

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA CONSTRUCCIÓ D'UNA PLATAFORMA OBERTA EN SALUT - COMPONENTS D'ARQUITECTURA, MERCAT D'APLICACIONS I SERVEIS DE PLATAFORMA

ANNEX 2: ARQUITECTURA

CTTI/2025/113

Barcelona, febrer 2025

Historial de versions i contribucions

Descripció de la revisió	Autor	Data	Versió
Esborrany inicial		20/01/25	0.1

Índex

1	INTRODUCCIÓ	6
2	Principis i decisions de disseny	7
2.1	Arquitectura de referència.....	7
2.2	Principis.....	7
2.3	Característiques de l'arquitectura	7
3	DESCRIPCIÓ DELS COMPONENTS REQUERITS COM A OBJECTE DEL CONTRACTE 8	
3.1	Nucli de la plataforma oberta	9
3.1.1	Orquestració i gestió de processos.....	9
3.1.2	Gestió de dades clíniques	11
3.1.3	Anàlisi de dades clíniques.....	11
3.1.4	Resiliència de l'arquitectura.....	11
3.1.5	Integració de serveis	12
3.1.6	Sistema de suport a la decisió clínica	12
3.2	Mercat d'aplicacions.....	14
3.2.1	Portal del Mercat d'aplicacions	20
3.2.2	Entorn de desenvolupament / Sandbox	22
3.2.3	Procés d'homologació	24
3.2.4	Proces de publicació de l'aplicació	25
3.2.5	Portal del Marketplace. Consum de les aplicacions	26
3.3	Enginyeria de Plataforma	30
3.3.1	Observabilitat.....	30
3.3.2	FinOps.....	30
3.3.3	Portal d'autoservei	31

3.3.4	Seguretat.....	31
3.3.5	Recuperació davant desastres	32
3.3.6	Documentació.....	32
3.3.7	Qualitat en el servei	33
3.3.8	Gestió de la capacitat.....	33
3.3.9	Operació plataformes.....	34
4	<i>Components Habilitadors de Salut d'Utilització Obligatoria</i>	35
4.1	Plataforma de Seguretat – PDS	35
4.2	Repositori de Dades Clíniques – RDC.....	35
4.3	Mestre de Pacients – MPI	35
4.4	Index Server.....	36
4.5	Servidor Terminològic	36
4.6	Plataforma Auditoria.....	37
4.7	Servidor de Recursos - Professionals i Organització	38
4.8	Traçabilitat Distribuïda	38
4.9	Gateway de Comunicacions.....	39
4.10	Gestor Documental.....	39
4.11	Plataforma Corporativa de gestió de claus d'encryptació	40
5	<i>REQUISITS DE LA SOLUCIÓ TECNOLÒGICA APORTADA.....</i>	41
5.1	Requisits de l'arquitectura de la plataforma	41
5.1.1	Connectivitat al Nus de comunicacions de la Generalitat de Catalunya.....	41
5.1.2	Adreçament dels servidors	41
5.1.3	Serveis de DNS	41

5.1.4	Encaminament.....	41
5.1.5	Serveis de Comunicacions.....	42
5.1.6	Alta Disponibilitat	42
5.1.7	Requisits detallats de l'arquitectura	42
5.1.8	Descripció de l'Arquitectura.....	44
5.2	Instal·lació, configuració i suport post-implantació de la solució tecnològica	45

1 INTRODUCCIÓ

Aquest annex està dedicat a definir l'arquitectura tecnològica sobre la que han d'executar-se els serveis i funcionalitats als que hauran de donar resposta els elements inclosos a la proposta. L'objectiu és implementar una plataforma oberta i flexible, que garanteixi l'escalabilitat i el rendiment, assegurant la qualitat i fiabilitat, facilitant la governança i el control, optimitzant el cost total de propietat, habilitant la innovació i l'agilitat i garantint la seguretat i privacitat de les dades tractades per la plataforma.

Amb el context donat per a la plataforma oberta de Salut, es preveuen tres divisions de l'arquitectura completament diferenciades.

La primera seria la que contemplaria l'execució de tots aquells components que conformarien l'entorn de treball dels professionals clínics, els serveis a altres entitats proveïdores i institucions sanitàries i els serveis a prestar al ciutadà beneficiari del sistema nacional de salut. A aquesta part l'anomenarem Nucli de la plataforma.

La segona seria la que contemplaria els components necessaris per a que les empreses desenvolupadores de programari de la salut, i les entitats proveïdores de serveis sanitaris, puguin oferir i consumir els productes digitals allà exposats. A aquesta part l'anomenarem Mercat d'Aplicacions de la plataforma.

La tercera seria la que contemplaria els components necessaris de l'arquitectura actual de Salut i CTTI que caldria utilitzar de forma obligatòria en les divisions anteriors, donat que cobreixen aspectes de negoci i tecnològics que es consideren habilitadors per a la plataforma oberta i el mercat d'aplicacions

En els següents capítols aprofundim en les seves diferències i característiques peculiars de cadascuna, i en un disseny preliminar dels seus components principals. Aquest disseny s'ha de considerar un marc de treball sobre el que desenvolupar una arquitectura que incorpori els elements, requerits per donar resposta a les funcionalitats presentades al present plec de prescripcions tècniques.

2 Principis i decisions de disseny

L'arquitectura de la plataforma oberta estarà subjecta als mateixos principis i característiques ja publicats per a les noves aplicacions del Pla director de Sistemes d'Informació (PDSIS). A continuació es proveeixen els enllaços als documents corresponents

2.1 Arquitectura de referència

Al pla director de sistemes hem establert el següent manifest per l'arquitectura de referència que és d'obligat compliment en tots el desenvolupament de nous sistemes com els que ens ocupen en aquesta licitació: <https://salutweb.gencat.cat/ca/ambits-actuacio/linies/tic/solucions-siscat/model-adhesio/arquitectura-tecnologica/manifest-referencia-iniciatives/index.html>

Específicament per aquesta licitació, aplicarien les següents restriccions addicionals:

- 1) La infraestructura necessària serà desplegada al cloud AWS sota el marc de seguretat de xarxa del CTTI NET0
- 2) No obstant el punt anterior, l'arquitectura haurà d'estar dissenyada per a poder-se desplegar en entorns multicloud. Aquest punt és especialment rellevant en l'elecció de components SaaS, que el mercat ja ofereix solucions que permeten el seu desplegament multicloud, com, per exemple, MongoDB Atlas. Aprofitant aquestes solucions, en un futur un desplegament multicloud només seria qüestió de configurar adequadament la connexió a aquests sistemes, sense duplicar la infraestructura ni requerir de coneixements experts d'operació d'aquestes solucions per l'equip que operarà la plataforma.
- 3) El component Shell principal dels microfrontals es desenvoluparà amb el marc de treball Single-Spa: <https://single-spa.js.org>

2.2 Principis

Els principis que regeixen l'arquitectura de les solucions del PDSIS es pot trobar a <https://hdl.handle.net/11351/10576>

2.3 Característiques de l'arquitectura

Les característiques de l'arquitectura de les solucions del PDSIS es poden trobar a la referència https://salutweb.gencat.cat/web/.content/_ambits-actuacio/Linies-dactuacio/tic/pdsis/caracteristiques-arquitectura-tecnologica-pdsis.pdf

3 DESCRIPCIÓ DELS COMPONENTS REQUERITS COM A OBJECTE DEL CONTRACTE

Tal i com s'ha reflectit la introducció d'aquest annex, la nova plataforma oberta consta de tres contextos diferenciats. En aquest capítol es detallen els que són objecte de construcció dins del contracte.

El primer contempla el nucli d'execució transaccional de la plataforma, on s'executaran les solucions admeses a operar dins de la mateixa, i que donarà servei a totes les necessitats d'atenció clínica dels diferents usuaris de la plataforma, siguin ciutadans, professionals assistencials, gestors de serveis de salut, entitats proveïdores de serveis de salut, empreses desenvolupadores de solucions, i operadors de la mateixa. Aquest context ha de gaudir dels nivells més alts de disponibilitat, fiabilitat i seguretat, sent un servei 24x7 en tots els seus components.

El segon context es el que anomenem "Mercat d'aplicacions", que contempla tot el necessari per a que les empreses desenvolupadores de solucions puguin oferir les seves solucions a la plataforma, i per a que els gestors de la plataforma oberta puguin certificar amb els màxims nivells de qualitat, seguretat i protecció de la informació, que una solució és apta per a operar en el context transaccional. Aquest context ha de gaudir de nivells alts de disponibilitat, fiabilitat i seguretat, sent un servei 12x5 en la majoria dels seus serveis, exceptuant aquells que haurien de permetre la resolució d'incidències en la plataforma transaccional, que també haurien de ser 24x7.

El tercer context es el que anomenem serveis transversals de la plataforma, i que seran utilitzats tant pel nucli d'execució com pel mercat d'aplicacions. Contemplen subsistemes com observabilitat, finops, seguretat, etc.

3.1 Nucli de la plataforma oberta

El nucli d'execució transaccional de la plataforma segueix el paradigma de les arquitectures componibles, en el que les solucions corresponents a dominis funcionals diferents col·laboren en oferir una solució composta per la combinació d'elles, sota uns processos definits. A continuació és mostra l'arquitectura de referència per a un d'aquests components:

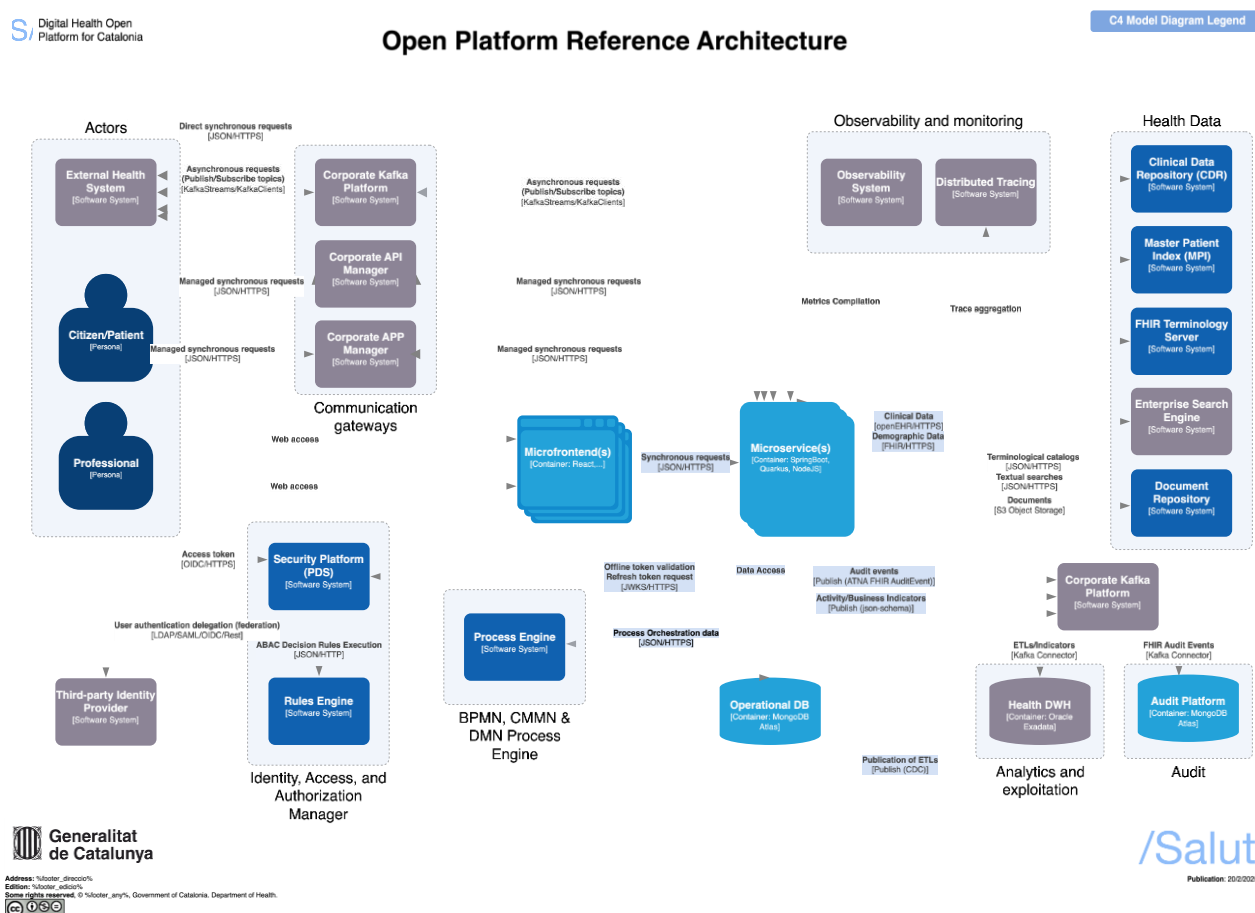


Figura 1. Arquitectura de Referència de Salut

Tal i com s'ha comentat en el paràgraf anterior, tots aquests components corresponen a dominis diferents i es combinen per a donar una visió conjunta en base a uns processos definits i amb característiques específiques per l'àmbit de salut.

Aquests sistemes que corresponen a dominis funcionals s'executen en el nucli de la plataforma oberta, que comprèn les següents característiques:

3.1.1 Orquestració i gestió de processos

Aquesta solució d'orquestració o coreografia de components de negoci és la que aporta la part més innovadora de la plataforma oberta, i que no té un referent clar en el sector de la salut. El

motor de processos haurà de suportar diferents notacions que seran aplicables com Business Process Modeling Notation (BPMN), Case Management Model and Notation (CMMN) i Decision Model and Notation (DMN). La previsió de l'ús de les tres notacions deriva de l'alt grau de flexibilitat que requereix qualsevol professional assistencial en l'aplicació d'aquests processos per adequar-los al cas clínic concret al que s'ha d'afegir la necessitat d'integritat i adequació a les regulacions dels processos i presa de decisions, i que permetessin la utilització de semàntica i ontologies clíniques apropant el disseny als professionals sanitaris

En conseqüència, malgrat que es defineixin processos a nivell global o local, caldrà que la plataforma incorpori mecanismes de feedback per a la millora continua dels processos definits, i fins i tot, avaluar tendències en l'ús dels processos per detectar si un procés definit per un professional assistencial gaudeix de més acceptació per la comunitat que el definit pels modeladors de processos corporatius.

L'eina de processos haurà de governar tant la presentació de cada mòdul mitjançant una estació de treball clínic (ETC), administratiu, o dirigit al pacient, com els contractes API que pugui oferir cada aplicació, així com el tractament d'esdeveniments que es puguin generar en altres aplicacions homologades.

En temps de disseny, caldrà definir:

- Els espais disponibles de la ETC i com s'omplen amb els microfrontends de cada mòdul, establint criteris de compatibilitat entre mòduls;
- Les APIs a consumir i com es mapegen resultats entre elles;
- Els esdeveniments disponibles i com es reacciona a cadascun d'ells.

El dissenyador de processos hauria de disposar:

- D'un mapa de possibles candidats a següent pas del procés;
- Facilitar una eina visual per mapejar dades entre apis i compondre els processos;
- Permetre la composició al vol de variants de processos en temps d'execució;
- Registrar l'execució dels processos per analitzar tendències en l'ús i retornar feedback de quin procés es el dominant en aquell episodi o tractament clínic;
- Tenir la llibertat que en algun moment de la cadena es pugui marcar un procés com a no modificable. S'hauria de poder evitar que els processos no modificables es puguin clonar i crear variants.

L'eina haurà de permetre les proves i validació dels processos abans de ser pujats a la plataforma productiva, incloent la seva presentació, el mapeig correcte de dades entre APIs i la reacció adient

als esdeveniments generats per altres mòduls del procés. Així mateix, la informació de disseny, ús i execució dels processos haurà de ser accessible pel seu anàlisi.

Un cop desplegat el procés, l'eina executarà l'automatització del procés en el moment que aquest sigui invocat per alguna de les aplicacions presents en el sistema o pel propi nucli en resposta a un esdeveniment donat.

La mateixa eina serà l'encarregada de realitzar el monitoratge i anàlisi de l'execució del procés, mitjançant un procediment de Process Mining que analitzant els logs, permeti optimitzar els processos, detectant ineficiències, colls d'ampolla, bloquejos indefinits i processos finalitzats de forma inesperada.

3.1.2 Gestió de dades clíniques

Els components que facin ús de dades clíniques hauran d'adequar-se a les estructures de definició semàntica del repositori de dades clíniques (openEHR). La plataforma haurà de disposar d'eines que permetin gestionar la seguretat d'accés a les dades clíniques d'acord amb uns perfils definits a la Plataforma de Seguretat.

Pels casos de "raw data" provinent de dispositius mèdics, s'hauran de proposar els models de persistència i gestió d'accés d'acord amb les indicacions del pacient.

3.1.3 Anàlisi de dades clíniques

Una altra característica del nucli de la plataforma oberta es la possibilitat de tenir un entorn d'execució privat, sobre tot per necessitats d'ús secundari (per exemple, recerca), on determinades aplicacions puguin operar sobre la plataforma però només siguin executables per certs col·lectius determinats prèviament. Tota la informació generada per aquestes aplicacions restringides haurà de ser restringida de la mateixa manera i no ser disponible per als usuaris en general.

Aquest entorn haurà de tenir accés a les dades clíniques i a la informació de disseny i execució dels processos per la recerca d'ús i efectivitat dels mateixos.

3.1.4 Resiliència de l'arquitectura

L'arquitectura de la plataforma oberta haurà d'aportar els màxims nivells de resiliència per la criticitat de la informació que manega i per l'abast de la població a la que dona servei. En aquest sentit, l'arquitectura estarà preparada per a un desplegament multi-proveïdor de Cloud, on fins i tot la caiguda de tot un proveïdor no causi una disrupció en el servei donat als ciutadans de Catalunya i als professionals sanitaris que utilitzaran la plataforma.

Tanmateix, en aquesta licitació no es requereix arribar a aquest nivell de funcionament multicloud, però sí que es requereix que la plataforma funcioni en almenys dues regions de AWS, atenent a criteris de latència i de disponibilitat dels productes propis d'AWS i SaaS que conformaran la

plataforma. Dins de les regions, es requereix alta disponibilitat multizona en tots els components del nucli de la plataforma.

3.1.5 Integració de serveis

Una part important de la plataforma oberta és precisament la capacitat d'integració dels serveis i aplicacions que es despleguin sobre la mateixa. En aquest sentit, comptarem amb tres plataformes d'integració corporatives i una pròpia de la plataforma per intercanvi de fitxers.

3.1.5.1 API Manager Corporatiu

La plataforma connectarà les aplicacions i plugins que requereixin de protocol REST/HTTPS mitjançant l'API Manager corporatiu que proporciona el CTTI. D'aquesta manera es poden aconseguir els següents avantatges:

- Centralitzar el control de les comunicacions
- Controlar la seguretat
- Gestionar les quotes de servei
- Proporcionar un catàleg de serveis disponibles i el seu versionat

3.1.5.2 Plataforma Transversal d'Interoperabilitat IPaaS

S'utilitzarà la plataforma transversal d'Interoperabilitat per a facilitar la transformació i intercanvi de missatges entre sistemes llegats de Salut i les aplicacions modernitzades dins de la plataforma.

3.1.5.3 Plataforma Transversal d'Esdeveniments

La plataforma transversal d'esdeveniments basada en Kafka, proporciona serveis comuns de missatgeria d'esdeveniments i CDC entre sistemes. La plataforma es àmpliament utilitzada actualment en diferents casos d'ús.

3.1.5.4 Plataforma d'intercanvi de fitxers de Salut

Per aquells sistemes d'informació amb el que es realitza una compartició de fitxers, caldrà habilitar un espai de compartició obert que assumeixi les capacitats de l'actual aplicació legacy de Gestió de Transferència de Fitxers. Els usuaris consumidors d'aquest servei formaran part del sistema de gestió d'identitats i accessos de la plataforma oberta.

3.1.6 Sistema de suport a la decisió clínica

Aquest sistema es centra en la implementació de regles de decisió clínica (CDS, Clinical Decision Support). Aquestes regles ajuden els professionals mèdics a prendre decisions basades en les dades del pacient i en algorismes clínics predefinitos.

Estarà compostat per les següents peces:

- **Motor de Regles:** Aquest plug-in treballa amb un motor de regles que permet definir regles mèdiques complexes, en llenguatge natural, que s'apliquen a partir de dades clíniques en temps real. Aquest motor pot utilitzar formats estàndard per a les regles i també models de IA Generativa pre-entrenats clínicament amb eines acceleradores de l'entrenament.
- **Integració amb la Base de Dades Clínica:** Les regles es poden executar en temps real sobre la base de dades clínica existent, avaluant informació rellevant com resultats de laboratoris, historial de tractaments o altres dades per donar suport a la presa de decisions.
- **Interacció amb altres Plug-ins:** Les regles poden influir o ser influenciades per altres plug-ins. Per exemple, un plug-in de regla clínica pot enviar una alerta a un widget que un metge consulta, o pot desencadenar automàticament un procés clínic.

3.2 Mercat d'aplicacions

El mercat d'aplicacions serà una solució que permetrà, a qualsevol empresa desenvolupadora, la integració de les seves solucions dins de la plataforma oberta. Per tant, es tracta d'un públic objectiu diferent al de la plataforma oberta transaccional i requerirà d'elements de seguretat diferents i un alt component de govern i homologació de les solucions proposades. En aquest sentit es podrien enumerar els seus components principals com:

- Portal del mercat d'aplicacions, dedicat bàsicament a perfils desenvolupadors i gestors de les empreses fabricants;
- Espai amb tota la documentació, eines i guies necessàries per a l'ús del mercat d'aplicacions;
- Aplicació d'administració del propi portal;
- Model plantilla d'entorn de desenvolupament pels proveïdors;
- Procés d'Homologació d'aplicacions i la seva documentació. Aquest cobriria els mínims per compondre processos en base a interfícies comunes de:
 - A quina regió de la Estació de Treball va el microfrontend;
 - Observabilitat;
 - Facturació per ús;
 - Documentació d'APIs i esdeveniments que es generen;
 - Normalització de les dades entre camps de les APIs;
- Repositori i entorn de desplegament de les aplicacions un cop homologades (Sandbox / Catàleg);
- Entorn beta de la plataforma oberta transaccional on les empreses puguin testear els seus productes abans d'entrar en producció, o per provar la seva compatibilitat amb noves versions de la plataforma;
- Registre d'usuaris;
- Catàleg d'artefactes i components de l'arquitectura componible;
- Observabilitat dels components propis per a les empreses desenvolupadores;
- Gestió de l'incidental dels components propis de les empreses;
- Entorn de gestió de la facturació / Pagament per ús;
- Altres.

Aquestes aplicacions es posaran a disposició de la ciutadania, el que identifica un altre tipus d'usuari amb necessitat de cerca i accés a les aplicacions que poden ser de lliure utilització i/o que requereixin prescripció professional.

L'ús de les aplicacions haurà de ser registrada i gestionada de forma que es pugui implantar un model de gestió de consums i costos.

A continuació, des del punt de vista del desenvolupament, es mostra un diagrama amb una proposta preliminar del que podria ser el portal del mercat d'aplicacions (Nota: els productes esmentats als diagrames estan expressats a mode d'exemple, no d'elecció ja realitzada):

Level 1 Context Diagram

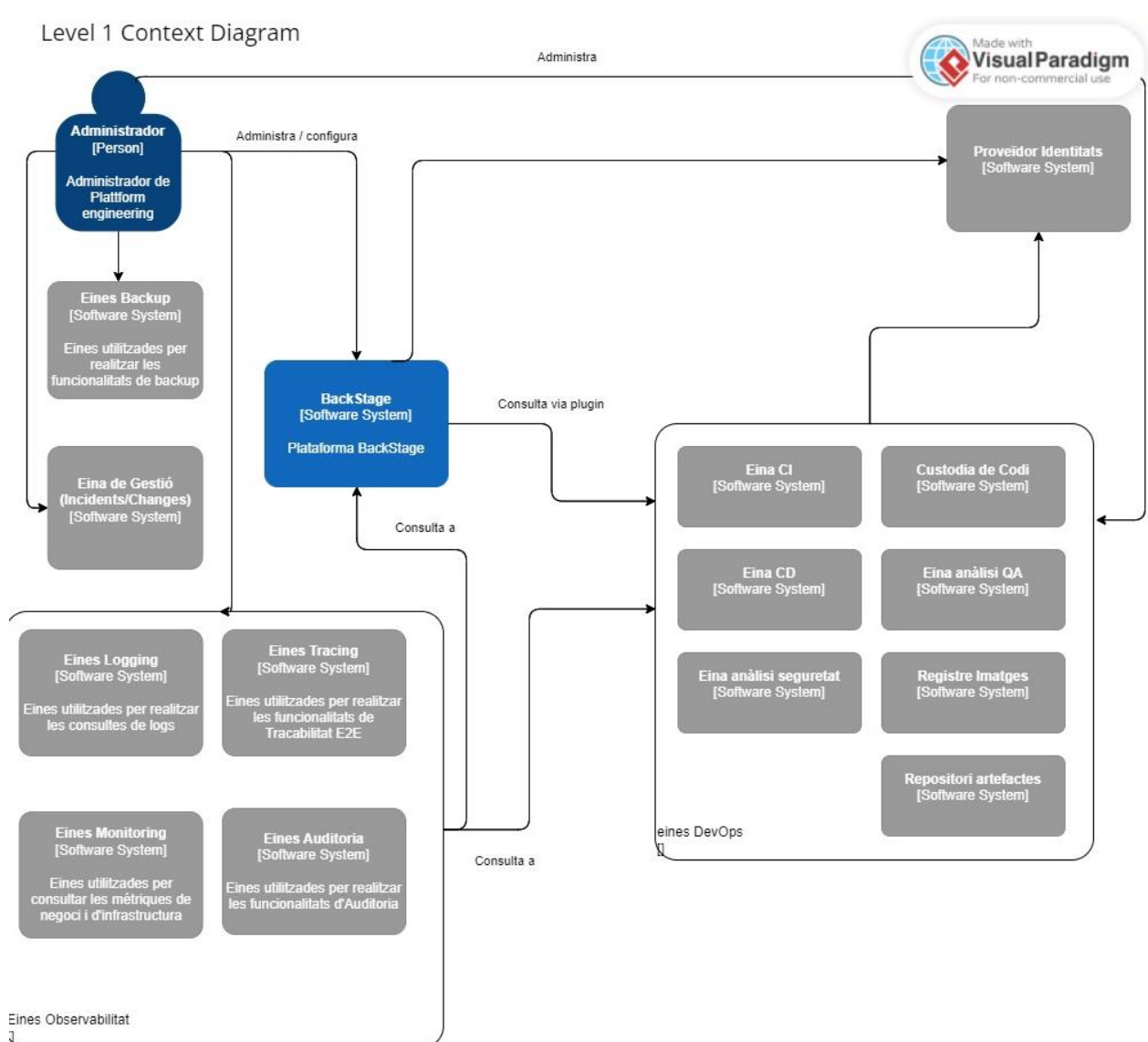


Figura 2. Diagrama de proposta preliminar de mercat d'aplicacions

Repositori d'aplicacions:

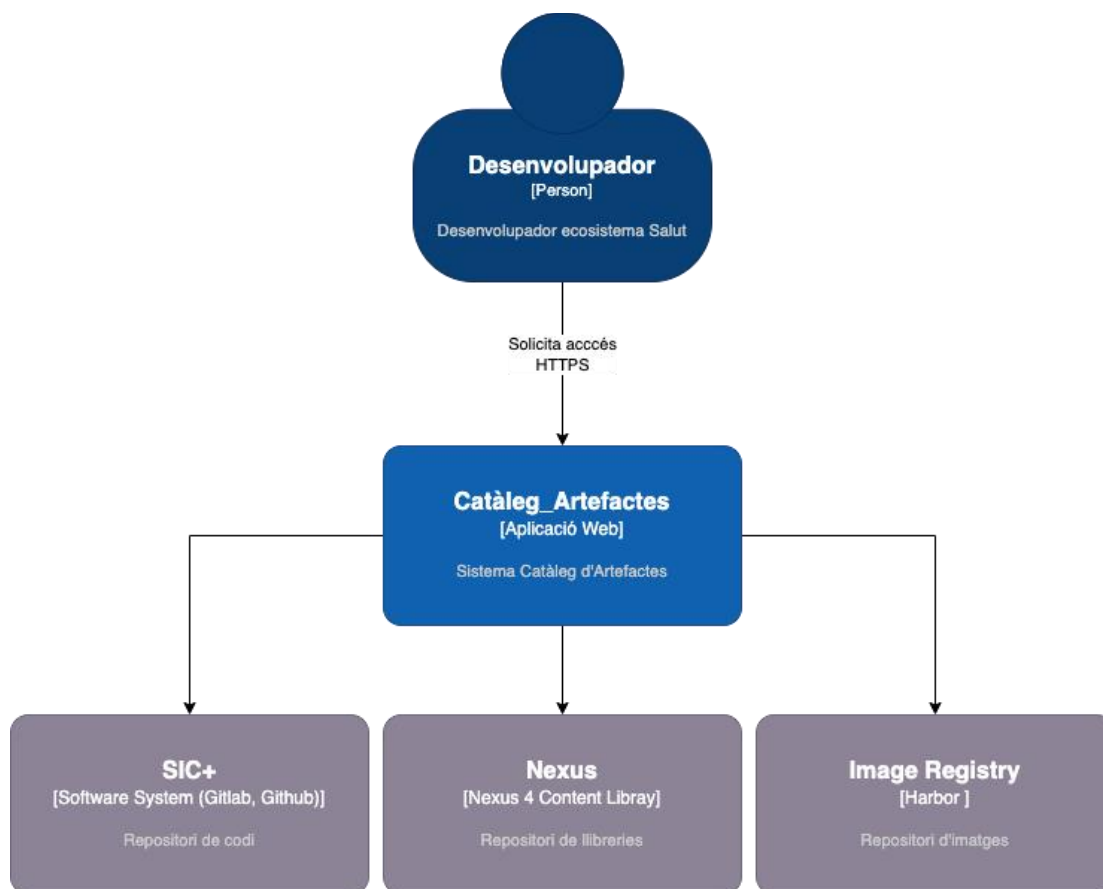


Figura 3. Diagrama de repositori d'aplicacions.

Consulta de guies d'ús i documentació:

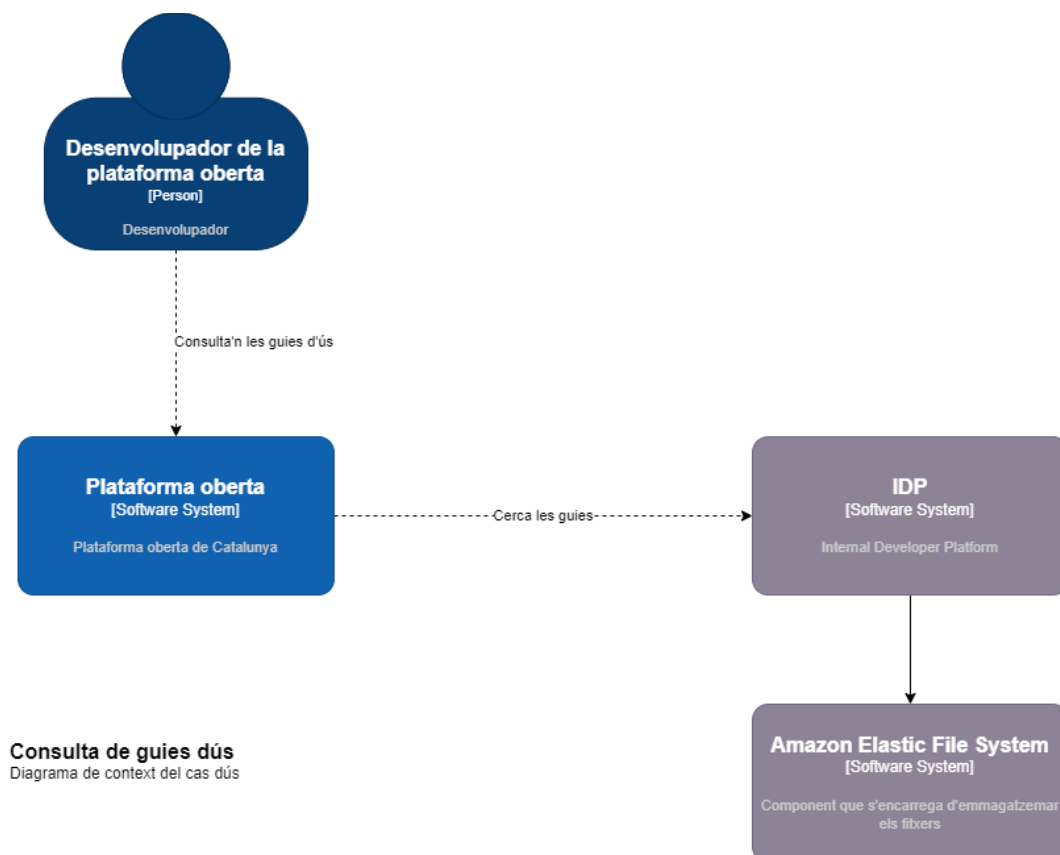


Figura 4. Diagrama de consulta de guies d'ús i documentació

Procés d'Homologació:

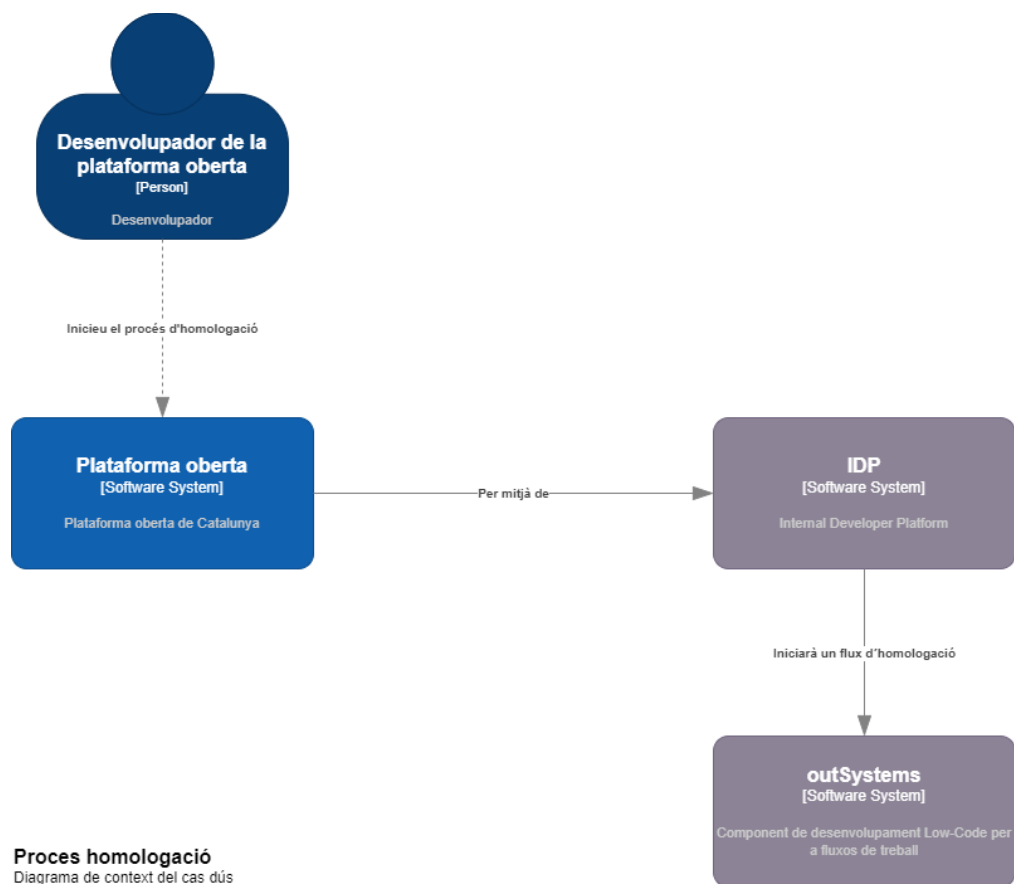


Figura 5. Diagrama de procés d'homologació

Entorn de Desenvolupament:

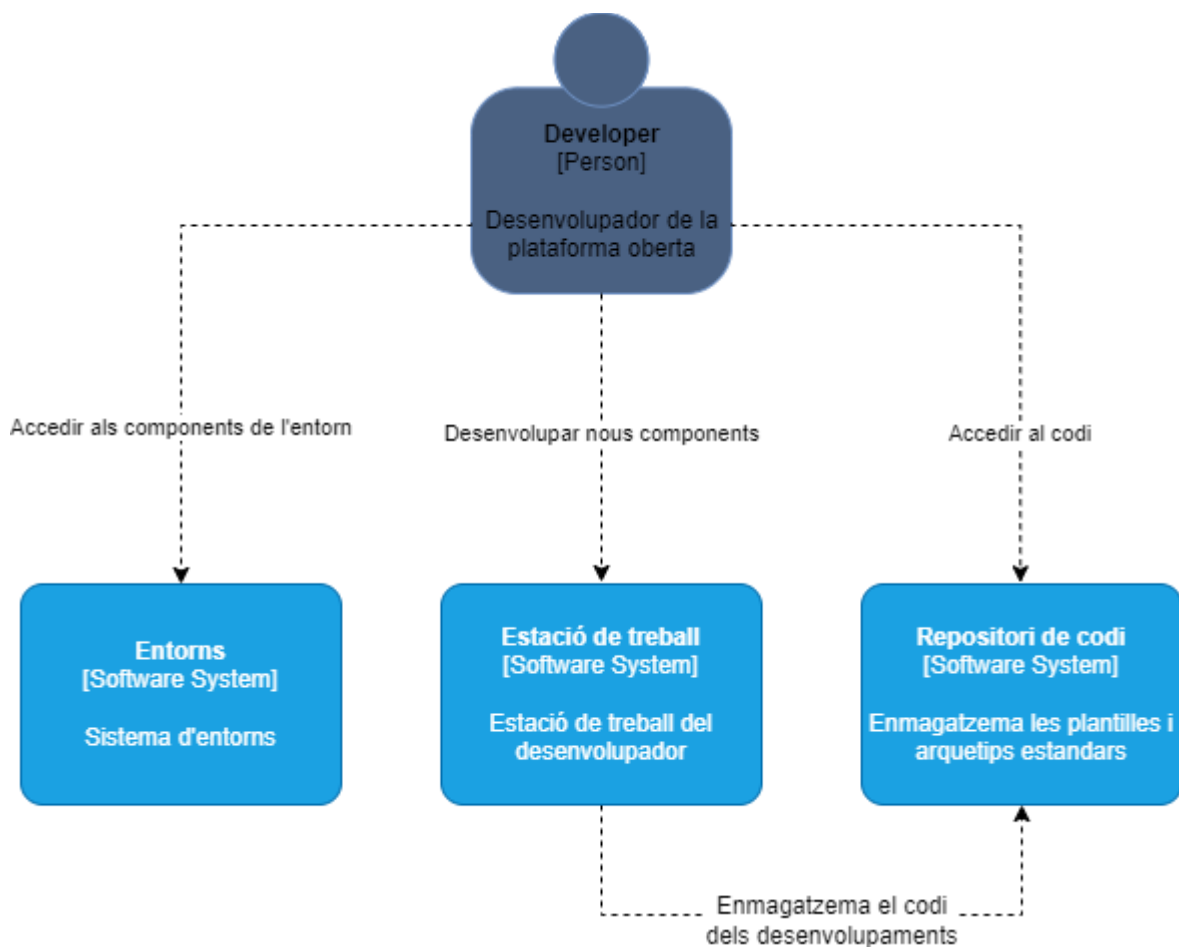


Figura 6. Diagrama d'entorn de desenvolupament

Sistema de Construcció i Desplegament:

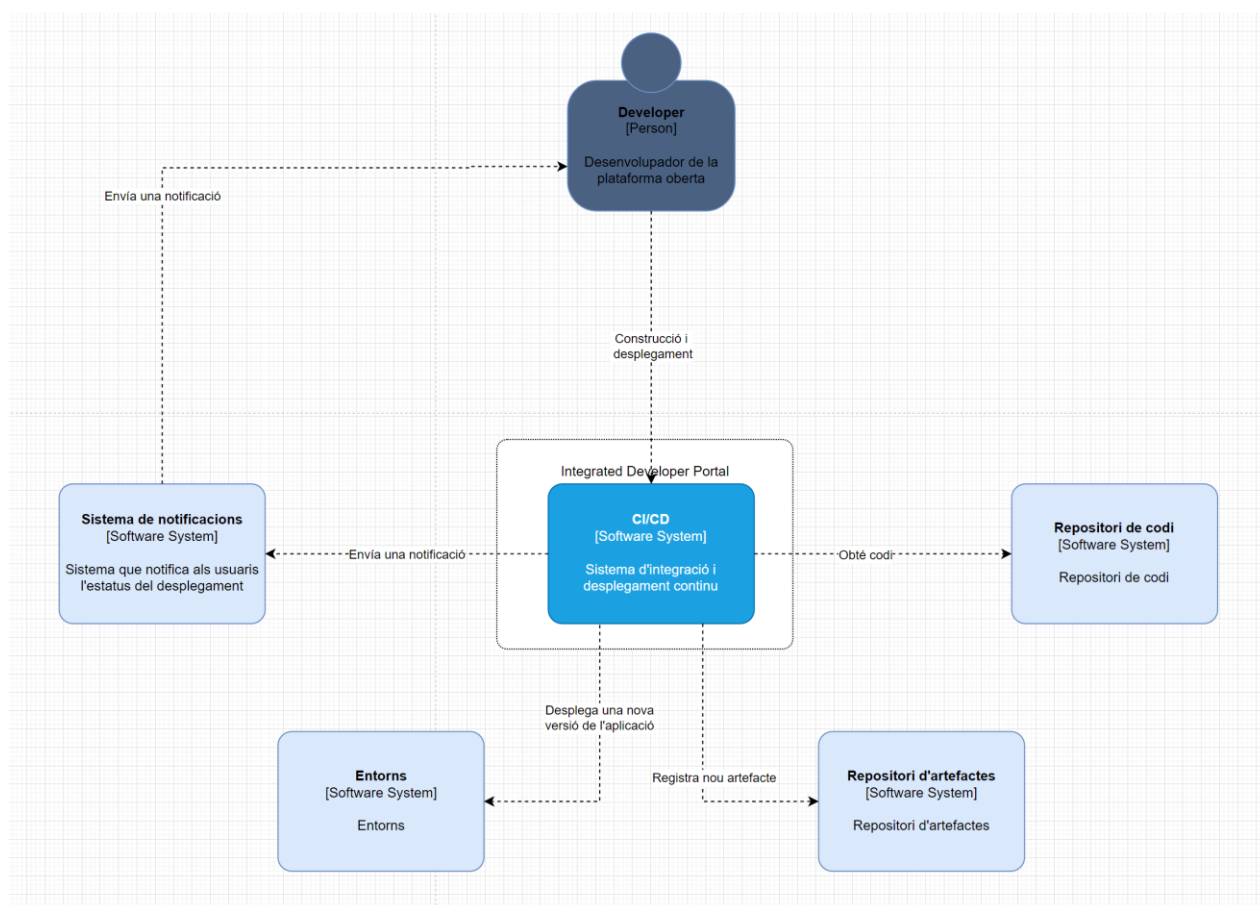


Figura 7. Diagrama de sistema de construcció i desplegament

3.2.1 Portal del Mercat d'aplicacions

El portal del mercat d'aplicacions es construirà segons el paradigma dels microfrontals per a cobrir les necessitats dels diferents tipus d'usuaris que hi entraran:

- Arquitectura de microfrontals amb Single-Spa com a gestor de la Shell i React com a framework de desenvolupament frontend
- Disseny responsiu basat en el Sistema de Disseny de Salut
- Aplicació web progressiva (PWA) per a accés mòbil
- Integrada amb el sistema d'autenticació corporatiu de Salut PDS

A continuació es detallen les diferents vistes d'aquest portal segons el tipus d'usuari que s'hi connectarà.

3.2.1.1 Àrea d'accés públic registrat

- Cercador d'aplicacions: Sistema de cerca avançada que permet trobar aplicacions per nom, categoria, funcionalitat o valoració
- Visualització de documentació: Accés a documentació tècnica i funcional de les aplicacions disponibles
- Sistema de registre i autenticació: Gestió d'usuaris amb diferents nivells d'accés i autenticació segura
- No permet consum directe de recursos: Només permet visualitzar informació, sense poder executar aplicacions

3.2.1.2 Consola d'Administració de la Plataforma

- Gestió de recursos: Administració de capacitats computacionals, emmagatzematge i recursos del sistema
- Control d'usuaris i permisos: Gestió granular de permisos i rols d'usuari
- Supervisió del funcionament: Monitoratge en temps real del rendiment de la plataforma
- Gestió de subscripcions: Administració de plans de subscripció i llicències
- Monitorització de seguretat: Control i seguiment d'aspectes de seguretat i compliment normatiu

3.2.1.3 Àrea del Desenvolupador

Estarà basada en el marc de treball de codi obert Backstage (<https://backstage.io>) per a desenvolupar portals per a desenvolupador (IDPs)

- Accés al catàleg de components: Biblioteca de components reutilitzables per al desenvolupament
- Documentació tècnica: Guies d'integració, APIs i exemples de codi
- Eines de desenvolupament: Plantilles, SDK i eines per facilitar el desenvolupament d'aplicacions
- Plataforma de cerca de components i infraestructura del portal
- Entorns sandbox: Espais aïllats per provar aplicacions sense afectar l'entorn productiu
- Sistema d'imatges Docker: Repositori d'imatges Docker per desenvolupament local
- Gestió del cicle de vida: Control de versions i desplegaments d'aplicacions, adaptat al marc que proporciona SIC+, l'estandard de CI/CD al núvol de CTTI
- Creació d'aplicacions incrustables en la plataforma oberta

3.2.1.4 Àrea d'Administrador Clínic

- Validació de plugins per l'ETC: Procés de verificació de components per l'Estació de Treball Clínic
- Consola de disseny de processos BPM: Eina visual per modelar fluxos de treball clínics
- Motor de regles clíniques: Sistema per definir i gestionar regles de decisió clínica
- Models IA pre-entrenats: Accés a models d'intel·ligència artificial específics per a l'àmbit clínic
- Gestió d'homologació: Control del procés d'aprovació i certificació de components

3.2.1.5 Àrea del Professional Clínic

- Layout personalitzable: Interfície adaptable a les necessitats de cada professional
- Selecció visual de plugins: Interfície drag & drop per configurar l'espai de treball
- Configuració del espai de treball: Personalització de l'entorn segons preferències
- Accés només a plugins validats: Garantia que només s'utilitzen components aprovats

3.2.2 Entorn de desenvolupament / Sandbox

L'entorn de desenvolupament disposarà de facilitats per als desenvolupadors que els permeti una ràpida integració de la seva aplicació amb la plataforma oberta i un procés d'homologació semiautomàtic.

Aquest model permet un entorn de desenvolupament completament aïllat, on el cost i la responsabilitat recauen en el desenvolupador, mentre el Marketplace manté el control i la governança sense assumir costos d'infraestructura, risc operacionals ni posar en risc l'escalabilitat de la plataforma. El desenvolupador manté el control total del seu entorn, gaudeix de flexibilitat de recursos, s'aïlla per complet de la plataforma oberta i pot obtenir contenció de costos mitjançant el pagament per ús de la plataforma que utilitza.

3.2.2.1 Model de Desplegament

- Cada desenvolupador/empresa té la seva pròpia subscripció al hiperescalar
- El Marketplace només actua com a punt de control i govern
- Backstage orquestra els desplegaments a les subscripcions dels desenvolupadors
- Es requereix un alt grau d'automatització:
 - Desplegament automatitzat via Backstage
 - Polítiques de govern automatitzades
 - Neteja automàtica de recursos
 - Monitoratge automàtic de costos

3.2.2.2 Model d'Operació

3.2.2.2.1 Procés d'Alta

- El desenvolupador es registra al Marketplace
- Proporciona les credencials de la seva subscripció al hiperescalar
- Es configura Backstage per desplegar en aquesta subscripció

- S'apliquen les polítiques de governança via IaC

3.2.2.2.2 Control de Recursos

- Límits per Sandbox
 - Màxim de CPU/memòria
 - Límit d'emmagatzematge
 - Quota d'APIs
 - Nombre màxim d'instàncies
- Polítiques de Neteja:
 - Auto-destrucció després de X dies
 - Neteja automàtica de recursos
 - Backup només de codi/configuració
 - No persistència de dades sensibles

3.2.2.3 Model de Costos

3.2.2.3.1 Responsabilitat del Desenvolupador

- Cost dels recursos cloud
- Llicències de software necessàries
- Emmagatzematge de dades
- Tràfic de xarxa

3.2.2.3.2 Inclòs al Marketplace

- Accés a Backstage
- Templates i pipelines
- Simuladors d'APIs
- Suport bàsic

3.2.2.4 Seguretat i Aïllament

3.2.2.4.1 Aïllament de Xarxa

La xarxa de les diferents sandbox estarà aïllada de la resta de sandbox i de la xarxa productiva de la plataforma oberta

3.2.2.4.2 Mesures de Seguretat

- Xarxes virtuals independents
- Sense accés a producció
- Només dades sintètiques
- Tokens d'accés temporals

3.2.2.5 Plantilles d'aplicacions predissenyades

- Clíriques openEHR
- Interoperabilitat FHIR
- Híbrides openEHR/FHIR
- Formularis

3.2.2.6 Integració amb dades

- Connectors predefinits: openEHR, FHIR, base de dades operacional
- Eines ETL, CDC i missatgeria asincrònica
- Capa de seguretat: PDS, Encriptació de dades, Auditoria, Anonimització

3.2.2.7 Generació de dades sintètiques

- Generadors de dades: pacients, històries clíniques, episodis, sèries temporals
- Models de dades: demogràfics, patrons de malalties, models de medicació, patrons de visites
- Eines de validació: coherència clínica, qualitat de dades, patrons, regles de negoci i coherència amb processos clínics

3.2.2.8 Catàleg de bases de dades disponibles

- Bases de dades clíniques: Repositori de dades clíniques, demogràfica, terminologia
- Components transversals: Cites, recursos, professionals, administració,...
- Eines de gestió: visor de models de dades, gestor de connexions, monitor de rendiment, analitzador d'ús

3.2.3 Procés d'homologació

El procés d'homologació proporcionarà eines per a proveïdors, equips d'homologació. Els aspectes a avaluar seràn:

- Arquitectura
- Seguretat
- Qualitat
- Accessibilitat
- Assistencials

El propi procés d'homologació utilitzarà l'eina de processos del nucli d'aplicació per a gestionar els diferents col·lectius i tasques que es derivaran de l'homologació d'aplicacions.

3.2.3.1 Automatització de l'homologació

Un punt important de l'homologació és la rapidesa en la mateixa i la contenció de costos de manteniment d'aquest procés, tant en recursos humans com tecnològics. Per tant, formarà part de la licitació la construcció d'automatitzacions de la mateixa, que constarà, sense ànim de ser exhaustius, de les següents peces:

1. Motor de processos i gestió de tiquets que permeti observar l'evolució de l'homologació a totes les parts. haurà de contemplar una part pública de cara als proveïdors d'aplicacions, i una interna de cara als propis equips d'homologació intervinents
2. Validació d'arquitectura, mitjançant una sèrie de fitness functions que validin els criteris d'arquitectura establerts per a les diferents tipologies d'aplicacions
3. Validació de la seguretat, anàlisi de vulnerabilitats, compliment normatiu (RGPD, ENS), etc
4. Validació de la qualitat, conforme a les quality gates establertes per la unitat de qualitat del departament de salut
5. Validació de l'accessibilitat, de forma que s'asseguri el compliment amb la doble AA i l'ús del Design System de Salut
6. Validacions assistencials, que confirmin que l'aplicació cobreix les funcionalitats esmentades de la solució, és segura pels usuaris i pacients i té el suport i horari de servei adequat

3.2.4 Procés de publicació de l'aplicació

El procés de publicació al marketplace contempla tres fases diferenciades:

3.2.4.1 Preparació Marketplace

- Creació fitxa producte
- Configuració pricing
- Materials marketing
- Documentació final

3.2.4.2 Desplegament Productiu

- Desplegament en pre-producció
- Validació final
- Desplegament en producció
- Configuració monitoratge

3.2.4.3 Activació al Marketplace

- Publicació al catàleg
- Activació llicències

- Configuració accés
- Notificació a interessats

3.2.5 Portal del Marketplace. Consum de les aplicacions

3.2.5.1 Accés públic / LMS / Professionals

Ús Primari:

- Catàleg d'Aplicacions
 - Cercador avançat amb filtres per tipus d'aplicació, especialitat, valoracions
 - Vista detallada de cada aplicació amb descripció, captures de pantalla i documentació
 - Sistema de valoracions i comentaris dels usuaris
 - Indicadors de qualitat i homologació
 - Estadístiques d'ús i satisfacció
- Integració amb Sistemes Corporatius
 - Integració nativa amb l'Estació de Treball Clínica (ETC)
 - Desplegament automàtic de components
 - Sincronització de dades i configuracions
 - Gestió de permisos unificada
 - Connexió amb els diferents HIS del SISCAT
 - Interoperabilitat basada en estàndards (HL7, FHIR)
 - Gestió de la identitat federada
 - Sincronització bidireccional de dades clíniques
 - Integració amb La Meva Salut (LMS)
 - Desplegament automàtic de components adaptats a dispositius mòbils
 - Sincronització de dades i configuracions
 - Gestió de permisos unificada
- Gestió d'Usuaris i Accés
 - Registre i autenticació d'usuaris integrat amb GICAR
 - Registre i autenticació d'usuaris propis no integrats amb GICAR (transitoris, col·laboradors externs (mútues, INSS, etc), etc.
 - Gestió de perfils i rols
 - Personalització de l'experiència d'usuari
 - Històric d'aplicacions utilitzades
- Gestió d'Incidències
 - Sistema multicapa de suport:
 - Primer nivell: 061/LMS per incidències de pacients
 - Primer nivell: SAU CTTI/Remedy per professionals
 - Segon nivell: Proveïdors de la plataforma
 - Tercer nivell: Proveïdors de les aplicacions
 - Traçabilitat completa de les incidències
 - SLAs definits per tipus d'incidència
 - Dashboards de seguiment i KPIs

Ús Secundari:

- Catàleg de Dades
 - Inventari complet de conjunts de dades disponibles
 - Metadades i documentació associada
 - Polítiques d'accés i ús
 - Qualitat i actualització de les dades
- Extraccions de Dades
 - Compliment amb el marc de l'Espai de Dades de Salut de Catalunya
 - Alineament amb EHDS (European Health Data Space)
 - Processos d'aprovació i traçabilitat
 - Controls de privacitat i seguretat
 - Formats estandarditzats d'extracció

3.2.5.2 Accés proveïdors / Administració Catsalut

- Gestió i Analítica
 - Dashboard de consum i ús de les aplicacions
 - Mètriques d'ús de les APIs
 - Models de monetització flexibles:
 - Pagament per ús
 - Subscripcions
 - Models mixtos
 - Facturació i reporting
- Gestió de Dades per Ús Secundari
 - Control d'accés granular a les dades
 - Auditoria d'accessos i usos
 - Compliment normatiu (RGPD, LOPDGDD)
 - Gestió de consentiments
 - Anonimització i pseudonimització
 - Traçabilitat d'extraccions
- Gestió Operativa
 - Monitoratge del rendiment
 - Gestió de la capacitat
 - Alertes i notificacions
 - Gestió de versions i actualitzacions
 - Reporting i analítica avançada

3.2.5.3 Procés de prescripció d'una aplicació

El procés de prescripció contempla les següents fases

3.2.5.3.1 Pre-prescripció

- Identificació de Necessitat
 - Avaluació clínica del pacient
 - Definició d'objectius terapèutics
 - Valoració de capacitat digital del pacient
 - Revisió d'apps disponibles
- Selecció d'Aplicació
 - Consulta catàleg d'apps prescribibles
 - Revisió d'evidència clínica
 - Verificació de compatibilitat
 - Comprovació de contraindicacions

3.2.5.3.2 Prescripció

- Acte de Prescripció
 - Registre a història clínica
 - Configuració de paràmetres específics
 - Definició de durada i freqüència d'ús
 - Establiment d'objectius mesurables
- Gestió d'Accés
 - Generació de codi d'activació
 - Configuració de permisos
 - Assignació de llicència
 - Vinculació amb història clínica

3.2.5.3.3 Activació

- Notificació al Pacient
 - Enviament d'instruccions
 - Codi d'accés segur
 - Guia d'instal·lació/ús
 - Informació de suport
- Primera Utilització
 - Verificació d'identitat
 - Tutorial guiat
 - Configuració inicial
 - Test de funcionalitat

3.2.5.3.4 Seguiment

- Monitoratge
 - Seguiment d'ús
 - Recollida de dades clíniques
 - Alertes de compliance
 - Indicadors de progrés
- Avaluació
 - Revisió d'objectius
 - Ajust de paràmetres
 - Valoració d'efectivitat
 - Decisions de continuïtat

3.2.5.3.5 Casos Especials

- Modificació de Prescripció
 - Ajust de paràmetres
 - Canvi de durada
 - Modificació d'objectius
 - Actualització de permisos
- Cancel·lació
 - Registre de motiu
 - Revocació d'accés
 - Notificació al pacient
 - Arxiu d'informació
- Renovació
 - Avaluació de resultats
 - Actualització de prescripció
 - Extensió de llicència
 - Ajust d'objectius

3.2.5.3.6 Seguiment de la prescripció

- Vista Metge
 - Llistat de prescripcions actives
 - Alertes de non-compliance
 - Indicadors de progrés
 - Agenda de revisions
- Vista Pacient
 - Apps prescrites actives
 - Progrés d'objectius
 - Properes activitats
 - Accés a suport

3.3 Enginyeria de Plataforma

En aquest punt s'indiquen aquells components que seran transversals a tota la solució, tant pel nucli com pel mercat d'aplicacions, i que seran desenvolupats i operats sota el paradigma de l'enginyeria de plataforma.

3.3.1 Observabilitat

3.3.1.1 Registres

Integració amb TALAIA Cloud (sistema de monitorització corporatiu del CTTI per aplicacions desplegades al núvol) per centralitzar la visibilitat global. La gestió de logs amb la suite Elastic permet realitzar la recerca i anàlisi d'informació als logs dels diferents components de les plataformes.

3.3.1.2 Traces

Correlació d'esdeveniments entre diferents components per detectar problemes de forma proactiva. S'utilitzarà AWS Xray per aquesta tasca utilitzant el protocol de codi obert OpenTelemetry

3.3.1.3 Mètriques

Mètriques de rendiment de les infraestructures es gestionaran des de la plataforma AWS CloudWatch, que al seu temps estarà connectada amb el sistema TALAIA Cloud per definir els corresponents panells de monitorització, i enllaç amb el Centre de Control i el seu sistema d'alertes i incidències. Caldrà seguir les normatives establertes en el nou Model d'Observabilitat de CTTI.

Mètriques de negoci de les aplicacions que es recolliran també emprant OpenTelemetry i es deixaran accessibles a CloudWatch per la seva posterior explotació des de TALAIA Cloud.

Capacitats d'anàlisi avançat amb IA per detectar anomalies i patrons

Retenció de dades històriques per anàlisi de tendències i optimització

3.3.2 FinOps

- Integració amb solució corporativa Cloudability/Apptio per la gestió multi-cloud
- Polítiques d'optimització de costos:
 - Aturada automàtica d'entorns no productius
 - Redimensionament de recursos infrautilitzats
 - Reserva de capacitat per optimitzar costos
- Assignació i seguiment de pressupostos per departament/projecte
- Alertes de desviacions de costos
- Recomanacions d'optimització basades en patrons d'ús

3.3.3 Portal d'autoservei

- Catàleg de serveis estandarditzat
- Workflows d'aprovació configurables
- Integració amb sistemes de ticketing corporatius
- Dashboards personalitzats per usuari/rol
- API per automatitzar peticions des d'altres sistemes
- Gestió del cicle de vida complet de les peticions
- Traçabilitat d'estat i auditoria d'accions

3.3.4 Seguretat

En aquest punt s'esmenten aspectes principals de la seguretat com la seguretat d'accessos, l'encryptació de dades i l'auditoria d'activitats

3.3.4.1 Seguretat d'accessos

Tal com s'esmenta més endavant al punt 4.1 Plataforma de Seguretat – PDS, la seguretat d'accessos es gestiona mitjançant aquest component transversal que actua a mode d'Identity Provider i que suporta dos models d'autorització: tokens OpenId Connect (principal) o tiquets SAML.

Un cop superada l'autenticació d'un subjecte usuari o sistema, la PDS generarà un parell de tokens d'accés i refresc, que es podran utilitzar durant tota la sessió. Les aplicacions hauran de recollir aquests tokens i gestionar l'autorització corresponent, és a dir validar que el subjecte autenticat té permisos per a efectuar les accions requerides.

En aquest sentit, les aplicacions implantaran el seu propi sistema de validació de tokens i tindran els seus propis criteris d'autorització per aplicar i permetre o no l'accés als serveis que publiquen.

3.3.4.2 Encryptació de dades

Distingim l'encryptació en dos aspectes; en trànsit i en repòs

Per a l'encryptació en trànsit, totes les comunicacions vindran encryptades per xifrat TLS 1.3 o superior

Per l'encryptació en repòs, tots els repositoris d'informació s'encryptaran amb una clau d'encryptació que proveirà el CTTI a partir del seu sistema corporatiu de gestió de claus. En cas que el servei no estigui actiu en el moment de l'inici del contracte, les claus que es facin servir per encryptar la informació residiran en un proveïdor de cloud diferent a AWS (Azure Key Vault o Cloud Key Management de Google).

3.3.4.3 Auditoria d'activitats

3.4 Per donar compliment al requeriment legal de mantenir una auditoria de l'accés o modificació de dades personals o mèdiques, s'utilitzarà la plataforma d'auditoria transversal de Salut Les seves característiques es detallen al punt 4.5 Servidor Terminològic

L'objectiu del servei es la resposta del servei implementant a l'estàndard mèdic FHIR R4. Els recursos estàndards utilitzats al projecte són els següents:

- CodeSystem: <https://hl7.org/fhir/codesystem.html>

On es representa el catàleg.

- ValueSet: <https://hl7.org/fhir/valueset.html>

On es representa el subconjunt d'un catàleg.

- ConceptMap: <https://hl7.org/fhir/conceptmap.html>

On es representa les relacions entre els conceptes dels catàlegs.

- Bundle: <https://hl7.org/fhir/bundle.html>

Que s'utilitza per representar una llista de resultats d'una cerca.

- Parameters: <https://hl7.org/fhir/parameters.html>

Que s'utilitza per representar el cos i la resposta d'una operació FHIR a un recurs.

Les relacions entre els recursos de terminologia FHIR es troben a la pàgina de l'estàndard: <https://hl7.org/fhir/terminology-module.html>

Les adhesions als serveis actius del Servidor Terminològic, actualment, seran en mode consulta en la seva totalitat, per part de les aplicacions consumidores.

Nota: El desenvolupament s'ha realitzat en base a FHIR R4 v4.0.1. Cal tenir en compte la informació que proporcionen les adreces web de l'estàndard FHIR, ja pot haver-hi canvis o actuacions sobre versions de l'estàndard.

Plataforma Auditoria

3.4.1.1 Repositori d'usuaris i Portal d'aplicacions

Caldrà implementar dins el marc de la Plataforma Oberta un Portal d'aplicacions que substitueixi els actuals Portal de GSA i la pàgina de login de l'ECAP de Primària.

Aquest portal d'aplicacions haurà d'estar integrat amb la PDS, que és qui oferirà la pàgina de login en els diferents fluxes d'autenticació descrits en l'apartat 4.1 Plataforma de Seguretat – PDS, i també haurà d'incloure el repositori d'usuaris i les seves credencials, que serveixi de font única i segura d'autenticació per la PDS, i també operacions per gestionar l'alta, modificació o baixa d'usuaris i el manteniment de les seves respectives credencials (alta, rotació, recuperació davant oblit, desactivació temporal o definitiva o per caducitat, etc.)

3.4.2 Recuperació davant desastres

Contemplarà els següents aspectes:

- Routing d'adreçament entre diferents zones de disponibilitat, regions i proveïdors de cloud
- Balanceig de càrrega entre zones de disponibilitat, regions i proveïdors de cloud
- Emmagatzematge federat o estès
- Infraestructura de capes de presentació i negoci que permeti usar mecanismes de recuperació avançats
- Plataforma de Base de dades basada en model PaaS per disposar d'alta disponibilitat multi-zona, multi-regió i multi-cloud
- Automatització del procés de DR amb proves periòdiques planificades
- RPO (Recovery Point Objective) i RTO (Recovery Time Objective) definits per servei
- Plans de continuïtat de negoci documentats i provats
- Procediments de failover i fallback automatitzats
- Còpies de seguretat amb retenció configurable
- Entorns de contingència preparats
- Proves periòdiques de recuperació
- Procediments de comunicació en cas d'incident

3.4.3 Documentació

El component transversal de documentació ha d'incloure:

- Un repositori centralitzat de documentació tècnica i funcional accessible per tots els actors involucrats en el desenvolupament i operació de la plataforma.
- Procediments estandarditzats per a la generació i manteniment de:
 - Documentació d'arquitectura i disseny tècnic
 - Manuals d'usuari i d'operació
 - Documentació d'APIs i interfícies
 - Guies de desenvolupament i bones pràctiques
 - Procediments d'operació i manteniment
 - Plans de contingència i recuperació
- Eines per a la gestió col·laborativa de la documentació com wikis o gestors documentals que permetin:
 - Control de versions
 - Col·laboració entre equips

- Cerca i indexació de continguts
 - Integració amb eines de desenvolupament
 - Actualització àgil de la documentació
- Processos de revisió i aprovació de la documentació abans de la seva publicació
- Mecanismes per mantenir la documentació actualitzada de forma contínua, especialment després de canvis en la plataforma

3.4.4 Qualitat en el servei

L'adjudicatari disposarà d'un equip d'experts en les diferents plataformes i components que componen els serveis, amb disponibilitat dels serveis professionals dels fabricants dels diferents components SaaS que formen part de la solució.

Adicionalment, es mesurarà la qualitat del servei en els següents aspectes:

- Acords de Nivell de Servei (ANS) definits al plec
- Processos de millora contínua
- Gestió d'incidències i problemes utilitzant les eines que proposa el CTTI
- Indicadors clau de rendiment (KPIs)
- Enquestes periòdiques de satisfacció d'usuaris
- Gestió de la capacitat proactiva
- Plans de formació contínua pels equips

3.4.5 Gestió de la capacitat

La gestió de la capacitat ha d'incloure:

- Monitoratge continu dels recursos utilitzats:
 - CPU, memòria i emmagatzematge
 - Ample de banda i latència de xarxa
 - Nombre d'usuaris concurrents
 - Volum de transaccions
 - Temps de resposta
- Eines de predicció i planificació:
 - Anàlisi de tendències d'ús
 - Predicció de necessitats futures
 - Models de creixement esperats
 - Planificació de l'escalat de recursos
- Mecanismes d'escalat automàtic:
 - Polítiques d'auto-escalat basades en mètriques
 - Escalat horitzontal i vertical
 - Balanceig de càrrega dinàmic
 - Optimització de recursos
- Gestió proactiva:

- Alertes preventives abans d'arribar a límits crítics
 - Recomanacions d'optimització
 - Ajust dinàmic de recursos
 - Prevenció de colls d'ampolla
- Informes i dashboards:
 - Ús de recursos en temps real
 - Tendències històriques
 - Previsió de necessitats futures
 - Cost associat al consum de recursos

3.4.6 Operació plataformes

La plataforma requerirà d'operació continua a les infraestructures al núvol, recolzada per un equip global integrat que asseguri un suport 24x7 per a la resolució d'incidents crítics, aplicant tècniques de CI/CD i automatització tant de les peticions que puguin venir dels diferents consumidors de la plataforma, com de la remediació d'incidents, com, per exemple, de disponibilitat o de capacitat. L'objectiu és automatitzar tota la gestió rutinaria de les operacions, potenciar la predictibilitat i proactivitat i evitar tasques manuals amb dependència dels operadors.

Per aquells proveïdors d'aplicacions que no puguin fer-se càrrec d'un suport 24x7 s'oferirà aquest servei. El licitador haurà de contemplar els equips necessaris per a poder donar aquest servei per aquelles aplicacions que el requereixin.

4 Components Habilitadors de Salut d'Utilització Obligatòria

4.1 Plataforma de Seguretat – PDS

La Plataforma de Seguretat HES (PdS) es l'Identity Provider transversal de Salut.

Els serveis que ofereix comprenen principalment la gestió de:

- L'autenticació: les credencials necessàries per consumir serveis o dades d'una iniciativa de Salut
- L'autorització: el control del permís sobre aquests serveis exposats per la iniciativa, segons les credencials presentades per el consumidor.

Es basa en la distribució open source de Keycloak com a gestor d'identitats i control d'accés (Identity Provider), i suporta els estàndards OpenIdConnect (OIDC) i SAML2.

Es contemplen dos possibles fluxes d'autenticació en la PDS: d'usuari o de sistema. En el cas de l'autenticació de sistema (*Client Credentials Flow* o també conegut com "Service Account") les credencials consisteixen en un parell client-id/client-secret, i a més, la PDS té capacitat d'afegir paràmetres addicionals (claims) en els tokens que poden ser validats contra catàlegs predefinits del Servidor Terminològic HES, o calculats en base a regles definides en el Motor de Regles HES.

En el cas d'autenticació d'usuari (*Authorization Code Flow*) la PDS ofereix la possibilitat de federar el login als sistemes corporatius GICAR (professionals) o VALID (ciutadans) o d'altres repositoris d'usuaris tant interns com externs. Per aquest tipus d'autenticació, la PDS és qui ofereix la pàgina de login i redirigeix al identity provider tercer per gestionar de forma segura les credencials.

4.2 Repositori de Dades Clíniques – RDC

El repositori de dades clíniques RDC openEHR es una base de dades clíniques d'acord amb les especificacions de l'estàndard openEHR que permet emmagatzemar models d'informació (en forma d'arquetips i plantilles) en temps d'execució, així com registrar dades clíniques de pacients mitjançant composicions i consultar aquesta informació mitjançant el llenguatge d'arquetips AQL (AQL v1.4).

Les aplicacions del sistema sanitari català utilitzaran el servei RDC i l'Index Server per al registre i consulta de les dades clíniques associades als pacients atesos al territori.

4.3 Mestre de Pacients – MPI

Les funcionalitats del MPI són:

- Identificar de forma unívoca d'un pacient atès pel Servei Català de Salut, essent consultat per sistemes de CatSalut o externs.

- Dades provinents de: RCA, ECAP i ICAM (provinents d'esdeveniments kafka)
- API FHIR per a consultes de pacients
- Servir de lligam entre MPI (ID_MPI) i CDR (ID_EHR), mitjançant "Index server"
- Dipositar auditoria de les altes i modificacions dels pacients (BDD MongoDB)

Permet garantir uns temps de resposta raonables en l'actualització de dades i facilitar la integració dels sistemes actuals amb les dades demogràfiques de pacients.

Usuaris: Professionals administratius.

4.4 Index Server

En aquest component es manté la relació entre el mestre de pacients i el repositori de dades clíniques. El seu objectiu es separar la informació del pacient de la informació clínica del pacient. Aquest repositori manté una relació entre els identificadors de pacient d'ambdues plataformes en una base de dades independent.

Permet obtenir l'identificador d'història clínica d'un pacient a partir del seu identificador del Mestre de Pacients (MPI), sistema on s'emmagatzemen les dades demogràfiques vinculades als pacients, i viceversa, és a dir, obtenir l'identificador de pacient a partir de l'identificador d'història clínica.

4.5 Servidor Terminològic

L'objectiu del servei es la resposta del servei implementant a l'estàndard mèdic FHIR R4. Els recursos estàndards utilitzats al projecte són els següents:

- CodeSystem: <https://hl7.org/fhir/codesystem.html>

On es representa el catàleg.

- ValueSet: <https://hl7.org/fhir/valueset.html>

On es representa el subconjunt d'un catàleg.

- ConceptMap: <https://hl7.org/fhir/conceptmap.html>

On es representa les relacions entre els conceptes dels catàlegs.

- Bundle: <https://hl7.org/fhir/bundle.html>

Que s'utilitza per representar una llista de resultats d'una cerca.

- Parameters: <https://hl7.org/fhir/parameters.html>

Que s'utilitza per representar el cos i la resposta d'una operació FHIR a un recurs.

Les relacions entre els recursos de terminologia FHIR es troben a la pàgina de l'estàndard:
<https://hl7.org/fhir/terminology-module.html>

Les adhesions als serveis actius del Servidor Terminològic, actualment, seran en mode consulta en la seva totalitat, per part de les aplicacions consumidores.

Nota: El desenvolupament s'ha realitzat en base a FHIR R4 v4.0.1. Cal tenir en compte la informació que proporcionen les adreces web de l'estàndard FHIR, ja pot haver-hi canvis o actuacions sobre versions de l'estàndard.

4.6 Plataforma Auditoria

HES-PAUD és l'aplicació transversal de Salut que permet rebre, per part de les aplicacions adherides, esdeveniments d'auditoria de forma asíncrona, i posteriorment, en un futur, consultar aquests amb una API REST que HES-PAUD exposa utilitzant FHIR Search.

Aquests esdeveniments estan estandarditzats amb l'especificació FHIR R4 i estan basats en la definició IHE-ATNA.

Podem distingir 3 tipus d'interaccions amb el sistema HES-PAUD:

1. Interfície web d' HES -PAUD:

L'aplicació HES-PAUD disposa d'una interfície web que permet als administradors del sistema cercar esdeveniments emprant filtres. També poden generar documents PDF amb la informació desitjada.

Aquesta interacció està reservada per administradors del sistema, per tant, no es descriu a aquest document.

2. API REST (síncron):

HES-PAUD exposa una API REST que permet cercar els esdeveniments d'auditoria de forma programàtica. Aquesta API utilitza el format HAPI FHIR per consultar els esdeveniments. A més, està securitzada amb la PdS.

S'està definint el model d'autorització d'aquesta API, que estarà integrada amb la Plataforma de Seguretat (PdS). A aquesta primera versió encara no es facilita informació per sol·licitar credencials per consumir-la.

3. Kafka (asíncron):

Les iniciatives adherides a HES-PAUD publiquen els seus esdeveniments a un tòpic corporatiu d'EventHub i posteriorment aquests són consumits per la Plataforma d'Auditoria.

Aquest procés és completament asíncron per la iniciativa adherida i pot publicar tants esdeveniments al tòpic com calgui.

Tots els missatges consumits es validen amb un Schema Registry mitjançant un JSON Schema i es validen els codis d'EP, UP i centre. Posteriorment, es guarden al repositori d'HES-PAUD (sempre que no hi hagi cap error de format) per la seva posterior consulta.

4.7 Servidor de Recursos - Professionals i Organització

És una iniciativa transversal que té per objectiu implementar un eina que permeti modelar de forma centralitzada els recursos No Clínics del SISCAT (Sistema Sanitari Integral d'Utilització Pública de Catalunya) i que permeti definir, els seus atributs i la relació entre ells (estructures organitzatives, estructures físiques, aparells, etc.)

En aquest servidor es trobaran:



4.8 Traçabilitat Distribuïda

Utilització d'AWS XRAY, com a solució de traçabilitat distribuïda

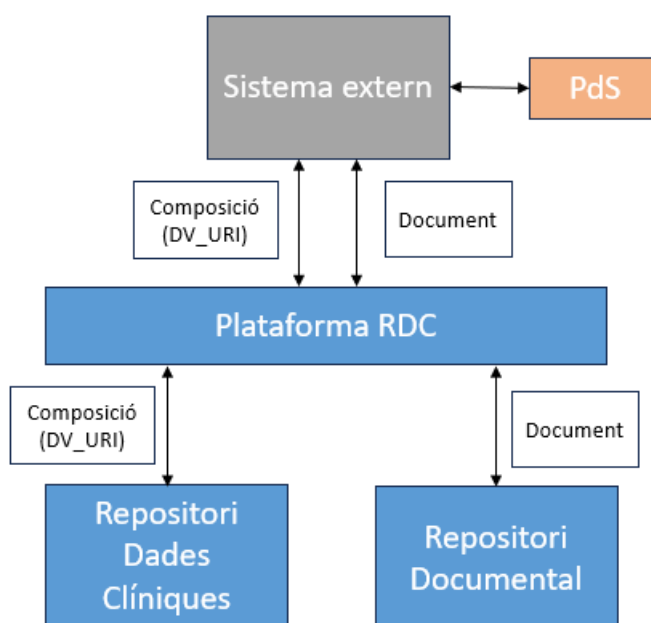
4.9 Gateway de Comunicacions

Servei en definició. Serà la passarel·la sobre la que es centralitzaran les comunicacions amb ciutadans i professionals que accedeixen a la plataforma.

4.10 Gestor Documental

La plataforma de gestió del coneixement inclou tant el repositori de dades clíniques (RDC), on emmagatzemar les dades clíniques dels pacients al llarg de la seva vida, com un repositori documental que permet emmagatzemar i consultar els documents generats en els diferents processos assistencials.

Amb el model definit, el repositori documental guarda únicament els documents, mentre que el RDC fa la funció de registre documental, registrant a les composicions les metadades del document i el directori on s'allotja (en un camp del tipus DV_URI). Dit això, s'hauran de fer peticions independents per interaccionar amb cada un dels components, a través de les API REST que ofereixen. S'adjunta un diagrama de flux amb els diferents elements:



Els sistemes orígens són els responsables de la consistència de dades, entre les metadades i els documents.

En el repositori documental també es podran guardar documents no referenciats en composicions gràcies a aquest model. En aquest cas, però, el sistema origen s'haurà d'assegurar que es guarda la URI i les metadades necessàries que permeten identificar la localització del document ja que el repositori documental no disposarà d'aquesta informació.

4.11 Plataforma Corporativa de gestió de claus d'encryptació

Per l'encryptació en repòs, tots els repositoris d'informació s'encryptaran amb una clau d'encryptació que proveirà el CTTI a partir del seu sistema corporatiu de gestió de claus (en construcció). En cas que el servei no estigui actiu en el moment de l'inici del contracte, les claus que es facin servir per encryptar la informació residiran en un proveïdor de cloud diferent a AWS (Azure Key Vault o Cloud Key Management de Google).

5 REQUISITS DE LA SOLUCIÓ TECNOLÒGICA APORTADA

5.1 Requisits de l'arquitectura de la plataforma

La solució tecnològica requerida ha de contemplar el desplegament sobre infraestructures de cloud públic del CTTI, per tant, el licitador haurà de proveir per complet tot els elements de la infraestructura com a codi que siguin necessaris per a donar el servei funcional requerit.

5.1.1 Connectivitat al Nus de comunicacions de la Generalitat de Catalunya

Pel fet de consumir serveis de cloud proveïts pel CTTI, el proveïdor disposarà d'adreçament de Nus corresponent al cloud escollit. El proveïdor haurà d'aportar en el seu disseny de seguretat dels components necessaris per a realitzar les funcions de tallafoc i balanceig, així com la interconnexió dels seus components. Totes les comunicacions entre el cloud i els datacenters onprem de CTTI s'hauran d'habilitar mitjançant les línies dedicades que GESNUS ha implementat a tal efecte segons cada hiperescalar i el seu corresponent gateway.

5.1.2 Adreçament dels servidors

L'assignació d'adreçament IPv4 i IPv6 serà una subxarxa dins de l'adreçament dedicat per al cloud públic per part de Nus. L'adreçament públic es gestiona des del Nus de comunicacions. Els servidors hauran de tenir definit aquest adreçament. Tots els servidors hauran de tenir xarxes de gestió i backup, diferenciades de les xarxes de servei. Si que es permet NAT en les subnets en cada hiperescalar. Precisament, per evitar esgotar els rangs IPV4 que NUS ha assignat a cada hiperescalar, l'aprovisionament de subnetting consisteix en CIDRs de NUS (amb una mida limitada) i en CIDRs interns (de mida molt més gran) i un nat gateway intern

5.1.3 Serveis de DNS

El servei de DNS es donarà de forma centralitzada des del Nus de Comunicacions a partir dels servidors DNS que ha ubicat a cada hiperescalar. El proveïdor del servei haurà de tenir configurada la resolució dels dominis intranet.gencat.cat a aquest a nivell de resolutor.

5.1.4 Encaminament

El proveïdor del servei enrutarà l'adreçament públic i privat definit a la Generalitat de Catalunya cap al Nus de comunicacions.

La sortida i/o entrada des d'Internet es realitzarà mitjançant el Nus de comunicacions mitjançant el servei de proxypass disponible a cadascun dels hiperescalars dedicats de sortida a internet per tràfic web.

5.1.5 Serveis de Comunicacions

Els serveis de comunicacions necessaris pels sistemes ubicats en la plataforma compliran els següents requisits:

El proveïdor del Nus de comunicacions serà el responsable de gestionar els certificats de servidor i l'acceleració de SSL i serveis de balanceig de nivell 7 i de reverse proxy (només per URL). En els casos que sigui necessari, aquests certificats podran ser gestionats pel proveïdor del servei.

El proveïdor del servei és el responsable de proporcionar, gestionar, administrar i operar la resta d'elements de comunicacions necessaris que el servei requereixi (tallafocs, balancejament, electrònica de xarxa, etc.)

5.1.6 Alta Disponibilitat

L'arquitectura de la solució contemplarà la seva execució en alta disponibilitat real entre dues regions de cloud remotes. En conseqüència, el licitador haurà de contemplar el maquinari en les dues regions amb el nivell de servei necessari.

Tanmateix tots els serveis s'executaran en tres zones de disponibilitat de les regions escollides.

5.1.7 Requisits detallats de l'arquitectura

A banda dels requisits funcionals indicats en l'apartat X del present plec, la instal·lació ha de cobrir els requisits tecnològics que es detallen a continuació:

- La solució haurà de complir amb el recollit en el Manifest de l'arquitectura de referència per a les noves iniciatives i solucions de Salut i en les característiques de l'arquitectura del HES, referenciades a 2.1 Arquitectura de referència i 2.3 Característiques de l'arquitectura en tots els seus termes, especialment els indicats en l'apartat que esmenta les característiques més rellevants.
- La solució haurà de complir amb les versions de productes suportades, disponibles al full de ruta del programari del CTTI (<https://qualitat.solucions.gencat.cat/estandards/estandard-full-ruta-programari/>) dels seus components durant tota la vida del contracte. En l'oferta s'haurà d'indicar de quina manera es mantindran al dia tots els components de la plataforma (gestió de l'obsolescència), indicant el procés de gestió de versions i pegats proposat.
- La solució s'haurà d'assimilar o integrar amb les eines de cicle de vida del CTTI, en el que respecta a gestió del codi font, integració contínua, pipelines de desplegament automàtic, qualitat del codi, proves automatitzades i infraestructura com a codi. Totes aquestes activitats venen emmarcades per les tècniques i metodologies DevOps de desplegament continuat.
- La solució s'haurà d'integrar amb les eines de control de l'operació, en el que respecta a:
 - Matriu d'escalats, oferint suport 24x7 a diferents nivells de resolució

- Incidental, peticions i consultes en la plataforma de tiqueting de CTTI
 - Sondatge i monitoratge amb les eines del Centre de Control
 - Centralització de logs i observabilitat de la plataforma amb les eines del Centre de Control
- La solució proposada constarà de 3 entorns d'execució: Integració, Preproducció i Producció i un entorn de desenvolupament "sandbox" que s'oferirà als desenvolupadors del mercat d'aplicacions de forma paquetitzada. Els entorns INT i PRE poden estar desplegats en una mateixa virtual network privada, sempre i quan no comparteixin recursos en les seves diferents capes (balancers, contenidors, bds,...) per estalviar elements redundants de networking en un entorn petit com INT. Els entorns de Preproducció i Producció hauran de ser idèntics en la seva arquitectura, excepte en la capacitat que, en el cas de l'entorn de Preproducció, podrà ser entre un 70% i el 100% de la de PRO. L'entorn d'Integració i el de "sandbox" podran tenir una arquitectura diferent simplificada, però contemplat els mateixos productes base. No es contempla l'entorn de desenvolupament dins del servei, quedant a discreció del licitador les característiques d'aquest. No obstant això, els productes i eines utilitzats en aquest entorn de desenvolupament hauran de ser els mateixos en les mateixes versions que els oferts en el servei.
- Les noves versions del programari de la solució s'hauran de desplegar de forma automàtica amb un únic pas de construcció i passant el mateix artefacte construït per tots els entorns INT, PRE, PRO. El temps requerit màxim de desplegament entre que es diposita el codi font en el repositori de codi i la seva disponibilitat en producció és d'una (1) hora. Es requereix que els desplegaments es puguin realitzar en horari de servei sense tall ni degradació del servei perceptibles per l'usuari final. Es recomana utilitzar la tècnica de les "feature toggles" per a contemplar marxes enrere ràpides i desplegaments selectius de les noves versions. De la mateixa manera es recomana l'ús de programari específic per a manejar les versions de les bases de dades i habilitar la seva automatització en els fluxos de desplegament, de la mateixa manera que es fa amb els components de lògica de negoci.
- La gestió i operació de la infraestructura de la plataforma es durà exclusivament de forma automàtica, evitant en tot cas tasques operatives de forma manual. Els scripts d'automatització seran considerats com a codi font i, per tant, seran subjectes a totes les consideracions de gestió del codi font que es requereixen per als components de negoci.
- Tots els productes de tercers utilitzats contemplaran serveis de suport empresarial pels respectius fabricants, en modalitat 24x7, amb un temps de resposta inferior a 1 h en el cas d'incidents de severitat crítica que comporti interrupció o degradació del servei. S'haurà d'adjuntar a l'oferta el detall de productes i les evidències de compliment d'aquest requeriment per cadascun d'ells. En cas d'utilitzar components sense aquesta mena de suport donat pel fabricant, l'adjudicatari assumirà aquest nivell de servei i temps de resposta.
- Totes les APIs que ofereixi el servei es donaran en tres modalitats:
 - Modalitat síncrona: api REST o GRAPHQL sobre protocol HTTPS (TLS1.3 o superior), publicats a la plataforma corporativa d'API Manager.
 - Modalitat asíncrona: tòpics Apache Kafka publicats al servei de la Plataforma corporativa de missatgeria Kafka.

- Modalitat microfrontend: components web que consumeixen serveis de negoci del servei i que poden ser incrustables en aplicacions contenidores.
- Donada la tendència actual dels sistemes d'informació, el sistema objecte d'aquest contracte haurà d'executar-se en plataformes al núvol (cloud native). Tots els productes i aplicacions que s'instal·lin al context d'aquesta licitació estaran preparats per poder ser migrats a un altre proveïdor de núvol amb poc esforç i poder donar el servei en dos o més proveïdors de núvol públic
 - S'utilitzaran eines de lowcode, SaaS o cloud native en aquest ordre de preferència
 - En el cas de cloud native, s'utilitzarà tecnologia de contenidors en tots els artefactes de programari, preferiblement en modalitat serverless
 - S'utilitzaran bases de dades MongoDB Atlas que permeten una execució multi-proveïdor i multi-regió als proveïdors de núvol públic.

Les bases de dades utilitzades hauran de ser dissenyades per a contemplar qualitats d'emmagatzematge diferents segons la funció o la vigència de les dades a recuperar, per maximitzar el rendiment de les consultes més comunes contenint el TCO (Total Cost of Ownership) de la plataforma.

El servei haurà de contemplar la realització de backups i els components de maquinari necessaris per a realitzar-los. Aquests backups tindran les següents característiques:

- Recuperació de les dades en un punt en el temps de les darreres 48h
- Retenció diària incremental amb 2 setmanes de retenció, setmanal completa amb 1 mes de retenció, mensual completa amb 3 mesos de retenció i anual completa amb 1 any de retenció

Aquest backup ha d'incloure els mecanismes adequats per obtenir la còpia en la finestra que s'indiqui i per obtenir una còpia amb la congruència i consistència demanada per l'aplicació i les dades.

5.1.8 Descripció de l'Arquitectura

El licitador haurà de presentar la solució tecnològica proposada per realitzar les activitats requerides en el present plec, detallant els diferents components i tecnologies que la sustenten. Concretament:

- Descripció de la solució tecnològica, indicant els diferents blocs funcionals que la componen, i la funció de cada un dels blocs (p.e.: plataforma execució principal, motor de processos, mercat d'aplicacions, procés d'homologació, etc.).
- Disseny detallat d'arquitectura (incloent-hi diagrames), les respectives justificacions de les decisions d'arquitectura preses en el disseny i les adaptacions realitzades sobre el manifest de l'arquitectura de referència de Salut o el document de característiques de l'arquitectura de HES, si s'escau.

- Disseny d'alt nivell de la solució tecnològica per cada bloc funcional, incloent-hi tots els components tecnològics requerits (p.e.: ETL, bases de dades, servidors d'aplicacions, orquestració de contenidors, etc.) i les interaccions amb altres blocs funcionals de la pròpia solució o externs.
- Entorns de treball requerits
- Producte i versió de cada tecnologia proposada
- Productes SaaS requerits a cada component de la solució
- Dimensionament de la infraestructura necessària per a donar el servei desglossat per entorn i domini funcional.

5.2 Instal·lació, configuració i suport post-implantació de la solució tecnològica

L'adjudicatari realitzarà les següents activitats relacionades amb la instal·lació, configuració i operació de la solució tecnològica, en els diferents entorns acordats:

- Elaboració de la documentació tècnica necessària segons el Model de Qualitat de Solucions propi de Salut (09_Annex_9_Model_Qualitat_Salut_WIP) per poder procedir a la instal·lació.
- Coordinació amb l'equip d'Integració de Solucions i de suport cloud de CTTI, per a la validació del Document d'Arquitectura i per l'aprovisionament de la infraestructura cloud necessària.
- Instal·lació de tots els components de la solució tecnològica proposats amb els scripts d'infraestructura com a codi necessaris seguint les indicacions de SIC+ de CTTI.
- Configuració i integració de tots els components de la solució.
- Certificació de la qualitat de la instal·lació:
 - Justificació de la correcta instal·lació amb evidències específiques de cada component.
 - Revisió de la instal·lació per part dels fabricants respectius, o de personal propi degudament certificat i acreditat pel fabricant.
- Elaboració de la documentació tècnica resultant de la instal·lació.
- Actualització de la CMDB amb tots els components de la solució.
- Elaboració de la documentació d'operació de la solució tecnològica requerida per l'Àrea d'Operacions.
- Realitzar el suport post-implantació de la solució tecnològica.
 - Incorporació de pegats i gestió de l'obsolescència tecnològica amb periodicitat semestral.
 - Pla de capacitat i creixement de la plataforma
 - Gestió del rendiment.
 - Planificació de proves periòdiques de recuperació de desastres i restauració de còpies de seguretat.