Principis i decisions d'arquitectura del Pla director de sistemes d'informació del SISCAT

Setembre de 2023

/Salut Generalitat de Catalunya

Direcció: Josep Antoni Mira, Joan Esteve Riasol

Autors: Josep Antoni Mira, Joan Esteve Riasol, Juan Manuel Miguel, Juan Carlos Cornejo i Carles Salvador

Unitat promotora:

Àrea de Tecnologies de la Informació i les Comunicacions del Departament de Salut.
Àrea de Sistemes d'Informació del Servei Català de la Salut.

1a edició, versió 2.0:

Barcelona, setembre de 2023.

Assessorament editorial:

Gabinet del Conseller. Serveis editorials.

Assessorament lingüístic:

Servei de Planificació Lingüística del Departament de Salut

Disseny de plantilla accessible 1.07.
Oficina de Comunicació. Identitat Corporativa.

Sumari

1 Introducció

L'objectiu d'aquest document és proporcionar un marc descriptiu sobre l'arquitectura tecnològica que han de complir les solucions o productes desenvolupats en l'àmbit del nou **Pla director de** sistemes **d'informació del sistema sanitari integral d'utilització pública de Catalunya** (SISCAT).

Aquest document estén i amplia els principis d'arquitectura de sistemes d'informació establerts pel CTTI [ARQCTTI], que s'han de difondre i complir.

Principalment, els nous sistemes de Salut busquen impulsar un enfocament d'arquitectura distribuïda orientat a microserveis, estructurats segons **dominis funcionals** (*domain-driven design*), amb tres modalitats d'interoperabilitat: síncrona, asíncrona o microfrontals web.

Es busca optimitzar algunes de les característiques d'arquitectura més rellevants:

- La capacitat d'establir una escalabilitat i elasticitat a mida per a cada component, segons criteris de rendiment, demanda o tràfic.
- La independència tecnològica de cada microservei o component, el desacoblament en les diferents capes de la solució: **presentació**, **negoci** i **base de dades**, i la constant evolució d'aquestes.
- L'agilitat en el desplegament en un model d'integració contínua, amb una definició d'infraestructura com a codi i de proves automatitzades.
- La resiliència i la tolerància a fallades, evitant punts de caiguda únics que puguin afectar globalment el sistema d'informació.

Per tant, aquest document s'organitza en tres àmbits descriptius:

- **Principis d'arquitectura tecnològica**: normes i directius generals sobre com organitzar, desenvolupar, integrar i implantar solucions en l'ecosistema del PDSIS.
- **Decisions d'arquitectura**: directrius, criteris, o fins i tot restriccions a l'hora de dissenyar i construir una solució i/o evolució d'un nou producte digital de Salut, per garantir els principis i característiques d'arquitectura establerts.
- **Arquitectura de referència**: vistes de context i desplegament genèriques de l'arquitectura, amb l'objectiu de comunicar i divulgar el model base de creació de productes digitals dins de Salut, i la uniformitat en la interoperabilitat, el llenguatge de comunicacions, els components transversals i la infraestructura escollits.

2 Principis de l'arquitectura tecnològica

Els principis d'arquitectura descrits en aquest document són normes i directrius generals destinades a ser perdurables i rarament modificades.

2.1. Adopció Cloud Native

Sempre que sigui possible, per a les capes de presentació i negoci d'una solució, prioritzarem models de desplegament basats en **contenidors**, que permeten escalar, actualitzar o substituir un component de forma desacoblada sense que afecti tot el producte.

Aquest principi d'arquitectura té una implicació directa en el disseny dels microserveis, que ha de ser **Cloud Native**, perquè estaran destinats a executar-se en entorns volàtils i portables com ara un *Pod*, fins i tot amb una computació sense servidor al darrere.

Cal evitar males pràctiques, com ara mantenir informació o logs en disc local, utilitzar adreces estàtiques per crides entre microserveis, implementar operacions que requereixin mantenir un estat (*stateful*), o desar dades de sessió de navegació en el mateix contenidor.

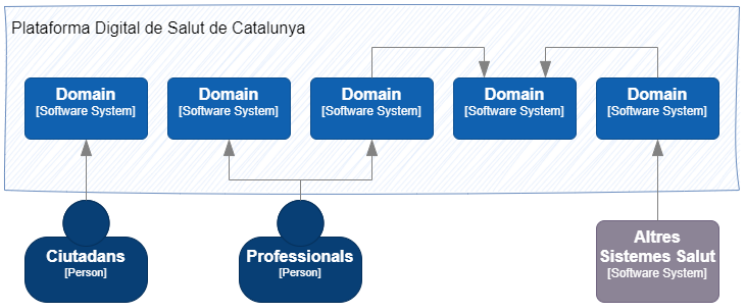
Cal dissenyar els microserveis de la forma més resilient i *stateless* possible: facilitant-ne l'escalabilitat, la resolució d'incidències o desplegaments fallits, i l'aplicació possible d'aquests a una versió anterior.

Finalment, l'equilibri entre serveis *stateless* permet que qualsevol instància pugui atendre qualsevol petició, facilitant-ne la portabilitat.

2.2. Estructuració en dominis funcionals

Permet definir equips específics i centrats en la unitat de negoci segons metodologies àgils de desenvolupament.

El domini funcional és el centre de la nostra arquitectura. Té una delimitació i abstracció clara del seu coneixement i del negoci que abasta, independent respecte de la resta.



2.3. Interoperabilitat entre dominis funcionals

Un domini funcional ofereix tres possibles mecanismes d'interoperabilitat:

Modalitat síncrona

A través de publicació d'una API d'operacions sobre https, cada domini pot ajustar la seva implementació formant una unitat atòmica lògica, sense interrompre altres serveis.

Emprant unes interfícies ben definides, els dominis encapsulen la seva lògica de negoci garantint un intercanvi d'informació homogeni entre sistemes, principalment **JSON**.

Es prioritzen estàndards específics de la indústria, com poden ser **FHIR** [FHIR] o **openEHR** [OPENEHR].

Dins l'ecosistema de Salut, disposem de diferents components transversals per a la publicació i gestió del cicle de vida de les API de microserveis:

- Bus de serveis de Salut (OSB) i Plataforma d'integració IS3 (AppConnect)
- Plataforma API Manager CTTI (ApiConnect) [APIMCTTI]
- Invocació directa de l'API REST des del mateix *endpoint* del fons del microservei.

Modalitat asíncrona

La interoperabilitat asíncrona orientada a esdeveniments (*event-driven design*) facilita la interacció que no necessita una resposta immediata, construint aplicacions que reaccionin en corrent de dades (publicació/subscripció).

Disposem d'arquitectures més robustes i tolerants a errors: desacoblant dependències entre dominis, oferint mecanismes de recuperació davant fallades puntuals d'un component...

Permeten escalabilitat horitzontal i baixa latència, assegurant que no es perdrà l'ordre ni la informació. Per exemple, els consumidors d'un microservei temporalment no disponible poden dipositar les operacions al voltant d'un tema de missatges que seran tractats posteriorment, un cop restablert.

Dins el PDSIS, disposem de la **Plataforma EventHub** del CTTI [EVENTHUB], com a agent de seguretat transversal de missatgeria asíncrona, basat en un sistema de publicació i subscripció a temes Kafka.

Els clients es poden subscriure com a productors i consumidors de temes amb l'afegit d'un component **Schema Registry** per gestionar l'esquema únic de missatges per cada tema.

Modalitat microfrontal

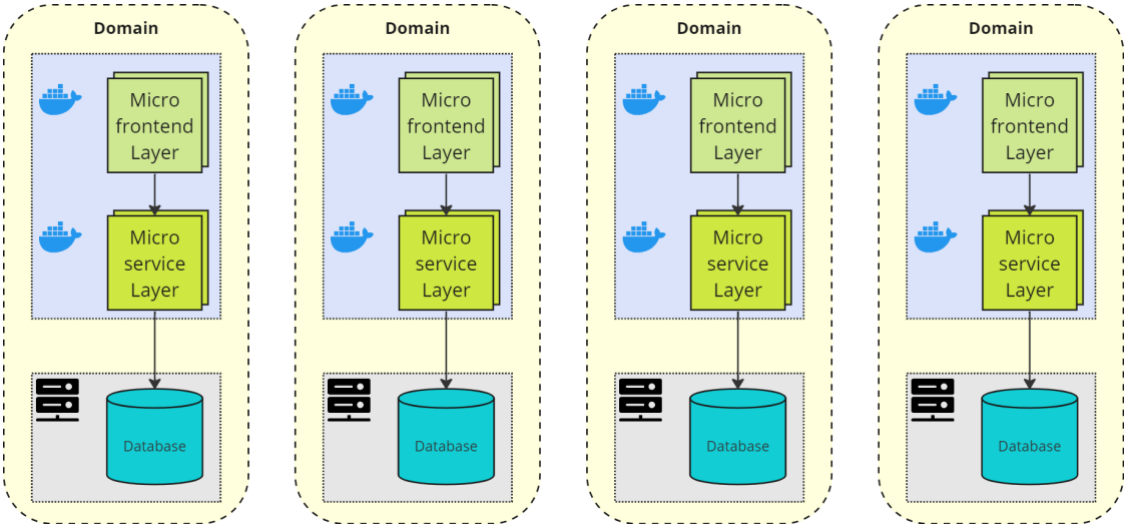
Consisteix en components web, principalment implementats com a *Single Page Applications*, que consumeixen serveis de negoci del seu propi domini.

Poden ser incrustables en altres aplicacions que han de presentar dades d'un altre domini funcional del qual no són responsables. En aquest cas, el microfrontal actua com un bloc d'informació proporcionat a un tercer, sempre que compleixin els requisits de seguretat d'aquest i respectin els principis i normatives de disseny, navegació i accessibilitat.

2.4. Elecció de la base de dades

Cada domini funcional és responsable de gestionar la integritat de les seves dades, com una base de dades per servei, evitant possibles punts de fallada amb afectació de tot el sistema.

No es permet compartir lògica de negoci amb altres serveis mitjançant una base de dades comuna entre aquests.



L'elecció del tipus de motor de base de dades, i el corresponent disseny del model de dades, resta determinat pels requeriments de rendiment, integritat i recuperabilitat de la informació, on cal complir les especificacions de la descripció d'arquitectura de la solució respecte dels indicadors d'RTO, RPO i PITR.

- Relacional o SQL, basat en taules i en integritat referencial.
- No-relacional o no-SQL, basat en col·leccions de documents.
- *Caché* o clau-valors en memòria.
- Textual, amb l'alternativa del producte Algolia, en modalitat SaaS.

També es revisarà les qualitats d'emmagatzematge sol·licitades en cada motor de base de dades, segons la funció o vigència de la informació persistida, per maximitzar el rendiment de les operacions més comunes, que contingui el *Total Cost of Ownership* de la plataforma.

2.5. Preferència per components transversals

Es basa a prioritzar la utilització de components transversals o ja existents en el catàleg de solucions CTTI o de Salut, abans de fer implementacions a mida de funcionalitats que ja es troben disponibles.

2.6. Estratègia Zero trust

Aquest principi d'arquitectura proporciona un model de protecció d'identitats, adreçaments i aplicacions, assegurant l'accés restringit a la infraestructura de xarxa i a les dades.

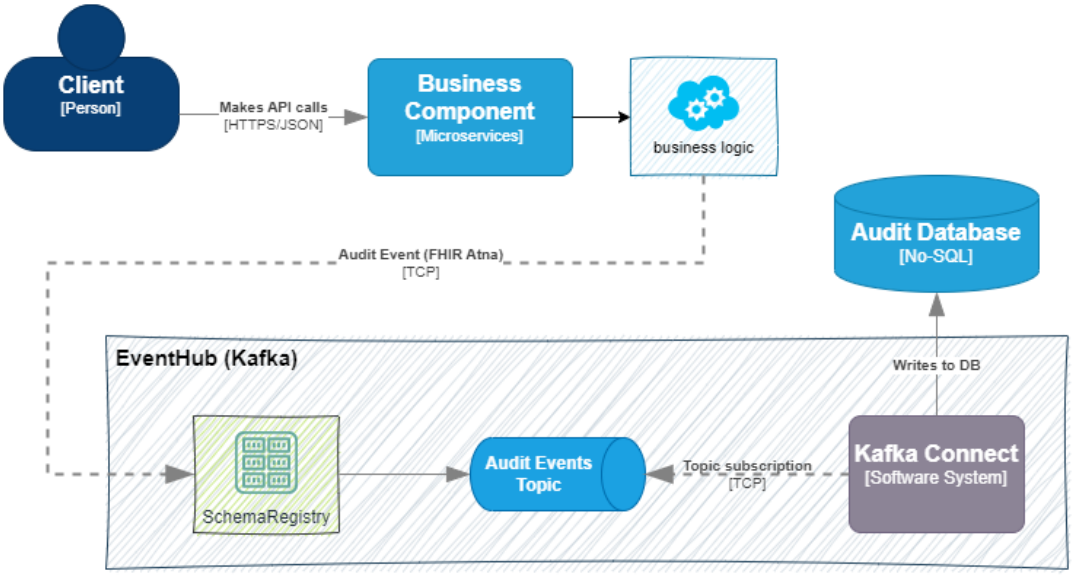
- Qualsevol connexió que s'estableixi és insegura.
- Sempre cal verificar, mai confiar entre aplicacions del sistema.
- Restringir els recursos, implementant controls dels principis de privilegis mínims.
- Aplicar polítiques de validació de la informació de context per aplicació.

2.7. Enregistrament d'auditoria

Els microserveis han de publicar registres d'auditoria d'accés a les seves operacions i recursos, segons els requeriments de l'Agència de Ciberseguretat establers a tal efecte.

A mode de resum [AUDITHES], consisteix en la publicació asíncrona d'aquests registres d'auditoria, en un format estàndard per sistemes de Salut, conegut com ATNA *Audit Trail Logs*, en format `FHIR Audit Event`.

Aquests missatges s'han de publicar en temes de l'Eventhub, on posteriorment se'n farà la consumició, persistència i explotació en una base de dades no relacional.



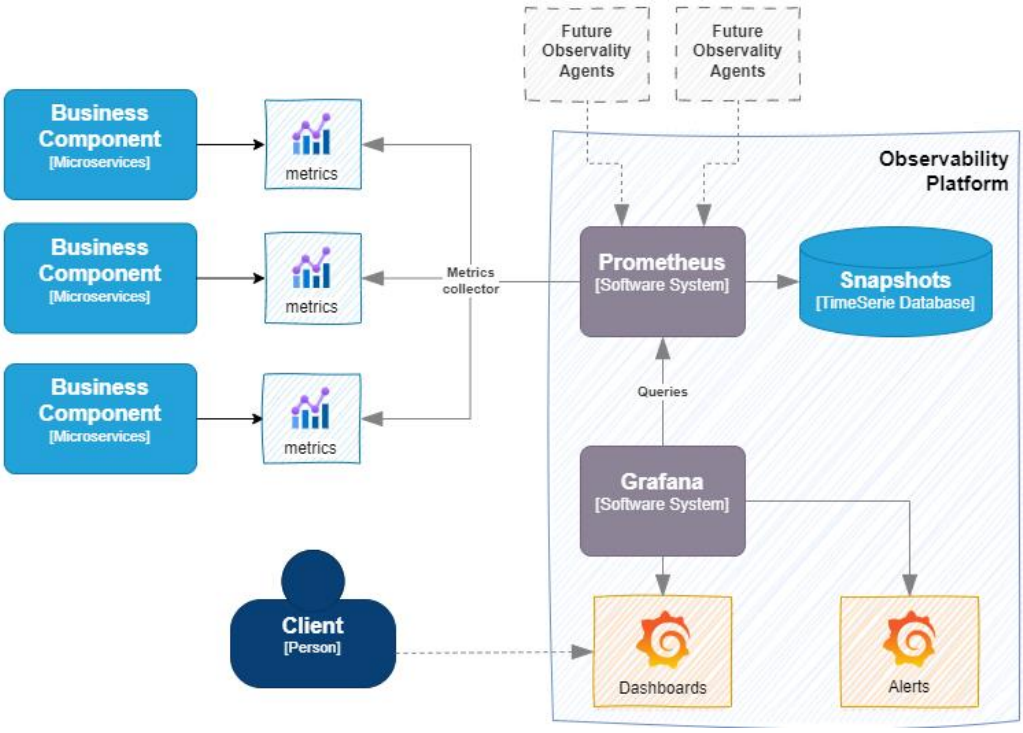
2.8. Mètriques d'observabilitat, monitorització i traces de log

Els microserveis d'un domini funcional han de proporcionar:

- Validació i sondes de salut: necessaris per a la plataforma d'orquestració de contenidors.
- Mètriques d'estat, com per exemple: consum de CPU, memòria, connexions a bases de dades, peticions ateses per segon o temps de resposta a les peticions.
- Mètriques d'indicadors de negoci pròpies de la solució.

Cal exposar aquestes mètriques (en format de comptadors o histogrames), en *endpoint*s específics del fons del microservei, que seran recopilades i persistides en un motor de base de dades de línia de temps **Prometheus**.

Això permetrà, posteriorment, implantar un sistema d'observabilitat transversal propi pels dominis funcionals de la plataforma digital de Salut, que podrà estar basat en panells de **Grafana**, o integrar-se en la plataforma TALAIA del Centre de Control del CTTI.



Per altra banda, quant a les traces, està en curs la definició d'un component transversal d'agregació de traces distribuïdes per operacions entre diferents microserveis, d'un mateix domini funcional o de diferents, per mitjà de l'estàndard **OpenTelemetry**.

De moment, es troben disponibles quadres de comandament de **Kibana** per consultar els diaris generats per cada aplicació en cas de plataformes de contenidors privades [LOGSCLOUD].

2.9. Automatització (CI/CD)

Es basa en la industrialització de l'entrega d'un producte de programari, tenint com a objectiu generar una infraestructura i eines per treballar amb automatismes:

- **Construcció**: la integració contínua permet generar els artefactes de forma automatitzada, a partir del codi font desat en eines centralitzades i autogestionades, on és possible localitzar i mesurar errors o factors erronis.
- **Desplegament**: el desplegament continu de components, gestió de dades i el sistema d'orquestració en contenidors del producte permet automatitzar les pujades de programari i les modificacions en les bases de dades.
- **Verificació**: la utilització del servei de lliurament continu permet incorporar proves automàtiques sobre el microservei en fase de desplegament.

La integració i desplegament continu (CI/CD) s'ha de fer a través de l'eina corporativa del **Servei d'Integració Contínua SIC 3.0** [SICTTI].

2.10. Gestió de l'obsolescència

Es basa en la necessitat de canviar o actualitzar la infraestructura o el sistema tecnològic perquè apareix una nova versió o un sistema més ràpid i eficaç.

Tipologia d'obsolescència:

- **De funció**: quan un producte es converteix en antiquat perquè apareix un altre amb millor rendiment i cost de funció.
- **De qualitat**: quan un producte, de manera planificada, es deteriora o es desvirtua per errors o limitacions en un temps determinat i curt.
- **De conveniència**: quan un producte, en termes de rendiment o qualitat, es considera obsolet per l'aparició d'un nou corrent o modificació de tendència tecnològica.

2.11. Mantenir la simplicitat del sistema

Es basa en normes de disseny i desenvolupament del producte.

- **KISS**: és la capacitat per poder descompondre un problema fins als seus elements més indivisibles, sense perdre l'objectiu d'evitar qualsevol complexitat agregada a l'estrictament necessari, prescindint de tot allò que no aporta un benefici clar i definit.

- **DRY**: és la capacitat de desenvolupar peces de codi úniques al sistema, sense ambigüitat i sense repetir-se. Permet que els evolutius o re-factoritzacions siguin mínimes i d'única ubicació, cosa que afavoreix la reusabilitat en l'àmbit de l'aplicació.

2.12. Benefici màxim al menor cost i risc possible

Es basa en l'aprofitament o reutilització de lògiques programades o integrades a la nostra solució (menor cost) i provades amb èxit o coneixent-ne les limitacions (menor risc).

- **Optimització de costos**: Utilització de contenidors per alleujar les dependències de la infraestructura i simplificar el procés d'implementació. Monitorar els serveis per identificar necessitats d'ampliació o reducció de recursos i ajustar els costos consegüentment. També cal tenir present el model de llicenciament a l'hora de posar en marxa una solució, atès que representen un cost recurrent.

- **Optimització d'actualització**: Mesura de l'impacte d'actualització que pugui tenir un canvi de sistema operatiu, programari intermediari o producte on s'executa l'aplicació. Per tant, cal no dissenyar una solució que depengui d'un maquinari específic. No dissenyar per al present, sinó intentar construir un sistema que es pugui reutilitzar a llarg termini.

2.13. Suport professional als sistemes implantats i futurs

Es basa a obtenir la millor solució tècnica o servei professional especialitzat als possibles esdeveniments del cicle de vida dels productes existents o desplegats, minimitzant riscos i costos i utilitzant:

- RFI (Request for Information): obtenció d'informació abans d'adquirir o mantenir un producte o servei. És un procés estructurat per conèixer la millor solució per cobrir una necessitat o mancança analitzant el mercat.

- RFP (Request for Proposal): obtenció de propostes detallades i assequibles de diferents proveïdors per un producte o servei definit. És un procés que ha de proporcionar la informació necessària per prendre una decisió de compra concreta.

3 Decisions d'evolució, d'integració o migració tecnològica

Aquesta és la relació de decisions d'arquitectura més rellevants per resoldre els principals problemes i necessitats dels sistemes d'informació del PDSIS.

3.1. Decisions referents a la capa de microserveis

Orquestració de contenidors

Per a l'orquestració dels contenidors on s'executen els microserveis, principalment s'optarà per plataformes basades en **Kubernetes**. Cal definir tota la seva **Infrastructura com a Codi** (IAC) amb els descriptors corresponents: ConfigMap, DeploymentConfig, Service, Ingress, Route ...

També cal definir correctament l'estratègia de desplegament (deploymentStrategy, maxSurge, maxUnavailable...) i els atributs de *health checks* i *readiness/liveness probes* necessaris per gestionar el cicle de vida del contenidor dins del clúster.

Alta disponibilitat

Per complir els criteris de continuïtat i recuperació de l'arquitectura de referència, cada microservei quedarà configurat en alta disponibilitat, amb una escalabilitat horitzontal dels servidors d'aplicacions o *Pod replica* en el cas de contenidors superior a 1, amb desplegaments sense talls de servei perceptibles per a l'usuari final.

Quant a l'aprovisionament, es demana també preferiblement alta disponibilitat actiu-actiu en dues ubicacions de CPD.

En cas que no sigui possible aquest actiu-actiu en la capa de microserveis, almenys s'ha de poder recuperar d'un desastre complet de la ubicació primària de CPD, amb trasllat de tots els contenidors a una ubicació secundària en un temps inferior a 1 hora.

Generació de mètriques per observabilitat

Els diferents microserveis han d'exposar mètriques d'estat, activitat i negoci en un *endpoint* específic en format **Prometheus** [METRICS] amb llibreries com Micrometer o Actuator.

Aquest *endpoint* no pot ser accessible des de l'exterior del motor de contenidors o servidor d'aplicacions on es troba desplegat el microservei per evitar que altres sistemes externs puguin generar la seva pròpia observabilitat envers els nostres sistemes.

Les mètriques han d'incloure, en forma de comptadors o histogrames:

Activitat i estat de l'aplicació: CPU, memòria, connexions a la base de dades, peticions ateses, temps de resposta...

Indicadors de negoci: relatius a cada microservei dins del domini funcional.

Les mètriques han d'estar correctament etiquetades per facilitar després l'explotació d'aquesta informació en panells d'observabilitat o configuració de regles d'alerta.

Generació de traces de *log*

Els microserveis han d'escriure els seus *logs* directament per sortida de consola. No es poden deixar les traces en cap fitxer dins el *Pod* on s'executa el contenidor. Cal complir la normativa NOR0016-C de traces de l'Agència Catalana de Ciberseguretat [ACC].

En el cas de plataforma de contenidors com Kubernetes, un agent **FluentD** instal·lat en el clúster recopilarà els *logs* de cada *Pod* i els agregarà en una memòria d'enregistraments basada en **ElasticSearch**, consultable a través d'un frontal visual **Kibana** [LOGSCLOUD].

De moment, no disposem de cap component per implementar traçabilitat compartida entre microserveis distribuïts. Però està en curs la definició d'un component transversal basat en **OpenTelemetry** per fer aquesta agregació distribuïda de traces.

Publicació de dominis i rutes d'*endpoints*

Un domini funcional ha de distingir els serveis que publica en els seus microserveis segons si són d'àmbit **intranet** o **internet**. El Departament de Salut posa a disposició els CPD d'un CIDR reservat (146.219.0.0/16) per a publicacions de dominis, conegut com **Anella de Salut**.

Per a l'àmbit intranet, la publicació dels serveis serà únicament dins la xarxa DNS d'XCAT, a decisió de si s'utilitza una adreça d'aquest CIDR d'Anella o la pròpia del CPD.

Per a l'àmbit internet, si és possible utilitzar el CIDR d'Anella, es farà una doble publicació: amb adreçament d'Anella al DNS d'XCAT, i amb adreçament públic per als DNS globals.

Per a un domini funcional únic que desplegui diferents microserveis, cal evitar la petició de *full-qualified domain names* (FQDN) individuals per a cada component. Sempre que sigui possible, cal sol·licitar un únic domini per evitar després la generació de massa certificats per a la comunicació amb TLS, amb la posterior gestió de les caducitats.

FQDN incorrectes (4 certificats requerits)	FQDN preferits (2 certificats requerits)
mservA.domain1.hes.catsalut.intranet.gencat.cat	domain1.hes.catsalut.intranet.gencat.cat/mservA
mservB.domain1.hes.catsalut.intranet.gencat.cat	domain1.hes.catsalut.intranet.gencat.cat/mservB
mservC.domain2.hes.catsalut.intranet.gencat.cat	domain2.hes.catsalut.intranet.gencat.cat/mservC
mservD.domain2.hes.catsalut.intranet.gencat.cat	domain2.hes.catsalut.intranet.gencat.cat/mservD

Els *endpoints* de mètriques, les verificacions de salut, o de consum privat intern del microservei no s'han de publicar fora del contenidor. En el cas de contenidors:

Tipus d'*endpoint*	Exposició en la plataforma
Health checks, readiness probes, liveness probes	No tenen publicació fora del Pod
Mètriques Prometheus Serveis REST consum intern dins del namespace	Publicació a nivell de servei
Serveis REST consum extern	Publicació a nivell Ingress/Route

3.2. Decisions referents a les bases de dades

L'Àrea d'Arquitectura i Qualitat de Solucions del Departament de Salut redactarà els diferents models de referència de base de dades específic per a cada tipus i tecnologia (relacional: postgres, noSQL: mongoDB, etc.), però els criteris comuns per a qualsevol solució de l'Àmbit Salut són els següents:

Model base de dades per servei

Un domini funcional pot disposar de més d'una base de dades, però sempre mantenint la responsabilitat única de la integritat de les dades sobre aquesta o aquestes.

No es permet traslladar lògica de negoci entre dominis funcionals o sistemes d'informació diferents mitjançant una base de dades comuna.

Recuperabilitat de la informació

Cal assegurar que la solució de base de dades compleix els requeriments de recuperabilitat consistent de les dades, complint l'RPO i RTO especificats en el DAQ.

Es demana un RTO màxim de 2 hores: arxivament de *logs* de transaccions per bases de dades relacionals, arxivament dels *logs* d'operacions per bases de dades noSQL, etc.).

En cas que la solució tingui requeriments d'RPO=darrera còpia de seguretat o Zero, o necessitats de PITR, es demanarà executar proves de recuperació de desastre a aquest efecte en l'entorn de preproducció per demostrar la recuperació consistent de la informació.

Aprovisionament per entorns

- A l'entorn d'INT: atès que principalment s'executen proves i validacions, es permet una infraestructura comuna per a motors de bases de dades de diferents dominis funcionals amb l'objectiu de reduir el cost total d'aprovisionament per a aquest entorn.

- A partir de l'entorn de PRE: cada base de dades ha de disposar del seu propi servidor, no es poden compartir recursos entre motors. Per a l'entorn de PRE, es demana el mateix aprovisionament horitzontal que per a PRO, malgrat que els servidors poden tenir una talla menys.

Seguretat i connexió des de l'exterior

Les bases de dades han d'oferir una separació segura d'usuaris i permisos, diferenciant l'usuari propietari de CPD, l'usuari d'aplicació, l'usuari de manteniment, i un usuari amb permisos només de consulta.

En cas que la connectivitat sigui possible, es facilitarà al lot proveïdor d'aplicacions l'accés a la base de dades dels entorns INT i PRE, mitjançant l'obertura de regles FW (NUS i CPD) des de la seva VPN. Disposaran de les credencials de l'usuari de manteniment o consulta.

En el cas de PRO: cal l'aprovació de la persona responsable de l'aplicació i **signar una excepció de seguretat**.

Repositoris de dades

Els repositoris centrals de dades de Salut de l'HES són els següents:

- Repositori de dades clíniques: plataforma de gestió del coneixement clínic d'acord amb l'estàndard openEHR per a la Generalitat de Catalunya.
- Mestre de pacients: repositori transversal de dades demogràfiques de pacients del sistema de salut de Catalunya segons l'estàndard FHIR R4.
- Servidor terminològic: sistema d'emmagatzemament i indexació de definicions terminològiques en format FHIR R4.
- Algolia: servei en modalitat SaaS, d'indexació i cerca textual de continguts, que de moment persisteix catàlegs terminològics o diagnòstics de Salut.

3.3. Decisions dirigides a la infraestructura

Descripció d’arquitectura (DAQ)

Les plantilles dels DAQ es poden trobar a la pàgina de lliurables del portal de Qualitat del CTTI, classificades segons el tipus d’aprovisionament de la solució: *on-premise,* núvol privat, núvol públic gestionat o no gestionat, o híbrid. [DAQCTTI].

El proveïdor defineix un pla de capacitat i el manté regularment en el DAQ per permetre, de manera anticipada, dimensionar la infraestructura i tots els elements necessaris a fi que el sistema d’informació pugui funcionar correctament.

Full de ruta de programari

Tots els artefactes han de complir amb les versions de productes suportades segons el full de ruta del programari del CTTI [FULLCTTI] i, en solucions ofertes en contenidors en modalitat al núvol, se segueix la normativa de núvol CTTI publicada a [CLOUDCTTI].

Requeriments de connectivitat

Tots els serveis de la Plataforma Digital de Salut es troben desplegats dins de la Xarxa d’Anella de Salut, i es diferencien dues topologies de domini: intranet o internet.

Els serveis publicats en domini internet són de públic accés, mentre que els serveis d’intranet (s’hi inclou la plataforma asíncrona Eventhub) requereixen connectivitat a aquesta xarxa i les corresponents regles de tallafocs habilitades.

Integració i desplegament continu (CI/CD)

Les infraestructures de Salut consideren habitualment tres entorns d'execució diferenciats: integració, preproducció i producció:

- Els entorns de PRE i PRO són idèntics en l'arquitectura, però PRE pot aprovisionar una capacitat d'entre el 70% i el 100% de la de PRO.
- L'entorn INT pot tenir una capacitat inclús menor, per exemple, sense escalabilitat horitzontal, però mantenint els artefactes de desplegament.

Se segueix la normativa de desplegaments mitjançant el servei d'integració contínua SIC 3.0 definit pel CTTI, consistent en gestió i custòdia del codi font, i en *pipelines* de construcció i desplegament dels artefactes en els diferents entorns.

- Les noves versions del programari de la solució s'han de desplegar de forma automàtica amb un únic pas de construcció, si cal, i passant el mateix artefacte construït per tots els entorns: INT, PRE i PRO.
- En solucions sobre plataformes de contenidors, és requisit separar correctament la construcció de l'aplicació o artefacte Docker de l'orquestració de la infraestructura com a codi, IAC, i la parametrització d'aquesta depenent de l'entorn: `ConfigMaps`, `AppConfig`, etc.
- La informació sensible (per exemple, credencials de bases de dades) que no sigui gestionada pel proveïdor de l'aplicació s'ha de desplegar de forma confidencial, sense registre en el control de versions: `Secrets`...
- El temps requerit màxim de desplegament des que es diposita el codi font, si cal, de l'artefacte en el repositori i la disponibilitat en producció és d'1 hora.
- Es requereix que els desplegaments es puguin fer en horari de servei, sense tall ni degradació de la solució perceptibles per l'usuari final, mitjançant estratègies de desplegament adients, com a mínim *rolling update*.
- Es recomana utilitzar addicionalment tècniques de *feature toggles* per aplicar desplegaments selectius de noves funcionalitats o modificacions en una solució, en lloc d'implantacions de canvis de caràcter *big bang*.
- Es recomana incorporar l'ús de programari específic per gestionar el model de bases de dades del microservei i habilitar-ne l'automatització en fluxos de CI/CD, juntament amb els components de lògica de negoci.

La gestió i operació a la plataforma es durà exclusivament de forma automàtica, evitant en qualsevol cas tasques operatives manuals. Els scripts d'automatització seran considerats codi font i, per tant, estan subjectes a totes les consideracions que es requereixen per als components de negoci.

El sistema d'informació ha de ser portable, és a dir, ha de poder ser desplegat en diferents servidors amb la mínima dificultat.

3.4. Analítica i explotació de dades

Els entorns d'analítica i explotació de dades de Salut consumiran tota la informació de forma asíncrona, a través de la plataforma **Eventhub** del CTTI.

L'objectiu és evitar operacions de consulta directament sobre les bases de dades transaccionals en entorns productius, cosa que en podria afectar el rendiment a causa de consultes pesades.

A aquest efecte, es proporcionaran les credencials necessàries d'Eventhub per consumir la informació i preparar les ETL, que poden ser de dos tipus:

- *Change-Data-Captures* del Confluent contra determinades taules en origen de les aplicacions, llegint dels seus *logs* de transaccions.
- Consumició de l'activitat publicada de forma asíncrona per part dels microserveis.

3.5. Model de seguretat. Autenticació i autorització dels serveis

Consumir els diferents serveis síncrons publicats per un domini funcional del PDSIS requereix una autenticació i autorització basada en tokens segons l'estàndard **OpenID Connect** [OIDC], que s'ofereix a través del proveïdor d'identitat transversal anomenat **Plataforma de Seguretat** [PDSHES].

PDS admet integracions amb protocol SAML i amb el directori corporatiu de GICAR, i és compatible amb models d'autorització RBAC (basat en rols) o ABAC (basat en atributs).

Per incorporar un nou client consumidor de serveis síncrons del PDSIS protegit per la PDS, cal sol·licitar una adhesió a l'Oficina eSalut (oficina.esalut@gencat.cat), on es farà una anàlisi de requeriments de les diferents modalitats possibles d'autenticació de sistema o d'usuari, informació incorporada en el token, etc.

En el cas de la interoperabilitat asíncrona, consumir o produir sobre els diferents temes exposats a la plataforma Eventhub requereix una autenticació MTLS basada en magatzems de certificats client, amb els quals es gestionen uns permisos, en aquest cas únicament amb un model RBAC.

Per incorporar un nou client per accedir als temes d'Eventhub, cal sol·licitar també una adhesió a l'Oficina eSalut, indicant quins permisos són necessaris.

3.6. Gestió del deute tècnic

Són totes aquelles decisions tecnològiques, tant físiques com de programari, basades en la resolució d'un problema, en temps real, i capaces de concebre i llançar un producte tecnològic que aborda la solució provisional o parcial de la necessitat. Per tant, ha d'haver-hi un equilibri entre les bones decisions i la rapidesa. Llavors:

Cal documentar tot el deute tècnic deliberat i imprudent de cada producte.

Cal reduir el deute tècnic deliberat i imprudent, bé sigui provinent d'integració, bé de migració o bé de mòdul nou, tan aviat com sigui possible de solucionar, recomanable a cada nova versió de l'aplicació.

Cal detectar el deute tècnic inadvertit i imprudent, provinent d'una integració o migració, disposant-lo al *backlog* pel seu disseny, construcció de la possible solució, intentant el mínim impacte en tercers, i alhora prioritzant-lo tan aviat com es pugui.

Cal verificar sempre, en introduir components nous o infraestructura nova, que no s'introdueixi deute tècnic deliberat i imprudent, atès que té un impacte.

4 Diagrames de l'arquitectura de referència

Des de l'Àrea d'Arquitectura i Qualitat de Solucions del Departament de Salut s'ha preparat un document descriptiu amb els diagrames de l'arquitectura de referència del PDSIS, dissenyats segons el model C4 [C4MODEL].

En aquest document es poden consultar exemples de les diferents vistes de context i components que cal incloure en les descripcions d'arquitectura de les noves solucions, per tenir així una estructura de diagrames homogènia per als diferents sistemes d'informació de Salut [ARQREFERENCIA].

Referències bibliogràfiques

Centre de Telecomunicacions i Tecnologies de la Informació. Principis d'arquitectura de sistemes d'informació CTTI. 2023. Disponible a: https://canigo.ctti.gencat.cat/arquitectura/principis_arq/

Centre de Telecomunicacions i Tecnologies de la Informació. Documentació Eventhub. 2022. Disponible a: https://canigo.ctti.gencat.cat/eventhub/

Centre de Telecomunicacions i Tecnologies de la Informació. Api Manager Corporatiu CTTI. 2022. Disponible a: https://canigo.ctti.gencat.cat/apim/

Centre de Telecomunicacions i Tecnologies de la Informació. Servei d'Integració Contínua SIC 3.0. 2019. Disponible a: https://canigo.ctti.gencat.cat/sic/

Àrea TIC del Departament de Salut, Àrea de Sistemes d'Informació del Servei Català de la Salut. 2023. Generació de registres d'auditoria a l'HES. Disponible a: https://gencat.sharepoint.com/sites/mapes_salut/SitePages/ARQUITECTURA-TECNOL%C3%92GICA.aspx

Centre de Telecomunicacions i Tecnologies de la Informació. Monitoratge i traces als contenidors. 2021. Disponible a: https://canigo.ctti.gencat.cat/cloud/monitoratge-contenidors/

Centre de Telecomunicacions i Tecnologies de la Informació. Exposició de mètriques en backend. 2021. Disponible a: https://canigo.ctti.gencat.cat/howtos/2021-01-02-Howto-spring-expose-metrics/

Centre de Telecomunicacions i Tecnologies de la Informació. 2019. Container Cloud CTTI. Disponible a: https://canigo.ctti.gencat.cat/cloud/

Centre de Telecomunicacions i Tecnologies de la Informació. Estàndard per al full de ruta del programari. 2022. Disponible a: https://qualitat.solucions.gencat.cat/estandards/estandard-full-ruta-programari

Àrea TIC del Departament de Salut, Àrea de Sistemes d'Informació del Servei Català de la Salut. Llibre blanc de la Plataforma de Seguretat HES. 2023. Disponible a: https://gencat.sharepoint.com/sites/mapes_salut/SitePages/ARQUITECTURA-TECNOL%C3%92GICA.aspx

Centre de Telecomunicacions i Tecnologies de la Informació. Plantilla de descripció d'arquitectura. 2021. Disponible a: https://canigo.ctti.gencat.cat/argctti/plantillada/

Health Level Seven Internacional. Especificació FHIR. 2023. Disponible a: https://www.hl7.org/fhir/

OpenEHR Foundation. Especificació OpenEHR. 2023. Disponible a: https://openehr.org/

Agència Catalana de Ciberseguretat. 2022. Disponible a: https://ciberseguretat.gencat.cat/ca/inici

OpenID Foundation. Especificació OpenID Connect. 2023. Disponible a: https://openid.net/

Simon Brown. The C4 model for visualizing software architecture. 2023. Disponible a: https://c4model.com/

Àrea TIC del Departament de Salut, Àrea de Sistemes d'Informació del Servei Català de la Salut. Disponible a: https://gencat.sharepoint.com/sites/mapes_salut/SitePages/ARQUITECTURA-TECNOL%C3%92GICA.aspx