts garanteixin els requisits de l'ENS.

Subcontractació

L'entitat proveïdora del servei haurà de disposar d'una documentació que detalli clarament els elements que formen part de la cadena de subcontractació, així com implicacions derivades de qualsevol canvi o modificació que pugui patir algun esglaó d'aquesta cadena.

El proveïdor haurà d'assegurar que els sistemes d'informació de les empreses subcontractades són conformes amb l'ENS pel que fa als serveis que afectin al Clínic, per la qual cosa el contingut del present document resultarà així mateix d'aplicació a la cadena de subministrament del proveïdor.

En aquest sentit, el Clínic podrà requerir del prestador, a més de la corresponent Certificació de Conformitat amb l'ENS, el detall de la Declaració d'Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries de vigilància utilitzades.

Requisits de serveis de Desenvolupament de Programari

Es presenten els requisits específics per a aquest tipus de Servei, segons ENS, nivell MITJÀ com a mínim:

- Desenvolupament Mitjançant Metodologia de Desenvolupament de Programari Segur:

mp.sw	Protecció de les aplicacions informàtiques	Dimensió	BAIX	MITJÀ	ALT
mp.sw.1	Desenvolupament de programari	Categoria	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Acceptació i posada en servei	Categoria	aplica	+ R1	+ R1

Requisits.

- [mp.sw.1.1] El desenvolupament d'aplicacions es realitzarà sobre un sistema diferent i separat del de producció, no havent d'existir eines o dades de desenvolupament en l'entorn de producció, ni dades de producció en el de desenvolupament.

Reforç R1-Mínim privilegi.

- [mp.sw.1.r1.1] Les aplicacions es desenvoluparan respectant el principi de mínim privilegi, accedint únicament als recursos imprescindibles per a la seva funció, i amb els privilegis que siguin indispensables.

Reforç R2-Metodologia de desenvolupament segur.

- [mp.sw.1.r2.1] S'aplicarà una metodologia de desenvolupament segur reconeguda que:
 - a) Tindrà en consideració els aspectes de seguretat al llarg de tot el cicle de vida.
 - b) Inclourà normes de programació segura, especialment: control d'assignació i alliberament de memòria, desbordament de memòria (*overflow*).
 - c) Tractarà específicament les dades usades en proves.
 - d) Permetrà la inspecció del codi font.

S'haurà de tenir en compte la guia de Desenvolupament Segur del CCN quan es tractin de desenvolupaments Web "CCN-STIC-812 Guia de Seguretat en Entorns i Aplicacions Web" així com la guia relativa a desenvolupament segur "CCN-CERT Recomanacions sobre desenvolupament segur"

Reforç R3-Seguretat des del disseny.

- [mp.sw.1.r3.1] Els següents elements seran part integral del disseny del sistema:
 - a) Els mecanismes d'identificació i autenticació.
 - b) Els mecanismes de protecció de la informació tractada.
 - c) La generació i tractament de pistes d'auditoria.

Reforç R4-Dades de proves.

- [mp.sw.1.r4.1] Preferiblement, les proves prèvies a la implantació o modificació dels sistemes d'informació no es realitzaran amb dades reals. En cas que fos necessari recórrer a dades reals es garantirà el nivell de seguretat corresponent.

Reforç R5-Llista de components programari.

- [mp.sw.1.r5.1] El desenvolupador elaborarà i mantindrà actualitzada una relació formal dels components programari de tercers emprats en l'aplicació o producte. Es mantindrà un històric dels components utilitzats en les diferents versions del programari. El contingut mínim de la llista de components, que contindrà, almenys, la identificació del component, el fabricant i la versió emprada.

- Protecció de les Comunicacions en el Desenvolupament:

Caldrà que el desenvolupament tingui en compte el compliment del requisits relatius a les comunicacions:

mp.com	Protecció de les comunicacions	Dimensió	BAIX	MITJÀ	ALT
mp.com.2	Protecció de la confidencialitat	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protecció de la integritat i de l'autenticitat	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separació en fluxos d'informació a la xarxa	Categoria	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4

Documentació general del sistema segons:

El desenvolupament ha d'incloure una descripció de la seva arquitectura de sistemes, si escau i la manera en que compleix els requisits d'arquitectura de seguretat.

op.pl.2	Arquitectura de Seguretat	Categoria	aplica	+ R1	+ R1 + R2 + R3
---------	---------------------------	-----------	--------	------	----------------

- Protecció dels Serveis desenvolupats:

Caldrà que el desenvolupament tingui en compte el compliment dels requisits relatius a la protecció de serveis i aplicatius web.

mp.s.2	Protecció de serveis i aplicacions web	Categoria	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
--------	--	-----------	-------------	-------------	-----------

Serveis al Núvol

Adicionalment si el servei ofert es tracta de serveis al núvol l'adjudicatari haurà de:

- Complir les guies del CCN-STIC (Centre Criptològic Nacional) ja siguin en modalitat IaaS, PaaS o SaaS vigents aplicables en funció de la modalitat relatives a la gestió, manteniment, configuració, administració, disseny i explotació
- Realitzar auditories de proves de penetració.
- Ser transparent en quant a facilitar informació relativa al servei i infraestructures prestada
- Utilitzar xifratge de dades i gestionar les claus d'acord amb les guies del CCN-STIC
- Facilitar una avaluació d'impacte associada al servei que es presta

Excepcions

Com a excepció, si l'entitat licitadora no disposés dels requisits anteriors, s'acceptarà el disposar de la certificació sobre l'abast del servei mitjançant ISO 27001 o un certificat de Nivell MITJA com a mínim de l'ENS.

No obstant això, en cas que una d'aquestes sigui l'opció escollida, l'empresa proveïdora **haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell MITJA com a mínim.**

Adicionalment, si es fa servir aquesta excepció, es requerirà s'aporti informació necessària sobre el sistema que suporta els serveis, respecte a la arquitectura de seguretat. Així mateix, aportarà els diagrames de xarxa, esquemes d'elements físics, esquemes de interconnexió i esquemes lògics de sistemes que mostrin al Clínic, la infraestructura física i lògica de la qual forma part el servei objecte de contractació. Tanmateix es requerirà una Declaració d'Aplicabilitat segons els requisits de l'Annex II de l'ENS per conèixer com compleix la solució aportada cadascun dels requisits, si li aplica o no i en cas d'haver-hi responsabilitats creuades entre el Clínic i el proveïdor, com està pensat s'organitzi i es doni suport a cadascuna de les mesures.

Aspectes Generals de Seguretat per a Productes

Per a productes de TI i OT, els dispositius del sistema han de tenir una configuració de seguretat adequada per garantir el control del flux definit d'entrada i sortida de la informació. Els dispositius presents a la xarxa que disposin d'algun tipus d'emmagatzematge temporal o d'informació permanent proporcionaran la funcionalitat necessària per eliminar informació de suports d'informació.

Per garantir que el producte o productes implantats a l'entitat Hospital Clínic de Barcelona compleix les directrius de seguretat mínimes, qualsevol producte haurà de complir algun dels següents requisits per ordre de rellevància:

4.1 Primera Opció – “Certificació del Producte al Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació”

Si el producte ja està a la llista del Catàleg CPSTIC de productes Qualificats segons la “Guia de Seguretat de les TIC CCN-STIC 105” caldrà remetre el certificat corresponent emès per entitat acreditada.

En cas de no complir amb el requisit anterior s'ha de complir amb alguna de les opcions presentades a continuació, exposats per ordre de preferència.

4.2 Segona Opció – Certificació Internacional del Producte

El producte o la solució amb qualsevol característica IT haurà d'estar certificada en alguna homologació nacional o internacional de seguretat.

Llistat de Certificacions admissibles:

- Common Criteria CC/CEM v3.1 (CC= Common Criteria for Information Technology Security Evaluation): EAL3
- SOGIS MRA v3 (Senior Officers Group for Information Systems, Mutual Recognition Agreement), per:
 - Smartcards and Similar Devices - Aquest domini tècnic està relacionat amb les targetes intel·ligents i dispositius similars.
 - Hardware Devices with Security Boxes - Aquest domini tècnic està relacionat amb productes compostos per una o més plaques de circuit imprès on gran part de la funcionalitat de seguretat requerida depèn del seu embolcall físic (l'anomenada Caixa de Seguretat)

4.3 Tercera Opció - Certificació de Conformitat amb l'Esquema Nacional de Seguridad (ENS) per part de la empresa subministradora del producte

Aquesta opció es vàlida si l'empresa que fabrica el component físic o de programari disposa de Certificació de Conformitat amb l'ENS per fabricar el dispositiu o programari corresponent, amb el nivell MITJA com a mínim.

En aquest sentit, l'Hospital Clínic de Barcelona podrà requerir del prestador, a més de la corresponent Certificació de Conformitat amb l'ENS de l'empresa, el detall de la Declaració d'Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries que implementa el component aportat.

4.4 Quarta Opció – Auditoria de Seguretat

Disposar d'un informe d'Auditoria de Seguretat de la informació aportat per una entitat certificada en el camp de la seguretat de la informació amb certificació ISO 27001 o ENS nivell MITJA, amb els resultats recents com a màxim de sis mesos, en què no es detectin riscos ni vulnerabilitats de nivell crític ni alts.

Aquesta auditoria ha de ser del tipus caixa blanca, presentant contra quins marcs de seguretat s'han realitzat, presentant un resum executiu del resultat i haurà d'indicar segons els criteris de l'article 19 de

l'ENS i els criteris de la Guia "CCN-STIC 140 Taxonomia de referència per a productes de seguretat TIC", si es considera:

- Favorable
- Favorable amb NO confirmades (en tal cas incloure Pla d'Accions Correctives)

Adicionalment, l'Hospital Clínic de Barcelona podrà requerir del prestador, el detall de la Declaració d'Aplicabilitat i, si s'escau, de les mesures compensatòries i complementàries que implementa el component aportat

En cas que aquesta sigui l'opció escollida per garantir el nivell de seguretat del producte, l'empresa proveïdora haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell Mitjà com a mínim.

4.5 Cinquena Opció – Declaració de Responsabilitat Legal i Qüestionari de Seguretat

S'haurà d'emplenar el següent formulari associat a les característiques del producte o productes oferts, per conèixer el grau de compliment de seguretat que ofereix, i el pla d'acció que prendrà l'oferent per solucionar-lo en cas de no complir els requisits.

Aquest formulari haurà d'anar acompanyada d'una declaració de responsabilitat signada per l'apoderat de l'entitat proveïdora avalant la veracitat de les dades proporcionades per part del proveïdor relatiu al nivell de compliment dels requisits de seguretat del producte.

S'hauran d'aportar per a cada apartat els detalls i evidències suficients per corroborar el compliment del requisit. Els aspectes per valorar són els següents:

- **El producte incorpora canals de comunicació fiables i assegurances:** Cal establir canals de comunicació segurs entre les parts utilitzant algorismes i protocols segons la guia CCNSTIC-807 (ex.: HTTPS/TLS 1.2 o superior, IPSEC, etc.).

Compleix requisits: **SI** ☐ **NO** ☐
En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte s'executa sobre una plataforma fiable:** incloent-hi el sistema operatiu o qualsevol entorn d'execució i dependència sobre el qual s'utilitzi. Les versions de les plataformes i productes relacionats han de ser les recomanades per les guies de seguretat CCN-STIC.

- Seran admissibles, encara que no recomanables, versions que estiguin properes al seu cicle de vida i que encara tinguin suport amb actualitzacions de seguretat, amb el compromís d'evolucionar a versions superiors i suportades.
- En cap cas no s'acceptaran versions o dependències sense suport del fabricant o fora del seu cicle de vida.

Compleix requisits: **SI** ☐ **NO** ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte té la capacitat anti-explotació:** *Depenent de l'àmbit del producte s'autoprotegirà quan estigui en execució, per exemple: protecció contra atacs de força bruta, protecció contra manipulacions, protecció contra manipulació de fitxers, etc. El producte ha d'estar configurat amb els permisos més restrictius, sense permisos d'accés a fitxers de manera anònima i protegir els accessos no autoritzats.*

Compleix requisits: **SI** ☐ **NO** ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte tindrà actualitzacions periòdiques per evitar vulnerabilitats i obsolescència:** *El desenvolupament del producte serà actualitzat pel proveïdor durant el cicle de vida d'aquest mantenint-lo certificat en versions suportades dels elements que componen la solució global, i comunicarà les actualitzacions evolutives o que corregeixin vulnerabilitats conegudes a fitxers i protegir els accessos no autoritzats.*

Compleix requisits: *SI* ☐ *NO* ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte aporta restriccions d'accés a àrees restringides:** *El producte ha de controlar l'accés a la interfície de gestió i control d'usuaris amb accés restringit mitjançant sessions no manipulables.*

Compleix requisits: *SI* ☐ *NO* ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte no permet la possibilitat d'injecció de codi:** *El producte ha de controlar que els paràmetres rebuts per part de l'usuari siguin correctes i no permetin la injecció de codi o manipulació de dades.*

Compleix requisits: *SI* ☐ *NO* ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte us permet assegurar una política de contrasenyes robustes:** *El producte ha de contenir un sistema de control i gestió d'autenticació mitjançant contrasenyes segures i/o certificats digitals.*

Compleix requisits: *SI* ☐ *NO* ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte incorpora un mètode de xifratge:** El producte ha de contenir un sistema de xifratge que garanteixi la protecció de dades sensibles.

Compleix requisits: SI ☐ NO ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte permet utilitzar usuaris d'administració nominals:** El producte ha de treballar amb usuaris nominals i no es permetran comptes genèrics o compartits.

Compleix requisits: SI ☐ NO ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

- **El producte incorpora capacitat d'auditoria:** El producte ha de permetre el control de sessions, la traçabilitat de les accions dels usuaris i administradors.

Compleix requisits: SI ☐ NO ☐

En cas de no complir indicar el pla d'acció:

Data prevista del compliment: __/__/__

Un cop rebudes les evidències i les respostes a cadascun dels punts, en cas d'incompliment de tres o més requisits que apliquin a la solució proposada es considerarà el producte com a NO APTE. Quan l'incompliment sigui d'un o dos punts, l'adjudicatari haurà de donar solució en temps d'implantació i en coordinació amb l'equip tècnic de l'Hospital Clínic de Barcelona. En cas que algun d'aquests requisits no apliqui s'hauran d'exposar els motius.

En cas que aquesta sigui l'opció escollida per garantir el nivell de seguretat del producte, l'empresa proveïdora haurà de presentar el pla d'adequació a l'Esquema Nacional de Seguretat en nivell Mitjà com a mínim.

4.6 Recordatori Documentació Tècnica exigible

Es recorda que qualsevol producte amb connexions de TI o OT ha d'incorporar com a documentació:

- Guies d'Instal·lació Segura
- Llistat de Components programari i maquinari que el constitueixen
- Proposta de Pla d'actualitzacions per cobrir elements obsolets de programari

Avaluació d'Impacte

Per complir els requisits que es desprenen de la legislació de protecció de dades personals vigent, en cas que, per tipologia de dades personals, finalitat, emplaçament de l'adjudicatari, quantitat de dades, tecnologia nova o qualsevol circumstància que aconselli realitzar una avaluació d'impacte sobre la privadesa, es traslladarà a l'adjudicatari l'obligació de realitzar aquesta avaluació, seguint les indicacions del delegat de protecció de dades de l'HCB per detectar els riscos derivats del tractament de dades personals.