PLEC TÈCNIC PER A LA CONTRACTACIÓ D'UN SERVEI DE DESENVOLUPAMENT I MANTENIMENT DE PROGRAMARI PER A L'HOSPITAL UNIVERSITARI DOCTOR JOSEP TRUETA, PER A LA GERÈNCIA D'ATENCIÓ PRIMÀRIA DE L'ICS GIRONA, I PER A L'INSTITUT D'ASSISTÈNCIA SANITARIA (IAS)

1 OBJECTE DE LA CONTRACTACIÓ

El present contracte té per objecte la prestació d'un servei integral de desenvolupament i manteniment de programari per a l'entitat contractant, mitjançant la contractació d'una bossa anual de serveis especialitzats en desenvolupament d'aplicacions web i aplicacions mòbils. Els centres destinataris d'aquest servei seran per una banda l'ICS Girona amb l'Hospital Universitari Doctor Josep Trueta de Girona (HUDJT) i la Gerència d'Atenció Primària i Comunitària de Girona (GAPICGI), i per altra banda l'Institut d'Assistència Sanitària (IAS).

L'objectiu principal és complementar la capacitat interna de desenvolupament de les Unitats de Tecnologies de la Informació i Comunicació (UTIC) dels centres, proporcionant suport extern especialitzat per fer front a l'augment de demandes TIC i assegurar la continuïtat i evolució dels sistemes d'informació existents.

El servei inclou tant el desenvolupament de noves aplicacions com el manteniment evolutiu, correctiu i normatiu dels programaris existents, sempre seguint les millors pràctiques de desenvolupament, assegurant la qualitat del codi, la seva documentació adequada i la realització de proves exhaustives.

Les prestacions contractades han de permetre:

- Donar resposta ràpida i eficient a les necessitats de desenvolupament de programari dels centres
- Mantenir i evolucionar les aplicacions existents segons les necessitats dels centres
- Implementar les millors pràctiques de desenvolupament i assegurar la qualitat del codi
- Proporcionar documentació tècnica adequada
- Assegurar la transferència de coneixement cap a les UTIC internes

2 DESCRIPCIÓ DEL SERVEI

2.1 Situació actual

Actualment, tant en l'àmbit ICS (HUDJT i GAPICGI) com en l'àmbit IAS, els sistemes d'informació i aplicatius utilitzats poden estar basats en productes comercials mantinguts per les empreses proveïdores que en tenen la propietat, com en desenvolupaments a mida realitzats des de les pròpies Unitats de Tecnologies de la Informació i Comunicació (UTIC) dels centres.

En el cas dels desenvolupaments a mida, la UTIC és la responsable de la presa de requeriments funcionals amb els usuaris clau per poder dur a terme el desenvolupament del programari demanat. És també responsabilitat de la UTIC assegurar el manteniment evolutiu, correctiu i normatiu d'aquests programaris, garantint la seva correcta operativitat i adaptació a les necessitats canviants de l'organització.

No obstant això, el ràpid augment de demandes TIC en els centres, juntament amb el creixement vegetatiu de les infraestructures i també de les estructures de professionals dins dels centres, provoca que cada cop les necessitats de nous desenvolupaments i manteniments dels programaris existents creixin a un ritme

molt elevat. Aquest increment exponencial de la demanda genera una situació en què les UTIC no són capaces de donar resposta a tota la demanda rebuda amb els recursos interns disponibles.

La situació actual es caracteritza per:

- Una demanda creixent de nous desenvolupaments i funcionalitats
- Necessitats de manteniment i evolució dels sistemes existents
- Recursos interns limitats per fer front a tota la demanda
- Temps de resposta que no sempre s'ajusten als requeriments dels usuaris
- Necessitat d'especialització en noves tecnologies i metodologies

Per aquest motiu, es vol fer un canvi d'orientació en el desenvolupament i manteniment del programari, contractant un servei extern que complementi la capacitat interna de desenvolupament i manteniment, permetent així una resposta més àgil i eficient a les necessitats tecnològiques dels centres.

2.2 Abast del servei

El servei s'haurà d'entregar en tres centres:

- **ICS Girona**: Hospital Universitari Doctor Josep Trueta (HUDJT)
- **ICS Girona:** Gerència d'atenció primària i comunitària de Girona (GAPiCGI)
- **IAS**: Institut d'Assistència Sanitària

Per tant la licitació s'organitzarà en tres centres:

CENTRE	DESCRIPCIÓ	CENTRE FINANÇADOR
1	Servei de desenvolupament i manteniment de programari per al HUDJT	ICS Girona (HUDJT)
2	Servei de desenvolupament i manteniment de programari per a la GAPiCGI	ICS Girona (GAPiCGI)
3	Servei de desenvolupament i manteniment de programari per a l' Institut d'Assistència Sanitària (IAS).	IAS

Per cada un dels centres es contracta el següent volum de desenvolupament i manteniment de programari, en total 2.000 hores de desenvolupament i manteniment de programari:

CENTRE	DESCRIPCIÓ	Volum d'hores
1	Servei de desenvolupament i manteniment de programari per al HUDJT	500
2	Servei de desenvolupament i manteniment de programari per al GAPiCGI.	500
3	Servei de desenvolupament i manteniment de programari per a l' Institut d'Assistència Sanitària (IAS).	1.000

El servei contractat comprèn les següents prestacions principals:

2.2.1 Desenvolupament de Nova Funcionalitat

- Desenvolupament d'aplicacions web responsives utilitzant tecnologies modernes
- Desenvolupament d'aplicacions mòbils multiplataforma
- Creació de components reutilitzables i llibreries internes
- Integració amb sistemes existents i APIs externes

2.2.2 Manteniment de Programari Existent

- Manteniment correctiu: Resolució d'errors i incidències detectades
- Manteniment evolutiu: Desenvolupament de noves funcionalitats i millores
- Manteniment normatiu: Adaptació a canvis legislatius i normatius
- Manteniment adaptatiu: Adequació a canvis en l'entorn tecnològic

2.2.3 Disseny

- Disseny d'arquitectura d'aplicacions
- Disseny de bases de dades i models de dades
- Disseny d'interfícies d'usuari (UI/UX)
- Elaboració de prototips i maquetes

2.2.4 Assegurament de la Qualitat

- Realització de proves unitàries, d'integració i sistema
- Proves de rendiment i càrrega
- Auditories de codi (code review)
- Proves d'usabilitat i accessibilitat
- Validació amb usuaris finals

2.2.5 Documentació

- Documentació tècnica de generació automàtica del codi
- Documentació d'APIs i serveis web
- Procediments de desplegament i configuració
- Plans de proves i resultats

2.2.6 Formació i Transferència de Coneixement

- Formació als equips interns en les tecnologies utilitzades

- Transferència de coneixement sobre els desenvolupaments realitzats
- Sessions de traspàs i documentació de processos
- Suport en la resolució de dubtes tècnics

El servei es prestarà mitjançant una bossa anual de 1.000 hores per als centres de l'ICS i 1.000 hores per a l'IAS (2.000 hores en total), distribuïdes segons les necessitats i prioritats establertes per l'entitat contractant. La gestió i assignació d'aquestes hores es farà de manera flexible, permetent adaptar-se a les demandes puntuals i estacionals dels centres.

3 Requeriments del servei

El servei de desenvolupament i manteniment de programari ha de complir amb els següents requeriments:

3.1 Aplicacions Web

Les aplicacions web desenvolupades han de complir amb els següents requeriments funcionals:

3.1.1 Interfície d'Usuari

- Disseny *responsive* que s'adapti a diferents dispositius (desktop, tablet, mòbil)
- Interfície intuïtiva
- Suport per a múltiples idiomes (català, castellà com a mínim)
- Integració amb sistemes d'autenticació corporatius (LDAP, Active Directory)
- Gestió de rols i permisos d'usuari granular

3.1.2 Funcionalitats Comunes

- Sistema de notificacions en temps real
- Generació d'informes i exportació de dades (PDF, Excel, CSV)
- Sistema d'auditoria i log d'accions dels usuaris
- Funcionalitats de cerca avançada i filtrat
- Gestió de fitxers i documents adjunts
- Workflow i aprovacions automatitzades

3.2 Aplicacions Mòbils

Les aplicacions mòbils desenvolupades han de disposar de:

3.2.1 Funcionalitats Natives

- Accés a funcionalitats del dispositiu (càmera, GPS, notificacions push)
- Funcionament offline amb sincronització posterior
- Integració amb l'agenda i contactes del dispositiu
- Suport per a biometria (empremta digital, reconeixement facial)

3.2.2 Rendiment i Usabilitat

- Temps de càrrega inferiors a 3 segons
- Navegació fluida i responsive
- Gestió eficient de la memòria i bateria
- Adaptació a les diferents mides de pantalla

3.3 Integració i Interoperabilitat

- Capacitat d'integració amb sistemes existents mitjançant APIs REST o SOAP
- Interoperabilitat amb bases de dades corporatives
- Integració amb serveis de directori corporatiu
- Suport per a Single Sign-On (SSO)
- Capacitat d'exportació/importació de dades en formats estàndard
- Utilització d'estàndards sanitaris (HL7..)
- Integració amb passarel·les de pagament

3.4 Seguretat i Privacitat

- Compliment del Reglament General de Protecció de Dades (RGPD)
- Xifrat de dades sensibles tant en trànsit com en repòs
- Implementació de mesures de seguretat contra atacs comuns (OWASP Top 10)
- Gestió segura de sessions i tokens d'autenticació
- Logs d'auditoria per a compliment normatiu

3.5 Arquitectura i Tecnologies

3.5.1 Frontend Web

- Desenvolupament principalment amb HTML5 i Vue.js 3
- Utilització de CSS amb Bootstrap 5 o Tailwind CSS per al disseny responsive
- Utilització de TypeScript per a major robustesa del codi
- Manteniment d'aplicacions legacy en HTML + jQuery i CSS amb Bootstrap 3

3.5.2 Aplicacions Mòbils

- Desenvolupament amb IONIC + Vue.js, IONIC + ANGULAR
- Compilació per a iOS i Android des d'una única base de codi
- Implementació d'estratègies de cache i sincronització offline

3.5.3 Backend

- Desenvolupament amb PHP 8 o superior utilitzant el framework Laravel 11
- Manteniment d'aplicacions legacy en PHP 7 amb CodeIgniter 3
- Arquitectura basada en APIs RESTful
- Implementació de patrons de disseny actuals
- Implementació de middleware per a autenticació, autorització i logging

3.5.4 Base de Dades

- MariaDB 11.x o MySQL 8.x com a sistema gestor de base de dades principal
- Disseny normalitzat de bases de dades seguint les millors pràctiques
- Implementació d'índexs per a optimització del rendiment
- Estratègies de backup i recuperació
- Migracions de base de dades versionades i reversibles

3.6 Control de Versions i Gestió del Codi

- Utilització obligatòria de Git com a sistema de control de versions
- Repositoris allotjats en Gitea corporatiu
- Repositoris legaxy en Subversion (svn) / Mantis.
- Commits amb missatges descriptius seguint convencions establertes
- Tags per al versionat semàntic (Semantic Versioning)

3.7 Testing i Proves

3.7.1 Tipologies de Proves

- Proves unitàries: Cobertura mínima del 80% del codi
- Proves d'integració: Validació de la interacció entre components
- Proves end-to-end: Simulació completa dels fluxos d'usuari
- Proves de rendiment: Validació dels temps de resposta i throughput
- Proves de seguretat: Detecció de vulnerabilitats i punts febles

3.8 Documentació Tècnica

3.8.1 Documentació del Codi

- Comentaris inline en el codi seguint estàndards PHPDoc i JSDoc
- README.md detallat per a cada projecte amb instruccions d'instal·lació
- Documentació d'arquitectura
- Documentació d'APIs generada automàticament (OpenAPI/Swagger)

3.8.2 Documentació de Processos

- Guies de desenvolupament i convencions de codi
- Procediments de desplegament i configuració
- Plans de proves i casos de test
- Documentació de troubleshooting i resolució d'incidències

3.9 Seguretat

3.9.1 Mesures de Seguretat Obligatòries

- Implementació de HTTPS amb certificats SSL/TLS vàlids
- Protecció contra OWASP Top 10 (injeccions SQL, XSS, CSRF, etc.)
- Validació i depuració de totes les entrades d'usuari
- Gestió segura de sessions i tokens d'autenticació
- Principi de menor privilegi en l'accés a dades i funcionalitats

3.9.2 Compliment Normatiu

- Compliment del Reglament General de Protecció de Dades (RGPD)
- Implementació de logs d'auditoria per a trazabilitat
- Xifrat de dades personals i sensibles
- Procediments de notificació en cas de bretxa de seguretat

4 DESPLEGAMENT DEL SERVEI

4.1 Entorns de Desenvolupament

4.1.1 Entorn de Desenvolupament Local

- Configuració d'entorns locals utilitzant Docker i Docker Compose
- Scripts automatitzats per a la configuració inicial del projecte
- Bases de dades de desenvolupament amb dades de prova anonimitzades
- Documentació detallada per a la configuració de l'entorn local

4.2 Entorns de Prova i Producció

4.2.1 Entorn de Testing

- Entorn idèntic a producció per a la validació de funcionalitats
- Base de dades amb dades anonimitzades representatives
- Accés restringit als equips de desenvolupament i testing
- Procediments automatitzats de desplegament i rollback

4.2.2 Entorn de Producció

- Desplegament en els servidors corporatius de l'ICS i IAS

4.3 Estratègies de Desplegament

4.3.1 Metodologia de Desplegament

- Zero-downtime deployments per a aplicacions crítiques
- Versionat consistent entre frontend, backend i base de dades
- Plans de rollback automatitzats en cas de problemes

4.3.2 Gestió de Configuracions

- Separació clara entre configuracions de desenvolupament, testing i producció
- Gestió segura de secrets i credencials utilitzant vault o similar
- Variables d'entorn per a la parametrització de l'aplicació
- Documentació de totes les configuracions necessàries

4.4 Monitorització i Alertes

4.4.1 Monitorització d'Aplicacions

- Implementació de logs estructurats per a debugging i auditoria
- Monitorització proactiva d'errors i excepcions

4.4.2 Sistema d'Alertes

- Alertes automàtiques per a errors crítics i caigudes de servei
- Notificacions per correu electrònic
- Escalat automàtic segons la criticitat de l'incident

5 ACORDS DE NIVELL DE SERVEI (SLA)

5.1 Qualitat del Codi Lliurat

5.1.1 Documentació

- 100% de les APIs documentades amb OpenAPI/Swagger
- Documentació tècnica actualitzada per a tots els components
- Manuals d'usuari per a funcionalitats noves o modificades
- Comentaris en codi per a funcions complexes (>10 línies)

5.2 Comunicació i Reporting

5.2.1 Informes Regulars

- Informe setmanal: Estat de les tasques en curs i planificació
- Informe mensual: Resum d'activitats, mètriques de qualitat i SLA
- Informe trimestral: Anàlisi de tendències i propostes de millora

6 ORGANITZACIÓ DE L'EQUIP

6.1 Estructura de l'Equip del Proveïdor

6.1.1 Rols Obligatoris

El licitador haurà de proporcionar de manera obligatòria en el seu equip professionals amb els següents rols:

- Desenvolupador Senior Frontend
- Desenvolupador Senior Backend

6.1.2 Rols opcionals

Es requerirà al licitador que pugui oferir de manera opcional, professionals amb els següents rols:

- Cap de Projecte: Responsable de la coordinació general i comunicació amb l'entitat
- Analista Funcional: Responsable de l'anàlisi de requeriments i disseny funcional

El consum d'hores d'aquest tipus de professionals en el projecte es farà en base a la següent equivalència prenent com a base l'hora de desenvolupador sènior FE/BE:

1 hora de Cap de Projecte	1,8 hores de desenvolupador
1 hora d'Analista Funcional	1,28 hores de desenvolupador

6.2 Requisits de Qualificació

6.2.1 Experiència Mínima Requerida

- Desenvolupadors Senior: Mínim 2 anys d'experiència en les tecnologies especificades
- Cap de Projecte: Mínim 5 anys d'experiència exercint aquest rol
- Analista Funcional: Mínim 3 anys d'experiència exercint aquest rol

6.3 Organització Interna de l'Entitat

6.3.1 Estructura de Governança

- Responsable del Contracte: Coordinació general i presa de decisions estratègiques
- Responsable Tècnic: Validació tècnica i supervisió de la qualitat
- Product Owners: Definició de requeriments funcionals per àrea
- Usuaris Clau: Validació de funcionalitats i feedback d'usabilitat

6.3.2 Comitès i Grups de Treball

- Comitè de Seguiment: Reunions mensuals de seguiment del servei

6.4 Comunicació i Coordinació

6.4.1 Canals de Comunicació

- Reunions presencials/videoconferència
- Plataforma de col·laboració: Microsoft Teams o similar
- Sistema de gestió de projectes: Jira, Planner o similar
- Documentació compartida: SharePoint o similar

6.4.2 Protocols de Comunicació

- Reunió de kick-off al inici del contracte
- Stand-ups diàries per als equips de desenvolupament
- Demos setmanals o quinzenals de funcionalitats desenvolupades
- Retrospectives mensuals per a la millora contínua

6.5 Gestió del Coneixement

6.5.1 Transferència de Coneixement

- Sessions de formació trimestral als equips interns
- Documentació tècnica actualitzada de tots els desenvolupaments

6.5.2 Continuïtat del Servei

- Documentació exhaustiva de tots els processos i procediments
- Rotació controlada dels membres de l'equip per evitar dependències
- Backup de coneixement amb almenys dos membres per rol crític
- Període de solapament en canvis de personal clau

7 METODOLOGIA DE TREBALL

7.1 Marc Metodològic

7.1.1 Metodologia Àgil SCRUM

El desenvolupament de projectes seguirà la metodologia SCRUM adaptada a les necessitats de l'entitat contractant:

- Sprints de 2 setmanes: Cicles curts per a lliurament continuu de valor
- Product Backlog: Llista prioritzada de funcionalitats i requeriments
- Sprint Planning: Planificació detallada al començament de cada sprint
- Daily Standups: Reunions diàries de coordinació de l'equip
- Sprint Review: Demostració de funcionalitats completades
- Sprint Retrospective: Anàlisi de millores per al següent sprint

7.2 Gestió de Requeriments

7.2.1 Procés de Captura de Requeriments

- Anàlisi inicial: Reunions amb usuaris clau i stakeholders
- Documentació funcional: Especificacions detallades amb casos d'ús
- Prototipatge: Maquetes i prototips per validació inicial
- Validació: Aprovació formal abans de l'inici del desenvolupament

7.2.2 Gestió de Canvis

- Control de canvis: Procediment formal per a modificacions de scope
- Impact analysis: Anàlisi de l'impacte en terminis i recursos
- Aprovació: Procés d'aprovació per part dels responsables
- Comunicació: Notificació a tots els stakeholders afectats

7.3 Assegurament de la Qualitat

7.3.1 Estratègia de Testing

A definir en funció de cada projecte:

- Test-Driven Development (TDD): Tests abans del desenvolupament quan sigui aplicable
- Automated testing pipeline: Tests automatitzats en CI/CD
- User acceptance testing: Proves amb usuaris finals
- Performance testing: Proves de rendiment per a funcionalitats crítiques

7.4 Gestió de Riscos

7.4.1 Identificació de Riscos

- Riscos tècnics: Complexitat, dependències externes, rendiment
- Riscos de projecte: Terminis, recursos, canvis de scope
- Riscos operacionals: Disponibilitat, seguretat, conformitat

7.4.2 Plans de Mitigació

- Risk register: Registre actual

8 CONDICIONS D'EXECUCIÓ

8.1 Condicions bàsiques d'execució

L'adjudicatari està obligat a documentar exhaustivament totes les seves actuacions, per tal de mantenir actualitzada la informació sobre versions, modificacions i funcionalitats dels aplicatius a mantenir. Si l'evolució aplicada a un programa ho fa necessari el contractista actualitzarà els manuals d'usuari existents o els crearà de nou.

L'adjudicatari haurà de disposar d'una eina d'enregistrament de les tasques i activitat realitzada que haurà de ser accessible per part del personal d'Informàtica de l'ICS.

Les funcions de seguiment i control del contracte seran exercides per l'ICS en la persona o figura que designi per tal d'assegurar en tot moment la correcta prestació del servei definit en el present plec.

Amb freqüència mensual es procedirà a revisar el compliment dels objectius del contracte. A tal efecte, els interlocutors elaboraran el corresponent informe que serà avaluat pel responsable del projecte per part de l'adjudicatari i pel Director de Sistemes d'Informació de l'ICS.

8.2 Formació

El proveïdor haurà de dur a terme accions de formació orientades a garantir l'autonomia i la seguretat dels diferents perfils d'usuari del sistema.

8.3 Pla de devolució del servei

A la finalització del contracte, per qualsevol causa (expiració del termini, resolució anticipada, incompliment, etc.), l'empresa adjudicatària haurà de garantir un pla de devolució del servei que inclogui com a mínim els següents punts:

- **Exportació de dades**

  L'empresa adjudicatària haurà de facilitar la descàrrega íntegra de totes les dades generades i emmagatzemades durant la vigència del contracte.

Les dades s'hauran de lliurar en formats oberts i interoperables (ex. CSV, JSON, XML), amb una estructura clara i documentada.

S'haurà de garantir la traçabilitat i la integritat de les dades exportades.

- **Documentació tècnica**

  Es lliurarà documentació completa sobre l'estructura de les dades, els processos de migració i les interfícies utilitzades.

  Aquesta documentació haurà de permetre la continuïtat del servei amb un altre proveïdor o mitjançant una solució pròpia.

- **Desactivació del servei**

  El proveïdor haurà de desactivar l'accés al servei de forma ordenada i segura, garantint que no quedi cap accés actiu ni cap dada residual en els seus sistemes.

  Es garantirà la eliminació segura de les dades dels sistemes del proveïdor, conforme a la normativa vigent (ex. RGPD).

- **Suport a la migració**

  Durant un període mínim de 30 dies naturals posteriors a la finalització del contracte, el proveïdor haurà de prestar suport tècnic per facilitar la migració de les dades i la posada en marxa del nou sistema.

  Aquest suport no podrà comportar cap cost addicional per a l'òrgan contractant.

- **Certificació de devolució**

  El proveïdor haurà d'emetre un informe de devolució que certifiqui:

  - La correcta exportació de les dades
  - La desactivació del servei
  - L'eliminació segura de les dades
  - Les accions de suport realitzades

8.4 Propietat intel·lectual, seguretat i confidencialitat

L'adjudicatari accepta expressament que la propietat i els drets d'explotació dels productes i sistemes desenvolupats a l'empara del present contracte corresponen únicament a ICS i IAS, amb exclusivitat i a tots els efectes.

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.

9 REQUERIMENTS DE SEGURETAT

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

9.1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

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

L'empresa adjudicatària ha de posar en coneixement de l'ICS, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

9.2 Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària del contracte donarà compliment com a encarregat de tractament el que estableix el Reglament General de Protecció de Dades.

Pel que fa a la seguretat en el tractament d'aquestes, l'empresa adjudicatària implementarà les mesures de seguretat establertes per l'Agència de Ciberseguretat en el Marc de Ciberseguretat per a la Protecció de Dades. Aquesta implementació i nivell de compliment seran incorporats al model de compliment normatiu de la Generalitat de Catalunya.

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.

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.

Així mateix, l'empresa adjudicatària haurà de **signar un contracte d'encarregat de tractament** de dades personals amb ICS i IAS.

En el cas de que el tractament de dades personals es faci en infraestructura en el núvol o s'apliquin algorismes de IA en les dades, **l'adjudicatari haurà de fer una AIPD** (Avaluació d'Impacte relativa a la Protecció de Dades).

9.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.

En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària del contracte haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir, amb l'ENS, **en nivell MITJÀ com a mínim**, durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'ICS. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc web d'aquesta Secretaria. Si escau, l'empresa adjudicatària del

contracte basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

9.4 Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'ICS i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'ICS i IAS des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte basat haurà de garantir que disposa dels perfils amb la capacitació i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitació per al personal que designi l'ICS/IAS per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'ICS/IAS, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional o bé complir amb els criteris que estableixi l'Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

9.5 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte i l'ICS/IAS o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'ICS/IAS.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'ICS/IAS.
- L'empresa adjudicatària del contracte haurà de participar en els mecanismes de coordinació que estableixi l'ICS/IAS i seguir els procediments establerts per aquest fi, per a poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

9.6 Verificació del compliment i auditoria

L'ICS/IAS es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'ICS/IAS podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'ICS/IAS. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'ICS/IAS.

9.7 Incidents de seguretat

El POC haurà de notificar a l'ICS/IAS qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària del contracte haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'ICS/IAS.

En cas que sigui necessari, l'empresa adjudicatària del contracte haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'ICS/IAS per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

9.8 Accés a la informació

L'empresa adjudicatària del contracte haurà de garantir l'accés del personal autoritzat de l'ICS/IAS a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'ICS/IAS i l'empresa adjudicatària establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

10 PREVENCIÓ DE RISCOS

L'empresa adjudicatària contractada haurà de respectar la normativa de prevenció de riscos laborals i de tractament de residus sanitaris, i complirà la legislació vigent en aquestes matèries (Llei 15/2003 de 15 de juny, entre altres).

Girona, 10 de desembre de 2025

Daniel Garcia Asquerda

Direcció Unitat de Tecnologies de la Informació i Comunicació (UTIC)