PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS QUE REGEIX LA CONTRACTACIÓ DELS SERVEIS DE CONSTRUCCIÓ I DESENVOLUPAMENT DEL SISTEMA D'INFORMACIÓ DE VACUNACIONS I D'IMMUNITZACIONS DE CATALUNYA (HES-IMMUNITZACIONS) DEL DEPARTAMENT DE SALUT (AP-E128).

Expedient núm.: CTTI-2024-13

Amb la presentació de la seva oferta, l'empresa licitadora accepta les prescripcions tècniques establertes en aquest plec.

Qualsevol proposta que no s'ajusti als requeriments mínims establerts en aquest plec quedarà automàticament exclosa de la licitació.

1. OBJECTE

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.

L'objecte de la present licitació és la contractació dels serveis de construcció i desenvolupament del Sistema d'Informació de Vacunacions i d'Immunitzacions de Catalunya del Departament de Salut.

El sistema s'ha de dissenyar com a producte i ha de respondre de forma integral a les necessitats de gestió i registre de processos vacunals i d'immunització i s'haurà d'integrar amb el nou sistema d'informació del Ministerio de Sanidad: SIVAIN.

Les principals tasques a dur a terme són:

- Disseny i implantació d'un model d'informació basat en openEHR: estàndard internacional i obert específic per al disseny de models d'informació clínica.

- Disseny i desenvolupament d'un sistema d'informació robust, modular i escalable amb les següents funcionalitats:

  Per al professional:
  - Disposar de la informació necessària per a permetre la presa de decisions en quan a la gestió de vacunacions i immunitzacions, a través d'una estació clínica.
  - Disposar d'una plataforma d'aplicació del calendari vacunal per la construcció i justificació de propostes.
  - Disposar d'un model de manteniment de catàlegs i calendaris.

  Per a la ciutadania:
  - Presentació de les vacunes administrades i calendari futur.

La irrupció de les TIC en l'àmbit de la salut pública no ha de passar únicament per un procés de digitalització de la situació actual i dels processos existents, sinó que s'han de dissenyar sistemes i models orientats al futur per tal de permetre l'aplicació de mètodes d'intel·ligència artificial i aprenentatge sobre les dades, que poden ser claus a l'hora de prendre decisions en contextos comunitaris i poblacionals específics.

Concretament s'emmarca en el:

Lot E: Administració digital i solucions a mida

Dins d'aquest lot s'inclouen les aplicacions i sistemes d'informació relacionats amb el desplegament de l'administració digital que no han quedat recollits en la resta de lots, normalment basats en els entorns tècnics que es descriuen a continuació:

- Plataformes basades en paradigma multi-capa (interfícies pesants o lleugeres). Principalment JEE, Canigó (framework de desenvolupament propi basat en JEE) i Microsoft .NET, entre altres.

- Plataformes de gestió de processos (BPM), plataformes de ESB (Enterprise Service Bus), i eines d'integració d'aplicacions. Principalment recollides al full de ruta del programari que revisa i publica el CTTI.
- Host, caracteritzat principalment per la utilització d'eines de base de dades DB2 i IDMS, i pel llenguatge de programació Cobol.
- Aplicacions desenvolupades per a escenaris de mobilitat sobre plataforma iOS, Android o altres sistemes que puguin incorporar els dispositius de mobilitat.
- Aplicacions orientades a serveis i microserveis.
- Tots els sistemes d'emmagatzematge de dades i documents que donen suport a aquestes aplicacions i entorns:
    - Sistemes de gestió de base de dades estructurades (Microsoft SQL Server, Oracle, MySQL o DB2, entre altres).
    - Sistemes de gestió de base de dades no SQL (MongoDB o ElasticSearch, entre altres).
    - Sistemes de gestió documental (Documentum, OpenText o Alfresco, entre altres).
- I d'altres arquitectures, presents en l'actualitat en sistemes d'informació que poden necessitar evolució, com Oracle APEX, PHP, Adobe Enterprise Manager, Powerbuilder, Acces, entre altres.

2. DESCRIPCIÓ DELS SERVEIS A PRESTAR

Els serveis a prestar són els següents:

- Serveis de construcció i desenvolupament (projectes sota demanda)
    - Construcció de noves aplicacions

Les condicions d'execució per a cadascun d'aquests serveis es descriu en el capítol 4.Condicions d'execució del servei.

2.1. Serveis de construcció i desenvolupament

Els serveis de desenvolupament, aniran d'acord amb l'enfocament metodològic definit al Playbook Agile de CatSalut, detallat a l'annex *8.7 ModelAgilSalut_AgilePlaybook* que especifica, entre altres: model de treball, estructura, processos, rols, eines, gestió del producte.

Els serveis de desenvolupament, d'acord amb l'enfocament metodològic que sigui d'aplicació (cascada, iteratiu, agile, ...) i que el licitador haurà de justificar, contemplarà les activitats extrem a extrem:

- **Anàlisi de requisits (programari i sistemes) / Anàlisi Funcional**. Transformació de les necessitats i requeriments del client en requisits del programari i requisits de sistemes.
- **Disseny de l'arquitectura de la solució (programari i sistemes)**. Transformació de l'anàlisi dels requisits en un disseny de solució, amb

l'organització fonamental del sistema en els seus components i les seves relacions detectades segons requeriments de l'arquitectura corporativa tècnica de dades i els principis que guiaran el disseny i la seva construcció. Inclou el disseny de la plataforma tecnològica, el seu dimensionament i la proposta de configuració tècnica de cada un dels components de la plataforma per garantir el correcte funcionament de l'aplicació segons els requeriments no funcionals exigits (rendiment, escalabilitat, disponibilitat, entre d'altres).

- **Disseny detallat (programari)**. Transformació dels requisits, l'anàlisi dels requisits i el disseny de l'arquitectura en un disseny detallat en el que es reflecteixi l'estructura interna de cadascun dels elements o components identificats al disseny de l'arquitectura de la solució. En el cas de que l'aplicació sigui crítica, caldrà detallar el disseny del monitoratge de l'aplicació de forma coordinada amb el Centre de Control del CTTI, així com la mesura dels indicadors de negoci (telemetria).
- **Construcció i Proves unitàries (programari)**. Desenvolupament de la solució seguint els estàndards i normatives del CTTI establertes.
- **Integració** dels diferents elements del sistema (elements de programari, elements de maquinari, i altres sistemes) per obtenir un sistema complet que satisfaci el disseny i les expectatives dels clients.
- **Proves de qualificació**. Validació de que el programari es pot instal·lar en l'entorn final i que el producte integrat compleix amb els requisits definits.
- **Instal·lació del programari**. Instal·lació del programari o suport a la seva instal·lació. Inclou totes les activitats requerides en cas que sigui necessari la paquetització i/o virtualització de l'aplicació per facilitar el seu desplegament i/o funcionament.
- **Suport a l'acceptació del programari**. Assistència als usuaris en la comprovació de que el programari compleix amb els requisits establerts.
- **Gestió del canvi**. Comunicació, formació i suport tant a nivell dels usuaris com del serveis posteriors de suport, principalment el SAU. En els cas d'una aplicació classificada com a crítica, la formació tècnica s'haurà d'estendre de forma específica al Centre de Control.
- **Pas a manteniment i/o post-implantació**. Traspàs del codi, documentació i coneixement al proveïdor que farà el manteniment i a d'altres unitats del model de servei del CTTI.

S'inclouen en aquest servei també els desenvolupaments realitzats sobre plataformes com a servei SaaS, sent en aquest cas tot el servei autocontingut, entenent com a tal la contractació del servei, la seva parametrització segons els requeriments tècnics i funcionals del negoci, i l'administració i operació de la plataforma SaaS.

Si el desenvolupament es fa basant-se segons els nous models de desenvolupament (DevOps, contenidors, cloud, ...) a banda de les tasques anteriors, entre d'altres també caldria fer:

- Infraestructura com a codi.
- Automatització de proves i controls de qualitat i seguretat.
- Generació d'indicadors tècnics de l'aplicació / Generació d'indicadors de negoci.

- Gestió extrem a extrem de la solució, d'acord amb el model de gestió del servei del CTTI i detallat en les condicions d'execució del servei.

Aquestes activitats són les que es realitzen actualment i per tant es consideren com el conjunt bàsic a realitzar. El CTTI podrà incorporar en un futur activitats addicionals en funció de la evolució dels estàndards metodològics disponibles a la indústria en cada moment.

3. DESCRIPCIÓ DE LA SOLUCIÓ

A continuació s'explica detalladament l'abast tant funcional com tecnològic de les diferents funcionalitats que cal desenvolupar en aquest contracte basat d'Acord Marc.

3.1. Antecedents

Les vacunes, així com altres immunitzacions, són essencials per a la prevenció, control i eliminació de malalties immunoprevenibles i una eina essencial en Salut Pública.

El Servei de Medicina Preventiva de la Subdirecció General de Promoció de la Salut (SDGPS) entre d'altres funcions, té com a missió planificar i gestionar el programa de vacunacions de la Secretaria de Salut Pública. Aquest servei estableix el calendari vacunal que ha de rebre la població de Catalunya amb totes aquelles vacunes necessàries per estar protegit contra certes malalties i que es va modificant sobre la base de l'evidència científica.

El Programa de vacunacions de Catalunya té la missió de controlar (i en cas que sigui factible, eliminar i col·laborar a erradicar) les malalties evitables per vacunació, a tot el territori i entre tota la població de Catalunya amb equitat.

Activitats

- ✓ Mantenir actualitzades les recomanacions de vacunació amb la participació del Consell Assessor de Vacunacions.
- ✓ Facilitar la formació i informació dels professionals sanitaris i de la població.
- ✓ Garantir la disponibilitat continuada de vacuna als més de mil centres de vacunació públics i privats als quals subministra vacunes.

Població destinatària

- ✓ Població infantil
- ✓ Persones grans
- ✓ Professionals sanitaris

Inclou vacunació selectiva per prevenir les malalties transmissibles en grups de risc, dirigida a:

- ✓ Persones amb criteris de risc per la seva condició mèdica o conductes de risc, ja que presenten un risc més alt d'infecció i/o complicacions, a més d'una taxa més alta d'hospitalització i, en alguns casos, de mort.
- ✓ Persones o grups que poden transmetre la malaltia a persones d'alt risc.

- ✓ Persones que realitzen serveis públics essencials per a la comunitat.
- ✓ Viatgers internacionals.
- ✓ Persones amb risc per la seva tasca laboral.

Les vacunes incloses en el calendari vacunal i altres marcades per les indicacions de l'estratègia vacunal, es compren i es distribueixen des del Departament de Salut. L'administració d'aquestes vacunes es realitza en diferents entorns, atenció primària, hospitals, centres privats, altres. Tenim diferents entitats proveïdores de serveis amb múltiples sistemes d'informació.

D'aquí es pot deduir que la informació referent a vacunacions i immunitzacions de Catalunya, està en aplicacions i sistemes d'informació diversos. La Història Clínica Compartida (HC3) comú a tota la ciutadania, inclou el registre d'unes dades mínimes de vacunacions i immunitzacions que provenen d'aquests diferents sistemes. Les dades estan registrades en els diferents sistemes i s'acaben replicant a HC3.

Davant d'aquesta situació, la SDGPS es planteja la creació d'un sistema d'informació centralitzat de vacunacions i d'immunitzacions. Aquest projecte suposa un gran repte però a la vegada representa un gran avenç per la millora de la seguretat, atenció i traçabilitat de les vacunes. L'objectiu principal és garantir la millor protecció de la ciutadania davant de les malalties immunoprevenibles.

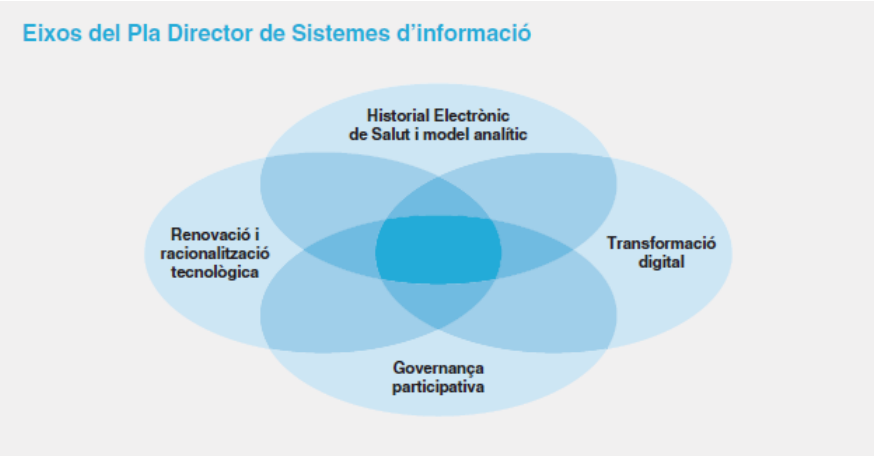
La creació d'aquest sistema també permetrà estar alineat amb el marc normatiu vigent:

- Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud (SNS) (2 de febrer de 2022)
- Real Decreto de Vigilancia en Salut Pública (en desenvolupament)

El nou sistema ha de ser modular, parametritzable, escalable, desenvolupat amb tecnologia avantguardista, orientat a procés, interoperable i interrelacionat.

3.2. Context. Transformació del Sistema Sanitari Català. Historial Electrònic de Salut (HES)

Aquest projecte s'emmarca dins de la transformació del sistema sanitari de Catalunya i constituirà un dels mòduls clínics del HES.



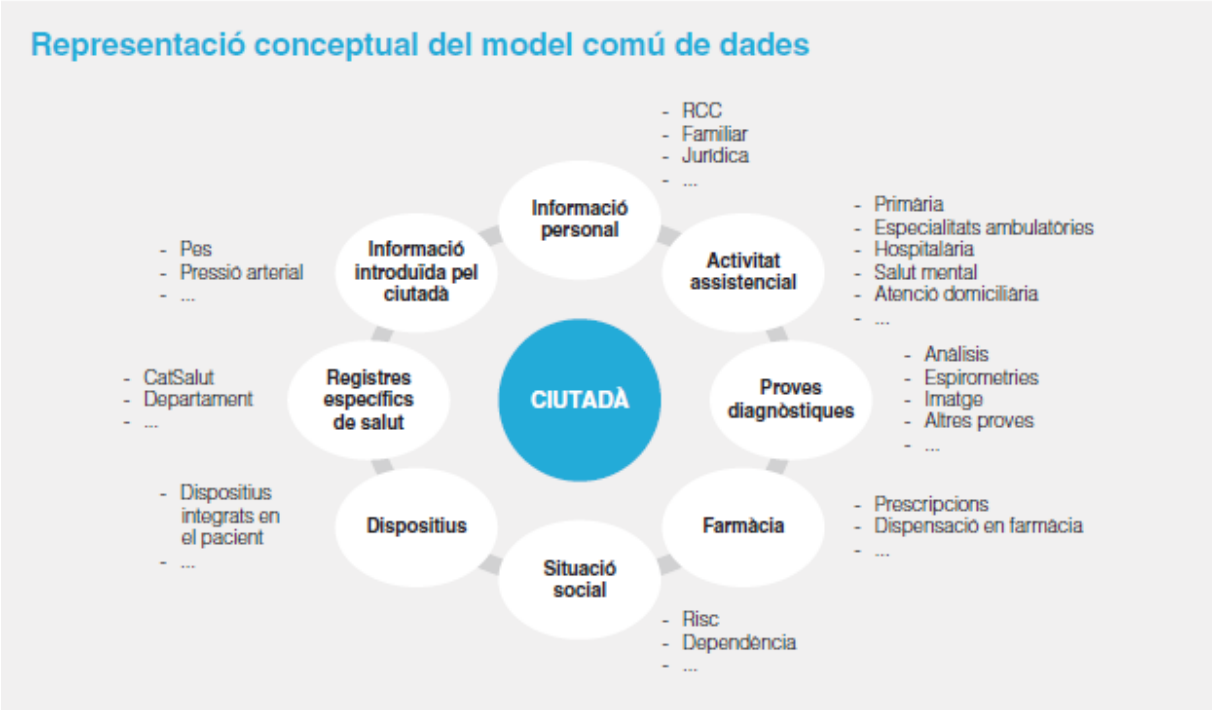
Tal i com està definit al Pla Director de Sistemes d'Informació del SISCAT, https://salutweb.gencat.cat/web/.content/_ambits-actuacio/Linies-dactuacio/Plans-sectorials/pd_sistemes_informacio/pla_director_final_v27.pdf les premisses d'aquesta transformació són:

- El sistema d'informació ha d'estar centrat en la persona, amb independència del professional o proveïdor que el pugui tractar en un moment determinat. El model ha de proporcionar una visió integral de la salut i benestar del pacient, de les seves interaccions amb el sistema sanitari i d'altres que afectin la seva salut al llarg de la seva vida. Les noves tecnologies han de facilitar al pacient l'accés a les seves dades, augmentar el seu nivell d'informació i coneixement, i permetre'n la interacció i la participació activa en la seva salut.
- El sistema ha de proporcionar suport tecnològic per a l'atenció i el seguiment integrat i continuat del malalt, i ha de facilitar els seus contactes dins el sistema i la col·laboració entre diferents professionals i dispositius assistencials. El nou model ha d'oferir al professional informació comuna de significat clínic que sigui rellevant, puntual (en el moment que la necessita) i de qualitat, fàcil de registrar, accedir i analitzar.
- El sistema ha d'incorporar funcionalitats que permetin interrogar i analitzar grans volums d'informació, així com comparar condicions de risc i diferents pràctiques i tractaments per ajudar a la presa de decisions i a la recerca. L'ús i l'anàlisi massiva de més dades de més fonts hauria de permetre el descobriment de patrons, per tal de millorar la presa de decisions i avançar cap a una medicina predictiva i personalitzada.

- El sistema d'informació ha d'incloure funcionalitats avançades que facilitin l'abordatge de problemes de salut més estesos i complexes (com els que deriven de la cronicitat i la pluripatologia) i el desenvolupament de nous models assistencials que poden substituir l'atenció presencial.
- Les noves tecnologies han de permetre l'automatització de tasques sense valor i l'augment del temps de qualitat dedicat a l'atenció al malalt.

Què és l'Historial Electrònic de Salut (HES)?

L'Historial Electrònic de Salut (HES) és la peça clau del Pla Estratègic del Departament de Salut i representa el repositori funcional i tècnic que facilitarà de forma longitudinal, la informació i el coneixement rellevant del ciutadà/na que cal enregistrar i compartir amb tots els actors del sistema sanitari (ciutadania, professionals, gestors, planificadors i reguladors), d'una forma visual i entenedora, evitant redundar la informació.
L'HES proporcionarà una visió integral de la salut i del benestar de les persones i de les seves interaccions amb el sistema sanitari i facilitarà l'atenció i el seguiment integrat i continuat del malalt.
Oferirà al professional informació comuna de significat clínic rellevant, puntual (en el moment que es necessita) i de qualitat, fàcil de registrar, accedir i analitzar. Respectant els diversos models d'història clínica de les diferents entitats i substituint progressivament els sistemes actuals basats en la interoperabilitat (la HC3 i la IS3) i l'enviament de registres dels proveïdors al CatSalut mitjançant múltiples circuits i mitjans.



Els beneficis que pot aportar l'HES són els següents:

- Clínics:
    - Millora la qualitat i la seguretat de l'atenció, ja que redueix errors i proves innecessàries.
    - Fomenta la comparació transparent entre diferents pràctiques assistencials i l'adopció de maneres de fer basades en l'evidència.
- Organitzacionals:
    - Millora la sostenibilitat gràcies a la reducció de codificacions errònies, dels costos dels sistemes en paper, dels processos de documentació i dels costos de coordinació de l'atenció, de l'administració i de la facturació.
    - Facilita la col·laboració entre professionals i dispositius al llarg de la cadena de cures, i posa la informació a disposició de tots els agents implicats en la salut d'un malalt.
    - Millora la seguretat i la confidencialitat de les dades dels pacients.
- Socials:
    - Augmenta la capacitat d'accés i resposta als canvis dels models d'assistència sanitària i social.
    - Permet respondre a nous requeriments i consultes del ciutadà/na, i promou l'apoderament del pacient pel que fa a la seva salut i qualitat de vida.

- Facilita la conducció de la recerca epidemiològica amb dades integrades del pacient en un context assistencial i social concret.

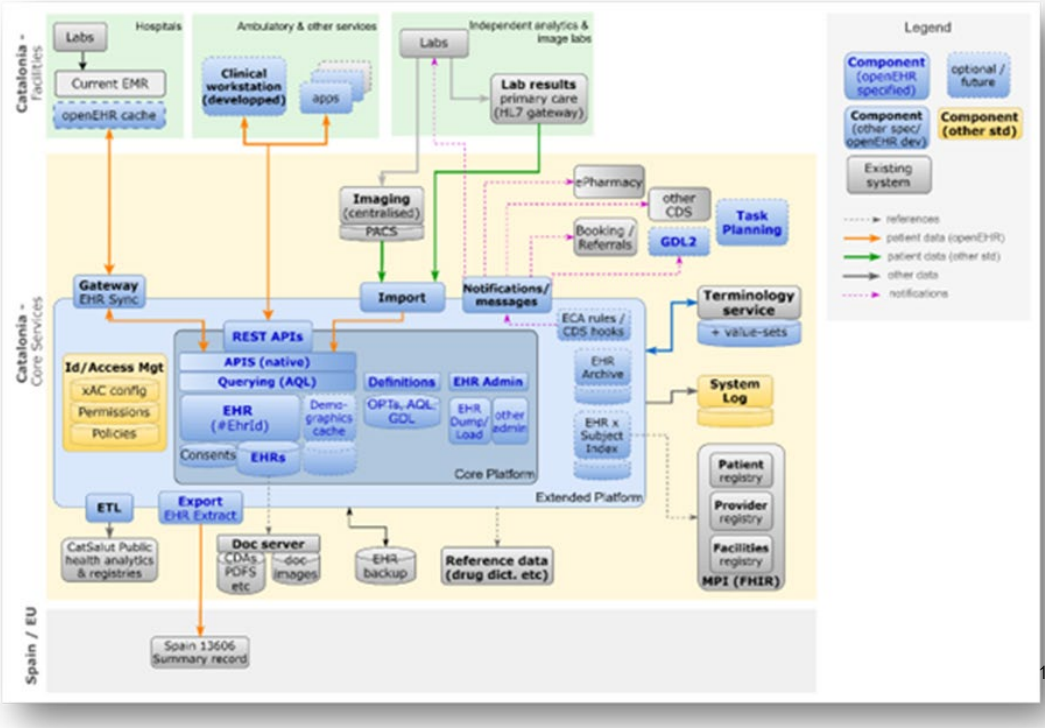
Tecnologies de la Informació per a la Salut i estàndards

La plataforma del CatSalut és dissenyada com una col·lecció de components coherent, reflectint una separació apropiada d'àmbits, p. ex. del HES amb la terminologia, integració de laboratori, altres. Un seguit de tecnologies i estàndards estan implicats, com es llisten a continuació:

- openEHR – nucli HES, formalismes (meta-models) pel planificador de tasques, guies per la pressa de decisions i altres components de coneixement relacionats.
- openEHR – base de coneixement d'arquetips (data groups), plantilles (data sets), guies, normes i subgrups de terminologia usats per definir la semàntica del sistema.
- IHE (Integrating the Healthcare Enterprise) – diferents APIs, p. ex. log de sistema ATNA, consentiment APPC, altres.
- HL7 (Health Level Seven), DICOM (Digital Imaging and Communication In Medicine) – diferents estàndards d'interoperabilitat (HL7v2, CDA, FHIR, CDS hooks) relacionat amb resultats de laboratori, ordres d'imatge i resultats, i altres dades clíniques i demogràfiques potencials.
- ICD, SNOMED, LOINC, altres – estàndards de terminologia.
- ISO 13606 (interoperabilitat semàntica en la comunicació de la Història Clínica Electrònica) – registre resum nacional.

Aquests estàndards seran adaptats segons les necessitats per assegurar la coherència de la plataforma.

Es presenta la **plataforma HES** a la il·lustració que segueix. Per raons de claredat, les aplicacions que no son estacions clíniques o openEHR genèric no es mostren al diagrama.



Components de la plataforma:

A- Nucli de la plataforma – Basat en openEHR

Conté el conjunt mínim de serveis i components requerits per donar suport a un HES basat en openEHR.

- HES – registre de dades de salut compartit i centrat en el pacient
- Caché de dades demogràfiques (opcional) – per registrar i mantenir informació de caràcter demogràfic en el HES de professionals de salut i altres professionals, referenciada localment i que no es manté en registres de proveïdors o externs de pacients
- Privacitat i consentiment – definicions computables de la privacitat del pacient i configuració d'ús de la informació
- Consultes (queries) – responsable de processar consultes sobre el pacient i la població al repositori principal del HES
- Bolcat/càrrega de l'HES – funció de bolcat/càrrega a nivell de sistema per transferir els HES a una nova versió del producte o repositori extern
- Referències als documents de registre de pacients antics mantingudes a servidors documentals – referències disponibles de llarga durada, entre registres regionals de pacients nous i dades antigues del mateix pacient -
- Serveis de coneixement: plantilles, arquetips, plans, guies conjunts de normes
- HES Admin: quadre de comandament d'administració
- REST APIs: Resource-oriented APIs accessibles mitjançant el protocol REST, basat en HTTP
- Comunicació asíncrona per esdeveniments amb protocol Apache Kafka.
- Microfrontends encapsulant funcionalitats dels dominis del RDC (Repositori de Dades Clíniques)

B- Plataforma estesa – Basat en openEHR

És el conjunt estès de serveis i components requerits per donar suport a utilitats per un HES compartit:

- Plataforma de Seguretat (PdS) per a la gestió d'identitats i accessos: responsable de representar identitats d'usuari, rols, funcions, altres
- Índex HES/Pacient: identificació al HES únicament per id d'història proporcionant una seguretat de referencia creuada amb l'identificador del pacient
- Arxiu a emmagatzemament de llarga durada de, per exemple, informació de difunts o de pacients que han deixat de tenir relació amb el sistema
- Extracció i exportació de l'HES: crea extractes per carregar a altres sistemes que no estiguin directament connectats, controlat per la privacitat i el consentiment
- Regles i notificacions de l'ECA (Event-Condition-Action): components per representar normes a partir de les quals successos específics (p. ex. enviament de cert contingut com pot ser un resultat positiu de test COVID) són generats juntament amb notificacions programades a parts i sistemes externs
- HES/HME gateway: sincronització de contingut entre HES i HME d'institucions
- Integrador de dades de pacient: importació i conversió a format openEHR de contingut HES generat externament, incloent resultats de laboratori o diagnosi d'imatge
- ETL: extract, transform and load per extraure contingut del HES a format genèric requerit per anàlisi de dades, registres (vacunes, etc) i/o sistemes de reporting

C- Serveis relacionats amb la plataforma

- Terminologia: Proporcionar terminologia per us operatiu, via una API com la del servei de terminologia FHIR
- Observabilitat del Sistema – traçabilitat segura d'interaccions específiques (p. ex. operacions CRUD) entre el HES i altres components
- Dades de referència del CatSalut / Serveis de coneixement (p. ex. diccionari de drogues, altres)
- MPI (MasterPatient Índex): registre de pacients

D- Altres interfícies

- Ordres i resultats de laboratori i imatge
- Prescripcions i farmàcia
- Fitxa resum de la ISO 13606
- Salut pública, anàlisi, recerca, altres del CatSalut

E- Principals aplicacions

- Lloc de treball clínic: l'aplicació clínica professional principal per interactuar amb el HES regional
- Portal del professional: un portal web genèric usat principalment per veure el registre del pacient, normalment amb algunes operacions de modificació
- Portal del pacient: un portal orientat al pacient del HES
- Ajuda a la pressa de decisions: habilitant la representació i execució informàtica de guies de pressa de decisions, escales i regles per generar notificacions a l'usuari i a altres sistemes
- Planificació de tasques: habilitant la representació i execució informàtica de processos i plans de cures

F- Desenvolupament de plataforma obert

- Entorn de desenvolupament de baix codi / SDK
- Eines de modelatge per desenvolupar arquetips, plantilles, guies, normes, altres
- Sandbox / instàncies d'entorns de desenvolupament i test
- Eines per inspeccionar dades genèriques i del sistema
- Consola d'instrumentació del sistema (monitoratge del rendiment, vista de càrrega, altres)

3.3. Requeriments del nou sistema

Els requeriments generals del sistema objecte del contracte es troben detallats a l'annex *8.6 Annex Tècnic HES-IMMUNITZACIONS,* on es presenta un document elaborat a partir de l'estudi dels requeriments generals i la proposta de necessitats de futur.

En línies generals, el document s'estructura en els següents apartats:

- **Introducció**

- **Sistema actual**
  - ✓ Procés
  - ✓ Mòdul d'immunitzacions
  - ✓ Registre Vacunal del Ministerio de Sanidad
  - ✓ Control i distribució d'estocs
  - ✓ Integracions amb altres sistemes d'informació de Salut

- **Plantejament del nou sistema**
  - ✓ Mòduls del sistema
    - Nucli immunitzacions
    - Programacions
    - Autoritzacions
    - Registres
    - Consultes
    - Anàlisi de Dades
    - Consultes i interacció estocs
  - ✓ Funcionalitats
    - Nucli immunitzacions
    - Catàleg de serveis al professional
    - Catàleg de serveis a la ciutadania

- **Arquitectura de referència**
  - ✓ Mapa de l'arquitectura de referència
  - ✓ Requisits d'arquitectura

- **Glossari**

4. CONDICIONS D'EXECUCIÓ DEL SERVEI

Per defecte, s'atendran les condicions descrites en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.

4.1. Gestió del servei de les aplicacions

Atenent l'apartat 3.1 del Plec de Prescripcions Tècniques de l'Acord Marc.

El detall dels processos es troba publicat a:

http://ctti.gencat.cat/ca/serveis/governanca_tic/desenvolupament_manteniment_aplicacions/operar-els-serveis/

4.2. Metodologia, estàndards i lliurables

Atenent l'apartat 3.2 del Plec de Prescripcions Tècniques de l'Acord Marc i tenint en compte el mètode de treball definit en el Playbook Agile de CatSalut que s'adjunta a l'annex *8.7 ModelAgilSalut_AgilePlaybook* del present document.

4.3. Assegurament i control de la qualitat

Atenent l'apartat 3.3 del Plec de Prescripcions Tècniques de l'Acord Marc.

Es pot consultar més informació a:

- Característiques de qualitat d'una solució (https://qualitat.solucions.gencat.cat/glossari/caracteristica_qualitat/)
- Característiques de qualitat dels lliurables (https://qualitat.solucions.gencat.cat/glossari/caracteristica_qualitat_lliurables/)

I en particular també atenent al Model de Gestió de QA HES que s'adjunta al l'annex *8.8 Model de Gestió de QA HES* del present document.

4.4. Seguretat

Atenent l'apartat 3.4 del Plec de Prescripcions Tècniques de l'Acord Marc sobre seguretat de la informació, 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.

El detall dels requeriments i model de seguretat es troba definit a l'apartat 8.4 dels annexes.

4.5. Gestió del codi font

Atenent l'apartat 3.5 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.6. Arquitectura Corporativa

Atenent l'apartat 3.6 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.7. Entorns de desenvolupament

Atenent l'apartat 3.7 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.8. Auditories

Atenent l'apartat 3.8 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.9. Equips i rols

Atenent l'apartat 3.9 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.10. Eines

Atenent l'apartat 3.10 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.11. Calendari i horaris

Atenent l'apartat 3.11 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.12. Localització física i recursos necessaris

Atenent l'apartat 3.12 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.13. Garantia

Atenent l'apartat 3.13 del Plec de Prescripcions Tècniques de l'Acord Marc.

4.14. Accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic

L'adjudicatari tindrà en compte l'establert en el RD 1112/2018, de 7 de setembre, sobre accessibilitat dels llocs web i aplicacions per a dispositius mòbils del sector públic i per tant aplicarà la norma "UNE-EN 301 549. Requisits d'accessibilitat per a productes i serveis TIC". Aquesta norma, és la versió espanyola a l'EN 301 549 V3.2.1 (2021-03) Accessibility requirements for ICT products and services, declarada com a estàndard harmonitzat en la Decisió d'Execució (UE) 2021/1339 de la Comissió, d'11 d'agost de 2021, i que és equivalent a complir tots els requisits de nivell A i AA de les WCAG 2.1.

5. FASES DE LA PRESTACIÓ DEL SERVEI

5.1. Fases del servei

L'adjudicatari haurà de presentar un Pla de servei que tingui en compte les característiques específiques que es detallen a continuació:

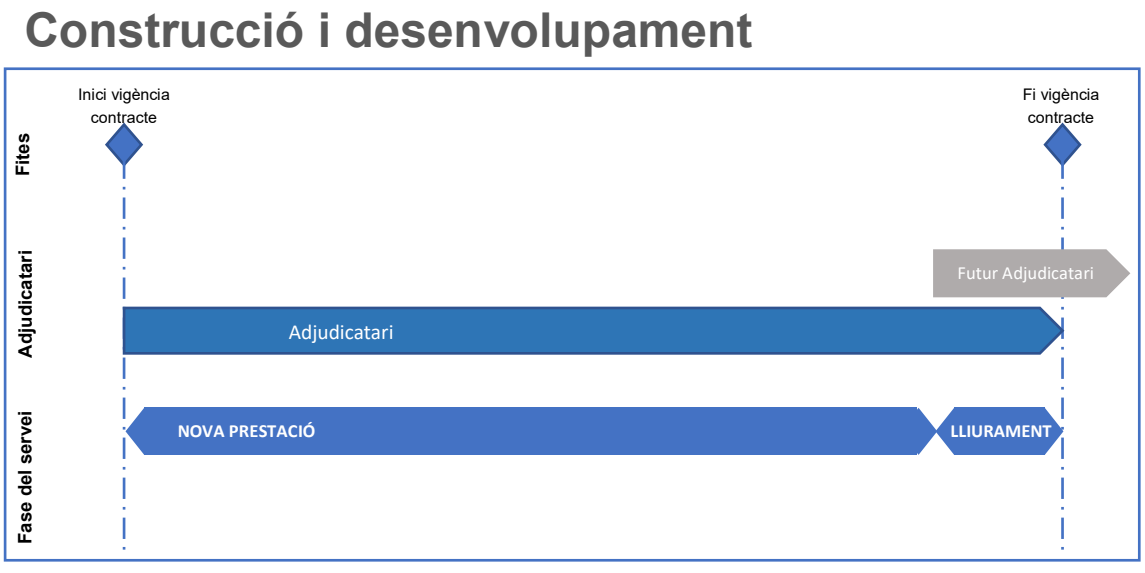


Figura 1: Fases del Servei de Construcció i Desenvolupament

- **Nova Prestació**: Un cop signat el contracte, s'iniciaran les diferents accions per la formalització dels projectes de desenvolupament. En aquest moment començarà la nova prestació del servei per als nous adjudicataris. En el cas de la construcció de nous sistemes d'informació, la nova prestació consistirà en la realització dels corresponents. En el cas de desenvolupament sobre sistemes

d'informació existents, el nou adjudicatari farà les actuacions necessàries per acomplir amb els objectius proposats i, un cop finalitzats, tornarà el servei al proveïdor de manteniment actual. En aquesta fase es desenvoluparan les activitat pròpies de l'objecte del lot que es descriguin en cada contracte basat. Inclou també, entre d'altres, les activitats de seguiment de control i millora del servei prestat al CTTI.
A partir d'aquest moment es podrà aplicar el model de penalitzacions associat al compliment dels ANS.

- **Devolució**: En cas de que l'objecte del contracte basat impliqui la transferència del servei a un nou proveïdor, l'adjudicatari haurà de desenvolupar el Pla de devolució que garanteixi la continuïtat del servei, continuarà sent el responsable del servei i s'aplicaran els ANS definits en aquest contracte. L'adjudicatari es posarà en contacte amb el futur proveïdor per començar les tasques de transferència del servei, del traspàs de coneixement i l'habilitació de l'operació.

  Aquest Pla de devolució constarà com a mínim d'una metodologia, documentació per la transferència del coneixement (per assegurar la continuïtat del servei) i els terminis.

  En cas de no poder completar la devolució d'un servei abans de la finalització d'aquest contracte, el CTTI es reserva el dret de perllongar el període de devolució del servei en qüestió. En aquest cas, l'adjudicatari haurà de continuar prestant el servei fins a la correcta devolució. S'estendrà durant un màxim de **4 mesos**.

5.2. Pla d'adquisició de coneixement

El Pla d'adquisició de coneixement, haurà de tenir els següents continguts:

- Planificació detallada d'activitats del procés de transferència del coneixement.
- Pla de fites principals amb el seu calendari.
- Equip compromès.

El Pla indicarà la seqüència d'activitats a realitzar per adquirir el coneixement necessari així com per assegurar que el proveïdor adjudicatari està en disposició per iniciar les activitats de desenvolupament. Així doncs, s'inclourà:

- L'estratègia per a l'adquisició de coneixement (entrevistes, auditoria, accés a documentació, entre d'altres).
- La verificació de la disponibilitat i correcta configuració de l'entorn de desenvolupament per part de l'adjudicatari.
- La verificació de la configuració adequada de les eines a utilitzar (grups, assignació de treballs, entre d'altres).

El Pla de fites principals ha d'incloure, almenys, per a cadascuna de les tasques a dur a terme, les dates d'inici i fi de cadascuna d'elles, la distribució de responsabilitats, els criteris aplicables d'acceptabilitat i qualsevol altre detall addicional que s'estimi pertinent.

El CTTI identificarà dependències i condicionants entre contractes que el proveïdor haurà de respectar, així com validarà l'estratègia i acompanyarà al proveïdor adjudicatari per tal assegurar l'èxit de l'adquisició de coneixement.

5.3. Pla de traspàs de desenvolupament a manteniment

L'adjudicatari haurà d'incloure un Pla de traspàs del desenvolupament portat a terme durant la prestació de servei cap al proveïdor que hagi de ser responsable del manteniment del sistema d'informació.

Aquest Pla de traspàs haurà d'incloure:

- Resum del desenvolupament realitzat indicant el seu impacte sobre el sistema d'informació (increment d'accés, rendiment, ampliacions d'arquitectura realitzades, entre d'altres).
- Documentació vinculada al desenvolupament realitzat (documents funcionals, tècnics, arquitectura, operacionals, entre d'altres).

El proveïdor de manteniment haurà d'acceptar formalment aquest Pla de traspàs en un període no superior a 2 setmanes des del seu lliurament.

Serà responsabilitat del proveïdor que ha fet el desenvolupament, assegurar l'acceptació del Pla de traspàs.

5.4. Pla de devolució del servei

L'adjudicatari inclourà un Pla de devolució del servei detallat que descrigui les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts en relació amb la devolució, i que inclogui els termes i condicions en què es realitzarà.

En cas de cessament o finalització del contracte, el proveïdor estarà obligat a tornar el control dels serveis objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb els de prestació del servei, sense cost addicional per al CTTI.

El Pla de devolució haurà de complir, com a mínim, els següents principis i continguts:

- El termini d'execució serà d'entre 2 i 4 mesos abans de la finalització del contracte ja sigui per haver exhaurit el termini o per cancel·lació anticipada. El CTTI es reserva el dret de poder reduir el termini d'execució segons consideri necessari.
- Inclourà la metodologia de transferència de coneixement dels aspectes fonamentals d'operació i, com a mínim, descriurà:
    - Suport al nou adjudicatari, formació i documentació sobre els procediments de negoci i del servei.
    - L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat per l'adjudicatari o la Generalitat de Catalunya en la provisió del servei.

  - La formació pràctica tutelada, en la qual el personal designat pel CTTI realitzi els treballs propis de cada procés o funcionalitat tutelats pel personal de l'adjudicatari.

- L'adjudicatari haurà d'oferir el maquinari i els equips informàtics, adscrits de forma exclusiva als serveis objecte del contracte, al CTTI o a terceres parts anomenades per aquest. La valoració dels equips es realitzarà per un tercer utilitzant el criteri de "preu de mercat" o, si no és possible, sostraient al seu preu de compra el cost de l'amortització sense valor residual. El CTTI, o terceres parts anomenades per aquest, podrà realitzar la compra de tots o part dels equips.
- El CTTI podrà subscriure un contracte de llicència d'ús sobre els sistemes de l'adjudicatari que fossin necessaris per assegurar la continuïtat del servei.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència al CTTI, o a terceres parts anomenades per aquest, de serveis subcontractats, garanties o contractes de manteniment existents fins al moment de la terminació en els mateixos termes pactats amb els adjudicataris d'aquests.
- L'adjudicatari haurà d'oferir un Pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, el CTTI i/o altres adjudicataris.
- Durant el període de devolució del servei, l'adjudicatari ha de complir els Acords de Nivell de Servei. El Pla de devolució no ha de causar cap discontinuïtat en el servei.
- El CTTI no assumirà una dedicació significativa de recursos propis o de la Generalitat de Catalunya en les activitats de devolució.
- L'adjudicatari haurà de garantir que es disposa de la documentació actualitzada de la gestió del servei (base de dades de coneixement) a transferir.
- Abans de l'inici de la fase de devolució, l'adjudicatari ha de garantir, per les aplicacions d'importància Alta, que la documentació base es troba actualitzada. Es considera documentació base la que es troba indicada com a grau de necessitat imprescindible a:

  https://qualitat.solucions.gencat.cat/guies/transicio/lliurables_transicio_devolucio/)

6. ACORDS DE NIVELL DE SERVEI (ANS)

L'objectiu d'aquest apartat és descriure el model d'ANS, que defineix els **indicadors** i els **nivells de servei** exigits, i estableix una base objectiva i mesurable que reflecteixi el compromís entre l'adjudicatari i el CTTI per a prestar els serveis requerits de forma satisfactòria, enfront de la Generalitat de Catalunya.

El CTTI pretén obtenir un nivell de servei d'alta qualitat, així com un grau de satisfacció elevat per part dels usuaris, basat en:

- L'establiment d'indicadors de servei, de manera que el CTTI pugui realitzar una avaluació objectiva del servei i els seus lliurables, i que l'adjudicatari tingui una base per a la correcció de les eventuals deficiències en la prestació, i per a la millora dels seus processos i organització.

- L'establiment d'un model de penalitzacions que relacioni el nivell de prestació del servei amb la seva facturació.

Per aquests motius es defineix la següent estructura d'ANS:

- ANS d'Aplicació. Són els indicadors que mesuren el nivell de servei de les aplicacions de manera individual per a cada una d'elles.
- ANS d'Àmbit. Són els indicadors que mesuren el nivell global de servei per a cada àmbit.
- ANS de Contracte. Són els indicadors que mesuren el grau de consecució dels acords administratius i la gestió global del contracte.

El llistat d'indicadors de servei es detallen a l'apartat 8.5.Detall Acords de Nivell de Servei.

Addicionalment als Acords de Nivell de Servei (ANS), es mesuraran els indicadors de qualitat de nivell de servei (MQE), que determinen la qualitat global en l'execució del contracte.

6.1. Característiques dels indicadors

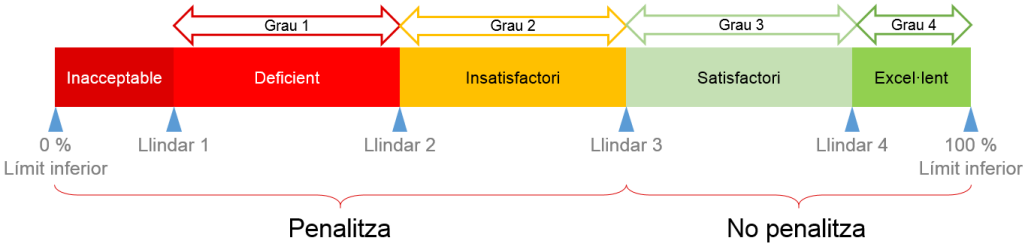
Els indicadors tindran les següents característiques:

- Codi. Identificador únic de l'indicador.
- Nom. Defineix l'objecte de mesura de l'indicador.
- Descripció. Descripció de l'indicador i el seu objectiu. S'inclouen les restriccions necessàries per dur a terme el càlcul del valor de l'indicador (per exemple restriccions horàries, tipificació dels incidents,...).
- Servei. Determina el servei tecnològic sobre el que s'aplica l'ANS.

Abreviatura	Servei
GN	General, aplica a tots els serveis
GO	Gestió operativa
SU	Suport a usuaris
MC	Manteniment correctiu
MP	Manteniment preventiu, perfectiu i adaptatiu tècnic
EV	Manteniment evolutiu

- Fórmula d'obtenció/eina. Fórmula a aplicar pel càlcul del valor de l'indicador de mesura, identificant les variables que intervenen al càlcul (mètriques) i, si s'escau, la referència a l'eina que permet l'automatització i extracció de les dades.
- Periodicitat. Freqüència de mesura del valor de l'indicador.

- Llindars de grau per a la definició dels trams. Valors que defineixen el grau de compliment del nivell de servei exigit. Per a cada indicador es definiran 4 llindars de grau. En funció de la banda en que es trobi l'indicador presentarà els valors següents:



- Penalització màxima. Determina el valor màxim al que pot arribar la penalització en el cas d'incompliment de llindar objectiu definit.

Grau de l'indicador

El grau de l'indicador pot prendre els següents valors:

- Grau 1: Deficient o Inacceptable
- Grau 2: Insatisfactori
- Grau 3: Satisfactori
- Grau 4. Excel·lent

El grau 4 serà el nivell objectiu, mentre que el grau 3 serà el nivell d'acompliment mínim per considerar que l'indicador és satisfactori.

6.2. Càlcul dels indicadors

Per tot indicador s'estableixen 4 llindars per definir els **trams** lineals que han de permetre l'obtenció del **grau** associat.

	Llindar Grau 1	**Llindar Grau 2**	**Llindar Grau 3**	**Llindar Grau 4**
Indicador de mesura	**Valor 1**	**Valor 2**	**Valor 3**	**Valor 4**

Pel valor mesurat per un indicador (valor indicador), s'haurà de cercar entre quins llindars es troba i aplicar el següent procediment, tenint en compte si els valors definits pels llindars (Valor 1 – Valor 4) son creixents o decreixents:

- Per valors de llindars creixents (valor Llindar Grau 1 < valor Llindar Grau 4)
  1) Si el valor és inferior al llindar 1, el grau serà 1.
  2) Si el valor és igual o superior al llindar 4, el grau serà 4.
  3) En la resta de casos s'aplicarà la fórmula de càlcul del Grau.
- Per valors de llindars decreixents (valor Llindar Grau 1 > valor Llindar Grau 4)
  1) Si el valor és superior al llindar 1, el grau serà 1.

2) Si el valor és igual o inferior al llindar 4, el grau serà 4.

3) En la resta de casos s'aplicarà la fórmula de càlcul del Grau.

Fórmula de càlcul del Grau:

$$\text{Grau} = \frac{(\text{Valor indicador} - \text{Valor llindar inferior})}{Valor\ llindar\ superior - Valor\ llindar\ inferior} + \text{Grau corresponent al llindar inferior}$$

En aplicar la fórmula de càlcul del Grau, cal tenir en compte les següents consideracions:

- Quan dos o més llindars prenen el mateix valor, el valor del *"Grau corresponent al llindar inferior"* correspon al del llindar coincident superior.

  Per exemple, quan el *Llindar Grau 1* i el *Llindar Grau 2* prenen el mateix valor, el "*Grau corresponent al llindar inferior"* correspon al del *Llindar Grau 2*, és a dir, pren valor 2.

- Quan el valor mesurat per un indicador (*valor indicador*) coincideix amb algun dels valors definits pels llindars (Valor 1, Valor 2, Valor 3), es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident. Quan dos o més llindars prenen el mateix valor, es prendrà com a "Valor llindar inferior" el valor corresponent al llindar coincident superior.

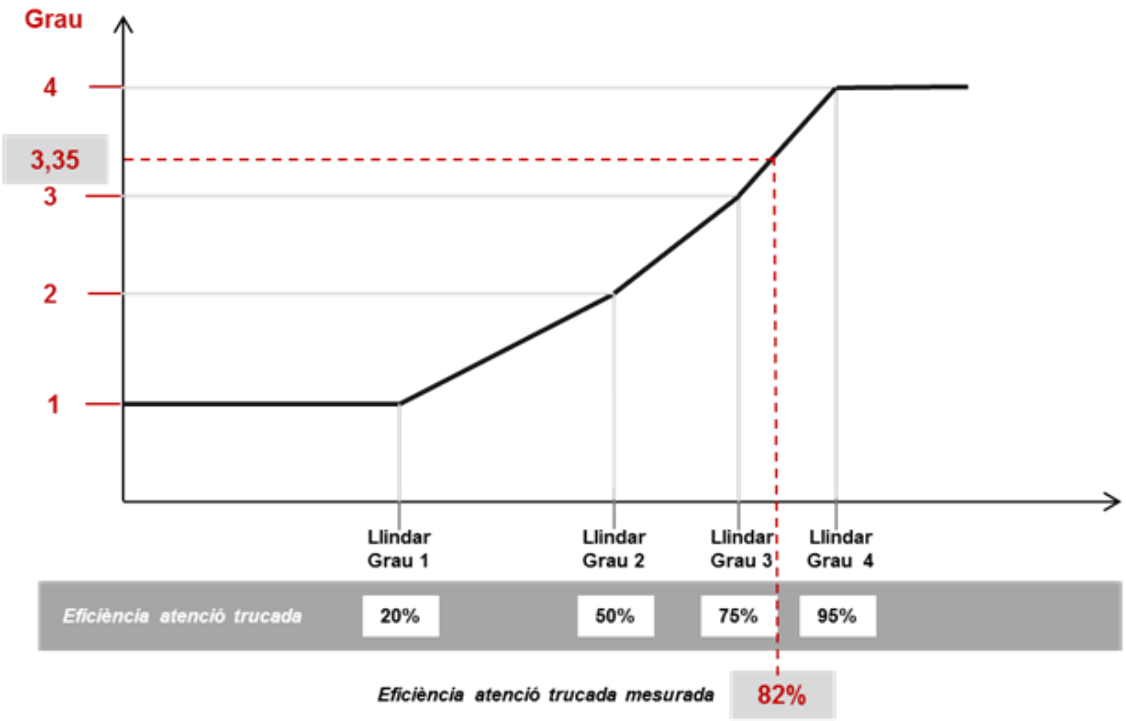
  Per exemple, suposant els següents valors de llindars: *Llindar Grau 1* i el *Llindar Grau 2* prenen el mateix valor, 20%, *Llindar Grau 3* pren valor 75% i *Llindar Grau 4* pren valor 95%; quan el valor mesurat pel l'indicador pren valor 20%, el "*Valor llindar inferior" pren valor 20%, el* "*Valor llindar superior" pren valor 75% i* el "*Grau corresponent al llindar inferior"* pren valor 2.

Exemple de càlcul:

Suposem que tenim l'indicador "Eficiència atenció trucada" que pot prendre valors percentuals entre 0% i 100% i que el valor objectiu és 95%. Si s'han definit els següents llindars:

- *Llindar Grau 1. El valor de l'indicador és 20%*
- *Llindar Grau 2. El valor de l'indicador és 50%*
- *Llindar Grau 3. El valor de l'indicador és 75%*
- *Llindar Grau 4. El valor de l'indicador és 95%*

Si el valor mesurat en un període per l'indicador "Eficiència atenció trucada" ha estat 82% el grau calculat és: ((82-75)/(95-75))+3=3,35.



Aquest model és dinàmic, ja que permet adaptar-se en el temps a nous nivells objectius i nivells mínims, sense variar els graus possibles.

Podríem determinar per exemple que durant la fase de transició del servei el llindar del grau 3 sigui del 85%, mentre que en la fase d'execució el segon any ja sigui del 95% i el llindar del grau 4 passi a 98%.

6.3. Relació ANS

Tot seguit es relacionen, segons l'estructura definida (aplicació, àmbit i contracte), els ANS a mesurar, el detall dels quals es troba a l'apartat 8.5.Detall Acords de Nivell de Servei.

6.3.1. ANS d'Aplicació

Codi	Nom	Servei	Periodicitat
AP-SU-01	Temps resposta consulta	SU	Mensual
AP-GO-01	Indisponiblitats generats per sonda resoltes per proveïdor aplicacions	GO	Mensual
AP-GN-03	Modificació de monitoratge	GN	Semestral
AP-SU-02	Temps màxim de resolució peticions de suport funcional o gestió usuaris	SU	Mensual

6.3.2. ANS d'Àmbit

Codi	Nom	Servei	Periodicitat
AM-SEG-01	Aplicacions crítiques que compleixen amb la norma de traces de la Generalitat de Catalunya	GN	Trimestral
AM-SEG-02	Vulnerabilitats crítiques i/o altes de l'aplicació	GN	Trimestral
AM-SEG-03	Correcció de vulnerabilitats crítiques d'aplicacions critiques de negoci	GN	Mensual
AC-SIC-01	Aplicacions amb codi font correctament custodiat	GN	Mensual
AC-SIC-02	Aplicacions amb automatització del desplegament implementada.	GN	Mensual
AC-IS-01	Iteracions per validar Documents d'Arquitectura	GN	Mensual
AC-IS-02	Termini de validació tècnica per entorn lliurat	GN	Mensual
AC-GOV-01	Aplicacions amb document d'arquitectura actualitzat	GN	Mensual

6.3.3. ANS de Contracte

Codi	Nom	Servei	Periodicitat
CT-GN-01	Factures invàlides realitzades per l'adjudicatari	GN	Anual
CT-GN-02	Proactivitat	GN	Quadrimestral

6.4. Fonts d'informació per a l'obtenció dels nivells de servei

El CTTI emprarà el sistema d'informació CONTIC (Control d'Acord de Nivell de Servei TIC) per al càlcul, anàlisi i emmagatzemament d'indicadors de servei i de procés. Tot i que a l'inici del servei el sistema d'informació CONTIC no sigui capaç de calcular tots els indicadors definits, s'aniran incorporant progressivament al seu catàleg. El proveïdor haurà de proveir els indicadors que estiguin sota la seva responsabilitat a través de les interfícies habilitades.

Sempre que sigui possible, l'origen de les dades utilitzat per al càlcul dels indicadors seran les eines de gestió dels tiquets i monitoratge del CTTI. Per aquells indicadors que el CTTI no sigui capaç d'obtenir de manera autònoma, serà responsabilitat de l'adjudicatari calcular-los i reportar-los amb la periodicitat establerta i el detall i format que requereixi el CTTI, podent arribar a nivell d'instància de servei o de tiquet.

El CTTI utilitzarà els indicadors de servei per realitzar els càlculs de compliment dels ANS i per generar els informes corresponents.

6.5. Modificació dels indicadors i nivells de servei

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei, el CTTI conjuntament amb el proveïdor consensuaran i planificaran la seva modificació.

Algunes de les causes que poden comportar aquestes modificacions són, entre d'altres, les variacions d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, les innovacions i les millores del servei.

6.6. Aplicació dels Acords de Nivell de Servei

Els Acords de Nivell de Servei definits per a cada servei seran d'obligat compliment al llarg del contracte, exceptuant la fase de transició del servei.

Per a cada servei, l'adjudicatari ha de complir plenament els Acords de Nivell de Servei definits una vegada finalitzada la fase de prestació en transició.

7. MODEL DE RELACIÓ

Per defecte, el model de relació i l'estructura de comitès que s'implementarà per la governança específica del serveis objecte d'aquest contracte basat són els detallats en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.
Addicionalment, el Comitè Operatiu del contracte basat establirà, amb la periodicitat determinada, el grau d'avenç del servei de desenvolupament i construcció.

ANNEXES

8.1. Classificació de les aplicacions

Per defecte, s'atendrà la classificació de les aplicacions descrita en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.

8.1.1. Criticitat de negoci

Atenent l'apartat 6.1.1 del Plec de Prescripcions Tècniques de l'Acord Marc.

8.1.2. Característiques de qualitat

Atenent l'apartat 6.1.2 del Plec de Prescripcions Tècniques de l'Acord Marc.

8.1.3. Classificació de seguretat de la informació

Atenent l'apartat 6.1.3 del Plec de Prescripcions Tècniques de l'Acord Marc.

8.2. Model de governança del contracte

Per defecte, el model de governança TIC de la Generalitat de Catalunya es troba detallat en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.

8.3. Funcions de l'Agència de Ciberseguretat de Catalunya

Les funcions de l'Agència de Ciberseguretat de Catalunya es troben detallades en el Plec de Prescripcions Tècniques de l'expedient CTTI-2019-20131 que regeix l'Acord Marc pel desenvolupament i manteniment de noves aplicacions de la Generalitat de Catalunya.

8.4. Requeriments i model de seguretat

8.4.1. Requeriments de seguretat

L'adjudicatari haurà de donar compliment al marc normatiu de seguretat vigent de la Generalitat de Catalunya. Tot i això, en aquest apartat es remarquen aquells aspectes de seguretat considerats de major rellevància dins l'abast del servei.

Classificació de seguretat de la informació

L'adjudicatari haurà de tenir en compte la classificació de la informació de les aplicacions/projectes a desenvolupar en el basat, realitzada pel negoci, per aplicar correctament el marc normatiu i legal de la Generalitat de Catalunya en matèria de seguretat.

Inventari

Informar i actualitzar la informació vinculada a les aplicacions (sobretot URLs, certificats digitals i nivell de classificació de les dades de l'aplicació) en el repositori que determini CTTI i l'Agència de Ciberseguretat de Catalunya.

Compliment Normatiu i Legal

- L'adjudicatari haurà de complir amb tots els requeriments que siguin d'aplicació d'acord al marc normatiu de seguretat vigent de la Generalitat de Catalunya i de totes les actualitzacions posteriors que es produeixin, així com a tot el marc legal en matèria de ciberseguretat que en sigui d'aplicació (per exemple, Esquema Nacional de Seguretat i GDPR – General Data Protection Regulation, eIDAS - electronic IDentification, Authentication and trust Services).
- L'adjudicatari haurà d'incorporar-se al model de compliment normatiu de la Generalitat de Catalunya, que porta a terme l'Agència de Ciberseguretat de Catalunya. En aquest model s'integren les possibles auditories que el CTTI o l'Agència de Ciberseguretat de Catalunya determinin realitzar, així com el seguiment dels plans d'acció derivats de les mateixes. També s'inclou en aquest model el compliment per part de l'adjudicatari de plans d'acció relatius a normatives o estàndards que el CTTI o l'Agència de Ciberseguretat de Catalunya determinin realitzar. L'adjudicatari haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en el model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat de Catalunya i el CTTI. La gestió del compliment es realitzarà amb l'eina que determini l'Agència de Ciberseguretat de Catalunya.
- L'adjudicatari haurà de garantir l'accés del personal autoritzat del CTTI i l'Agència de Ciberseguretat de Catalunya a la informació de seguretat (procediments, registre d'incidents, traces, entre d'altres). Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. El CTTI, l'Agència de Ciberseguretat de Catalunya i l'adjudicatari establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.
- En relació al tractament de dades de caràcter personal, l'adjudicatari donarà compliment com a encarregat de tractament a allò establert al Reglament General de Protecció de Dades. Pel que fa la seguretat en el tractament de les mateixes, l'adjudicatari implementarà les mesures de seguretat establertes per l'Agència de Ciberseguretat de Catalunya 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.
- En cas d'execució d'auditories i seguiment dels plans d'acció derivats, aquestes hauran de realitzar-ne amb la metodologia i eines establertes per l'Agència de Ciberseguretat de Catalunya.

Gestió d'excepcions de seguretat

L'empresa adjudicatària haurà de:

- Tramitar una excepció de seguretat per a cada control definit en el Marc Normatiu de Seguretat al que no es doni compliment, incloent un pla de mitigació i mesures compensatòries.
- Fer un seguiment continu de les excepcions de seguretat a les quals es veuen afectats els serveis objecte del contracte.

- Elevar riscos als Comitès de Seguiment en relació a excepcions considerades de risc alt, per assegurar la seva gestió i seguiment.
- Garantir que un cop les excepcions hagin expirat, es procedeixi a eliminar la mesura d'excepció. El CTTI i l'Agència de Ciberseguretat de Catalunya hauran d'autoritzar de forma expressa aquestes eliminacions.

Sistemes d'Identificació i Signatura Electrònica

A l'hora de desenvolupar una nova solució s'haurà d'utilitzar, sempre que sigui possible, la plataforma GICAR per autenticar els usuaris, considerant en el cas de les aplicacions crítiques l'ús de captcha i el doble factor d'autenticació.

Així mateix, es tindrà en consideració preferiblement el catàleg de sistemes d'identificació i signatura electrònica de la Generalitat de Catalunya i la guia d'ús que la desenvolupa per proposar solucions d'identificació i signatura a integrar als tràmits i procediments de l'Administració de la Generalitat de Catalunya en la seva relació amb la ciutadania.

Gestió de Traces:

L'adjudicatari haurà de complir amb la norma de gestió de traces vigent. L'adjudicatari haurà d'assegurar que l'aplicació emmagatzema totes les traces que li són d'aplicació d'acord a la seva classificació d'informació i al marc normatiu i legal aplicable.

Les traces hauran de ser accessibles en mode lectura i s'assegurarà el marcatge de les traces amb requeriments específics de conservació segons la legislació aplicable.

L'adjudicatari, tenint en compte el nivell de classificació de seguretat de l'aplicació, haurà de facilitar els mecanismes per a que les traces de l'aplicació siguin accessibles i estiguin integrades amb el repositori de traces corporatiu de la Generalitat de Catalunya.

Entre d'altres, aquestes traces han de permetre:

- La identificació i accessos dels diferents tipus d'usuaris i les accions realitzades (intents de connexions amb èxit i fallits, tasques d'administració dins l'aplicació, traces de la tramitació d'expedients administratius (qui i quan han fet què), consulta de dades especialment protegides, entre d'altres).
- La detecció/solució d'incidències.
- La detecció de possibles incidents de seguretat.

En el cas d'aplicacions Devops, l'adjudicatari haurà de garantir la configuració dels logs de seguretat de la infraestructura conforme la normativa aplicable.

Comunicacions Segures:

L'adjudicatari haurà de garantir que les aplicacions, ja siguin publicades a internet com a intranet, utilitzin canals de comunicació segurs (HTTPS/TLS) a la seva interfície d'usuari i en la interconnexió amb d'altres aplicacions, configurant protocols i algorismes criptogràfics robustos d'acord a les indicacions de l'Agència de Ciberseguretat de Catalunya.

Arquitectura, proves de recuperació de desastres i proves de recuperació de backups

L'adjudicatari haurà de:

- Garantir que el disseny de l'arquitectura de la solució/aplicació permet assolir els requeriments de disponibilitat/continuïtat requerits.
- Participar en la preparació i execució de les proves de continuïtat/recuperació de desastres (PRDs) i en les proves de recuperació de backups, realitzant proves que certifiquin que l'aplicació està operativa i s'accedeix a la informació recuperada de forma correcta.

Signatura del codi de les aplicacions:

- Signatura d'applets per qualsevol sistema d'informació. El codi objecte dels applets haurà d'anar signat amb un certificat digital de la Generalitat de Catalunya per tal de garantit la integritat.

Gestió d'usuaris administradors/ desenvolupadors:

L'adjudicatari haurà de complir la Guia de Gestió de Comptes d'Administració de la Generalitat de Catalunya.

Entre d'altres mesures, l'adjudicatari haurà de:

- Caldrà limitar al màxim els usuaris amb elevats privilegis. Sempre s'haurà de fer amb comptes nominals. En cas de requerir un usuari privilegiat per part dels desenvolupadors, aquest fet s'haurà de notificar a l'Agència de Ciberseguretat de Catalunya per la seva autorització i avaluació del risc associat.
- Recertificar els usuaris privilegiats de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades.

Seguretat en la prestació el servei:

L'adjudicatari haurà de:

- Tots els equips dels administradors/desenvolupadors hauran complir amb les mesures de seguretat que estableixi l'Agència de Ciberseguretat de Catalunya i el CTTI (EDR, antivirus, per exemple) per poder accedir als equips i xarxa de la Generalitat de Catalunya. En cap cas es farà ús d'equips que la Generalitat de Catalunya (CTTI i Agència de Ciberserguretat de Catalunya) no hagi autoritzat.
- En cas d'accés remot, tots els administradors/desenvolupadors hauran d'accedir a través de la solució de VPN corporativa i disposar d'un segon factor d'autenticació (MFA) per minimitzar el risc de robatori de credencials. Igualment, si les eines corporatives ho permeten, qualsevol accés d'un administrador/desenvolupador des de dins de la xarxa corporativa, també haurà de disposar d'un doble factor d'autenticació.
- De forma general, aplicar les mesures de prevenció i protecció de la informació d'acord als estàndards de la Generalitat de Catalunya.
- L'adjudicatari podrà serà auditat de forma periòdica per valorar el grau de compliment i identificar riscos de seguretat.

8.4.2. Descripció del model de seguretat en el desenvolupament d'aplicacions

Per garantir un adequat nivell de seguretat de les aplicacions, l'adjudicatari haurà de contemplar la seguretat en els diferents moments del cicle de vida d'una aplicació. Aquestes actuacions permetran gestionar els riscos de seguretat de qualsevol aplicació en tot moment, i prendre les decisions que es considerin oportunes.

El proveïdor haurà de:

- A la fase de recollida de requeriments funcionals:
    - El proveïdor haurà de tenir en compte els requeriments de seguretat, funcionals i no funcionals, per tal que la solució doni resposta a aquests requeriments. Si no els coneix, haurà de demanar-los al responsable del sistema o Gestor de Solucions o, en el seu defecte, a l'Agència de Ciberseguretat de Catalunya.
- A la fase de desenvolupament de l'aplicació:
    - Completar i lliurar a l'Agència de Ciberseguretat de Catalunya el Document d'Arquitectura (DA) incloent la següent informació:
        - Tipus d'informació tractada.
        - Solució proposada per donar resposta als requeriments, funcionals i no funcionals, definits prèviament.
    - Desenvolupar i implantar totes aquelles mesures de seguretat definides en el DA.
    - Donar tota la documentació o informació relativa a la solució que l'Agència de Ciberseguretat de Catalunya pugui requerir.
    - Per les aplicacions web, l'adjudicatari haurà de realitzar l'anàlisis de seguretat dinàmics (OWASP) durant les diverses fases del desenvolupament. Aquestes proves s'hauran de realitzar en els entorns no productius i haurà d'utilitzar una eina d'anàlisi dinàmic configurada segons les indicacions de l'Agència de Ciberseguretat de Catalunya. El proveïdor haurà de lliurar a l'Agència de Ciberseguretat de Catalunya l'informe resultant de l'anàlisi proporcionat per l'eina i realitzarà les correccions corresponents.
    - Vetllar per aplicar les millors pràctiques de seguretat en el desenvolupament de les aplicacions. Per validar això, el proveïdor haurà de revisar les vulnerabilitats de seguretat identificades en l'anàlisi de codi estàtic realitzat amb l'eina de Qualitat de CTTI o amb l'eina que el proveïdor proposi (prèvia validació per part de l'Agència de Ciberseguretat de Catalunya). Caldrà que el proveïdor corregeixi les vulnerabilitats identificades.
    - Serà un requisit per passar l'aplicació a producció que la informació aportada als apartats de seguretat del DA sigui completa i de qualitat, i

que el resultat de les proves realitzades per l'adjudicatari estigui dins dels llindars permesos.

- L'Agència de Ciberseguretat de Catalunya podrà executar qualsevol mena d'anàlisi (dinàmic o estàtic) que consideri oportú en qualsevol moment per determinar si el nivell de seguretat de l'aplicació compleix els requisits de seguretat previ el pas a producció. En aquests casos l'adjudicatari haurà de proveir d'un usuari de prova per la completa execució de les anàlisis.

8.5. Detall Acords de Nivell de Servei

En les taules següents es detallen els Acords de Nivell de Serveis que s'apliquen a la present licitació.

8.5.1. ANS d'Aplicació

						Grau				
Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	Penalització màxima
AP-SU-01 **(IM.PRO.1.TS)**	Temps resposta consulta	Percentatge de tasques finalitzades en el mes a mesurar	SU	Nombre de tasques finalitzades en temps en el mes a mesurar / Nombre de tasques finalitzades totals en el mes a mesurar * o Prioritat Critica < 8h o Prioritat Alta < 14h o Prioritat Mitja < 32h o Prioritat Baixa < 32h *(Independentment de la data d'arribada)	mensual	65%	75%	80%	90%	2% Import mensual recurrent aplicació
AP-GO-01	Indisponiblitats detectades per les sondes, resoltes per proveïdor d'aplicacions	Disponibilitat inferior al llindar establert segons criticitat de negoci, per causes atribuïbles al proveïdor d'aplicacions durant l'horari de servei	GO	Si (Temps de servei / Temps total < llindar de disponibilitat segons criticitat de negoci) = 1 En cas contrari = 0 Llindar de disponibilitat segons criticitat de negoci: o Molt alta: 99,90% o Alta: 99,5% o Mitja: 95% o Baixa (no aplica)	mensual	1	0	0	0	Sobre l'import de recurrent de l'aplicació segons la seva criticitat de negoci: o 2,5% per molt alta o 2% per alta o 1,5% per mitja
AP-GN-03	Modificació de monitoratge	Hores laborables entre la modificació d'un servei existent i el seu monitoratge, així com la integració amb l'eina de monitoratge de CTTI	GN	Data i hora de modificació del monitoratge de l'aplicació - data i hora de posada en producció de l'evolutiu de l'aplicació	semestral	16	8	4	2	2% de l'import de recurrent de l'aplicació

Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Grau				Penalització màxima
						Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	
AP-SU-02 **(IM.APL.006)**	Temps màxim de resolució peticions de suport funcional o gestió usuaris	Nombre de tasques resoltes en temps en el mes a mesurar / Nombre de tasques resoltes totals en el mes a mesurar	SU	Nombre de tasques resoltes en temps en el mes a mesurar / Nombre de tasques resoltes totals en el mes a mesurar * o Prioritat Crítica < 8h o Prioritat Alta < 8h o Prioritat Mitja < 16h o Prioritat Baixa < 32h *(Independentment de la data d'arribada) **Inclou tiquets gestionats a Remedy o altre eina de proveïdor ***Les mètriques comptabilitzaran 10x5 sense tenir en compte l'horari de l'aplicació	Mensual	65%	75%	90%	100%	2% Import mensual recurrent aplicació

8.5.2. ANS d'Àmbit

Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Grau				Penalització màxima
						Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	
AM-SEG-01	Aplicacions crítiques de negoci que compleixen amb la norma de traces de la Generalitat de Catalunya	Percentatge d'aplicacions crítiques de negoci que compleixen la normativa de traces de la Generalitat de Catalunya	GN	Nombre d'aplicacions crítiques compleixen norma traces / Nombre total aplicacions crítiques	Trimestral	50%	60%	80%	100%	2% de l'import de la suma del recurrent de les aplicacions que no compleixen
AM-SEG-02	Webs publicades a Internet amb HTTPS	Percentatge de webs publicades a Internet amb HTTPS	GN	Nombre total de webs publicades a internet amb HTTPS / Nombre total de webs publicades a Internet, d'acord a la planificació acordada amb el CTTI	Bimensual	70%	80%	90%	100%	2% de l'import de la suma del recurrent de les aplicacions que no compleixen

						Grau				
Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	Penalització màxima
AM-SEG-03	Correcció de vulnerabilitats crítiques i/o altes d'aplicacions critiques de negoci	Percentatge d'aplicacions critiques de negoci auditades amb vulnerabilitats crítiques i/o altes que no han estat corregides durant els 2 mesos posteriors a la seva identificació o que no s'han aplicat mesures de contenció sobre aquestes vulnerabilitats.	GN	Nombre d'aplicacions critiques de negoci auditades amb vulnerabilitats crítiques i/o altes que no han estat corregides durant els 2 mesos posteriors a la seva identificació o que no s'han aplicat mesures de contenció sobre aquestes vulnerabilitats / Nombre total d'aplicacions critiques de negoci auditades amb vulnerabilitats crítiques i/o altes	Trimestral	10%	5%	0%	0%	2% de l'import de la suma del recurrent de les aplicacions que no compleixen
AC-SIC-01	Aplicacions amb codi font correctament custodiat.	Percentatge d'aplicacions amb codi font correctament custodiat.	GN	Nombre d'aplicacions amb codi font al SIC / Nombre total d'aplicacions adjudicades que no tinguin una excepció d'exempció	Mensual	50%	75%	100%	100%	2% Import mensual recurrent aplicacions sense codi font correctament custodiat
AC-SIC-02	Aplicacions amb automatització del desplegament implementada.	Percentatge d'aplicacions amb automatització del desplegament implementada.	GN	(Nombre d'aplicacions sense planificació + Nombre d'aplicacions amb incompliment de planificació) / Nombre total d'aplicacions adjudicades que no tinguin una excepció d'exempció	Mensual	50%	75%	100%	100%	2% Import mensual recurrent aplicacions sense automatització del desplegament implementada
AC-IS-01	Iteracions per validar Documents d'Arquitectura	Mitjana d'iteracions per aconseguir la validació d'un Document d'Arquitectura	GN	Nombre total d'iteracions necessàries per aconseguir la validació /Nombre total de documents presentats en el període d'anàlisi[1] [1]Són els documents presentats en vigència comptabilitzant a partir de la primera versió revisada	Mensual	5	4	2	2	2% import mensual recurrent de l'àmbit

Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Grau				Penalització màxima
						Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	
AC-IS-02	Termini de validació tècnica per entorn lliurat	Percentatge de compliment del termini de validació tècnica per entorn lliurat	GN	Nombre d'entorns lliurats[1] que han excedit els dies establerts en el procés d'integració de solucions / Total acumulat d'entorns lliurats per aquest adjudicatari en la vigència del contracte. [1]Són els entorns lliurats per projecte d'acord als requeriments indicats per part de l'adjudicatari	Mensual	65%	75%	90%	100%	2% Import mensual recurrent aplicacions sense automatització del desplegament implementada
AC-GOV-01	Aplicacions amb document d'arquitectura actualitzat	Percentatge d'aplicacions amb document d'arquitectura actualitzat	GN	Nombre d'aplicacions[1] amb Document d'Arquitectura disponible i actualitzat / Nombre total d'aplicacions adjudicades que no tinguin una excepció d'exempció. [1]Són les aplicacions gestionades per l'adjudicatari	Mensual	50%	75%	100%	100%	2% Import mensual recurrent aplicacions sense document d'arquitectura actualitzat

8.5.3. ANS de Contracte

Codi	Nom	Descripció	Servei	Fórmula d'obtenció/eina	Periodicitat	Grau				Penalització
						Llindar grau 1	Llindar grau 2	Llindar grau 3	Llindar grau 4	
CT-GN-01	Factures invàlides realitzades per l'adjudicatari	Percentatge de factures de l'adjudicatari que no compleixen l'estàndard, que estan mal emeses o tenen un error	GN	Nombre de factures invàlides realitzades per l'adjudicatari / Nombre total de factures realitzades per l'adjudicatari	Anual	30%	20%	10%	0%	0,1% facturació global del lot
CT-GN-02	Proactivitat	Nombre d'iniciatives de millora implantades i aprovades	GN	Nombre d'iniciatives de millora presentades amb indicadors de millora associats	Quadrimestral	2	3	4	10	0,1% facturació global del lot

8.6. Annex Tècnic HES-IMMUNITZACIONS

8.7. ModelAgilSalut_AgilePlaybook

8.8. Model de Gestió de QA HES