

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DELS SERVEIS D'INTEGRACIÓ INFORMÀTICA AMB EL NOU SISTEMA D'INFORMACIÓ HOSPITALÀRIA (HIS) SAP ARGOS, AMB DESTÍ ALS CENTRES DEL CONSORCI MAR PARC DE SALUT DE BARCELONA

1. OBJECTE DEL CONTRACTE

L'objecte del contracte correspon al desenvolupament dels serveis d'integració informàtica necessaris per garantir la interoperabilitat entre diferents sistemes clínics i logístics actualment operatius al Consorci Mar Parc de Salut de Barcelona (CMPSPB) i el nou Sistema d'Informació Hospitalària (HIS) SAP Argos.

Aquesta integració és essencial per assegurar:

- La traçabilitat completa del medicament i processos clínics.
- La seguretat del pacient, evitant duplicitats i errors de medicació.
- L'eficiència operativa, automatitzant fluxos de treball manuals.
- La coherència de dades entre sistemes (demogràfics, clínics i logístics).

Els serveis objecte d'aquest contracte inclouen, per a cada lot, l'anàlisi tècnic, desenvolupament d'interfícies (HL7/FHIR, Web Services, APIs), proves d'integració, validació funcional, documentació tècnica i suport durant el període de garantia.

2. LOTS I ABAST DEL CONTRACTE

2.1 Estructura en lots

El contracte s'estructura en 5 lots independents, cadascun amb un objecte tècnic específic i un proveïdor convidat únic degut a motius d'exclusivitat tècnica (propietat intel·lectual, codi font tancat o certificació de fabricant). Cada lot s'executarà de manera independent, sense que l'adjudicació d'un condicioni la resta.

- Lot 1: Integració sistema ATHOS DOSYS ↔ SAP Argos.
- Lot 2: Integració sistema GOTA® (teràpia anticoagulante) ↔ SAP Argos.
- Lot 3: Integració plataforma IntelliSpace Perinatal (ISP) ↔ SAP Argos.
- Lot 4: Migració de servidor i actualització iECG ↔ SAP Argos.
- Lot 5: Serveis d'integració transversals ViewPoint ↔ SAP Argos.

2.2 Estructura en lots

Cada proveïdor haurà de desenvolupar les actuacions següents per al lot corresponent:

LOT 1: Integració ATHOS DOSYS (APD)

- Desenvolupament d'interfícies per a la sincronització del catàleg de medicaments entre ATHOS DOSYS i SAP Argos.
- Integració del cens de pacients per a la dispensació nominativa.
- Intercanvi de moviments i transaccions de medicació per a la traçabilitat.
- Validació funcional de les dades intercanviades i resolució d'incidències durant el període de proves.

LOT 2: Integració GOTA® (Werfen)

- Implementació de la connexió entre el Sistema d'Informació GOTA® (gestió de teràpia anticoagulant) i SAP Argos.
- Intercanvi de dades clíniques rellevants per al seguiment del pacient anticoagulat.
- Configuració dels canals de comunicació segurs garantint la confidencialitat de les dades sanitàries.
- Formació als usuaris finals sobre el nou flux d'integració.

LOT 3: Integració IntelliSpace Perinatal (ISP) (Dextro Médica)

- Actualització de la integració demogràfica utilitzant el cens de SAP Argos com a font principal.
- Desenvolupament i implementació del partograma corporatiu alineat amb els estàndards de SAP Argos.
- Implementació d'un applink de verificació de camps per garantir la qualitat de la dada clínica.
- Integració dels documents d'alta i traça de part dins del flux de treball corporatiu.

LOT 4: Migració Servidor + iECG (Dextro Médica)

- Instal·lació i configuració de l'aplicació en Windows Server 2019.
- Instal·lació de la instància de base de dades i migració de la base de dades actual sense pèrdua d'informació.
- Actualització de l'aplicatiu iECG a la versió compatible amb el nou entorn.
- Posada en funcionament i validació de la connectivitat amb SAP Argos per a la recuperació de proves.

LOT 5: Integracions Transversals ViewPoint (HNC-Salud Conectada España)

- Configuració i manteniment del motor d'integració (Mirth Connect) per a la gestió de cues i missatgeria HL7/FHIR.
- Implementació de llicències de Desktop Integration per a la connexió de dispositius locals amb el HIS.
- Serveis de manteniment evolutiu i correctiu de les interfícies durant el període contractat (48 mesos segons oferta).
- Suport tècnic per a la resolució d'incidències de connectivitat general.

2.3 Criteris tècnics d'implementació

Atesa la naturalesa exclusiva de cada sistema i per garantir la màxima eficiència tècnica, s'estableixen els següents criteris oberts:

- Estàndards d'integració: El proveïdor proposarà l'estàndard de comunicació més adequat (HL7 v2, FHIR, Web Services, APIs propietàries, etc.) sempre que garanteixi la seguretat, l'escalabilitat i la compatibilitat amb l'arquitectura de SAP Argos. Aquesta proposta haurà de ser validada pel Servei d'Informàtica del CMPSB abans del desenvolupament.
- Entorns de proves: No s'exigeix la disposició d'un entorn sandbox específic per part del proveïdor. Les proves es realitzaran en els entorns de pre-producció i producció del CMPSB, sota supervisió del Servei d'Informàtica. El proveïdor haurà de garantir que les

integracions no afectin la disponibilitat dels sistemes en producció durant la fase d'implementació.

- Seguretat: Totes les comunicacions hauran de realitzar-se a través de canals xifrats i seguint les polítiques de seguretat de la informació del CMPSB (RGPD, LOPdGDD).

3. REQUISITS TÈCNICS GENERALS I COMPLIMENT NORMATIU

3.1. Seguretat i Protecció de Dades

- Canals xifrats: Totes les comunicacions hauran d'utilitzar TLS 1.2 o superior.
- Accés remot: Només amb autorització prèvia del Servei d'Informàtica del CMPSB i traça d'auditoria.
- Dades sanitàries: Tractament conforme RGPD/LOPDGDD. Ús de dades fictícies/anonimitzades per a proves, llevat d'autorització expressa.
- Confidencialitat: NDA obligatori per a tot el personal del proveïdor amb accés a informació del CMPSB.

3.2. Propietat Intel·lectual i Lliurables

- El proveïdor manté la propietat del seu programari base.
- El CMPSB disposarà de llicència d'ús perpètua per a les interfícies desenvolupades.
- Documentació mínima a lliurar (format digital):
 - o Especificació tècnica de la interfície (fluxos, formats, freqüència).
 - o Mapatge de dades (origen ↔ destí SAP Argos).
 - o Manual d'explotació (monitoratge, gestió d'errors).

3.3. Acceptació del Servei

- La recepció definitiva es formalitzarà mitjançant acta signada pel Servei d'Informàtica del CMPSB, un cop verificat el correcte funcionament de la integració en entorn de producció.

4. METODOLOGIA D'IMPLEMENTACIÓ (COMÚ A TOTS ELS LOTS)

4.1. Fases del projecte

Cada proveïdor haurà de seguir les fases següents per a l'execució del lot adjudicat:

Fase	Activitats principals	Lliurable
1. Anàlisi	Revisió de fluxos, mapatge de dades, definició d'abast	Document d'Especificacions Tècniques
2. Desenvolupament	Configuració d'interfícies i proves unitàries	Entorn de proves funcional
3. Validació	Proves d'integració amb SAP Argos	Certificat de proves signat
4. Posada en producció	Desplegament en entorn real, acompanyament inicial	Acta de recepció provisional
5. Tancament	Lliurament de documentació, formació (si escau), recepció definitiva	Documentació tècnica completa

4.2. Terminis d'execució

- Termini màxim per lot: 2 mesos des de la formalització del contracte.

4.3. Coordinació amb el CMPSB

- Designació d'un responsable tècnic de referència per part del proveïdor.
- Reunions de seguiment (presencials o telemàtiques) durant la fase de desenvolupament.
- Canal únic de comunicació per a incidències: Servei d'Informàtica del CMPSB.

4.4. Gestió de canvis

- Qualsevol modificació de l'abast inicial haurà de ser sol·licitada per escrit i autoritzada pel CMPSB abans de la seva execució.
- Els canvis no autoritzats no seran objecte de pagament addicional.

5. 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.

El proveïdor haurà de seguir les directrius de l'Agència de Ciberseguretat de Catalunya en matèria de seguretat de la informació.

5.1. 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.

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.

5.2 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.

5.3 Mesures organitzatives

L'empresa adjudicatària informará al tècnic encarregat del desenvolupament dels serveis d'integració informàtica assignat al projecte, 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 del CMPSB.

5.4 Altres requeriments de seguretat

És fonamental que l'adjudicatari assoleixi entre d'altres, els següents objectius:

- La correcta implantació de la seguretat de la informació al llarg de tot el seu cicle de vida.
- El seguiment de la política marcada per l'Agència de Ciberseguretat de Catalunya per garantir la correcta implantació del model de seguretat en el manteniment d'aplicacions, involucrant als equips de seguretat des de l'inici del servei, fent les proves que siguin necessàries i seguint les pautes marcades en general.
- La implementació de les mesures necessàries per l'acompliment de la legislació vigent en matèria de seguretat en funció de la classificació d'informació de les aplicacions.
- La implantació dels controls de seguretat que permetin mitigar els riscos als quals està exposada l'aplicació i tots els actius dels quals en depèn.

Donada la naturalesa canviant de les amenaces de seguretat, la pròpia evolució tecnològica i els canvis que es puguin produir, l'empresa adjudicatària haurà d'adequar els controls i les mesures de seguretat durant l'execució del servei si fos necessari. De forma general, és fonamental que les mesures de seguretat a desplegar per l'empresa adjudicatària permetin fer front a, com a mínim, amenaces del tipus:

- Robatori d'informació, amb el posterior impacte al negoci i legal (com la RGPD).
- Intrusió als equips, canvis de configuració/seguretat per agafar-ne el control.
- Robatori de credencials dels usuaris.
- Explotació de les vulnerabilitats de les aplicacions desenvolupades o evolutius.
- Interceptar el tràfic de xarxa per la captura d'informació (DNS spoofing, HTTPS spoofing, entre altres).
- Incompliment legal. Per exemple, incompliment de la RGPD per accés a dades personals dels usuaris.
- Provocar una denegació del servei.
- Accés per part d'administradors/desenvolupadors no autoritzats o per un ús il·legítim. Ús no autoritzat de recursos.
- Errors dels administradors/desenvolupadors del servei. Per exemple, configuracions errònies, mesures de seguretat mal aplicades, entre d'altres.
- Accessos remots no controlats. Els atacants podrien aprofitar mecanismes d'accés remot febles (per exemple, VPN amb contrasenyes febles).
- Enginyeria social per accedir a informació confidencial del personal que presta el servei.

Els estàndards vigents es podran consultar al portal de seguretat de l'Agència de Ciberseguretat de Catalunya.

6. GARANTIA POST-IMPLEMENTACIÓ:

Un cop signada l'acta de recepció conforme i efectuat el pagament, el proveïdor romandrà obligat a garantir el correcte funcionament de la integració desenvolupada durant un període mínim de 12 mesos, durant el qual haurà de corregir, sense cost addicional per al CMPSB, qualsevol defecte funcional o error d'interoperabilitat atribuïble al desenvolupament executat.

Barcelona, a data de la signatura electrònica

Jordi Mediavilla de Haro

Cap del CAU i Logística de SSII del CMPSB