Justification Report for the contracting of "Open Platform in Health - Architecture components, application market and platform services"

1. Data identifying the file and main characteristics of the tender:

1.1. Object of the contract:

The object of this tender is the contracting of the service/ for the construction and deployment of an "Open Health Platform - Architecture components, application market and platform services". It also includes specialized support services for the use of platform components and SaaS software procurement services.

The open health platform is conceptualized as a distributed and modular system that must support integrated and people-centered care. This system must allow the automation of routine tasks, facilitate personalized care and enable the systematic use of health data for the continuous improvement of health services. The platform is based on the paradigm of open systems, which is characterized by the use of open standards and interfaces that allow native interoperability between different components and applications.
From a technological perspective, the platform is structured in three main blocks:

1. Transactional execution core that includes:
   - Integration, deployment and maintenance of a standards-based healthcare process orchestration and management system (BPMN, CMMN, DMN) that can interoperate with clinical decision support systems, AI modules and form management environments.
   - Construction, deployment and maintenance of a clinical and demographic data access management system integrated with openEHR that manages access security and CRUD action logic while maintaining the integrity and consistency of openEHR information models (e.g. consistency of events and persistent elements, updating of composition statuses,...).
   - Integration with corporate components (MPI, PDS, terminology server, etc.).

2. App marketplace that includes:
   - Integration, adaptation and maintenance of a portal for developers with documentation and tools.
   - Deployment of a development environment (sandbox) for suppliers.
   - Design and deployment of an application homologation system.
   - Development, implementation and maintenance of a catalog of applications with commercial and administrative management.
   - Design and deployment of an application prescription system.

3. Transversal platform services:
    - Observability and monitoring.
    - Safety management.
    - Platform engineering and self-service.
    - Capacity management and recovery.

The system must be deployed on the CTTI's public cloud infrastructure, with high availability and compliance with the architecture, security and operation requirements defined in the annexes:

- Annex 1: Digital Health Strategy for Catalonia 2024-2030
- Annex 2: Architecture
- Appendix 3: Application Market
- Appendix 4: Orchestration and Processes
- Annex 5: Use cases
- Annex 6: Health Quality Model
- Annex 7: Access to clinical and demographic data
- Annex 8: Conditions of Execution of the PPTP Service
- Appendix 9: Hi Playbook

This specification is framed in the context of line 6 of investment 3 of component 11 of the *Digital Transformation Plan for Primary and Community Care* of the *Recovery, Transformation and Resilience Plan* to benefit from the NextGenerationEU Recovery Plan for Europe.

.

1.1.1. Contribution to the milestones and objectives of the PRTR

The action is incorporated into the Recovery, Transformation and Resilience Plan (PRTR), in Lever IV, Component 11, Investment 03.

- Palanca IV: An Administration for the Twenty-First Century
- Component 11: Modernisation of Public Administrations.
- Investment 03: Digital transformation and modernisation projects of the Ministry of Finance and Civil Service and the Ministry of Territorial Policy and the Administrations of the Autonomous Communities and Local Entities.
- Working group: GT4 – Digital Health History. This group has different lines of work, one of them is the individual non-collaborative project with other communities of "Integrated Health modeling and longitudinal management of care processes"
- The milestones defined within the framework of WG4 are:
    - Promote the normalization and common semantics of the EHR
    - Contain the set of normalized variables for the exchange of information between primary care data and the epidemiological surveillance system

1.1.2. Mechanisms for monitoring milestones and objectives

The degree of progress of the construction and development service will be periodically monitored; and quarterly, reports justifying the actions that will be put into operation will be delivered in full compliance with the provisions of the PRTR, defining the corresponding legal instruments in such a way as to allow the evaluation of the achievement of the milestones and objectives set out in the PRTR, in accordance with the provisions of sections 3. Description of the solution and 7. PPT Relationship and Governance Model

In order to carry out the monitoring and evaluate the achievement of the objectives set out in the previous point, the following indicators will be reported:

- Backlog status: Bi-weekly meeting on the status of the backlog with prioritization and refinement of user stories if deemed necessary. The provider will generate a meeting minutes and a report on the status of the user stories.
- Sprint demo: The developer will provide a dynamic demo that will include a presentation of the results achieved during the sprint.
- Sprint retrospective: When a sprint is completed, a report will be generated that will include the added value with the increase generated, an analysis of the quality tests carried out, and an update of the general status of the project.

1.1.3. Green and digital labelling

In accordance with the approved Transformation, Recovery and Resilience Plan (PRTR), this investment does not affect green labelling but is adapted to digital label 011 and contributes 100% in terms of digital labelling, and this PRTR does not include specific obligations regarding both labels. The digital label used is 011, corresponding to the field of intervention "ICT solutions for the Administration, electronic services, applications".

1.2. CPV:

72212900-8 Software development services and miscellaneous computer systems.
This CPV code responds to the different services to be provided, described in the Specific Technical Specifications.

1.3. Lots:

Given the characteristics of the service, it is not appropriate to divide it into lots.

This tender is structured in a single lot, given that it is necessary to treat the Open Health Platform homogeneously towards the same standardised technological and methodological implementation.

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

Batch separation could produce a risk in a possible deviation of schedules and quality problems since different functionalities and technologies will be part of the same service.

This homogenization cannot be guaranteed in the case of structuring the tender in several lots, since it cannot be ensured that different suppliers propose the same solution in terms of functionality, design, and architecture. This would entail the added need to integrate the different technological solutions proposed, with an increase in the cost and duration of the project, and a high risk of non-integration.

The object of the contract corresponds to the development and implementation of a new application and the maintenance services associated with it, this object is composed of a single objective, which is articulated by continuous activities that interact with each other in the different phases of the service, requiring an uninterrupted workflow with a set of processes to guarantee continuity in the final object of the contract, which entails execution with the same supplier.

Additionally, if there are multiple providers, there is a risk of having more than one framework for the development of the different services that the Platform must present, with different de-standardised processes and heterogeneous life cycles. In this sense, the governance of this ecosystem and its monitoring may be compromised, since the resources and efforts to govern them would be doubled. For this reason, a homogeneous and centralized ecosystem is required, which can only be achieved by not dividing into batches.

1.4. Duration of the contract:

The duration of the contract will be twelve (12) months, from the formalization of the contract. The possibility of extending specialized support services for the use of platform components (recurring and on-demand) and SaaS software procurement services for 12 months is contemplated.

2. Need for contracting

The current health information systems model is highly fragmented into multiple systems that store health and social data in different formats. This model is insufficient not only to effectively manage the growing volume of health and social data, but also does not help the deployment of people-centred care.

Information sources are trapped in silos and, with current levels of interoperability, it is not possible to take full advantage of the benefits of the free flow of data. To meet this challenge, it is necessary to develop an information infrastructure ("infostructure") that systematically prioritizes the persistence of data beyond the specific applications that use it, that these are extensible and that promotes data liquidity between systems.

Finançat per
Unió Europea
Fons Europeu
Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

The technologies to create an ecosystem like this have been around for a long time and are available. However, the main challenge lies in developing an infrastructure that transparently integrates data from various sources, including electronic health records, personal health devices (wearables) and social information. This infrastructure should also allow the use of advanced analytics techniques such as artificial intelligence and natural language processing to manage the complexity of heterogeneous health data.

The aim is to create a distributed and modular system that supports integrated and people-centred care, which allows the automation of routine tasks and facilitates personalised care. Existing central services, such as electronic medical records and digital imaging systems, should not be abandoned but should evolve towards the information infrastructure.

From a technological perspective, the solution to the problems of fragmentation in health information systems lies in what is known as the paradigm of open platforms. The concept of open platforms is not new and exists in other industrial sectors. In the context of health, this refers to systems designed to be natively interoperable, flexible and extensible, and that allow for seamless integration with various applications and data sources. Unlike closed platforms, which are often proprietary and limited in terms of compatibility with other systems, open platforms are based on standardized, open-source technologies and interfaces. This design philosophy allows different healthcare applications and systems to communicate and work together effectively.

In October 2017, the Apperta Foundation (United Kingdom) published the report "Defining an open platform", which this year is considered the reference document in this field. According to this report, open health platforms are characterised by the following principles:

1. Open standards-based - Implementation must be based on agile open standards. In this context, any player in the ecosystem should be able to use these standards at no charge to build a separate and compatible instance of the platform.
2. Common and shared information models – There should be a set of common information models in use by all instances of the open platform, regardless of any particular technical implementation.
3. Application portability support – Applications designed to run on one platform implementation should be able to work with trivial changes or no changes at all on another platform that has been developed independently.
4. Federable – It should be possible to connect any implementation of the open platform with all others that have been developed independently, in a federated structure, to allow for the sharing of appropriate information and workflows between them.
5. Vendor and technology neutral – Standards should not be dependent on particular technologies or require specific vendor components. Any ecosystem actor building an open platform implementation can choose to use any available technology and can choose to include or exclude proprietary components.

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

6. Support for open data – Data should be exposed as necessary (subject to good information governance practice) in an open, shareable and computable format in near real-time. Implementers can choose to use this format natively in their persistence layer (storage) of the open platform itself or meet this requirement by using mappings and transformations from some other open or proprietary format.
7. Providing open APIs – The full specification of APIs (the means by which applications connect to the platform) should be freely accessible.
8. Operability (as in DevOps) – The platform should support operability principles (this is about the qualities of a system that allow applications to operate well throughout their full lifecycle). Software systems that follow good operating practices tend to be simpler to operate and maintain, with a lower cost of ownership, and probably with fewer operational problems.

In summary, the benefits of open platforms are:

1. **People-centered care** – Open platforms can enhance patient-centered care by providing patients with easier access to their own health data. This empowerment allows patients to participate more actively in their healthcare decisions and management, leading to better outcomes and health satisfaction.
2. **Data standardization** – Open platforms are built on standard information models, which improves the quality and consistency of health data. This standardization is essential for data exploitation, research, and the development of evidence-based clinical practices.
3. **Interoperability between ecosystem actors** – One of the most significant advantages of open platforms is their ability to interoperate with various health systems and technologies. This means that patient data can be easily shared and accessed between different healthcare providers, improving continuity and quality of care. For example, different specialists, laboratories, and pharmacies can access a patient's electronic medical record, ensuring that all parties have the most up-to-date information.
4. **Flexibility and scalability** – Open platforms are inherently more flexible and scalable compared to closed systems. They can be easily upgraded and expanded to accommodate new technologies and changing healthcare needs. This ability to adapt is crucial in a field that is constantly evolving due to advances in medical research and technology.
5. **Fostering Innovation** – Open platforms foster innovation by enabling developers and healthcare providers to collaboratively create and integrate new applications and tools. This open ecosystem promotes a culture of continuous improvement and creativity, which leads to the development of advanced healthcare solutions.
6. **Cost-effectiveness** – Using open-source technologies and standard interfaces, open platforms can be more cost-effective than proprietary systems. They reduce the need for costly custom integrations, while allowing healthcare organizations to choose from a wider range of solutions that best fit their needs and budget.

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

7. **Enhanced data security** – While open platforms must be carefully managed to ensure security, their transparent nature allows a wider community of users and developers to identify and address vulnerabilities. This collective supervision can lead to the implementation of robust security measures.

3. Justification of the insufficiency of means

Given the need for high specialization for the correct execution of the object of the contract, both with the focus of the activity of the providers of the specific service and the personnel involved and the evolution of the knowledge necessary for each specific area, external contracting is the ideal and essential tool to respond efficiently and effectively to the needs that the contract aims to cover.

4. Economic data

Estimated value of the contract and base tender budget

The **estimated value of the contract** is 7,105,730.12 euros excluding VAT and is distributed as follows:

Base tender budget excluding VAT: 5,044,678.38 euros. Maximum amount of the planned extensions: 2,061,051.74 euros (VAT not included) in accordance with the application in the initial contract of specialized support services for the use of platform components and SaaS software procurement services.

In accordance with the justification of the price, the base budget of the tender is determined, which is 5,044,678.38 euros (VAT not included) and is distributed as follows:

- Provision of construction and development services determined as a lump sum for an amount of €2,983,626.64 euros (VAT not included).

- Provision of recurring technological services of specialised support for the use of components of the platform determined at a flat rate for an amount of 84,651.73 euros (VAT not included).

- Provision of technological services on demand for specialised support for the use of components of the platform determined by unit prices for a maximum amount of 216,400.01 euros (VAT not included), which will be consumed with the following maximum unit prices per type of evolution:

Evolutionary type	Evolutionary import
Very simple	€2,378.00
Simple	€7,134.00
Half	€14,268.00
Complex	€21,402.00
Very complex	€42,804.00

- Provision of SaaS software procurement services determined as a lump sum for a maximum amount of €1,760,000.00 euros (VAT not included).

Multi-year file with the following breakdown of amounts (VAT excluded):

2025	2026	Total
€2,017,871.35	€3,026,807.03	**€5,044,678.38**

This file is 100% eligible for funding by the European Union Recovery and Resilience Facility, established by Council Regulation (EU) 2020/2094 of 14 December 2020 establishing a European Union Recovery Instrument to support the Recovery after the COVID-19 crisis, and regulated in accordance with Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, and therefore, it is stated that there is no double financing and that, if there is, there is no risk of incompatibility with the State aid scheme.

Lever: 4
Component: 11
Investment: 3
Project: Integrated health modeling and longitudinal management of care processes

The CTTI, as its instrumental body, states that this action is incorporated into the Recovery, Transformation and Resilience Plan (PRTR). This action contributes to the achievement of the objectives set for Component 11 of the PRTR.

Justification of the price calculation

To calculate the base budget of the tender, an estimate of the effort (hours) dedicated to each of the activities to be carried out and the different professional profiles has been used, to allow the achievement of the different tasks to be carried out.

Finançat per
Unió Europea
Fons Europeu
Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

- For **construction and development services**, taking as a reference the contracts based, with complexity and magnitude of similar services, tendered in the last two years on the Framework Agreement for the construction, development and maintenance of applications service of the Generalitat de Catalunya and its public sector (CTTI-2021-20131).

Construction & Development Services	Effort (hours)
Requirements analysis (software and systems)	2.509
Functional analysis	2.509
Design of the solution architecture (software and systems)	7.528
Detailed design (software)	2.509
Construction, unit testing (software) and integration	12.547
Qualification tests (Includes performance, quality and safety, if applicable)	7.528
Software Installation	4.015
Software acceptance support	5.019
Change management	3.513
Transition to maintenance and/or post-implementation	2.509
Total	**50.186**

- For **recurrent specialised support services for the use of platform components**, taking as a reference the type of technologies and actions described in the scope of file CTTI-2023-12 on Application Maintenance.

Recurring specialized support services for the use of platform components	Effort (hours)
Operational management	160
User support (functional, technical and operational)	320
Component integration	400
Technical office	220
Training and documentation	320

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

Total	**1.420**

- For the estimation of specialized support **services on demand for the use of platform components**, the execution of different types of small evolutionary devices has been considered, taking into account their complexity, carried out in applications of similar size and characteristics, and implemented on the same technology (within the scope of the CTTI-2023-12 file on Application Maintenance).

Evolutionary type	Estimated evolutionary number	Average evolutionary effort (h)	Effort (hours)
Very simple	10	40	400
Simple	5	120	600
Half	5	240	1200
Complex	2	360	720
Very complex	1	720	720
		Total	**3.400**

Subsequently, the company/hour cost of each of the profiles has been determined. This has been calculated taking into account the salary studies of different consulting and human resources companies (Michael Page, Hays, Randstad, Robert Walters), corresponding to the last financial year (2024), which include a wide range of companies from different sectors. The annual salary, according to years of experience, of the ICT profiles that best suit the professionals required to perform the service, according to the years of experience, has been taken as a reference, assimilating the reference profiles to the ET3 technological environment, defined in the CTTI-2023-12 file on Application maintenance according to technical complexity and the associated family of technologies.

The company/hour cost of the profiles corresponding to the ET3 environment, results from the average of the different salary figures of the referenced studies once increased by 35% for Social Security, compulsory permanent training, occupational risk prevention and those of surveillance and health at the expense of the company, considering the resulting cost (total annual cost) for 1760 hours[1].

Therefore, taking the ET3 environment as the basis for calculation, the amount corresponding to the ET1-ET2 and ET4-ET5 environments has been projected by applying the average percentage of increase between environments defined in the CTTI-2023-12 Application

[1] 1760 hours per year are defined given that a weekly working day of 40 hours and 30 days of vacation per year has been estimated.

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

Maintenance file, 4% for ET1-ET2 and 10% for ET4-ET5 respectively, considering that these differences are still valid at the market level.

Below is a summary table of the total effort for construction and development services, specialized support services for the utilization of recurring and on-demand platform components.

	Effort (hours)
Construction & Development Services	50.186
Specialized support services for the use of platform components (recurring)	1.420
Specialized support services for the use of platform components (on request)	3.640
Total	**55.246**

In accordance with the above premises, the following rates are determined for each technological environment:

Professional profiles	Cost/hour Company (Without VAT) - Studies year 2025				
	ET1	ET2	ET3	ET4	ET5
Project Manager	€58.43	€58.43	€56.18	€61.80	€61.80
Architect	€51.33	€51.33	€49.36	€54.30	€54.30
Cloud Security Engineer	€51.33	€51.33	€49.36	€54.30	€54.30
Consultant / analyst	€46.07	€46.07	€44.30	€48.73	€48.73
Cloud Engineer	€46.07	€46.07	€44.30	€48.73	€48.73
Analyst-developer	€38.29	€38.29	€36.82	€40.50	€40.50
Developer	€31.21	€31.21	€30.01	€33.01	€33.01
DevSec Ops Technician	€31.21	€31.21	€30.01	€33.01	€33.01

For the calculation of the price corresponding to the specific object, the ET1 environment has been set as the corresponding work environment, given that the technologies used in the development and the technical knowledge necessary to achieve the object of this tender would be assimilated within the Web technological family (J2EE, .net, PHP, VB, portals, content manager,...), as defined in file CTTI-2023-12 on Application Maintenance.

Taking into account the different profiles defined, their effort and the company/hour cost to be applied to each of them, the total amount **of personnel costs is 2,488,392.71 euros**, as detailed below:

Construction and development services:

Profile	Effort (hours)	Cost/hour company	Amount
Project Manager	3.302	€58.43	€192,935.86
Software Architects	6.374	€51.33	€327,177.42
Senior Developers	16.310	€38.29	€624,509.90
Experts en UX/UI	3.202	€38.29	€122,604.58
Consultants/Business Analysts specialising in health	4.866	€46.07	€224,176.62
Cloud Security Engineer	4.863	€51.33	€249,617.79
Experts in health interoperability	4.863	€46.07	€224,038.41
Experts in change management	3.202	€46.07	€147,516.14
Training experts	3.207	€46.07	€147,746.49
Total	**50.189**		**2.260.323,21**

Once the percentages of 20% and 10%, corresponding to indirect costs and industrial profit, respectively, have been applied to the total amount of construction and development services, the result is an amount of €2,983,626.64 for the consumption of services.

<u>Specialized support services for the use of platform components:</u>

Recurring services

Profile	Effort (hours)	Cost/hour company	Amount
Project Manager	30	€58.43	€1,752.90
Software Architects	266	€51.33	€13,653.78
Senior Developers	355	€38.29	€13,592.95
Experts en UX/UI	118	€38.29	€4,518.22

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

Consultants/Business Analysts specialising in health	148	€46.07	€6,818.36
Cloud Security Engineer	118	€51.33	€6,056.94
Experts in health interoperability	148	€46.07	€6,818.36
Experts in change management	118	€46.07	€5,436.26
Training experts	119	€46.07	€5,482.33
	1.420	**-**	**€64,130.10**

Once the percentages of 20% and 10%, corresponding to indirect costs and industrial profit, respectively, have been applied to the total amount of recurring specialized support services for the use of platform components, it results in an amount of 84,651.73 euros for the consumption of the services.

On-demand services

Profile	Effort (hours)	Cost/hour company	Amount
Project Manager	240	€58.43	€14,023.20
Software Architects	462	€51.33	€23,714.46
Senior Developers	1183	€38.29	€45,297.07
Experts en UX/UI	232	€38.29	€8,883.28
Consultants/Business Analysts specialising in health	353	€46.07	€16,262.71
Cloud Security Engineer	353	€51.33	€18,119.49
Experts in health interoperability	353	€46.07	€16,262.71
Experts in change management	232	€46.07	€10,688.24
Training experts	232	€46.07	€10,688.24
	3.640	**-**	**€163,939.40**

Once applied to the total amount of specialized support services for the use of components of the platform on demand, the percentages of 20% and 10%, corresponding to indirect costs and industrial profit respectively, result in an amount of 216,400.01 euros for the consumption of the services.

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

For the consumption of on-demand technological services, five (5) different types of evolution are determined, in accordance with the provisions of section 5.2. Model for the classification of the development of the evolutionaries of the Annex to the Specific Technical Specifications. The price of these services is determined by an average duration expected for each of the types of evolution according to their classification and by the cost per half hour, which includes indirect costs and industrial profit, established at 59.45 euros/hour.

Evolutionary type	Average hours (h)	Average cost/hour	Evolutionary import
Very simple	40	€59.45	€2,378.00
Simple	120		€7,134.00
Half	240		€14,268.00
Complex	360		€21,402.00
Very complex	720		€42,804.00

In conclusion, based on the calculations detailed above, an amount of personnel costs of 2,488,392.71 euros (excluding VAT) is determined.

Service		Personnel costs
Construction & Development Services		€2,260,323.21
Specialized support services for the use of on-demand platform components	Recurring services	€64,130.10
	On-demand services	€163,939.40
	Total	**€2,488,392.71**

SaaS Provisioning Services:

The estimate of the quantities required for the provision of SaaS software has been calculated based on the actual volumes of similar data services of the Tax Agency of Catalonia data platform and the transversal data platform of Catalonia.

Service	Amount of other direct costs
SaaS software provisioning	1.600.000,00 €
Total	**1.600.000,00 €**

In conclusion, based on the calculations detailed above, an amount of direct costs of **4,088,392.71** euros (excluding VAT) is determined.

In accordance with the provisions of article 100.2 of the LCSP, the base bidding budget for professional construction, development and specialized support services for the use of platform components, is set once the direct and indirect costs and industrial profit have

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

been determined, in accordance with the distribution of the following table, resulting in a base bidding amount for construction services, development, specialized support services for the use of platform components and SaaS procurement of **5,044,678.38** euros (excluding VAT):

Concept	Amount	Observations / percentage applied
Direct Costs		
Personnel costs	€2,488,392.71	Salaries, S.S., training and occupational risks
Other direct costs	1.600.000,00 €	SaaS Software
TOTAL DIRECT COSTS	**€4,088,392.71**	
Indirect Costs		
General expenses	€497,678.54	Approximate percentage of 20% of personnel costs[2]
TOTAL INDIRECT COSTS	€497,678.54	
SUBTOTAL COSTSDIR + INDIR	**€4,586,071.25**	
Industrial Benefit		
Industrial Benefit	€458,607.13	Approximate percentage of 10%[3]
TOTAL WITHOUT VAT	**€5,044,678.38**	
TOTAL INCLUDING VAT	**€6,104,060.84**	21% VAT

5. Justification of the procedure for awarding:

This tender will be processed through an open procedure subject to harmonised regulation, regulated by article 156 of the LCSP and following, given that the VEC is greater than 221,000.00 euros.

[2] The amounts of these concepts have been determined in accordance with the report of the Spanish Association of Consulting Companies *"The quality-price relationship in the IT and consulting sector, under the provisions of Law 9/2017 on Public Sector Contracts"* in which the reasonable percentages in the ICT sector for the calculation of general expenses and industrial profit are determined, taking into account data extracted from the database of sector ratios of non-financial corporations, published by the Bank of Spain.

6. Solvency criteria

Economic solvency

Equity of the company at the end of the last financial year for which the obligation to approve annual accounts expires, must be at least 20% of the estimated value of the contract

This requirement is motivated by proving the solvency of the bidder and that its financial situation is sufficiently reliable for the development of the object of the contract.

Technical and professional solvency

Companies must prove that they have carried out a minimum of works or projects related to the object of the contract with public or private clients over the course of the last three years. The works and/or projects must meet one of the following conditions:

a) Up to three projects whose sum is equal to or greater than 2,200,000 euros (excluding VAT)
b) A project with a value equal to or greater than 1,450,000 euros (excluding VAT)

In the case of joint ventures, the work carried out individually by each company may be added.

This relationship is evidence that the bidder has sufficient knowledge to develop the contract.

In addition, the bidding companies must assign a work team to the execution of the contract, which meets the following requirements according to the profile requested in each support service:

1 100% dedicated project manager

- They must have at least a higher degree in the technological field.

- They must prove that they have participated in projects or services related to the object of the contract during the last **five years**, whether in the public or private sector. Projects must consist of software development lifecycle management (SDLC).

2 100% dedicated software architects

- The assigned profiles must have, at least, a university degree in the technological field.

- They must prove participation in projects or services linked to the object of the contract during the last five years, whether in the public or private sector. These projects must include some of the main technologies or architectural principles that the Department wants to promote in its reference architecture, contained in the link https://salutweb.gencat.cat/ca/ambits-actuacio/linies/tic/solucions-siscat/model-adhesio/arquitectura-tecnologica/manifest-referencia-iniciatives/

4 Senior Developers at 100% Dedication

- The assigned profiles must have, at least, a university degree in the technological field or a higher level training cycle in software development.

- They must prove experience in projects or services linked to the object of the contract during the last **five years**, in public or private environments. The projects to be accredited must include software development in technologies and frameworks aligned with the Department's reference architecture.

2 UX/UI experts with 100% dedication

- The assigned profiles must have, at least, a university degree or a higher level training cycle.

- They must prove that they have participated in projects or services related to the object of the contract during the last **three years**, whether in the public or private sector. The projects to be accredited must consist of defining and managing design processes, generating prototypes, and creating scalable and sustainable design solutions.

2 Consultants/Business Analysts specialized in health with 100% dedication

- The assigned profiles must have, at least, a university degree.

- They must prove participation in projects or services linked to the object of the contract during the last **five years**, whether in the public or private sector. The projects to be accredited must be included in the field of information and communication technologies in health.

2 Cloud Security Engineer with 100% dedication

- The assigned profiles must have, at least, a university degree in the technological field or specific professional certifications in cloud security (AWS Certified Security, Google Professional Cloud Security Engineer, Microsoft Certified: Azure Security Engineer, among others).

- They must prove experience in projects for the deployment, management and security of services in cloud environments during the last **five years.** The projects to be accredited must include the implementation of secure cloud architectures, identity and access management, application of threat protection measures and regulatory compliance.

2 Experts in healthcare interoperability with 100% dedication

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

- The assigned profiles must have, at least, a university degree in health sciences, computer engineering, telecommunications or related disciplines.

- They must prove experience in projects or services related to health interoperability during the last 3 years. The projects to be accredited must include knowledge and application of HL7, FHIR, CDA, openEHR, DICOM, SNOMED CT or LOINC standards.

2 Change management experts with 100% dedication

- The assigned profiles must have, at least, a university degree.

- They must prove experience in organizational and digital change management projects or services during the last three years. The projects to be accredited must include digital transformation strategies in the health sector, management of resistance to change, agile methodologies in technological adoption and implementation of communication plans and training for users.

2 Training experts with 100% dedication

- The assigned profiles must have, at least, a higher university degree.

- They must prove experience in technological training projects or services during the last three years. The projects to be accredited must include the development and execution of training plans on digital platforms and/or interoperability solutions.

7. Award criteria

In accordance with article 145.1 of the LCSP and taking into account the purpose of the reference contract, the award criteria are established with a maximum score of 100 points and distributed as follows:

- Criteria that can be assessed by value judgment, up to 49 points.
- Criteria that can be assessed using automatic formulas, up to 51 points.

Criterion	Punctuation
Criteria that can be assessed by value judgment	**49**
1. Functional Solution	10
1.1 Approach to the first operational product	10
2. Technical Solution	30
2.1 Technological model for the transactional core	10
2.2 Technological model of the application market	10
2.3 Technological model of platform and integration services	10
3. Service Solution	9

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

3.1 Approach to the application of CTTI models, methodologies and tools to the project.	2
3.2 Planning the implementation of the solution	4
3.3 Change management approach	3
Criteria that can be assessed using automatic formulas	**51**
1. Economic offer	18
2. Improvement of the profiles requested by the work team	9
3. Extended warranty	5
4. ANS Improvements	5
5. Degree of partnership between the bidder and the manufacturers involved	5
6. Technical certifications of the team assigned to the service	7
7. Improvements for gender equality	2

7.1. Subjective criteria or those assessable by value judgment (up to a maximum of 49 points)

For each of the criteria that can be assessed through a value judgment, its assessment will be carried out according to the valuable aspects indicated in each of the criteria.

This assessment will be carried out in accordance with the following parameters:

Excellent	100%	The bidder's proposal significantly and significantly exceeds all aspects of the evaluation criterion
Nice one	75%	The bidder's proposal prominently complies with all aspects of the evaluation criterion
Acceptable	50%	The bidder's proposal complies in an adjusted manner with all the aspects of the evaluation criterion
Basic	25%	The bidder's proposal partially complies with the aspects of the evaluation criterion
Null	0%	The bidder's proposal does not meet the aspects of the evaluation criterion

Finançat per
Unió Europea
Fons Europeu
Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

In the event that a bid equals or exceeds 80% of the assessment of the criterion/sub-criterion with its own identity (identified with CIP), the final score for this criterion will be obtained by applying the formula of Directive 1/2020 on the application of formulas for the assessment and scoring of economic and technical proposals, approved by the Directorate General for Public Procurement, which is as follows:

$$P_{op} = P \times \frac{VT_{op}}{VT_{mv}}$$

Where:

Octopus is the score of the section for the offer to be evaluated.

P is the maximum score for the section.

VTop is the technical assessment of the section for the offer that is scored.

VTmv is the technical rating of the section with the best rating.

The score resulting from the application of the formula will be rounded to two (2) decimal places.

In accordance with the provisions of Directive 1/2020 on the application of formulas for the evaluation and scoring of economic and technical proposals of the Directorate General for Public Procurement, the award of contracts must guarantee an objective comparison of the relative value of the bidders' bids that allows it to determine, under conditions of effective competition, which is the most economically advantageous offer, evaluated on the basis of the best value for money.

To find out which proposition has the best value for money, it is necessary to assess both criteria, quality and price, equally. Thus, the assessment and subsequent scoring of the economic proposal and the technical proposal must be carried out with the same parameters, so as to guarantee that if the best economic offer is attributed the best possible score, the best technical proposal must also obtain the best possible score. Likewise, the score of the proposals submitted by the bidders must be proportional, so that the difference in quality and price between the different proposals is reflected proportionally in the score.

In this sense, and in order to comply with the guideline, it is established that the criteria with their own identity (CIP) are those that will provide the highest quality to the bids and require greater demand from bidders at the time of evaluating them, and therefore, the above weighting formula will be applied to them.

1. **Functional Solution (up to a maximum of 10 points) CIP**
1.1 Proposal of the first operational product (up to a maximum of 10 points) **Justification:** The consideration of the approach to the availability period of a first operational product and the functionalities included in it as a criterion for evaluating the offer

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

makes it possible to guarantee the efficiency and viability of the project. A first operational product facilitates the early detection of possible improvements and adjustments, minimizing risks associated with deviations in deadlines and quality. It also corresponds to an agile and results-oriented approach from the early stages of development.

Specifications and rating guidelines:

The amount of the requirements included in the first operational product and the group of users affected will be assessed, with the period required to achieve it, in accordance with the content of section 3.Description of the PPT solution and according to the 3 use cases set out in Annex 3.

2. Technical Solution (up to a maximum of 30 points) CIP

2.1 Technological model for the transactional core (up to a maximum of 10 points)

2.2 Technological model of the application market (up to a maximum of 10 points)

2.3 Technological model of platform and integration services (up to a maximum of 10 points)

Justification:

The solidity of the technological model is a critical factor for the success of the open platform in health, as it will determine its capacity to support, the operation of the platform itself, the interoperability between systems and its future scalability. This criterion ensures that the proposed solution not only meets the requirements defined in the PPT, but is also prepared to evolve according to the needs of the health system.

Specifications and rating guidelines:

For each of the technological models, the following will be assessed:

- The **architectural approach** of the proposed technological model in accordance with the corporate architecture roadmap, taking into account the different services or products necessary to respond to the requirements and the **justification** of how the principles of corporate architecture have been applied in the proposed technological model, taking into account the content of section 3.Description of the PPT solution. **(2 points)**
- The **resilience** of the mechanisms proposed on the solution in the face of any service outage of the reused components or infrastructures that may impact the availability of the solution (for example: integration processes,

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

infrastructure problems), in accordance with the content of section 3.Description of the PPT solution**. (1 point)**

- The ease **of scalability** of the technological model to absorb increases/decreases in load on the solution (more/fewer users or more/fewer transactions) automatically and without affecting the service, in accordance with the content of section 3. PPT Solution Description. **(2 points)**
- The **redundancy and recovery mechanisms** of the technological model to ensure the fault tolerance of the solution to meet the requirements related to continuity and availability indicated, in accordance with the content of section 3.Description of the PPT solution. **(2 points)**
- The **ease of maintaining** the technological model to apply changes, improvements or make updates to the solution with the least impact on the service, in accordance with the content of section 3. PPT Solution Description. **(2 points)**
- The **ease of interoperating** and integrating with other systems using standard protocols, in accordance with the content of section 3. Description of the PPT solution**. (1 point)**

3. Service Solution (up to a maximum of 9 points)

3.1 Approach to the application of CTTI models, methodologies and tools to the project (up to a maximum of 2 points)

Justification:

The application of CTTI methodologies and tools in the project is essential to ensure the correct execution of the service. The use of standard models such as the quality model, SCRUM/CTTI and corporate architecture guarantees efficient management, minimizing risks and ensuring the quality and traceability of the service offered

Specifications and rating guidelines:

The following will be valued:

- The **lines of improvement** that are proposed on the current methodologies for each of the phases of the project, according to the content of section 3.Description of the PPT solution. **(1 point)**
- The **methodology for reporting and monitoring the service** , taking into account different communication channels, periodicity of communication and specific aspects to be addressed, in order to obtain detailed and updated information on the status of the project **(1 point)**

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

3.2 Planning the implementation of the solution (up to a maximum of 4 points)

Justification:

A robust and detailed planning allows you to establish a realistic schedule that guarantees an orderly implementation of the solution. Segmentation in implementation phases, based on agile methodologies, ensures an iterative delivery of functionalities that adds value from the early stages of deployment. Coordination with other existing actors and services is essential to optimize implementation times and guarantee the delivery of the product in the required time.

Specifications and rating guidelines:

The following will be valued:

- The **coherence** of the planning and the **reasonableness** of the deadlines of the overall project schedule, considering the description of the tasks to be carried out in each phase considering the effort and dedication planned for each phase with detail of all the activities required, taking into account the content of section 3.Description of the PPT solution **(1 point)**
- The **anticipation of functionalities**and/or value delivered to the user, until the solution is delivered with all the requirements implemented, in accordance with the content of section 3.Description of the PPT solution. **(2 points)**
- **additional proposals for** coordination with other actors participating in the solution (other maintenance providers, infrastructure providers, etc.) that facilitate the reduction of the implementation period, in accordance with the content of section 3. PPT Solution Description. **(1 point)**

3.3 Change management approach (up to a maximum of 3 points)

Justification:

Implementing an effective change management strategy is essential to facilitate end-user adoption of the solution. The incorporation of innovative tools for change management (such as virtual learning environments and interactive material) optimises the learning curve and facilitates the adoption of the new platform in the Catalan Health System.

Specifications and rating guidelines:

The following will be valued:

- The **proposed communication and training plan** , taking into account the content of section 3.Description of the PPT solution, and taking into account: **(2 points)**
  - The contents of the plan, ensuring that it contains all the necessary information of interest in relation to the project.

Finançat per
Unió Europea Fons Europeu Next Generation
Gobierno de España
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

  - The communication channels proposed to reach all those interested.
  - The **frequency** and **continuity** of the proposed communication and training sessions, which guarantee a progressive assimilation by the users of the system.
  - the **digital and innovative nature** of the mechanisms, tools (office automation, virtual learning environments, etc.) and materials used for change management (training material, dissemination material, etc.).
- The **organization** of the project team to attend to post-implementation support to users in order to ensure the correct use of the new solution, in accordance with the content of section 3.Description of the PPT solution. **(1 point)**

7.2. Criteria that can be assessed using automatic formulas (up to a maximum of 51 points)

1. Economical offer (up to 18 points)

In application of Directive 1/2020 on the application of formulas for the assessment and scoring of economic and technical proposals, approved by the Directorate General for Public Procurement of the Generalitat de Catalunya.

Economic offers with a reduction of more than 10% with respect to the base tender budget (excluding VAT) will not be evaluated. For valuation purposes, the bid will be calculated with the maximum percentage established of 10% and, therefore, this excess percentage will not be taken into account exclusively for valuation purposes.

This limitation (satiety threshold) is motivated by ensuring the best quality-price in the tender by discouraging the submission of mediocre bids in the qualitative evaluation criteria that obtain excellent scores due to the excessive reduction of the prices offered, considering that all the amounts offered that exceed the established satiety threshold, in this case 10%, do not meet the minimum expected quality.

1.1 Services for the construction and deployment of the Open Health Platform **(9 points)**

In this section, the economic proposal for construction and development services will be assessed, with flat-rate prices, according to the value "Total amount offered by the "construction and development services" of the Annex "Economic offer model".

The following formula will be applied for the evaluation of the economic offer (Directive 1/2020, of 24 July, of the Directorate General for Public Procurement, on the application of formulas for the evaluation and scoring of economic and technical proposals):

$$P_v = \left[1 - \left(\frac{O_v - O_m}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P_{max}$$

Where:

Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the section.
Backbone: This is the best "Amount of the economic offer" offer received.
Ov: It is the offer of "Amount of the economic offer" to be evaluated.
IL: It is the maximum bid amount.
PV: Weighting Value

In this formula, the weighting value (PV) will be assigned a value of 3.

The formula, with a weighting value of 3, has been determined in accordance with Directive 1/2020 on the application of formulas for the assessment and scoring of economic and technical proposals. approved by the Directorate General of Public Procurement of the Generalitat de Catalunya. And a weighting value of 3 is chosen since it is required that the services covered by the contract be performed with a high level of quality, given the technical complexity.

The accuracy of the assigned scores will be limited to two (2) decimal places, applying symmetrical rounding.

1.2 Specialized support services for the use of recurring platform components **(1 point)**

In this section, the economic proposal for specialised support services for the use of recurring platform components will be assessed, with flat-rate prices, according to the value "Total amount offered by specialised support services for the use of recurring platform components" in the annex "Economic offer model".

The following formula will be applied for the evaluation of the economic offer (Directive 1/2020, of 24 July, of the Directorate General for Public Procurement, on the application of formulas for the evaluation and scoring of economic and technical proposals):

$$P_v = \left[1 - \left(\frac{O_v - O_m}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P_{max}$$

Where:

Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the section.
Backbone: This is the best "Amount of the economic offer" offer received.
Ov: It is the offer of "Amount of the economic offer" to be evaluated.
IL: It is the maximum bid amount.
PV: Weighting Value

In this formula, the weighting value (PV) will be assigned a value of 3.

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

The formula, with a weighting value of 3, has been determined in accordance with Directive 1/2020 on the application of formulas for the assessment and scoring of economic and technical proposals. approved by the Directorate General of Public Procurement of the Generalitat de Catalunya. And a weighting value of 3 is chosen since it is required that the services covered by the contract be performed with a high level of quality, given the technical complexity.

The accuracy of the assigned scores will be limited to two (2) decimal places, applying symmetrical rounding.

1.3 Specialised support services for the use of on-demand platform components **(2 points)**In this section, the economic proposal for specialised support services for the use of on-demand platform components will be assessed, with unit prices, according to the value "Total amount offered by specialised support services for the use of on-demand platform components" in the "Economic offer model" annex.

The score, for each type of evolutionary, is distributed as follows:

Evolutionary type	Punctuation
Very simple	0,1
Simple	0,3
Half	0,4
Complex	0,5
Very complex	0,7

The following formula will be applied for the evaluation of the economic offer (Directive 1/2020, of 24 July, of the Directorate General for Public Procurement, on the application of formulas for the evaluation and scoring of economic and technical proposals):

$$P_v = \left[1 - \left(\frac{O_v - O_m}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P_{max}$$

Where:

Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the section.
Backbone: This is the best "Amount of the economic offer" offer received.
Ov: It is the offer of "Amount of the economic offer" to be evaluated.
IL: It is the maximum bid amount.
PV: Weighting Value

In this formula, the weighting value (PV) will be assigned a value of 3.

The formula, with a weighting value of 3, has been determined in accordance with Directive 1/2020 on the application of formulas for the assessment and scoring of economic and technical proposals. approved by the Directorate General of Public Procurement of the Generalitat de Catalunya. And a weighting value of 3 is chosen since it is required that the services covered by the contract be performed with a high level of quality, given the technical complexity.

The accuracy of the assigned scores will be limited to two (2) decimal places, applying symmetrical rounding.

1.4 SaaS software provisioning services **(6 points)**

In this section, the economic proposal for SaaS software procurement services will be assessed, according to the value "Total amount offered by SaaS services" in the "Economic offer model" annex.

For the evaluation of the economic offer, the formula of Directive 1/2020, of 24 July, of the Directorate General for Public Procurement, on the application of evaluation and scoring formulas for the following economic and technical proposals, will be applied:

$$P_v = \left[1 - \left(\frac{O_v - O_m}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P_{max}$$

Where
Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the section.
Om: It is the best offer of "Amount of the economic offer" received.
Ov: It is the offer of "Amount of the economic offer" to be evaluated.
IL: It is the maximum bid amount.
PV: Weighting value.

In this formula, the weighting value (PV) will be assigned a value of 3.

A weighting value of 3 is chosen since this tender requires the service to be executed with a high level of quality, given the technical complexity.

The accuracy of the assigned scores will be limited to two (2) decimal places, applying symmetrical rounding.

2. Improvement of the profiles requested by the work team (up to 9 points)

In this section, proposals to expand the work team above the minimum required equipment will be assessed as solvency.

The offer with the highest score (will have the highest score, and the rest will be awarded the score proportionally.O_v)

Required Profile	Amount required	Improved quantity	Weight
Project Manager	1		1
Software Architects	2		1,5
Senior Developers	4		1,5
Experts en UX/UI	2		1
Consultants/Business Analysts specialising in health	2		1
Cloud Security Engineer	2		1
Experts in health interoperability	2		1
Experts in change management	2		1

The value of the offer will be obtained with the following formula:

$$O_v = \sum (Pes\ perfil\ x\ (Nombre\ de\ recursos\ millorats\ d'aquest\ perfil))$$

The score of the bids will be obtained from the values obtained, applying the following formula:

$$P_v = \left(\frac{O_v}{O_m}\right) \times P_{max}$$

Where

Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the evaluation criterion.
Om: It is the highest value obtained from the previous formula (Ov).
Ov: It is the value obtained from the previous formula of the offer to be valued.

The results of all calculations will be rounded to two decimal places. If the maximum bid value is zero, the score for all bids will be zero.

3. Extended warranty (up to 5 points)

Number of additional months of guarantee above the minimum required described in point 1.16 Guarantee of Annex 8 of the Conditions of Execution of the Service.

The offer with the most additional months of guarantee (will have the maximum score, and the rest will be awarded the score proportionallyO_v)

The score of the bids will be obtained from the values obtained, applying the following formula:

$$P_v = \left(\frac{O_v}{O_m}\right) \times P_{max}$$

Where

Pv: It is the score of the offer to be evaluated.
Pmax: It is the maximum score of the evaluation criterion.
Om: It is the highest value obtained from the previous formula (Ov).
Ov: It is the value obtained from the previous formula of the offer to be valued.

The results of all calculations will be rounded to two decimal places. If the maximum bid value is zero, the score for all bids will be zero.

4. ANS improvements (up to 5 points)

The increase in the SLAs with respect to the minimums specified in section 6 will be assessed. Service Level Agreements (SLAs) of the Technical Specifications.

- To increase the threshold from grade 3 to grade 4: 1 points in the event that the grade 3 threshold is equaled the value of the grade 4 threshold indicated in the Technical Specifications.
- To increase the threshold from grade 2 to grade 3: 0.5 points in the event that the grade 2 threshold is equal, the value of the grade 3 threshold indicated in the Technical Specifications.

The indicators that can be assessed for improvement are the following:

- Delay of commitments of the agreed calendar
- AM-EV-01 - Failure to comply with the conditions of execution
- AM-SG-03 - Correction of critical and/or high vulnerabilities in information systems
- Maximum critical incident resolution time
- Accumulated backlog in incident resolution
- AC-GOV-04 - Exceptions managed with an action plan in force
- GEQ002- Staff rotation

5. Degree of partnership between the bidder and the manufacturers involved (up to 5 points)

Given the nature of the solution to be developed, it is considered valuable that the winning company has a current degree of partnership with the openEHR International foundation:

- Maximum degree of partnership (Diamond): 5 points
- High level of partnership (Platinum): 4 points
- Medium level of partnership (Gold): 3 points

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

- Medium-basic level of partnership (Silver): 2 points
- Basic level of partnership (Bronze): 1 points
- No partnership level: 0 points

6. Technical certifications of the team assigned to the service (up to 7 points)

Given the nature of the solution to be developed, it is valued that the team members who are part of the project have certificates in the specific products and technologies involved in the provision of the service:

Project Manager
Accredit one of the following professional certifications on agile project management and/or product management:

- PMI-PMP (Project Management Professional)
- PMI-ACP (Agile Certified Practitioner)
- PMI-CAPM (Certified Associate in Project Management)
- Scrum.org-Professional Scrum Product Owner (PSPO)
- Scrum Alliance-Certified Scrum Product Owner (CSPO)
- SAFe Product Owner/Product Manager
- PRINCE2 Foundation
- PRINCE2 Practitioner

0.5 points are awarded for each certification submitted, up to a maximum of 1 points.

Expert en UX/UI
Accredit any of the following professional certifications:

- IDEO U Design Thinking Certificate
- IDEO U Human-Centered Design Certificate
- ICP-DES (ICAgile Certified Professional in Design Thinking)
- ICP-LED (ICAgile Certified Professional in Lean Design)
- EventStorming Master Class Certification (for Alberto Brandolini)
- Certified Design Thinking Professional
- Design Thinking Institute Design Thinking Master Certification
- Interaction Design Foundation (IDF) Design Thinking Professional Certification
- Interaction Design Foundation (IDF) UX Design Professional Certification
- Lean UX Association Certified Lean UX Practitioner
- Lean UX Association Lean UX Master Certification
- SAFe® Design Thinking Practitioner

0.5 points are awarded for each certification submitted, up to a maximum of 2 points.

Software Architects

Finançat per
Unió Europea Fons Europeu Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

Accredit any of the following professional certifications:

- AWS (Amazon Web Services):
  - AWS Certified Solutions Architect - Professional
  - AWS Certified Solutions Architect - Associate
  - AWS Certified DevOps Engineer - Professional
- Microsoft Azure:
  - Microsoft Certified: Azure Solutions Architect Expert
  - Microsoft Certified: Azure DevOps Engineer Expert
- Google Cloud Platform (GCP):
  - Google Cloud Professional Cloud Architect
  - Google Cloud Professional DevOps Engineer
- Linux Foundation:
  - Certified Kubernetes Administrator (CKA)
  - Certified Kubernetes Application Developer (CKAD)
- Docker:
  - Docker Certified Associate (DCA)
- Red Hat OpenShift:
  - Red Hat Certified OpenShift Application Developer
  - Red Hat Certified OpenShift Administrator
- MongoDB:
  - MongoDB Certified DBA Associate
  - MongoDB Certified Developer Associate
- PostgreSQL:
  - EDB EDBPostgres Advanced Server Associate or Professional Levels
  - EDB Community PostgreSQL Associate or Professional Levels

0.5 points are awarded for each certification submitted, up to a maximum of 4 points.

Qualifications accredited by the competent training centres, public and private, will be accepted. In any replacement of a professional in the team, the new profile proposed must have at least the same training and must be previously approved by the CTTI

7. Gender equality measures (up to 2 points)

The percentage of women assigned to the execution of the contract will be assessed.

2 points will be awarded if the percentage of women in the team assigned to the execution of the contract is equal to or greater than 33%. Otherwise 0 points.

8. Special conditions of execution:

Finançat per
Unió Europea
Fons Europeu
Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

It is established as a special condition of execution the guarantee, by the contractor company: that in the activities derived from the execution of the contract no sexist language or images are used, that they do not violate the equality of people with functional diversity of any kind, the rights of the child, or that they are not respectful of the care of the environment, sustainability and animal rights; the use of a communication that does not incur in any type of discrimination on the basis of sexual orientation, origin, age, beliefs or other personal or social conditions or circumstances; in their communications derived from the execution of the contract, to avoid the exaltation of violence and to promote cultural diversity, fleeing from negative stereotypes that perpetuate prejudices.

This condition has the character of an essential condition of the contract and its non-compliance may be subject to penalty as a very serious misconduct or cause for contractual termination.

9. Essential obligations of the contract:

The following special conditions of execution are established for socially responsible contracting.

The obligations assumed in terms of green labelling or digital labelling will be mandatory, in accordance with the established.

The proposed professional resources will be assigned to the execution of the contract. Any replacement of the equipment must be previously approved by the CTTI and notified in advance within a minimum of 10 working days.

10. Outsourcing:

Only the performance of specialised support tasks or consultancy tasks may be subcontracted to third parties to the manufacturers of the SaaS products that are implemented.

Given the high degree of specialisation required for the execution of the services covered by the contract, the main activity of the contract cannot be subcontracted because it is considered a critical task for the correct execution of the services and could negatively affect the quality of the execution of the services

The successful bidder must report, prior to accepting the service, the development of the subcontracting carried out, reporting the quality control metrics that have been carried out on the subcontracted companies, in order to demonstrate that as a company they have complied with quality control towards the subcontracted companies.

In accordance with the above,

PROPOSE

That the administrative contracting of the Open Health Platform begin, in charge of the budget for the year 2025 and following, with the characteristics specified in this report and the proposal of technical specifications that have also been prepared by this promoting unit.

Digitally signed in L'Hospitalet de Llobregat.

Jordi Gabaldà i Azofra
Director of the ICT Area of Health

Finançat per
Unió Europea
Fons Europeu
Next Generation
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

SPECIFIC TECHNICAL SPECIFICATIONS GOVERNING THE CONTRACTING OF SERVICES FOR THE CONSTRUCTION OF AN OPEN HEALTH PLATFORM - ARCHITECTURE COMPONENTS, APPLICATION MARKET AND PLATFORM SERVICES

File no.: CTTI/2025/113

1. OBJECT

The object of this tender is the contracting of the service/ for the construction and deployment of an "Open Health Platform - Architecture components, application market and platform services". It also includes specialized support services for the use of platform components, and SaaS software procurement services and licenses necessary for the productive operation of the platform.

The open health platform is conceptualized as a distributed and modular system that must support integrated and people-centered care. This system must allow the automation of routine tasks, facilitate personalized care and enable the systematic use of health data for the continuous improvement of health services. The platform is based on the paradigm of open systems, which is characterized by the use of open standards and interfaces that allow native interoperability between different components and applications.

From a technological perspective, the platform is structured in three main blocks: a transactional execution core that provides a service to health professionals and citizens, an application market that allows developer companies to offer their solutions, and a set of transversal services that guarantee the correct functioning of the entire system. This modular and standards-based architecture should facilitate the progressive incorporation of new functionalities and adaptation to the changing needs of the healthcare system.

The platform must respond to the current challenges of the health system, such as:

- The need for greater integration between levels of care.
- The increase in chronicity and complexity of patients.
- The demand for more accessible and personalized health services.
- The pressure to optimize health resources.
- The need to incorporate innovation in a systematic way.
- The demand for greater participation of citizens in their health.

At the same time, the platform must be prepared to face future challenges, incorporating capabilities such as:

- The integration of medical devices and *wearables*.
- Telemedicine and remote patient monitoring.
- Personalized and precision medicine.
- Collaboration between professionals and centres.
- Research and innovation in health.
- The democratization of data in line with data strategy.

This service is part of the broader context of the digital transformation of the National Health System and is financed by Next Generation EU funds. Its execution must follow the guidelines and standards established at Catalan, state and European level, guaranteeing interoperability and alignment with other digital transformation initiatives in the health field.

The main purpose of this contract is the provision of the construction service of an open health platform that implements:

1. Transactional execution core that includes:
   - Integration, deployment and maintenance of a standards-based healthcare process orchestration and management system (BPMN, CMMN, DMN) that can interoperate with clinical decision support systems, AI agents and form management environments.
   - Construction, deployment and maintenance of a clinical and demographic data access management system integrated with openEHR that manages access security and CRUD action logic while maintaining the integrity and consistency of openEHR information models (e.g. consistency of events and persistent elements, updating of composition statuses,...).
   - Integration with corporate components (MPI, PDS, terminology server, etc.).
2. App marketplace that includes:
   - Integration, adaptation and maintenance of a portal for developers with documentation and tools.
   - Deployment of a development environment (sandbox) for suppliers.
   - Design and deployment of an application homologation system.
   - Development, implementation and maintenance of a catalog of applications with commercial and administrative management.
   - Design and deployment of an application prescription system.
3. Transversal platform services:
   - Observability and monitoring.
   - Safety management.
   - Platform, operation and self-service engineering.
   - Capacity management and recovery.
   - Documentation
   - Quality of service

The platform must provide an open and flexible environment that allows:

- The automation of care processes.
- The secure integration of new applications and services.
- The systematic use of health data for continuous improvement.
- The prescription of digital applications in health.
- Innovation through an ecosystem of applications.

The system must be deployed in the CTTI's public cloud infrastructure, with high availability and compliance with the architecture, security and operation requirements defined in the annexes.

This specification is framed in the context of line 6 of investment 3 of component 11 of the *Digital Transformation Plan for Primary and Community Care* of the *Recovery, Transformation and Resilience Plan* to benefit from the NextGenerationEU Recovery Plan for Europe.

2. DESCRIPTION OF THE SERVICES TO BE PROVIDED

The services to be provided are as follows:

1. **Construction and development services:** Aimed at developing a robust and flexible platform that meets the established functional and technical requirements, integrating appropriately with the ecosystem of existing health systems.

   Construction of a new self-contained information system in the cloud (SaaS)

2. **Specialized support services for the use of platform components:** Aimed at ensuring the correct functioning of the platform, its constant evolution according to the needs of users and the agile resolution of incidents.
   - Operational management
   - Maintenance of information systems (corrective, perfective, preventive and technical adaptive)
   - Support service specialized in the use of transversal solutions and frameworks

3. **SaaS provisioning services required for the operation of the platform:** management and operation services of the information system technology platform. Focused on guaranteeing the availability, performance and security of the technological infrastructure that supports the platform.
   - Management and operation of the technology platform

SaaS provisioning services required by the operation of the platform

The mandatory conditions of execution for each of these services are described in the chapter Conditions of execution of this specification.

2.1. Construction & Development Services

The construction services will include the activities described in the quality model for the delivery of IT solutions to the Generalitat de Catalunya, described in the execution conditions, section of "Methodology, standards and deliverables":

- **Requirements Specification (Software and Platform) / Functional Analysis**. Transformation of customer needs and requirements into software requirements and platform requirements.
  This phase will be part of the boarding sprints and the successive "discovery tracks" that will be carried out in the continuous iterations, according to the Health Playbook model. They will be collected in the Roadmap and in the Backlog in the form of Epics and User Stories.
- **Design of the solution architecture (software and platform).** Transformation of the analysis of requirements into a solution design, with the fundamental organization of the system in its components and its relationships detected according to the requirements of the corporate technical data architecture and

the principles that will guide the design and its construction. It includes the design of the technological platform, its sizing and the proposal for the technical configuration of each of the components of the platform to guarantee the correct functioning of the information system according to the non-functional requirements demanded (performance, scalability, availability, etc.).

A first definition of architecture will be made in Sprint 0, which will be successively outlined by the discovery of the functional requirements and their characteristics.

- **Usability design.** Carrying out UX tasks to understand and define the consumer user profiles of the product to be built and their characteristics and needs.
  - Understand the needs of users: typification of these, identification of their needs, motivations for using the platform, factors that will build loyalty, expectations about how it works, channels and points of contact required
  - Design of the main journeys corresponding to the different types of users
  - Establish user satisfaction and user behaviour indicators aimed at identifying problems and prioritising actions based on data
  - Alignment with the business promoter: involving the Product Owner and the promoter.
- **Detailed design (software).** Transformation of the requirements, the analysis of the requirements and the design of the architecture into a detailed design that reflects the internal structure of each of the elements or components identified in the design of the solution architecture. It will be necessary to detail the design of the monitoring of the information system in coordination with the CTTI Control Centre, as well as the measurement of business indicators (telemetry) in accordance with the observed requirements indicated.

  The activities of the detailed design phase are modelled on the development of a product roadmap that serves as a planning and communication tool, to establish the priorities and the overview of the product to be built. Including:
  - Product vision: which describes the value it will bring to users and the business needs it will meet
  - Epics and most important features that will be included in each iteration or increment of the program. Also including detailing the design of the observability of the product following the recommendations of the CTTI, as well as the measurement of business indicators related to the value provided by the product
  - Priorities of epics and functionalities, as well as their dependencies.
  - Milestones, deliverables and Releases or putting into production new functionalities
  - Program Increments (PI) are fixed periods of time (typically 3 to 5 sprints) during which the team develops a portion of the product. Displays the POIs and the capabilities provided for each.
- **Construction and Unit Tests (software).** Development and unit testing of the solution following the established CTTI standards and regulations.

  This service also includes the construction carried out on platforms as a SaaS service, in which case the entire service is self-contained with its parameterization according to the technical and functional requirements of the business.

- **Integration** of the different elements of the system (software elements, hardware elements and other systems) to obtain a complete system that meets the design and expectations of customers.
- **Qualification tests**. Validation that the software can be installed in the final environment and that the embedded product meets the defined functional and non-functional requirements.
- **Installation of the software**. Installation of the software or support for its installation. It includes all the activities required in the event that it is necessary to package and/or virtualize the required functionalities of the information system to facilitate its deployment and/or operation.
- **Support for software acceptance**. Assistance to users in verifying that the software complies with the established requirements.
- **Change management**. Communication, training and support both at the level of users and subsequent support services, mainly the UAA. In the case of an information system classified as critical, the technical training must be extended specifically to the Control Centre.
- **Transition to maintenance and/or post-implementation**. Transfer of the code, documentation and knowledge to the supplier who will carry out the maintenance (even if it is the same one) and to other units of the CTTI service model.

This service also includes the contracting of the subscription of the SaaS services required for the operation of the platform, such as:

- Orchestration of traditional processes (BPM+Health) and AI agents
- Clinical Decision Support System (CDS)
- AI system for clinical models
- Billing system for cloud resources consumed by each application deployed in the marketplace
- IAM Identity Management Solution
- Documentation Manager (Public and Internal Wiki) – Confluence type
- Ticketing Manager - Jira

These activities are those that are currently carried out and are therefore considered as the basic set to be carried out. The CTTI may incorporate additional activities in the future depending on the evolution of the methodological standards available in the industry at any given time.

2.2. Specialized support servicesfor the use of platform components

Maintenance services include the following activities and tasks:

- **Operational management services for information systems**, managing the daily activity of the maintenance service, proactively managing all the necessary actions and ensuring those of the rest of the suppliers during the life cycle of the information system, thus guaranteeing its operability over time. The activities and their main tasks are described in the conditions of execution, section "Management of the information systems service". In addition, the following activities are part of this service:

- End-to-end service control and monitoring
- Managing the demand for new needs
- Activity backlog management
- Risk management
- Quality management
- Preparation of on-demand service offers
- Incorporation of third-party evolutionary developments

- **Support service specialized in the use of transversal solutions and frameworks,** required by the specificity and product orientation of information systems such as technological component, framework or transversal solution.
- **Evolutionary and adaptive functional maintenance services for information systems**, software modifications that are necessary to provide the new information system with new functionalities, adaptations to changes in current regulations or in order to avoid technological obsolescence.

  In the event that a third party has to develop major evolutions of new functionalities of an information system, the maintenance service will transfer the knowledge required to allow its development and will provide the necessary support both for its development and for its implementation and maintenance.

The classification of the different types of evolutionary is described in the execution conditions, section "Classification model for the development of evolutionary organisms".

2.3. Platform management and operation services

The management and operation services of the platform will include at least the activities required for the proper functioning of the new solution:

- Carry out end-to-end administration and operation of the platform
- Architecture management
- Product management and administration
- Container management and administration
- Proactive monitoring according to the guidelines of the CTTI (Control Center), and in accordance with the requirements of the level of criticality of the information system.
- Capacity management.
- Availability management, backup and recovery.
- Management of the security of the information system.

And in general all the activities of the management and operation to ensure compliance with the different conditions of execution to ensure the availability, security, capacity and continuity of the solution.

3. SOLUTION DESCRIPTION

3.1. Solution context

3.1.1. Administrative context

At the meeting of the Council of Ministers on 1 August 2022, the Agreement authorising the proposal for territorial distribution and the criteria for the distribution between the Autonomous Communities, the National Institute of Health Management (Ingesa) and the cities of Ceuta and Melilla of the budget appropriations for the investment "Digital transformation and modernisation of the Autonomous Communities", was approved. component 11 of the "Recovery, Transformation and Resilience Plan" for the years 2022 and 2023, with six strategic lines of investment, including line L6. "Health".

Strategic line 6 includes projects aimed at digital transformation in the field of health, which will have an impact on different areas such as improving interoperability, developing new digital services and promoting data analytics and the exploitation of information in the National Health System. Within the framework of the "Digital Health Strategy", approved by the CISNS on 2 December 2021, the "Digital Transformation Plan for Primary and Community Care" will be developed.

This Specific Technical Specification (PPTP) is framed in the context of line 6 of investment 3 of component 11 dedicated to the "Digital Transformation Plan for Primary and Community Care" of the "Recovery, Transformation and Resilience Plan" to benefit from the NextGenerationEU Recovery Plan for Europe.

Once the Preliminary Market Consultation (CPM) carried out between July and October 2024 on the construction of an open health platform has been completed, and having incorporated its final report into the file as established in article 115 of the LCSP, the tender for this contract will be carried out, which includes the conclusions and recommendations obtained during the CPM, especially with regard to the essential architectural components, the technological approach for the construction of the application market and the services necessary to operate the platform.

3.1.2. Digital Health Strategy of the National Health System

This tender is part of the projects framed in the Digital Health Strategy of the National Health Service (SNS) at the state level, focused on the objective of achieving Primary Care that is comprehensive, accessible, of quality, with the capacity to solve and longitudinal and that favors equity in health. This plan corresponds to objective number 4 of the Health Recovery, Transformation and Resilience Plan (PERTE) and is financed by RRF funds.

In order to execute the different projects framed in this "Plan for the digital transformation of Primary Care", the Autonomous Communities have been organized into working groups. In Catalonia and the Catalan Health Service, it participates, among others, in Working Group 4 - "Digital Health History". This group has different lines of work, one of them is the individual non-collaborative project with other communities of "Integrated Health: modeling and longitudinal management of care processes". The milestones defined in the framework of Working Group 4 are:

- Promote the normalization and common semantics of the EHR

Contain the set of standardised variables for the exchange of information between primary care data and the epidemiological surveillance system. This project focuses on responding to the paradigm shift of providing people-centred care. More specifically, this specification aims to address the challenge from a technological perspective, building the components of the architecture that must enable the deployment of integrated care services throughout the Catalan Health System. The initial milestones approved for this project are:

- Identification of a common framework for the representation of care processes.
- Deployment of the technological platform for the representation of healthcare processes.
- Modelling of the main care processes.

Projects financed with RRF funds are subject to the sustainability indicators defined for each working group. In the GT4 group, the following has been established:

- iGTT4: number of channels, platforms and tools integrated and/or interoperable with the developed system

3.1.3. The Digital Health Strategy of Catalonia 2024-2030

The Digital Health Strategy of Catalonia 2024-2030 is surely the most strategic initiative of the Catalan Health System for the coming years and aims to transform and modernise the Catalan health system through a radical change in the model of health information systems. This strategy seeks to enhance the quality of health services, as well as to promote collaboration and technological innovation to improve health care and the health of the citizens of Catalonia.

According to how it is defined in it, its main motivation is:

> Integrated and people-centred care, supported by an information systems model that systematically takes advantage of health data to build value-added services, which encourages innovation and is built on a collaboration model based on open standards

In order to respond to this main objective, a series of secondary objectives have been identified that are considered essential:

1. Construction and deployment of the Health Record of Catalonia.
2. Deployment of an information systems model based on the paradigm of open platforms.
3. Deployment of innovation through the systematic use of health data.

4. Establishment of a robust and participatory governance model for information systems by all the actors of the health ecosystem in Catalonia.

Thus, this tender is part of this strategic positioning and aims to achieve secondary objective number 2.

3.1.4. Interoperability

In terms of interoperability, the standards and procedures for coordination, standardisation and interoperability defined by the contracting organisation, approved by the Digital Health Commission of the National Health System (SNS) and compulsorily aligned with the promotion of interoperability throughout the National Health System, must be used, in accordance with the provisions of Law 16/2003. cohesion and quality of the National Health System (SNS). Special consideration will be given to the resources that are incorporated into the Reference Terminology Server of the National Health System (strSNS).

The services of the SNS will be based on an interoperability scheme that allows the integration of the different systems of the Autonomous Communities, using transmission standards adapted to the technological environment in force within the national health field and to the type of data sent, such as SOAP, HL7 V2. X, HL7 CDA, HL7 FHIR and DICOMWeb; allowing the exchange of different formats, such as JSON, XML or DICOM, between platforms and applications independently. These SNS services are the ones that enable the exchange of information for the Health Card User Database, the Cohesion Fund, and will allow the exchange of information on Electronic Prescription, Medical History and other services.

Therefore, the solutions covered by this contract must ensure compliance with the technical standards that are applicable in each case:

a) Interoperability at the transmission level (HL7 V2. X, HL7 CDA, HL7 FHIR, DICOMWeb...)

b) Semantic interoperability, adapted to the domain (SNOMED CT, CIE-10-ES, CIE-O-3.1, CIAP-2, ORPHA, LOINC, ATC, SERAM, SEMNIM, OMIM...)

According to the asset defined in this line of work of the Common Standardization and Semantics Document, for the use of open standards for the representation of clinical knowledge, which allow progress towards semantic interoperability (terminologies, standard vocabularies and information representation models such as ISO13606, HL7-FHIR or openEHR)

3.2. Functional requirements of the service

The main purpose of this contract is the provision of the construction, installation and maintenance service of an open health platform that implements:

1. **Transactional execution core:** Primary execution environment that serves clinical professionals, citizens, and healthcare managers. Requires 24x7 availability.
2. **Application market:** Environment that allows developer companies to offer their solutions and managers to certify them. Requires 12x5 availability, except for critical services.
3. **Transversal platform services:** Aimed at the management and operation of the transactional execution core and the application market. They require 24/7 availability.

The information system resulting from this tender is considered to have a Very High level of business criticality, and therefore the additional requirements indicated throughout the different execution conditions corresponding to its criticality will apply.

The characteristics of each of these elements are detailed below.

3.2.1. Transactional execution core

The contractor must develop the following components:

- Healthcare process orchestration and management systemIn accordance with the requirements of Annex 4 Orchestration and Processes, it must allow:
    - Process design, clinical decision modeling and case-based process management.
    - Import of designs based on BPM+Health
    - AI Agent Integration
    - Process instance management
    - Access control and security
    - Management of the modification of processes in their execution
    - Integration with third-party systems and data export for analytics
    - Ability to interoperate with CDS tools and, in general, other AI modules and agents
    - Production, pre-production, integration and sandbox environments
    - Process and rule repository management and synchronization environment
    - Integration with openEHR, FHIR and forms/low code tools
    - In accordance with the requirements of Annex 7 Access to clinical and demographic data, it must allow the management of the interfaces developed for access to clinical and demographic data that must be used by the applications to ensure:
    - Integration with openEHR repository.
    - Security and access management by mapping user security profiles with information model structures.
    - Implement the necessary logic to maintain the integrity and consistency

    of the openEHR information model (e.g. consistency of events and persistent elements, updating of composition states,...)
    - Management of access to other types of data (e.g. raw data from medical devices).
- Effective integration with current data spaces for analytical uses.
- Integration with existing components in accordance with the requirements of Annex 2 Architecture. As for transversal services, specifically:
    - Security Platform.
    - RDC – Clinical Data Repository
    - MPI – Patient Master
    - Index Server
    - Terminology server
    - Audit platform
    - Server Resources – Professionals and Organization
    - Distributed Traceability
    - Communications Gateway
    - Document Manager
    - API Gateway
    - Kafka Event Manager
    - Transversal Interoperability Platform
    - Health Data Space of Catalonia

3.2.2. App Market

The contractor must develop, in accordance with the requirements of Annex 3 Application Market:

- Application market portal, including the migration of the current Catsalut application portal to the application market professionals portal
- User and Access Management, including the migration of users from the current GSA (Security and Access Management) application and its administration.
- Documentation and user guides.
- Development environment for suppliers. Sandbox
- Application homologation system.
- Repository and sandbox.
- Catalogue of artefacts and components.
- Observability system.
- Incident management.
- Billing and pay-per-use system.
- Prescription and consumption of published applications.

3.2.3. Platform engineering

The contractor must define, dimension, document and put into operation the service model necessary for the management of the transactional execution core and the application market in accordance with the requirements of Annex 2 Architecture, including:

- Observability Services:
  - Centralized logging system.
  - Trace system
  - Performance monitoring.
  - Alerts and notifications.
  - Operational dashboards.
- FinOps services and expense control
- Platform Services Self-Service Portal
- Safety
  - Access control via the PDS
  - Data encryption
  - Audit of activities
  - User repository
- Disaster Recovery:
  - Containers and orchestration.
  - Automatic scaling.
  - Load balancing across different Availability Zones.
  - Configuration management.
  - Backup and recovery.
- Documentation
- Quality of service
- Capacity Management
- Platform operation

3.3. Non-functional requirements

The non-functional requirements that must be met by the different solutions to be developed in this contract are explained in detail below.

In general, the successful bidder must comply with all the requirements detailed in the different sections of the conditions for the execution of the tender according to the level of criticality of the information system, the following additional requirements being specific to this tender.

- Technological requirements
  - The technological platform on which the new system is to be built will be based on the architectural patterns defined in Annex 2 – Architecture of this tender.
  - The design of the technological platform (Pre-Production and Production environment) must consider:
    - the ability to scale both vertically and horizontally.

        - a portability that involves the minimum effort to deploy the information system on the different hyperscalars available in the CTTI catalogue.
        - that its components have a 24x7 manufacturer's support or equivalent of a business type.
        - that it has the ability to manage errors and limit conditions while the information system is in service, even if the error is derived from external causes such as network connectivity, hardware failures, etc.
    - The execution environments of the information systems will be:
        - Development, to be provided by the successful bidder according to the conditions of execution, section "Development environments".
        - Sandbox, to be provided by companies that want to deploy applications in the application market, and which will follow the architecture defined by the successful bidder for this environment.
        - Integration, to be provided by CTTI
        - Pre-production, to be provided by CTTI
        - Production, to be provided by CTTI

- Service Requirements
    - A 24x7 level of platform maintenance and management service
    - 99.95% availability of the information system
    - The level of service and support for users and attention to incidents is Continuous Extended
    - a service recovery time (RTO) target < 1h
    - a data loss rate target since last backup (RPO) of 0h
- Data requirements
    - It will be necessary to define the policy of auditing and historicization of information and to design the technological mechanism required for its implementation.
    - It will be necessary to have a first version of the business data entities identifying the master data and the relationship between them.
    - It will be necessary to define the integration model with corporate data solutions, such as the º of Health Data of Catalonia hereinafter ESDC, the Transversal Data Platform, and the Directory of Companies, Establishments and Registries.

  - Specifically, the ESDC will contain the information of the different operational systems and will be the basis for building data products for primary and secondary use in Health. The different applications will have at their disposal the services of the ESDC for the construction of complex data products and analytical models with the aim of maximizing efficiency in the exploitation of data knowledge.

    The information will be governed according to the procedures established by the CatSalut data governance office.

    In the construction of the applications, the data objects that represent the business components must be defined, so that their integration into the ESDC becomes natural and facilitates the consolidation and exploitation of the information.

- Usability and accessibility requirements
  - The information system must be available in the following languages: Catalan and Spanish, with multilingual support for the incorporation of translations into the interfaces.
  - The user interface must comply with current legal requirements (WCAG-AA)
  - The design of the presentation must be responsive, guaranteeing the compatibility of the information system with different devices and platforms.
  - The presentation layer must comply with the Health Design System (https://sisdisseny.salut.gencat.cat).
- Security requirements
  - The information security classification levels that the information system data resulting from this tender will have are [Very critical / Critical.
- Observability requirements
  - According to the needs of the information system, the level of observability and measurement required corresponds to that of the advanced package.
- Platform Operation Requirements
  - In accordance with the provisions of the conditions of execution, section 1.12.3.

In addition, the following services are part of the non-functional requirements:

3.3.1. Integration and testing

Once the main components have been developed, the following integration and testing tasks will need to be carried out:

- Integration tests between components:
  - Integration of the transactional core with platform services.
  - Integration of the application market with platform services.
  - Verification of interoperability between all components.
  - Validation of data flows between systems.
- Functional tests of the system:
  - Test of all the functionalities of the transactional core.
  - Process orchestration system test.
  - Validation of the application homologation system.
  - Performance and scalability tests.
  - Security and access control tests.
- Acceptance tests with end users:
  - Validation with healthcare professionals.
  - Validation with application providers.
  - Validation with system managers.
  - Collection and incorporation of feedback.

3.3.2. Deployment plan

The deployment plan should include the tasks to ensure an efficient transition to the new system:

- Deployment strategy:
  - Identification of phases and components to be deployed.
  - Dependencies between components.
  - Contingency and recovery plan.
  - Matrix of risks and mitigations.
- Detailed procedures:
  - Deployment protocols for each component.
  - Acceptance criteria for each phase.
  - Post-deployment verification procedures.
  - Communication protocols during deployment.
- Change management:
  - Communication plan for the ecosystem.
  - Training in the different user profiles.
  - Support during the transition.
  - Feedback and continuous improvement mechanisms.

3.3.3. Training and documentation

The following elements of training and documentation are required:

- Technical documentation:
  - Detailed system architecture.
  - API and service specifications.

  - Integration guides for developers.
  - Interoperability protocols.
  - Data models and dictionaries
- Training materials:
  - User guides for each profile
  - Materials for face-to-face training
  - Tutorial videos
  - Practical examples and use cases
  - FAQs and Common Troubleshooting
- Process documentation:
  - Operational protocols
  - Incident management procedures
  - System Administration Manuals
  - Monitoring and operation guides
  - Backup and recovery procedures

4. CONDITIONS OF EXECUTION OF THE SERVICE

4.1. Activities associated with the management of the information systems service

In accordance with section 1 of the document Annex 8-Conditions of Execution

4.2. Activities associated with the methodology, standards and deliverables

In accordance with section 1.2 of the document Annex 8-Execution Conditions, the project will follow an agile methodology based on 2-week sprints with the following main stages that correspond to the "New Provision" phase of section 5-Phases of this PPT:

Stage 1: Analysis and detailed design (2 months)

- Sprint 0: Kick-off and establishment of environments.
- Sprints 1-3: Definition of detailed architecture.
- Sprint 4: Validation of the design with stakeholders.

Main milestones:

- Detailed technical architecture document.
- Development plan and tests.
- Data model and APIs.
- Validated design of the main components.

Stage 2: Transactional core development (4 months)

- Sprints 5-8: Process orchestration and management system.
- Sprints 9-12: Clinical Data Management System.
- Sprints 9-12: Data analysis system.

Main milestones:

- Functional orchestration system.
- Integration with openEHR repository.
- Operational analysis engine.
- Documented and tested APIs.

Stage 3: Application Market Development (3 months)

- Sprints 13-15: Portal and documentation.
- Sprints 16-17: Homologation system.
- Sprint 18: Invoicing system.

Main milestones:

- Operational market portal.
- Validated homologation system.
- Functional test sandbox.
- Integrated billing system.

Stage 4: Integration and testing (2 months)

- Sprints 19-20: Integration tests.
- Sprints 21-22: Performance and safety tests.

Main milestones:

- Integration test report.
- Performance test report.
- Security audit report.

Stage 5: Deployment (1 month)

- Sprint 23: Pre-production deployment.
- Sprint 24: Deployment, production and support.

Main milestones:

- System deployed in production.
- Complete documentation submitted.
- Teams formed.
- Final acceptance of the system.

Each sprint will include:

- Planning.
- Development.
- Unit and integration tests.
- Demonstration with actors involved.
- Retrospective.

The coordination model will include:

- Daily follow-up meeting (15 min).
- Sprint planning (2h).
- Sprint demonstration (1h).
- Sprint retrospective (1h).
- Monthly follow-up meeting with the steering committee (2 hours).

4.3. Activities associated with quality certification

In accordance with section 1.3 of the document Annex 8 - Conditions of Execution.

4.4. Activities associated with carrying out tests with dedicated teams

In accordance with section 1.4 of the document Annex 8 - Conditions of Execution.

4.5. Activities associated with safety

In accordance with section 1.5 of the document Annex-Conditions of Execution.

4.6. Activities associated with Corporate Architecture

In accordance with section 1.6 of the document Annex 8 - Conditions of Execution published in.

In addition to the previous section, it will be necessary to consider what is defined in Annex 2 - Architecture as specific requirements of this tender.

4.7. Activities associated with observability and monitoring

In accordance with section 1.7 of the document Annex 8-Conditions of Execution.

4.8. Activities associated with the Control Center

In accordance with section 1.8 of the document Annex 8-Conditions of Execution.

4.9. Activities associated with the accessibility of websites and apps for mobile devices

In accordance with section 1.9 of the document Annex 8 - Conditions of Execution.

4.10. Activities associated with audits

In accordance with section 1.10 of the document Annex-Conditions of Execution.

Within the framework of projects financed by RRF funds, the successful bidder must collaborate and assist the contracting entity in the definition, preparation and closure of the assets described within the framework of the PTDAP Working Group. It must collaborate and facilitate the upload of assets to the SNS Asset Portal, following the applicable regulations for the preparation of the Autonomous Community and the SNS as a whole."

4.11. Teams and roles

In accordance with section 1.11 of the document Annex 8-Execution Conditions.the profiles required for this tender are:

- 1 Project Manager profile with 5 years of experience in equivalent activities
- 9 profiles of Software Architects with 5 years of experience in equivalent activities
- 12 profiles of Senior Developers with 5 years of experience in equivalent activities
- 4 profiles of UX/UI Experts with 3 years of experience in equivalent activities
- 5 profiles of Consultants/Business Analysts specialized in health with 5 years of experience in equivalent activities
- 4 Cloud Security Engineer profiles with 5 years of experience in equivalent activities
- 5 profiles of Experts in health interoperability with 3 years of experience in equivalent activities
- 4 profiles of Change Management Experts with 3 years of experience in equivalent activities
- 4 profiles of Experts in training with 3 years of experience in equivalent activities

It is necessary to provide for a stable core of the work team (called "core"), that is, there must be the minimum changes in resources assigned and whenever a replacement occurs, it will be necessary that the replacement person has at least the training and demonstrable experience that the person replaced. In any case, and always prior to the incorporation of the substitute person into the work team, the approval of the CTTI will be required.

This "core" team must be identified in the proposal and will be made up of:

- Project manager (1 person, 100% dedication):
    - Responsible for coordinating and directing the project.
    - Main point of contact for communications.
    - Risk and dependency management.
    - Coordination with all the actors involved.
    - Quality assurance of deliverables.
- Architect (2 people, 100% dedication):
    - Design of the overall architecture of the platform.
    - Definition of standards and development patterns.
    - Technical validation of components.
    - Ensuring architectural coherence.
    - Technical guidance from the development team.
- Senior Developers (4 people, 100% dedication):
    - Implementation of the core components of the platform.
    - Development of integration services.
    - Implementation of security mechanisms.
    - Development of APIs and web services.
    - Testing and resolution of incidents.
- Experts in UX/UI (2 people, 100% dedication):
    - Design of the user interface of the application market.
    - Definition of the user experience for the different profiles.
    - Creation of prototypes and wireframes.
    - Usability tests.
    - Style guides and visual components.
- Consultants / Business analysts specialising in health (2 people, 100% dedication):
    - Analysis of functional requirements.
    - Modelling of healthcare processes.
    - Specification of use cases.
    - Validation with end users.
    - Functional documentation.
- Cloud Security Engineer (2 people, 100% dedication):
    - Design of the security architecture.
    - Implementation of access controls.
    - Security audit.
    - Management of identities and authorizations.
    - Regulatory compliance (GDPR, ENS, etc.)

- Experts in health interoperability (2 people, 100% dedication):
  - Implementation of health standards (HL7, FHIR, etc.).
  - Integration with external systems.
  - Mapping of clinical terminologies.
  - Interoperability validation.
  - Technical documentation of integrations.
- Experts in change management (2 people, 100% dedication):
  - Design and execution of the change management plan
  - Analysis of the impact on the different groups
  - Development of communication strategies
  - Coordination with the different stakeholders
  - Monitoring and evaluation of adoption
- Training experts (2 people, 100% dedication):
  - Design of the training plan
  - Development of training materials
  - Execution of training sessions
  - Evaluation of the effectiveness of the training
  - Adaptation of content according to feedback

The training and experience requirements of the team members must meet the requirements indicated in the Table of Characteristics of the tender.

The presentation of each professional proposed by the bidder who must be part of the work team is required, indicating the name, profile assigned to the project, detailed curriculum highlighting the projects that may be similar or relevant for this service.

4.12. Activities associated with the CTTI's governance tools

In accordance with section 1.12 of the document Annex 8-Conditions of Execution.

4.13. Calendar and schedules

In accordance with section 1.13 of the document Annex 8-Conditions of Execution, the level of service required by this tender is continuous extended.

4.14. Physical location and necessary resources

In accordance with section 1.14 of the document Annex 8-Conditions of Execution.

The professionals who are part of the "core" team defined in section 4.11 Teams and roles will be located in the Catsalut facilities. In these spaces, the Generalitat will provide the furniture of the workplace and connection to the LAN network and Internet access, and the successful bidder will be responsible for the provision of the rest of the necessary equipment (desktop computers/laptops, tablets, mobile phone terminals, software, etc.) for the development of the tasks.

The rest of the professionals who are part of the service will be located for the most part in the facilities of the successful bidder, and all the costs associated with their jobs and their operation and maintenance will be borne by the successful bidder: office space, furniture, personal computers, technical and communications infrastructure, consumables and the like.

The facilities, buildings and dependencies used for the location of the service must comply at all times with all the requirements of construction, habitability, safety and ergonomics stipulated by the current regulations of the Generalitat and the State in their most demanding expression.

It should be borne in mind that, due to the needs of the service, any member of the contractor's team may be requested to travel to the premises determined by the CTTI, either during specific periods, for project coordination or resolution of critical incidents, or on a more continuous basis, for the operation of the service itself. In these spaces, the Generalitat will provide the furniture of the workplace and connection to the LAN network and Internet access, and the successful bidder will be responsible for the provision of the rest of the necessary equipment (desktop computers/laptops, tablets, mobile phone terminals, etc.) for the development of the tasks.

At any time during the execution of the contract, the CTTI reserves the right to request the successful bidder to provide the service in person at the facilities of the Generalitat de Catalunya. The successful bidder must adapt to these agreed changes within the agreed period.

Likewise, the successful bidder will assume, at no additional charge, any travel costs that, due to the need for the service, are required to be carried out within the Catalan territory.

The use of a Teams and Sharepoint environment will be required for communication and information sharing.

4.15. Guarantee

In accordance with section 1.16 of the document Annex 8-Conditions of Execution.

4.16. Model for quantifying maintenance services

In accordance with section 4.3 of the document Annex 8-Conditions of Execution.

.

5. PHASES OF SERVICE PROVISION

5.1. Phases of the service

Bidders must submit a Service Plan that takes into account the specific characteristics detailed below:

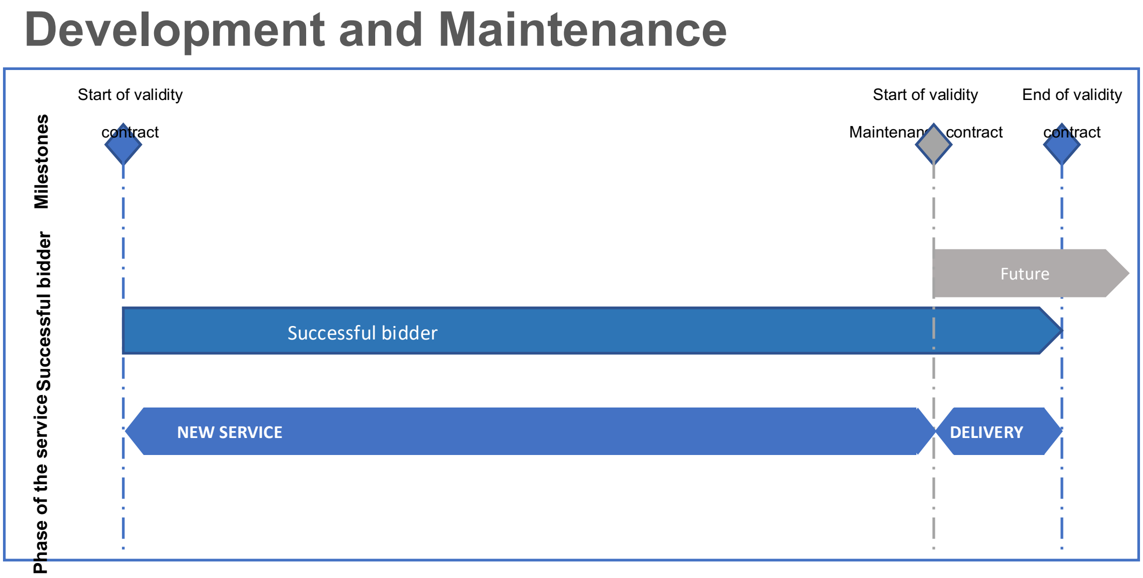


Figure 1: Phases of the Development and Subsequent Maintenance Service

4. **New Benefit**: Once the contract has been signed, the different actions for the formalisation of the development and maintenance projects will begin. At this time, the new provision of the service for the new successful bidders will begin. In the case of the construction of new information systems, the new service will consist of carrying out the corresponding developments and, once completed, the successful bidder will begin to carry out the tasks of Recurring Maintenance and Evolution. In the case of development on existing information systems, the new contractor will carry out the necessary actions to meet the proposed objectives and, once completed, will return the service to the current maintenance provider. In this phase, the activities of the object described will be developed. It also includes, among others, activities to monitor control and improve the service provided to the CTTI.

   From that moment on, the penalty model associated with compliance with the SLAs may be applied.

5. **Return/Delivery**: In the event that the object of the contract involves the transfer of the service to a new supplier, the successful bidder must develop the Return Plan that guarantees the continuity of the service, will continue to be responsible for the service and the SLAs defined in this contract will be applied. The successful bidder will contact the future supplier to begin the tasks of transferring the service, transferring knowledge and enabling the operation.

   This Return Plan will consist of at least one methodology, documentation for the transfer of knowledge (to ensure continuity of the service) and deadlines.

In the event that it is not possible to complete the return of a service before the end of this contract, the CTTI reserves the right to extend the return period of the service in question. In this case, the successful bidder must continue to provide the service until the correct return. It will last for a maximum of **4 months**.

In the case of Services for the development of large evolutions of new functionalities, there will be a Knowledge Capture phase, prior to those already indicated.

- **Knowledge Capture:** It is the period that goes from the entry into force of the contract, until being in a position to start the maintenance service. In this phase, the successful bidder must carry out different actions in order to acquire the necessary knowledge and start the different development projects as soon as possible. It will be extended for a maximum of **2 months** from the date of signing the contract.

5.2. Service Return Plan

The bidder will include a detailed Service Return Plan that describes the obligations and tasks that must be carried out by each of the parties in relation to the return, and that includes the terms and conditions under which it will be carried out.

In the event of termination or termination of the contract, the supplier will be obliged to return control of the services covered by the contract, having to carry out the return work in parallel with that of providing the service, at no additional cost to the CTTI.

The Repayment Plan must comply with at least the following principles and contents:

- The execution period will be between 2 and 4 months before the end of the contract, either due to having exhausted the term or due to early cancellation. The CTTI reserves the right to reduce the execution period as it deems necessary.
- It will include the methodology for the transfer of knowledge of the fundamental aspects of the operation and, at least, will describe:
  - Support for the new successful bidder, training and documentation on business and service procedures.
  - Access to the hardware, software, information, documentation and other material used by the successful bidder or the Government of Catalonia in the provision of the service.
  - Supervised practical training, in which the personnel designated by the CTTI carry out the work of each process or functionality supervised by the staff of the successful bidder.
- The successful bidder must offer the hardware and computer equipment, assigned exclusively to the services covered by the contract, to the CTTI or to third parties appointed by it. The valuation of the equipment will be carried out by a third party using the "market price" criterion or, if this is not possible, subtracting from its purchase price the cost of depreciation without residual value. The CTTI, or third parties appointed by it, may purchase all or part of the equipment.

- The CTTI may sign a user license contract on the successful bidder's systems that are necessary to ensure the continuity of the service.
- The successful bidder must offer all the assistance in the transfer to the CTTI, or to third parties appointed by it, of subcontracted services, guarantees or maintenance contracts existing up to the time of termination under the same terms agreed with the successful bidders.
- The successful bidder must offer a Plan to define the responsibilities and manage the resolution of problems between the new successful bidder, the CTTI and/or other successful bidders.
- During the service return period, the successful bidder must comply with the Service Level Agreements. The Return Plan must not cause any interruption in the service.
- The CTTI will not assume a significant dedication of its own resources or those of the Generalitat de Catalunya in the return activities.
- The successful bidder must guarantee that the updated documentation of the management of the service (knowledge database) to be transferred is available.
- Before the start of the return phase, the successful bidder must guarantee, through the High Importance information systems, that the basic documentation is up to date. Base documentation is considered to be that which is indicated as an essential degree of need in: https://qualitat.solucions.gencat.cat/guies/transicio/lliurables_transicio_devolucio/)

It is the responsibility of the successful bidder to lead and ensure the quality and transparency of the service return process.

The return of the service by the outgoing successful bidder includes two phases:

- **Refund service:** during the execution of the Return Plan, the outgoing successful bidder must ensure the continuity of the service with compliance with the SLAs established for each of the services and all the responsibilities for its correct execution, as specified in these specifications. The outgoing successful bidder is fully responsible for the service.
- **Return of the service**: while the outgoing successful bidder continues to provide the service under the conditions expressed in these specifications, it must ensure a correct transfer of the information and services to the new supplier that incorporates the products developed into the information systems for which it provides maintenance services.

6. SERVICE LEVEL AGREEMENTS (SANS)

The following tables detail the Service Level Agreements that apply to the contract:

1.1. List of ANS

6.1.1. ANS for Evolutionary Construction and Maintenance Service

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
	Delay of commitments of the agreed calendar	Amount of delay in agreed milestones.	GN	For each event	Number of breaches of agreed milestone planning	Monthly	10	5	1	0	1% monthly amount of evolutionary maintenance
	Evolutionary projects executed after the planned deadline	Percentage of evolutions executed outside the planned period with respect to the evaluated period	EV	Formula	Evolutionary executed after the deadline / Evolutionary executed in the period	Quarterly	15%	10%	5%	0%	1 % monthly amount of evolutionary maintenance
	Failure to comply with Quality Gates' performance	Non-compliance events	GN	For each event	Number of Quality Gates not completed with respect to those required by the milestones foreseen in the period	Monthly	2	1	0	0	1 % monthly amount of evolutionary maintenance
AM-EV-01	Failure to comply with the conditions of execution	Non-compliance events	EV	For each event	Number of breaches of the conditions of execution with respect to the activities carried out in the period	Quarterly	2	1	0	0	1 % monthly amount of the service

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
AM-GN-01	Release plan	The successful bidder will submit a version change plan, in accordance with the established version policy	GN	Formula	If the release plan has NOT been delivered within the agreed deadline = 1If the release plan has been delivered within the agreed deadline = 0	Quarterly	1	0	0	0	1 % monthly amount of evolutionary maintenance
AM-SG-03	Correction of critical and/or high vulnerabilities in information systems	Number of critical and/or high vulnerabilities that have not been patched within 2 months of their identification or that containment measures have not been applied to these vulnerabilities	MP	For each event	Number of critical and/or high vulnerabilities that have not been patched within 2 months of their identification or that containment measures have not been applied to these vulnerabilities	Quarterly	2	1	0	0	3% monthly amount of corrective maintenance

6.1.2. ANS Maintenance Service

Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Degree				Maximum penalty
							Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	
	Availability of the information system	Availability of the information system to be used by users during its service hours.	GP	Formula	Yes (Service Time / Total Time < Availability Threshold According to Service Level Indicated) = 1Otherwise = 0	Monthly	1	1	0	0	2 % monthly amount of platform maintenance
	Maximum time of attention or response to request or query	Percentage of tasks attended in time in the month to be measured	SU	Formula	Number of tasks attended in time in the month to be measured / Number of total tasks attended in the month* - High Priority < 2h - Medium Priority < 4h - Low Priority < 16h*(Associated with the stipulated service level)	Monthly	65%	75%	85%	90%	1 % monthly user support amount
	Maximum time for attention or response to requests or queries, of a critical nature	Non-compliance events	SU	Event	For each event, number of hours to respond with respect to the stipulated value. - Critical Priority < 1h*(Associated with the stipulated service level)	Monthly	3	2	1	0	1 % monthly user support amount
	Maximum time for resolving a request or query	Percentage of requests or queries resolved in the month to be measured	SU	Formula	Number of requests or queries resolved in time in the month to be measured / Number of total requests or queries resolved in the month to be measured* - High Priority < 16h - Medium Priority < 48h - Low Priority <	Monthly	65%	75%	85%	90%	1 % monthly user support amount

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
	Maximum time for resolving critical request or query	Non-compliance events	SU	Event	For each event, number of hours to respond with respect to the stipulated value. - Critical Priority < 8 h*(Associated with the stipulated service level)	Monthly	20	15	10	8	1 % monthly user support amount
	Maximum incident resolution time	Percentage of incidents resolved in the month to be measured	MC	Formula	Number of incidents resolved in time in the month to be measured / Number of total incidents resolved in the month to be measured* - High Priority < 12h - Medium Priority < 40h - Low Priority < 80h*(Associated with the stipulated level of service).	monthly	65%	75%	80%	90%	1% monthly user support amount
	Maximum critical incident resolution time	Non-compliance events	MC	Event	For each event, number of hours to respond with respect to the stipulated value. - Critical Priority < 4h*(Associated with the stipulated service level)	monthly	10	8	6	4	1% monthly user support amount

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
	Maximum time for resolving requests for functional support or user management	Average time to resolve user requests	SU	Formula	Number of tasks solved in time in the month to be measured / Number of total tasks solved in the month to be measured * o Critical Priority < 8 a.m. o High Priority < 8h o Medium Priority < 4 p.m. o Low Priority < 32 hours *(Associated with the stipulated service level) **Includes tickets managed in Remedy or other provider tool	Monthly	65%	75%	80%	100%	1 % monthly user support amount
	Accumulated backlog in incident resolution	Percentage of unresolved incidents that have exceeded the measured period	MC	Formula	(Unresolved incidents at the end of the period)/(Cumulative incidents)	Monthly	15%	13%	10%	5%	2 % monthly amount of corrective maintenance
	Backlog accumulated in the resolution of requests or queries	Percentage of unresolved requests or queries that have exceeded the measured period	SU	Formula	(unresolved requests at the end of the period)/(cumulative requests)	Monthly	15%	13%	10%	5%	1 % monthly user support amount
	Corrective measures executed for the reopening of incidents	Number of corrective measures executed for the reopening of incidents in the measured period	MC	Formula	Number of reopened patches = volume of reopened issues (all reopenings are considered, regardless of the supplier's responsibility).	Monthly	9	3	1	0	1 % monthly amount of corrective maintenance

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
AM-GN-02	Capacity Plan	The successful bidder will present a six-month capacity plan, according to the established policy	GP	Event	If the capacity plan has NOT been delivered within the agreed period = 1If the capacity plan has been delivered within the agreed period = 0	Semiannual	1	0	0	0	1 % monthly amount of platform maintenance
AM-EV-02	Failure to comply with the agreed date for the submission of offers for new developments	Percentage of non-compliance with the agreed date for the submission of bids (both those delivered in the evaluated period and those pending delivery)	EV	Formula	Number of bids after the deadline (both delivered and pending) / Total number of bids	Quarterly	40%	30%	20%	10%	1% monthly amount of evolutionary maintenance
AC-GOV-04	Exceptions managed with an action plan in force	Percentage of architecture and security exceptions managed with a current action plan	GN	Formula	Number of security and architecture exceptions¹ with the action schedule to mitigate the current exception / Total number of security and architecture exceptions¹These are the architecture and security exceptions managed by the successful bidder	Monthly	50%	75%	100%	100%	1% monthly amount of recurring maintenance
	Obsolescence management	The scope of the tender has obsolescence correctly managed	GP	Formula	Number of apps with unmanaged deprecations / Total number of assigned apps that don't have a management exemption exception	Quarterly	75%	80%	90%	100%	1% monthly amount of platform maintenance

							Degree				
Code	Name	Description	Service	Type	Obtaining formula/tool	Periodicity	Grade 1 threshold	Grade 2 threshold	Threshold Grade 3	Grade 4 threshold	Maximum penalty
MON-07	Running backup recovery tests	Backup recovery tests carried out compared to the planned one to validate the effectiveness of the recovery process	GP	Event	Number of recovery tests carried out compared to those planned.	Monthly	75%	80%	90%	100%	1% monthly amount of platform maintenance
MON-08	Running disaster recovery tests	Running an annual retake test	GP	Event	If the test has NOT been carried out within the agreed period = 1 (*)If the test has been carried out within the agreed period = 0 (*) unless it is for reasons beyond the control of the	Annual (at least once during the term of the contact)	1	1	0	0	1% monthly amount of platform maintenance
	Compliance with platform performance levels for REST API calls	Response time of REST API calls for registration, modification, deregistration or query of unique records, and query of recordsets by lists in any service			Percentile of response time required in ANNEX II. DOCUMENT OF CHARACTERISTICS OF THE TECHNOLOGICAL ARCHITECTURE of the REST APIs for registration, deletion, modification, consultation of unique records, and consultation of recordsets by lists in any service	Monthly	75%	80%	85%	95%	1% monthly contract amount

6.1.3. YEARS of Contract

						Degree				
Code	Name	Description	Service	Obtaining formula/tool	Periodicity	Grade 1	Grade 2	Threshold	Grade 4	Penalty
CT-GN-01	Invalid invoices made by the successful bidder	Percentage of awardee invoices that do not meet the standard, are incorrectly issued or have an error	GN	Number of invalid invoices made by the successful bidder / Total number of invoices made by the successful bidder	Annual	30%	20%	10%	0%	0.5% overall contract turnover
CT-GN-02	Proactivity	Number of improvement initiatives implemented and approved	GN	Number of improvement initiatives submitted with associated improvement indicators	Quarterly	0	2	4	10	0.5% overall batch turnover
GEQ002	Staff turnover	Percentage of staff turnovers assigned to the service.	GN	Percentage of staff turnovers assigned to the service: $\frac{\#rotacions}{\#persones\_equip\_contracte} x100$ Where: *#rotacions*: number of personnel changes in the work team assigned to the service during the period. *#persones_equip_contracte*: Number of people assigned in the contract.	Quarterly	20%	15%	10%	5%	The value equivalent to 1% of the result of dividing the contract award amount by its duration in months, to be reflected in the next invoice

7. RELATIONSHIP AND GOVERNANCE MODEL

7.1. Obligations of the CTTI

It is the responsibility of the CTTI to provide the successful bidder's team with all the information it deems necessary for the development of the project.

The issues raised by the successful bidder will be resolved by the CTTI within the period of time agreed at the beginning of the project.

7.2. Obligations of the successful bidder

At the time of providing the service, the successful bidder must provide the IT infrastructures, development spaces, development licenses and any other component or technical means necessary to carry out the work at no additional cost to the CTTI.

7.3. Governance structure

The project will be governed by the following committees:

- **Steering Committee**: Monthly meeting
  - CTTI Project Manager
  - Awarded project manager
  - Key actors
  - Strategic monitoring and risks
- **Operating Committee**: Biweekly meeting
  - CTTI Project Manager
  - Awarded project manager
  - Key technical team
  - Technical monitoring and blockage resolution

The following monitoring reports will be provided periodically:

- **Sprint Report**: Biweekly
  - Completed tasks
  - Deviations and risks
  - Code quality metrics
  - Next sprint planning
- **Monthly Report**:
  - Project KPIs
  - Risks and mitigations
  - Updated planning
  - Budget consumption

7.4. Matrix RACI of responsibilities

Activity	CTTI	Successful bidder	Actors

Project Management			
Strategic management	In	And	C
Operational management	C	R/A	And
Risk management	In	R	C
Development			
Architecture	In	R	C
Development	And	R/A	C
Quality control	In	R	And
Deployment			
Pre-production	In	R	And
Production	In	R	And
Execution			
Techniques	C	R/A	And
Functional	In	R	R
Acceptance	R/A	C	R
Formation			
Materials	In	R	C
Execution	C	R/A	R

Legend:

- A: Responsible
- A: Approves
- C: Consulted
- I: Informed

SPECIFIC TECHNICAL SPECIFICATIONS FOR THE CONSTRUCTION OF AN OPEN PLATFORM IN HEALTH - ARCHITECTURE COMPONENTS, APPLICATION MARKET AND PLATFORM SERVICES

ANNEX 2: ARCHITECTURE

CTTI/2025/113

Barcelona, February 2025

Unió Europea
Fons Europeu
Next Generation

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

Pla de Recuperació, Transformació i Resiliència

Next Generation Catalunya

Generalitat de Catalunya

Version history and contributions

Description of the review	Author	Date	Version
Initial draft		20/01/25	0.1

Index

1 INTRODUCTION

This annex is dedicated to defining the technological architecture on which the services and functionalities to which the elements included in the proposal must respond must be executed. The objective is to implement an open and flexible platform, which guarantees scalability and performance, ensuring quality and reliability, facilitating governance and control, optimizing the total cost of ownership, enabling innovation and agility and guaranteeing the security and privacy of the data processed by the platform.

With the context given for the open Health platform, three completely differentiated divisions of architecture are envisaged.

The first would be the one that would contemplate the execution of all those components that would make up the work environment of clinical professionals, the services to other provider entities and health institutions and the services to be provided to the beneficiary citizen of the national health system. We will call this part the Core of the platform.

The second would be the one that would contemplate the necessary components for health software development companies, and health service providers, to be able to offer and consume the digital products exhibited therein. We will call this part the Platform App Market.

The third would be the one that would contemplate the necessary components of the current architecture of Health and CTTI that would have to be used on a mandatory basis in the previous divisions, given that they cover business and technological aspects that are considered enablers for the open platform and the application market

In the following chapters we delve into their differences and peculiar characteristics of each one, and a preliminary design of their main components. This design must be considered a framework on which to develop an architecture that incorporates the elements required to respond to the functionalities presented in this technical specification.

2 Design principles and decisions

The architecture of the open platform will be subject to the same principles and characteristics already published for the new applications of the Information Systems Master Plan (PDSIS). Below are the links to the corresponding documents

2.1 Reference architecture

In the systems master plan we have established the following manifesto for the reference architecture that is mandatory in all the development of new systems such as those that concern us in this tender: https://salutweb.gencat.cat/ca/ambits-actuacio/linies/tic/solucions-siscat/model-adhesio/arquitectura-tecnologica/manifest-referencia-iniciatives/index.html

Specifically for this tender, the following additional restrictions would apply:

1) The necessary infrastructure will be deployed in the AWS cloud under the CTTI NET0 network security framework
2) Notwithstanding the previous point, the architecture must be designed to be able to be deployed in multicloud environments. This point is especially relevant in the choice of SaaS components, which the market already offers solutions that allow their multicloud deployment, such as, for example, MongoDB Atlas. Taking advantage of these solutions, in the future a multicloud deployment would only be a matter of properly configuring the connection to these systems, without duplicating the infrastructure or requiring expert knowledge of the operation of these solutions for the team that will operate the platform.
3) The main Shell component of the micro-fronts will be developed with the Single-Spa framework: https://single-spa.js.org

2.2 Principles

The principles that govern the architecture of PDSIS solutions can be found at https://hdl.handle.net/11351/10576

2.3 Characteristics of the architecture

The characteristics of the architecture of the PDSIS solutions can be found in the reference https://salutweb.gencat.cat/web/.content/_ambits-actuacio/Linies-dactuacio/tic/pdsis/caracteristiques-arquitectura-tecnoloogica-pdsis.pdf

3 DESCRIPTION OF THE COMPONENTS REQUIRED AS THE OBJECT OF THE CONTRACT

As reflected in the introduction to this annex, the new open platform consists of three different contexts. This chapter details those that are the object of construction within the contract.

The first contemplates the transactional execution core of the platform, where the solutions admitted to operate within it will be executed, and which will provide service to all the clinical care needs of the different users of the platform, whether citizens, healthcare professionals, health service managers, health service providers, solution development companies, and operators of the same. This context must enjoy the highest levels of availability, reliability and security, being a 24/7 service in all its components.

The second context is what we call the "Application Market", which includes everything necessary for solution development companies to be able to offer their solutions on the platform, and for the managers of the open platform to certify with the highest levels of quality, security and information protection, that a solution is suitable for operating in the transactional context. This context must enjoy high levels of availability, reliability and security, being a 12x5 service in most of its services, except for those that should allow the resolution of incidents on the transactional platform, which should also be 24x7.

The third context is what we call transversal services of the platform, which will be used by both the execution core and the application market. They contemplate subsystems such as observability, finops, security, etc.

3.1 Core of the open platform

The core of the platform's transactional execution follows the paradigm of composable architectures, in which the solutions corresponding to different functional domains collaborate in offering a solution composed of the combination of them, under defined processes. Below is the reference architecture for one of these components:

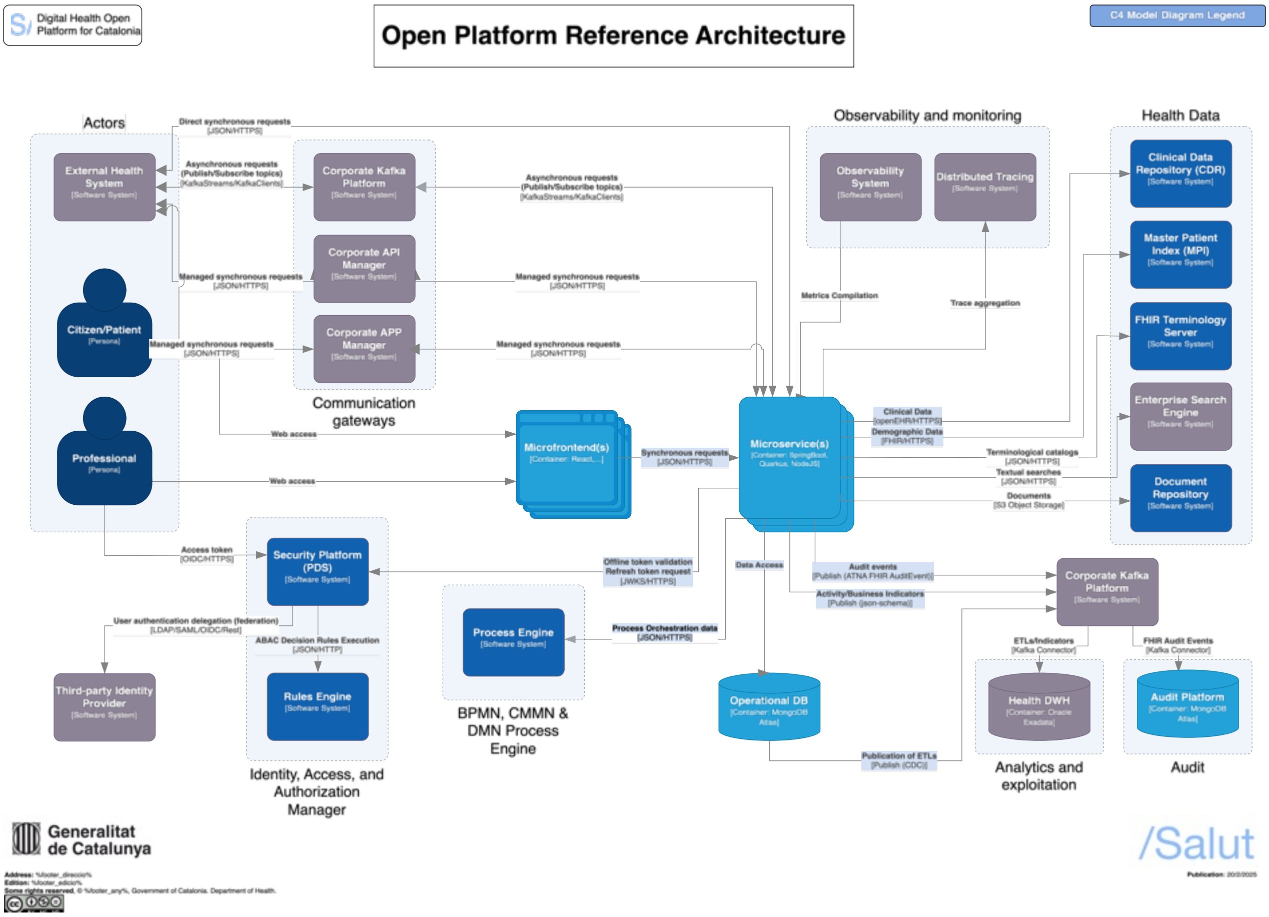

Digital Health Open Platform for Catalonia
Open Platform Reference Architecture
C4 Model Diagram Legend
Actors
External Health System [Software System]
Citizen/Patient [Persona]
Professional [Persona]
Direct synchronous requests [JSON/HTTPS]
Asynchronous requests (Publish/Subscribe topics) [KafkaStreams/KafkaClients]
Managed synchronous requests [JSON/HTTPS]
Corporate Kafka Platform [Software System]
Corporate API Manager [Software System]
Corporate APP Manager [Software System]
Communication gateways
Web access
Microfrontend(s) [Container: React,...]
Synchronous requests [JSON/HTTPS]
Microservice(s) [Container: SpringBoot, Quarkus, NodeJS]
Observability and monitoring
Observability System [Software System]
Distributed Tracing [Software System]
Metrics Compilation
Trace aggregation
Health Data
Clinical Data Repository (CDR) [Software System]
Master Patient Index (MPI) [Software System]
FHIR Terminology Server [Software System]
Enterprise Search Engine [Software System]
Document Repository [Software System]
Clinical Data [openEHR/HTTPS]
Demographic Data [FHIR/HTTPS]
Terminological catalogs [JSON/HTTPS]
Textual searches [JSON/HTTPS]
Documents [S3 Object Storage]
Access token [OIDC/HTTPS]
Security Platform (PDS) [Software System]
Offline token validation Refresh token request [JWKS/HTTPS]
User authentication delegation (federation) [LDAP/SAML/OIDC/Rest]
ABAC Decision Rules Execution [JSON/HTTP]
Third-party Identity Provider [Software System]
Rules Engine [Software System]
Identity, Access, and Authorization Manager
Process Engine [Software System]
Process Orchestration data [JSON/HTTPS]
BPMN, CMMN & DMN Process Engine
Data Access
Operational DB [Container: MongoDB Atlas]
Audit events [Publish (ATNA FHIR AuditEvent)]
Activity/Business Indicators [Publish (json-schema)]
Corporate Kafka Platform [Software System]
ETLs/Indicators [Kafka Connector]
FHIR Audit Events [Kafka Connector]
Publication of ETLs [Publish (CDC)]
Health DWH [Container: Oracle Exadata]
Analytics and exploitation
Audit Platform [Container: MongoDB Atlas]
Audit
Generalitat de Catalunya
/Salut
Address: %footer_direccio%
Edition: %footer_edicio%
Some rights reserved. © %footer_any%, Government of Catalonia. Department of Health.
Publication: 20/2/2025

Figure 1. Health Reference Architecture

As mentioned in the previous paragraph, all these components correspond to different domains and are combined to give a joint vision based on defined processes with specific characteristics for the field of health.

These systems that correspond to functional domains run at the core of the open platform, which comprises the following characteristics:

3.1.1 Orchestration and process management

This solution for orchestrating or choreographing business components is the one that provides the most innovative part of the open platform, and which does not have a clear reference in the health sector. The process engine will have to support different notations that will be applicable such as Business Process Modeling Notation (BPMN), Case Management Model and Notation (CMMN) and Decision Model and Notation (DMN). The provision for the use of the three notations derives from the high degree of flexibility required by any healthcare professional in the application of these processes to adapt them to the specific clinical case, to which must be added the need for integrity and adaptation to the regulations of processes and decision-making, and that allow the use of semantics and clinical ontologies, bringing design closer to health professionals

Consequently, despite the fact that processes are defined at a global or local level, it will be necessary for the platform to incorporate feedback mechanisms for the continuous improvement of the defined processes, and even to evaluate trends in the use of the processes to detect whether a process defined by a healthcare professional enjoys more acceptance by the community than that defined by corporate process modelers.

The process tool must govern both the presentation of each module through a clinical workstation (ETC), administrative, or patient-directed, as well as the API contracts that each application may offer, as well as the processing of events that may be generated in other approved applications.

In design time, it will be necessary to define:

- The available spaces of the ETC and how they are filled with the microfrontends of each module, establishing compatibility criteria between modules;

- The APIs to consume and how results are mapped to each other;

- The events available and how to react to each of them.

The process designer should have:

- A map of possible candidates for the next step in the process;

•Provide a visual tool to map data between APIs and compose processes;

- Allow on-the-fly composition of process variants at runtime;

- Record the execution of processes to analyze trends in use and provide feedback on which process is dominant in that clinical episode or treatment;

- To have the freedom that at some point in the chain a process can be marked as non-modifiable. It should be possible to prevent immutable processes from being cloned and creating variants.

The tool must allow the testing and validation of processes before they are uploaded to the production platform, including their presentation, the correct mapping of data between APIs and the appropriate reaction to events generated by other modules of the process. Likewise, the information on the design, use and execution of the processes must be accessible for analysis.

Once the process has been deployed, the tool will execute the automation of the process when it is invoked by one of the applications present in the system or by the kernel itself in response to a given event.

The same tool will be in charge of monitoring and analyzing the execution of the process, through a Process Mining procedure that, by analyzing the logs, allows optimizing the processes, detecting inefficiencies, bottlenecks, indefinite blockages and processes terminated unexpectedly.

3.1.2 Clinical data management

Components that make use of clinical data will have to adapt to the semantic definition structures of the clinical data repository (openEHR). The platform must have tools that allow the security of access to clinical data to be managed in accordance with profiles defined in the Security Platform.

For cases of "raw data" from medical devices, persistence and access management models must be proposed in accordance with the patient's indications.

3.1.3 Analysis of clinical data

Another feature of the open platform core is the possibility of having a private execution environment, especially for secondary use needs (e.g. research), where certain applications can operate on the platform but are only executable by certain previously determined groups. All information generated by these restricted applications must be restricted in the same way and not be available to users in general.

This environment must have access to clinical data and information on the design and execution of processes in order to investigate their use and effectiveness.

3.1.4 Architecture resilience

The architecture of the open platform will have to provide the highest levels of resilience due to the criticality of the information it handles and the reach of the population it serves. In this sense, the architecture will be prepared for a multi-vendor deployment of the Cloud, where even the fall of an entire provider does not cause a disruption in the service provided to the citizens of Catalonia and the health professionals who will use the platform.

However, in this tender it is not required to reach this level of multicloud operation, but it is required that the platform works in at least two AWS regions, taking into account latency and availability criteria of the AWS and SaaS products that will make up the platform. Within regions, multi-zone high availability is required across all platform core components.

3.1.5 Service integration

An important part of the open platform is precisely the ability to integrate the services and applications that are deployed on it. In this sense, we will have three corporate integration platforms and one of the platform's own for file sharing.

3.1.5.1 Corporate API Manager

The platform will connect the applications and plugins that require the REST/HTTPS protocol through the corporate API Manager provided by the CTTI. In this way, the following advantages can be achieved:

- Centralize the control of communications
- Control security
- Manage service quotas
- Provide a catalog of available services and their versioning

3.1.5.2 Transversal Platform for Interoperability IPaaS

The transversal Interoperability platform will be used to facilitate the transformation and exchange of messages between legacy health systems and modernized applications within the platform.

3.1.5.3 Transversal Events Platform

The cross-functional event platform based on Kafka, provides common event messaging and CDC services between systems. The platform is currently widely used in different use cases.

3.1.5.4 Health file sharing platform

For those information systems with which a file sharing is carried out, it will be necessary to enable an open sharing space that assumes the capabilities of the current legacy File Transfer Management application. Consumer users of this service will be part of the identity and access management system of the open platform.

3.1.6 Clinical decision support system

This system focuses on the implementation of clinical decision rules (CDS, Clinical Decision Support). These rules help medical professionals make decisions based on patient data and predefined clinical algorithms.

It will be composed of the following pieces:

- Rules Engine: This plug-in works with a rules engine that allows you to define complex medical rules, in natural language, which are applied based on clinical data in real time.

This engine can use standard formats for the rules and also Generative AI models clinically pre-trained with training accelerator tools.

- Integration with the Clinical Database: Rules can be executed in real-time on top of the existing clinical database, evaluating relevant information such as laboratory results, treatment history, or other data to support decision-making.
- Interaction with other plug-ins: Rules can influence or be influenced by other plug-ins. For example, a clinical rule plug-in can send an alert to a widget that a doctor consults, or it can automatically trigger a clinical process.

3.2 App Market

The application market will be a solution that will allow any developer company to integrate its solutions within the open platform. Therefore, it is a different target audience from that of the transactional open platform and will require different security elements and a high component of governance and homologation of the proposed solutions. In this sense, its main components could be listed as:

- Application market portal, basically dedicated to developer profiles and managers of manufacturing companies;
- Space with all the documentation, tools and guides necessary for the use of the application market;
- Portal administration application;
- Model template of development environment for suppliers;
- Homologation process of applications and their documentation. This would cover the minimums for composing processes based on common interfaces of:
    - Which region of the Workstation the microfrontend goes to;
    - Observability;
    - Pay-as-you-go billing;
    - Documentation of APIs and events that are generated;
    - Normalization of data between API fields;
- Repository and deployment environment of the applications once approved (Sandbox / Catalog);
- Beta environment of the open transactional platform where companies can test their products before going into production, or to test their compatibility with new versions of the platform;
- User registration;
- Catalogue of artefacts and components of modular architecture;
- Observability of the own components for the developing companies;
- Management of the incidental of the company's own components;
- Billing Management Environment / Pay-As-You-Go;
- Others.

These applications will be made available to the public, which identifies another type of user with a need to search for and access applications that may be free to use and/or that require a professional prescription.

The use of the applications must be recorded and managed in such a way that a consumption and cost management model can be implemented.

Below, from the point of view of development, a diagram is shown with a preliminary proposal of what could be the portal of the application market (Note: the products mentioned in the diagrams are expressed as an example, not as a choice already made):

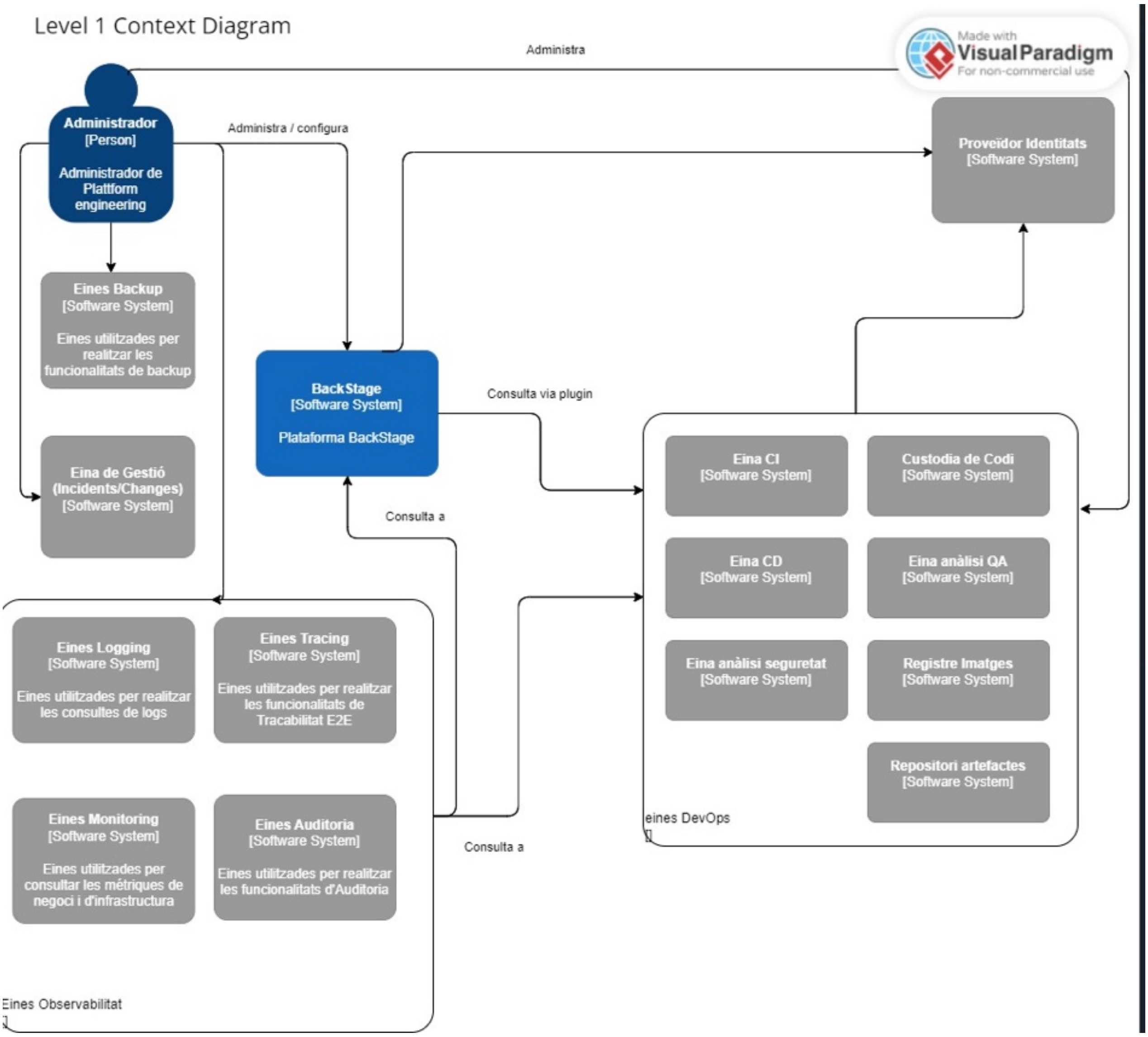


Figure 2. Preliminary Application Market Proposal Diagram

Application repository:

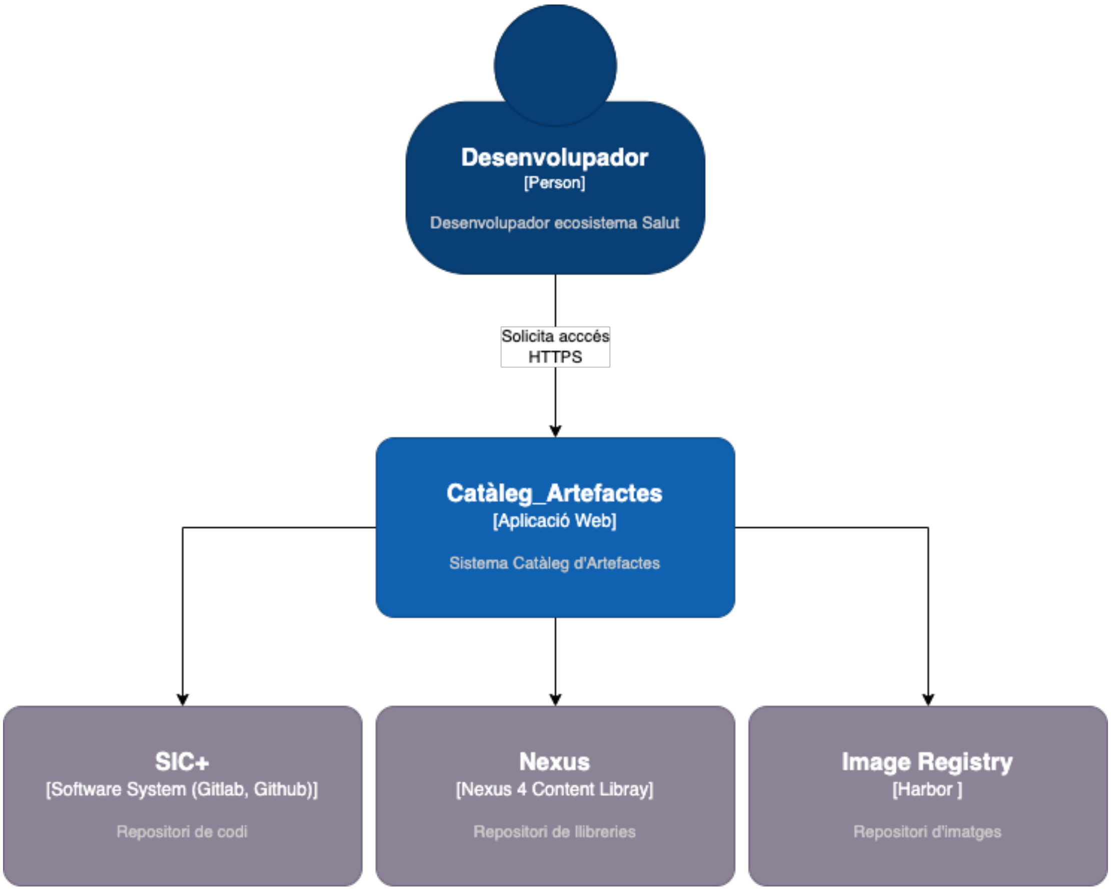


Figure 3. Application repository diagram.

Consultation of user guides and documentation:

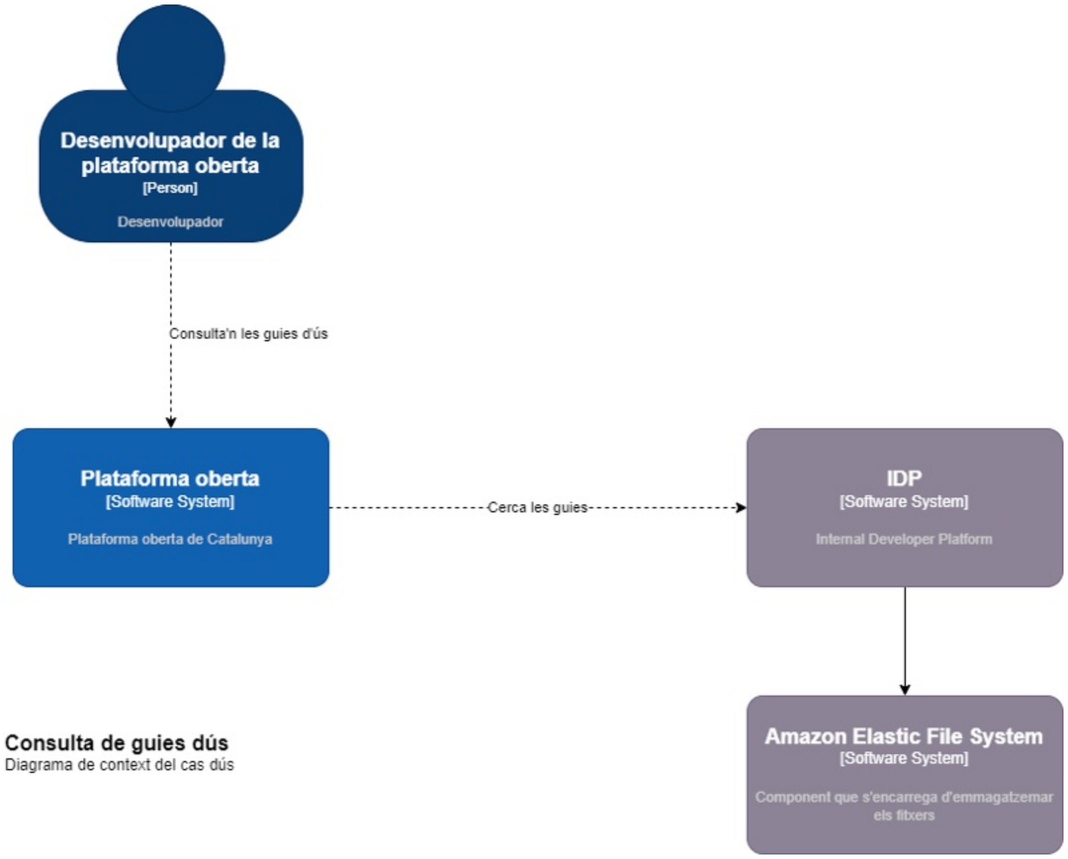

Desenvolupador de la plataforma oberta
[Person]
Desenvolupador
Consulta'n les guies d'ús
Plataforma oberta
[Software System]
Plataforma oberta de Catalunya
Cerca les guies
IDP
[Software System]
Internal Developer Platform
Amazon Elastic File System
[Software System]
Component que s'encarrega d'emmagatzemar els fitxers
Consulta de guies dús
Diagrama de context del cas dús

Figure 4. Consultation diagram of user guides and documentation

Homologation process:

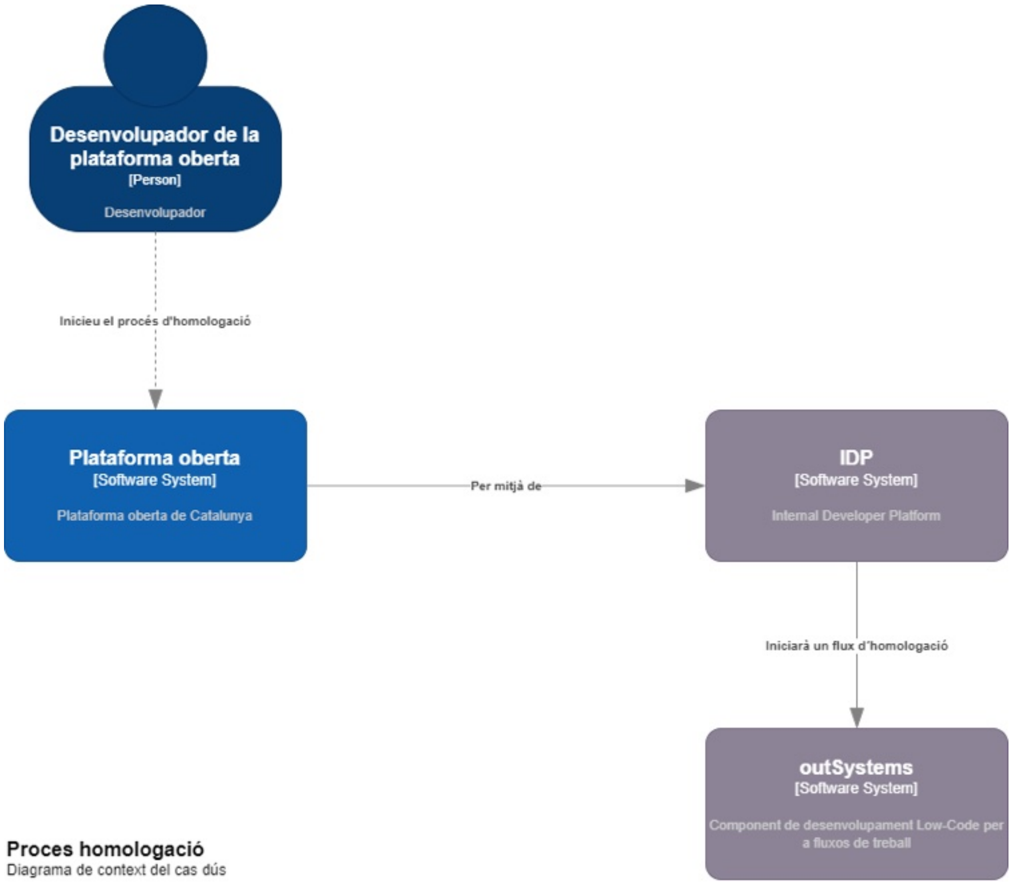

Desenvolupador de la plataforma oberta
[Person]
Desenvolupador
Inicieu el procés d'homologació
Plataforma oberta
[Software System]
Plataforma oberta de Catalunya
Per mitjà de
IDP
[Software System]
Internal Developer Platform
Iniciarà un flux d'homologació
outSystems
[Software System]
Component de desenvolupament Low-Code per a fluxos de treball
Proces homologació
Diagrama de context del cas dús

Figure 5. Homologation process diagram

Development Environment:

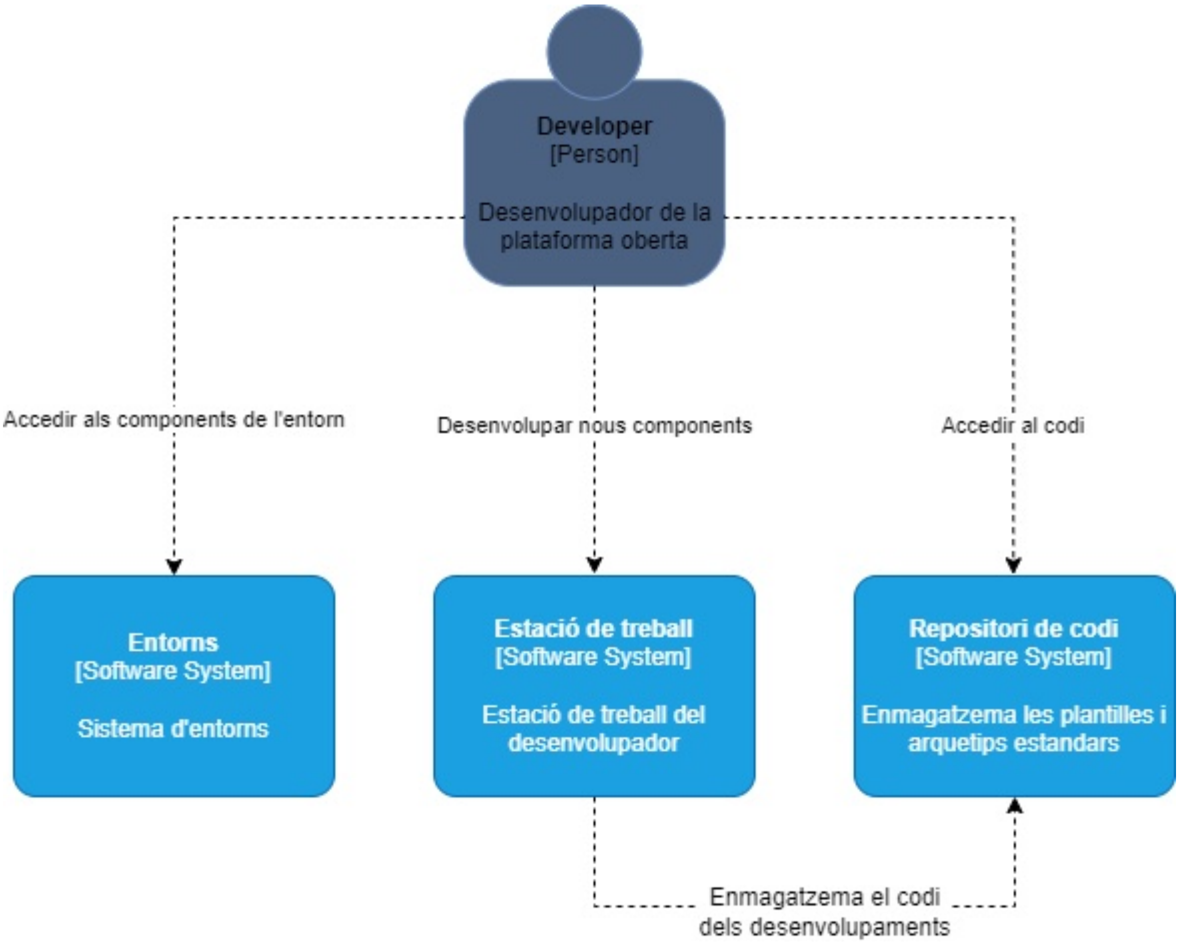

Developer
[Person]
Desenvolupador de la plataforma oberta
Accedir als components de l'entorn
Desenvolupar nous components
Accedir al codi
Entorns
[Software System]
Sistema d'entorns
Estació de treball
[Software System]
Estació de treball del desenvolupador
Repositori de codi
[Software System]
Enmagatzema les plantilles i arquetips estandars
Enmagatzema el codi dels desenvolupaments

Figure 6. Development Environment Diagram

Construction and Deployment System:

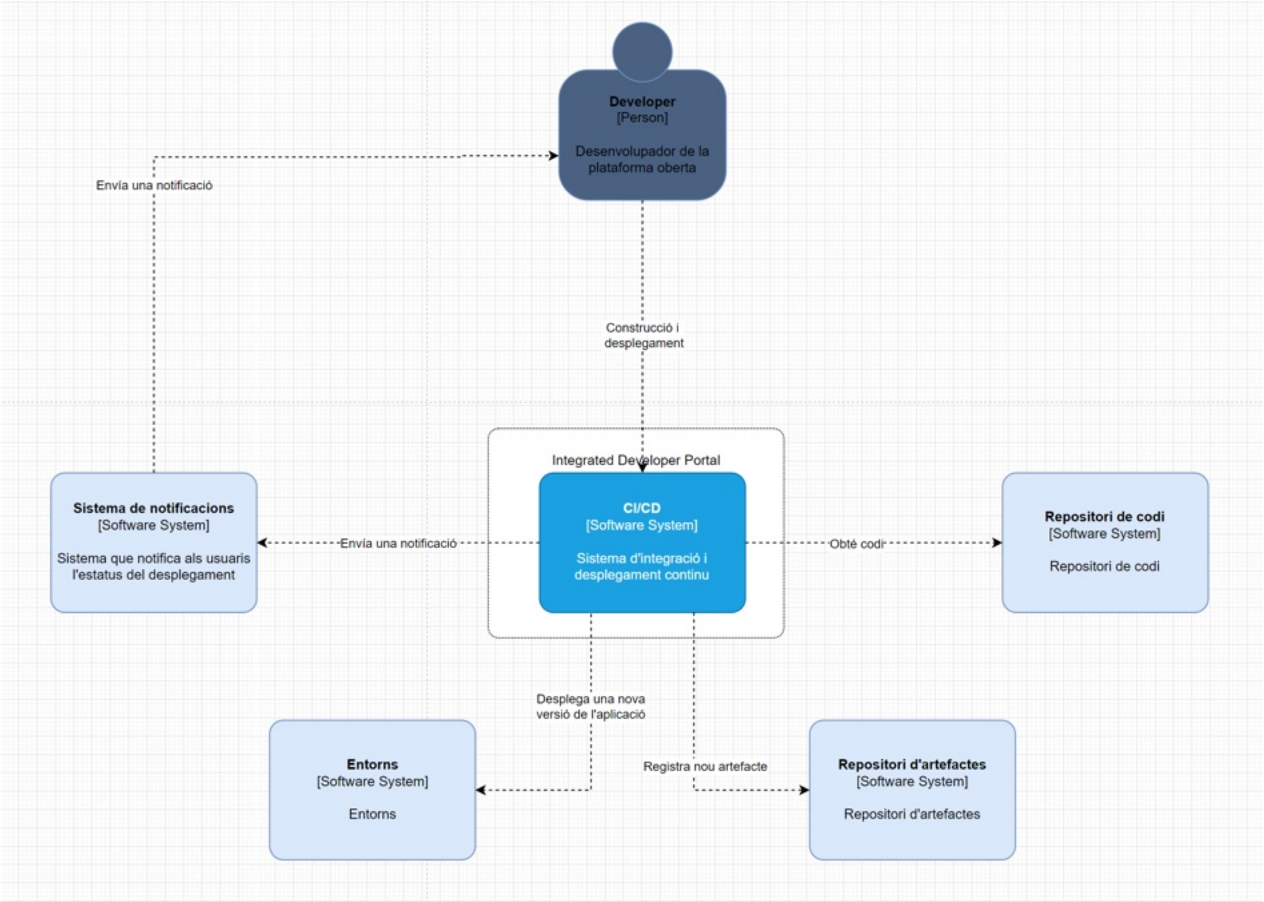


Figure 7. Construction and deployment system diagram

3.2.1 App Marketplace Portal

The application market portal will be built according to the micro-frontal paradigm to meet the needs of the different types of users who will enter it:

- Micro-front-end architecture with Single-Spa as the Shell manager and React as the frontend development framework
- Responsive design based on the Health Design System
- Progressive Web Application (PWA) for Mobile Access
- Integrated with the PDS Health corporate authentication system

Below are the different views of this portal according to the type of user who will connect to it.

3.2.1.1 Registered public access area

- Application search engine: Advanced search system that allows you to find applications by name, category, functionality or rating
- Documentation viewing: Access to technical and functional documentation of the available applications
- Registration and authentication system: User management with different levels of access and secure authentication
- Does not allow direct consumption of resources: It only allows you to view information, without being able to run applications

3.2.1.2 Platform Administration Console

- Resource Management: Management of computational capacities, storage, and system resources
- User and Permission Control: Granular management of user roles and permissions
- Operation monitoring: Real-time monitoring of platform performance
- Subscription Management: Subscription Plan and License Management
- Security monitoring: Control and monitoring of security and regulatory compliance aspects

3.2.1.3 Developer Area

It will be based on the open source Backstage (https://backstage.io) framework for developing developer portals (IDPs)

- Access to the component catalog: Library of reusable components for development
- White paper: Integration guides, APIs, and code samples
- Development tools: Templates, SDKs, and tools to facilitate app development
- Portal Infrastructure and Component Search Platform
- Sandbox environments: Isolated spaces to test applications without affecting the production environment
- Docker Image System: Docker Image Repository for Local Development
- Lifecycle management: Application version control and deployments, tailored to the framework provided by SIC+, CTTI's cloud-based CI/CD standard
- Creation of embeddable applications in the open platform

3.2.1.4 Clinical Administrator Area

- Validation of plugins by the ETC: Component verification process for the Clinical Workstation

- BPM Process Design Console: Visual tool for modeling clinical workflows
- Clinical Rules Engine: System for defining and managing clinical decision rules
- Pre-trained AI models: Access to clinical-specific AI models
- Homologation management: Control of the approval and certification process of components

3.2.1.5 Clinical Professional Area

- Customizable layout: Interface adaptable to the needs of each professional
- Visual selection of plugins: Drag & drop interface to configure the workspace
- Workspace configuration: Customization of the environment according to preferences
- Access only to validated plugins: Guarantee that only approved components are used

3.2.2 Development Environment / Sandbox

The development environment will have facilities for developers that allow them to quickly integrate their application with the open platform and a semi-automatic approval process.

This model allows for a completely isolated development environment, where the cost and responsibility falls on the developer, while the Marketplace maintains control and governance without assuming infrastructure costs, operational risk, or putting the scalability of the platform at risk. The developer retains full control of their environment, enjoys resource flexibility, completely isolates themselves from the open platform, and can gain cost containment by pay-as-you-go for the platform they use.

3.2.2.1 Deployment Model

- Each developer/company has their own hyperscalar subscription
- The Marketplace only acts as a control and governance point
- Backstage orchestrates deployments to developer subscriptions
- A high degree of automation is required:
  - Automated deployment via Backstage
  - Automated government policies
  - Automatic Resource Cleanup
  - Automatic cost monitoring

3.2.2.2 Operating model

3.2.2.2.1 Registration process

- Developer signs up for the Marketplace
- Provide your hyperscalar subscription credentials
- Backstage is configured to deploy in this subscription
- Governance policies are applied via IaC

3.2.2.2.2 Resource Control

- Limits per Sandbox
  - Maximum CPU/Memory
  - Storage limit
  - API Quota
  - Maximum number of instances
- Cleaning Policies:
  - Self-destruct after X days
  - Automatic Resource Cleanup
  - Code/configuration only backup
  - Non-persistence of sensitive data

3.2.2.3 Cost Model

3.2.2.3.1 Developer's Responsibility

- Cost of cloud resources
- Required software licenses
- Data storage
- Network Traffic

3.2.2.3.2 Included in the Marketplace

- Access to Backstage
- Templates and pipelines
- API simulators
- Basic support

3.2.2.4 Security and Isolation

3.2.2.4.1 Network Isolation

The network of the different sandboxes will be isolated from the rest of the sandboxes and the productive network of the open platform

3.2.2.4.2 Security Measures

- Independent Virtual Networks
- No access to production
- Synthetic data only
- Temporary access tokens

3.2.2.5 Pre-designed app templates

- openEHR clinics

- FHIR Interoperability
- openEHR/FHIR hybrids
- Forms

3.2.2.6 Data integration

- Built-in plugins: openEHR, FHIR, operational database
- ETL, CDC and asynchronous messaging tools
- Security Layer: PDS, Data Encryption, Auditing, Anonymization

3.2.2.7 Synthetic data generation

- Data generators: patients, medical records, episodes, time series
- Data models: demographics, disease patterns, medication models, visit patterns
- Validation tools: clinical consistency, data quality, patterns, business rules and consistency with clinical processes

3.2.2.8 Catalogue of available databases

- Clinical databases: Repository of clinical data, demographics, terminology
- Cross-cutting components: Appointments, resources, professionals, administration,...
- Management tools: data model viewer, connection manager, performance monitor, usage analyzer

3.2.3 Homologation process

The homologation process will provide tools for suppliers, homologation equipment. The aspects to be evaluated will be:

- Architecture
- Safety
- Quality
- Accessibility
- Healthcare

The homologation process itself will use the process tool of the application core to manage the different groups and tasks that will arise from the homologation of applications.

3.2.3.1 Automation of homologation

An important point of the homologation is the speed in which it is carried out and the containment of maintenance costs of this process, both in human and technological resources. Therefore, the construction of automations of the tender will be part of the tender, which will consist, without wishing to be exhaustive, of the following pieces:

1. Process engine and ticket management that allows you to observe the evolution of the homologation in all parts. it will have to include a public part for the application providers, and an internal part for the homologation teams involved
2. Architecture validation, through a series of fitness functions that validate the architecture criteria established for the different types of applications
3. Security validation, vulnerability analysis, regulatory compliance (GDPR, ENS), etc
4. Quality validation, in accordance with the quality gates established by the quality unit of the Department of Health
5. Validation of accessibility, in order to ensure compliance with the double AA and the use of the Health Design System
6. Healthcare validations, which confirm that the application covers the aforementioned functionalities of the solution, is safe for users and patients and has the appropriate support and service hours

3.2.4 App publishing process

The process of publishing on the marketplace includes three different phases:

3.2.4.1 Marketplace Readiness

- Creation of product sheet
- Pricing configuration
- Marketing materials
- Final documentation

3.2.4.2 Productive deployment

- Pre-production deployment
- Final validation
- Deployment in production
- Monitoring configuration

3.2.4.3 Activation in the Marketplace

- Publication in the catalogue
- License activation
- Access configuration
- Notification to interested parties

3.2.5 Marketplace Portal. Application consumption

3.2.5.1 Public Access / LMS / Professionals

Primary Use:

- Application Catalogue
    - Advanced search engine with filters by type of application, specialty, ratings
    - Detailed view of each app with description, screenshots, and documentation
    - User ratings and feedback system
    - Quality and homologation indicators
    - Usage and satisfaction statistics
- Integration with Corporate Systems
    - Native integration with the Clinical Workstation (ETC)
        - Automatic deployment of components
        - Synchronization of data and configurations
        - Unified permission management
    - Connection with the different SISCAT HISs
        - Standards-based interoperability (HL7, FHIR)
        - Federated identity management
        - Bidirectional synchronization of clinical data
    - Integration with My Health (LMS)
        - Automatic deployment of components adapted to mobile devices
        - Synchronization of data and configurations
        - Unified permission management
- User and Access Management
    - User registration and authentication integrated with GICAR
    - Registration and authentication of own users not integrated with GICAR (transients, external collaborators (mutual societies, INSS, etc.), etc.
    - Profile and role management
    - Personalization of the user experience
    - History of applications used
- Incident Management
    - Multilayer support system:
        - First level: 061/LMS for patient incidents
        - First level: SAU CTTI/Remedy for professionals
        - Second level: Platform providers
        - Third level: Application providers
    - Complete traceability of incidents
    - SLAs defined by incident type
    - Monitoring dashboards and KPIs

Secondary Use:

- Data Catalogue
    - Complete inventory of available datasets
    - Metadata and associated documentation
    - Access and use policies

    - Data quality and updating
- Data Extractions
    - Compliance with the framework of the Health Data Space of Catalonia
    - Alignment with EHDS (European Health Data Space)
    - Approval and traceability processes
    - Privacy and security controls
    - Standardized extraction formats

3.2.5.2 Supplier access / Catsalut Administration

- Management and Analytics
    - Application consumption and usage dashboard
    - API usage metrics
    - Flexible monetization models:
        - Pay-as-you-go
        - Subscriptions
        - Mixed models
    - Invoicing and reporting
- Data Management for Secondary Use
    - Granular data access control
    - Audit of accesses and uses
    - Regulatory compliance (GDPR, LOPDGDD)
    - Consent management
    - Anonymization and pseudonymization
    - Traceability of extractions
- Operational Management
    - Performance monitoring
    - Capacity Management
    - Alerts and notifications
    - Version and update management
    - Advanced reporting and analytics

3.2.5.3 Application prescription process

The statute of limitations process includes the following phases

3.2.5.3.1 Pre-prescription

- Identification of Need
    - Clinical evaluation of the patient
    - Definition of therapeutic goals
    - Assessment of the patient's digital capacity

  - Review of available apps
- Application Selection
  - Consult the catalog of prescription apps
  - Review of clinical evidence
  - Compatibility check
  - Checking for contraindications

3.2.5.3.2 Prescription

- Statute of Limitations
  - Record in medical records
  - Configuring specific parameters
  - Definition of duration and frequency of use
  - Setting measurable goals
- Access Management
  - Generation of activation code
  - Permission settings
  - License assignment
  - Link to medical history

3.2.5.3.3 Activation

- Notification to the Patient
  - Sending instructions
  - Secure access code
  - Installation/Usage Guide
  - Support information
- First use
  - Identity verification
  - Guided tutorial
  - Initial configuration
  - Functionality test

3.2.5.3.4 Follow-up

- Monitoring
  - Usage tracking
  - Collection of clinical data
  - Compliance alerts
  - Progress indicators
- Evaluation
  - Review of objectives
  - Parameter adjustment
  - Effectiveness assessment

  - Continuity decisions

3.2.5.3.5 Special Cases

- Modification of Prescription
  - Parameter adjustment
  - Change in duration
  - Modification of objectives
  - Updating permissions
- Cancellation
  - Reason register
  - Revocation of access
  - Notification to the patient
  - Information archive
- Renewal
  - Evaluation of results
  - Prescription update
  - License extension
  - Goal adjustment

3.2.5.3.6 Prescription monitoring

- Doctor's View
  - List of active prescriptions
  - Non-compliance alerts
  - Progress indicators
  - Revision agenda
- Patient View
  - Prescription apps active
  - Goal progress
  - Upcoming activities
  - Access to support

3.3 Platform Engineering

This point indicates those components that will be transversal to the entire solution, both for the core and for the application market, and that will be developed and operated under the paradigm of platform engineering.

3.3.1 Observability

3.3.1.1 Records

Integration with TALAIA Cloud (CTTI's corporate monitoring system for applications deployed in the cloud) to centralize global visibility. Log management with the Elastic suite allows you to search and analyze information in the logs of the different components of the platforms.

3.3.1.2 Traces

Correlation of events between different components to proactively detect problems. AWS Xray will be used for this task using the open-source OpenTelemetry protocol

3.3.1.3 Metrics

Performance metrics of the infrastructures will be managed from the AWS CloudWatch platform, which in turn will be connected to the TALAIA Cloud system to define the corresponding monitoring panels, and link with the Control Center and its alert and incident system. It will be necessary to follow the regulations established in the new CTTI Observability Model.

Business metrics of the applications that will also be collected using OpenTelemetry and will be made accessible to CloudWatch for subsequent exploitation from TALAIA Cloud.

Advanced AI analytics capabilities to detect anomalies and patterns

Historical data retention for trend analysis and optimization

3.3.2 FinOps

- Integration with Cloudability/Apptio corporate solution for multi-cloud management
- Cost optimization policies:
  - Automatic shutdown of non-productive environments
  - Resizing underutilized resources
  - Capacity reservation to optimize costs
- Allocation and monitoring of budgets by department/project
- Cost deviation alerts
- Optimization recommendations based on usage patterns

3.3.3 Self-service portal

- Standardised service catalogue
- Configurable approval workflows
- Integration with corporate ticketing systems
- Custom dashboards by user/role
- API to automate requests from other systems

- Management of the complete life cycle of requests
- Status traceability and stock audit

3.3.4 Safety

This point mentions main aspects of security such as access security, data encryption and activity auditing

3.3.4.1 Access security

As mentioned below in point 4.1 Security Platform – PDS, access security is managed through this transversal component that acts as an Identity Provider and supports two authorization models: OpenId Connect tokens (primary) or SAML tickets.

Once the authentication of a user or system subject has been passed, the PDS will generate a pair of access and refresh tokens, which can be used throughout the session. The applications will have to collect these tokens and manage the corresponding authorization, that is, validate that the authenticated subject has permissions to perform the required actions.

In this sense, applications will implement their own token validation system and will have their own authorization criteria to apply and allow or not access to the services they publish.

3.3.4.2 Data encryption

We distinguish encryption in two aspects; in transit and at rest

For encryption in transit, all communications will be encrypted by TLS 1.3 or higher encryption

For encryption at rest, all information repositories will be encrypted with an encryption key that will be provided by the CTTI from its corporate key management system. In the event that the service is not active at the time of the start of the contract, the keys used to encrypt the information will reside in a cloud provider other than AWS (Azure Key Vault or Google Cloud Key Management).

3.3.4.3 Audit of activities

3.4 To comply with the legal requirement to maintain an audit of access to or modification of personal or medical data, the Health Transversal Audit Platform will be used. Its characteristics are detailed in the point 4.5 Terminology Server

The objective of the service is the response of the service by implementing the FHIR R4 medical standard. The standard resources used in the project are as follows:

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

Where the catalogue is represented.

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

Where the subset of a catalog is represented.

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

Where the relationships between the concepts of the catalogues are represented.

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

Which is used to represent a list of search results.

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

Which is used to represent the body and response of a FHIR operation to a resource.

The relationships between FHIR terminology resources can be found on the standard page: https://hl7.org/fhir/terminology-module.html

Subscriptions to the active services of the Terminology Server, currently, will be in consultation mode in their entirety, by consumer applications.

Note: The development has been carried out based on FHIR R4 v4.0.1. It is necessary to take into account the information provided by the web addresses of the FHIR standard, there may already be changes or actions on versions of the standard.

Audit Platform

3.4.1.1 User Repository and App Portal

It will be necessary to implement within the framework of the Open Platform an Application Portal that replaces the current GSA Portal and the login page of the Primary ECAP.

This application portal must be integrated with the PDS, which is the one that will offer the login page in the different authentication flows described in the section 4.1 Security Platform – PDS, and must also include the user repository and their credentials, which serves as the sole and secure source of authentication for the PDS, as well as operations to manage the registration, modification or deregistration of users and the maintenance of their respective credentials (registration, rotation, recovery from oblivion, temporary or permanent deactivation or due to expiration, etc.).

3.4.2 Disaster Recovery

It will cover the following aspects:

- Addressing routing between different availability zones, regions, and cloud providers
- Load balancing across availability zones, regions, and cloud providers
- Federated or Extended Storage
- Presentation and business layer infrastructure that allows the use of advanced recovery mechanisms
- Database platform based on PaaS model to have multi-zone, multi-region and multi-cloud high availability
- Automation of the DR process with scheduled periodic tests
- RPO (Recovery Point Objective) and RTO (Recovery Time Objective) defined by service
- Documented and proven business continuity plans
- Automated failover and fallback procedures
- Backups with configurable retention
- Prepared contingency environments
- Periodic recovery tests
- Reporting procedures in the event of an incident

3.4.3 Documentation

The transversal component of documentation must include:

- A centralised repository of technical and functional documentation accessible to all actors involved in the development and operation of the platform.
- Standardised procedures for the generation and maintenance of:
  - Architecture and technical design documentation
  - User and Operation Manuals
  - API and Interface Documentation
  - Development guides and best practices
  - Operation and maintenance procedures
  - Contingency and recovery plans
- Tools for the collaborative management of documentation such as wikis or document managers that allow:
  - Version control
  - Cross-team collaboration
  - Content search and indexing
  - Integration with development tools
  - Agile updating of documentation
- Processes for reviewing and approving documentation before publication
- Mechanisms to keep documentation updated on an ongoing basis, especially after changes to the platform

3.4.4 Quality of service

The successful bidder will have a team of experts in the different platforms and components that make up the services, with the availability of the professional services of the manufacturers of the different SaaS components that are part of the solution.

In addition, the quality of the service will be measured in the following aspects:

- Service Level Agreements (SLAs) defined in the specifications
- Continuous improvement processes
- Management of incidents and problems using the tools proposed by the CTTI
- Key Performance Indicators (KPIs)
- Periodic user satisfaction surveys
- Proactive capacity management
- Continuous training plans for teams

3.4.5 Capacity Management

Capacity management should include:

- Continuous monitoring of the resources used:
  - CPU, Memory, and Storage
  - Bandwidth and network latency
  - Number of concurrent users
  - Transaction volume
  - Response Time
- Prediction and planning tools:
  - Analysis of usage trends
  - Prediction of future needs
  - Expected growth models
  - Resource scaling planning
- Autoscaling mechanisms:
  - Metric-based auto-scaling policies
  - Horizontal and vertical scaling
  - Dynamic load balancing
  - Resource optimization
- Proactive management:
  - Preventive alerts before reaching critical limits
  - Optimization recommendations
  - Dynamic adjustment of resources
  - Prevention of bottlenecks
- Reports and dashboards:
  - Real-time resource usage
  - Historical trends

- Forecasting future needs
- Cost associated with resource consumption

3.4.6 Platform operation

The platform will require continuous operation in the cloud infrastructures, supported by an integrated global team that ensures 24x7 support for the resolution of critical incidents, applying CI/CD techniques and automation of both the requests that may come from the different consumers of the platform, as well as the remediation of incidents, such as, for example, availability or capacity. The aim is to automate all the routine management of operations, enhance predictability and proactivity and avoid manual tasks dependent on operators.

For those application providers who cannot take care of 24x7 support, this service will be offered. The bidder must consider the necessary equipment to be able to provide this service for those applications that require it.

4 Mandatory Health Enabling Components

4.1 Security Platform – PDS

The HES Security Platform (PdS) is the transversal Health Identity Provider.

The services it offers mainly include the management of:

- Authentication: the credentials needed to consume services or data from a Health initiative
- Authorization: the control of the permission on these services exposed by the initiative, according to the credentials presented by the consumer.

It is based on the open source distribution of Keycloak as an identity and access control (Identity Provider), and supports the OpenIdConnect (OIDC) and SAML2 standards.

Two possible authentication flows are contemplated in the PDS: user or system. In the case of System Authentication (*Client Credentials Flow* or also known as "Service Account") the credentials consist of a client-id/client-secret pair, and in addition, the PDS has the ability to add additional parameters (claims) to tokens that can be validated against predefined catalogs of the HES Terminology Server, or calculated based on rules defined in the HES Rules Engine.

In the case of user authentication (*Authorization Code Flow*), the PDS offers the possibility of federating the login to the GICAR (professionals) or VALID (citizens) corporate systems or other user repositories, both internal and external. For this type of authentication, the PDS is the one who offers the login page and redirects to the third-party identity provider to securely manage the credentials.

4.2 Clinical Data Repository – RDC

The openEHR RDC clinical data repository is a clinical database in accordance with the specifications of the openEHR standard that allows to store information models (in the form of archetypes and templates) at runtime, as well as to record clinical patient data through compositions and query this information using the AQL archetype language (AQL v1.4).

The applications of the Catalan health system will use the RDC service and the Index Server for the registration and consultation of clinical data associated with patients treated in the territory.

4.3 Patient Master – MPI

The functionalities of the MPI are:

- To uniquely identify a patient treated by the Catalan Health Service, being consulted by CatSalut or external systems.
    - Data from: RCA, ECAP and ICAM (from kafka events)

- FHIR API for Patient Consultations
- Serve as a link between MPI (ID_MPI) and CDR (ID_EHR), through "Index server"
- Deposit audit of patient discharges and modifications (BDD MongoDB)

It guarantees reasonable response times in updating data and facilitates the integration of current systems with patient demographic data.

Users: Administrative professionals.

4.4 Index Server

In this component, the relationship between the patient master and the clinical data repository is maintained. Its objective is to separate patient information from clinical patient information. This repository maintains a relationship between the patient identifiers of both platforms in a separate database.

It allows a patient's medical record identifier to be obtained from their Patient Master Identifier (MPI), a system where demographic data linked to patients is stored, and vice versa, i.e. to obtain the patient identifier from the medical record identifier.

4.5 Terminology Server

The objective of the service is the response of the service by implementing the FHIR R4 medical standard. The standard resources used in the project are as follows:

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

Where the catalogue is represented.

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

Where the subset of a catalog is represented.

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

Where the relationships between the concepts of the catalogues are represented.

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

Which is used to represent a list of search results.

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

Which is used to represent the body and response of a FHIR operation to a resource.

The relationships between FHIR terminology resources can be found on the standard page: https://hl7.org/fhir/terminology-module.html

Subscriptions to the active services of the Terminology Server, currently, will be in consultation mode in their entirety, by consumer applications.

Note: The development has been carried out based on FHIR R4 v4.0.1. It is necessary to take into account the information provided by the web addresses of the FHIR standard, there may already be changes or actions on versions of the standard.

4.6 Audit Platform

HES-PAUD is the transversal Health application that allows adhered applications to receive audit events asynchronously, and later, in the future, consult them with a REST API that HES-PAUD exposes using FHIR Search.

These events are standardized with the FHIR R4 specification and are based on the IHE-ATNA definition.

We can distinguish 3 types of interactions with the HES-PAUD system:

1. Web interface of HES -PAUD:

The HES-PAUD application has a web interface that allows system administrators to search for events using filters. They can also generate PDF documents with the desired information.

This interaction is reserved for system administrators, so it is not described in this document.

2. REST API (synchronous):

HES-PAUD exposes a REST API that allows auditing events to be searched programmatically. This API uses the HAPI FHIR format to query events. In addition, it is secured with the PdS.

The authorization model for this API is being defined, which will be integrated with the Security Platform (PdS). This first version does not yet provide information to request credentials for consumption.

3. Kafka (asynchronous):

The initiatives adhered to HES-PAUD publish their events in a corporate topic of EventHub and then they are consumed by the Audit Platform.

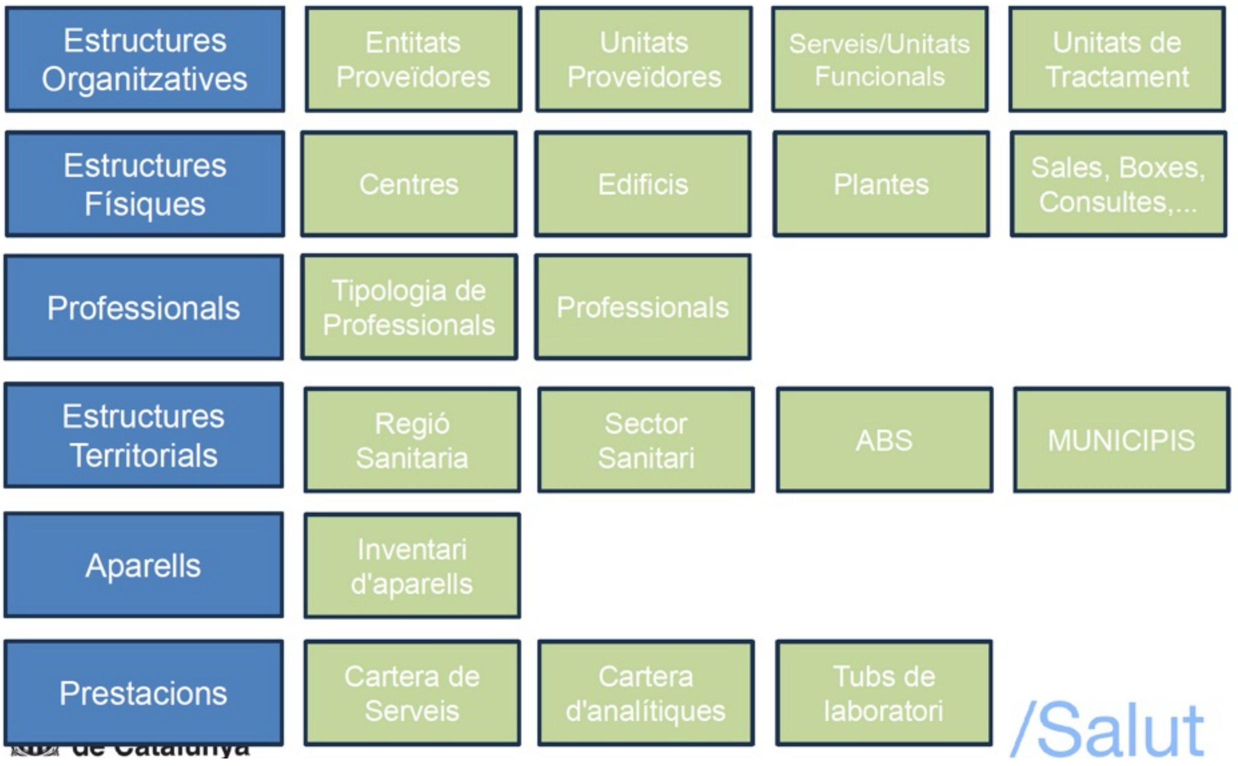
This process is completely asynchronous for the adhered initiative and can publish as many events to the topic as needed.

All consumed messages are validated with a Schema Registry using a JSON Schema and the EP, UP and center codes are validated. Subsequently, they are saved in the HES-PAUD repository (as long as there are no formatting errors) for later consultation.

4.7 Server Resources - Professionals and Organization

It is a transversal initiative that aims to implement a tool that allows the non-clinical resources of SISCAT (Integral Health System for Public Use of Catalonia) to be centrally modelled and that allows them to define their attributes and the relationship between them (organisational structures, physical structures, devices, etc.).

On this server you will find:



Estructures Organitzatives	Entitats Proveïdores	Unitats Proveïdores	Serveis/Unitats Funcionals	Unitats de Tractament
Estructures Físiques	Centres	Edificis	Plantes	Sales, Boxes, Consultes,...
Professionals	Tipologia de Professionals	Professionals		
Estructures Territorials	Regió Sanitaria	Sector Sanitari	ABS	MUNICIPIS
Aparells	Inventari d'aparells			
Prestacions	Cartera de Serveis	Cartera d'analítiques	Tubs de laboratori	

4.8 Distributed Traceability

Using AWS XRAY, as a distributed traceability solution

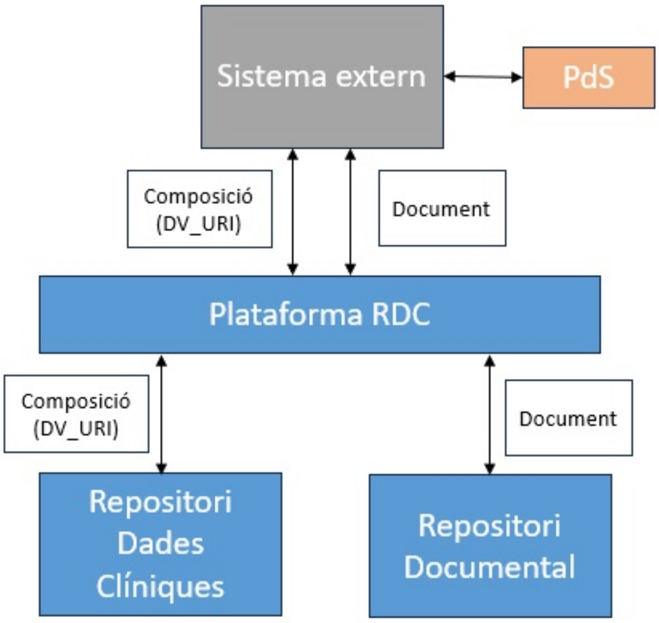
4.9 Communications Gateway

Service in definition. It will be the gateway on which communications with citizens and professionals who access the platform will be centralised.

4.10 Document Manager

The knowledge management platform includes both the clinical data repository (RDC), where patients' clinical data can be stored throughout their lives, and a document repository that allows the documents generated in the different care processes to be stored and consulted.

With the defined model, the document repository saves only the documents, while the RDC acts as a document record, registering the metadata of the document and the directory where it is hosted in the compositions (in a field of type DV_URI). That said, separate requests will have to be made to interact with each of the components, through the REST APIs they offer. A flowchart with the different elements is attached:



Source systems are responsible for data consistency, between metadata and documents.

In the documentary repository it will also be possible to save documents not referenced in compositions thanks to this model. In this case, however, the source system must ensure that the URI and the necessary metadata are saved to identify the location of the document, since the document repository will not have this information.

4.11 Corporate Encryption Key Management Platform

For encryption at rest, all information repositories will be encrypted with an encryption key that will be provided by the CTTI from its corporate key management system (under construction). In the event that the service is not active at the time of the start of the contract, the keys used to encrypt the information will reside in a cloud provider other than AWS (Azure Key Vault or Google Cloud Key Management).

5 REQUIREMENTS OF THE TECHNOLOGICAL SOLUTION PROVIDED

5.1 Platform Architecture Requirements

The technological solution required must contemplate the deployment on public cloud infrastructures of the CTTI, therefore, the bidder must fully provide all the elements of the infrastructure as code that are necessary to provide the required functional service.

5.1.1 Connectivity to the Communications Node of the Government of Catalonia

By consuming cloud services provided by the CTTI, the provider will have Node addressing corresponding to the chosen cloud. The supplier must provide in its safety design the components necessary to perform the functions of firewall and balancing, as well as the interconnection of its components. All communications between the cloud and CTTI's onprem datacenters must be enabled through the dedicated lines that GESNUS has implemented for this purpose according to each hyperscalar and its corresponding gateway.

5.1.2 Server Addressing

The IPv4 and IPv6 addressing assignment will be a subnet within the dedicated addressing for the public cloud by Node. Public addressing is managed from the Communications Node. The servers must have this address defined. All servers must have management and backup networks, differentiated from service networks. NAT is allowed on the subnets in each hyperscalar. Precisely, to avoid exhausting the IPV4 ranges that NUS has assigned to each hyperscaler, the subnetting provisioning consists of NUS CIDRs (with a limited size) and internal CIDRs (of much larger size) and an internal gateway

5.1.3 DNS services

The DNS service will be provided centrally from the Communications Node from the DNS servers that it has located in each hyperscalar. The service provider must have the resolution of the domains intranet.gencat.cat it configured at the resolver level.

5.1.4 Routing

The service provider will route the public and private address defined in the Generalitat de Catalunya to the Communications Node.

Exit and/or entry from the Internet will be carried out through the Communications Node through the proxypass service available in each of the dedicated hyperscalar Internet access by web traffic.

5.1.5 Communications Services

The communications services required by the systems located on the platform will meet the following requirements:

The provider of the Communications Node will be responsible for managing the server certificates and the acceleration of SSL and Level 7 balancing and reverse proxy services (by URL only). In cases where necessary, these certificates may be managed by the service provider.

The service provider is responsible for providing, managing, administering and operating the other necessary communications elements that the service requires (firewalls, balancing, network electronics, etc.).

5.1.6 High Availability

The architecture of the solution will contemplate its execution in real high availability between two remote cloud regions. Consequently, the bidder will have to contemplate the hardware in both regions with the necessary level of service.

However, all services will run in three Availability Zones in your chosen regions.

5.1.7 Detailed Architecture Requirements

In addition to the functional requirements indicated in section X of these specifications, the installation must meet the technological requirements detailed below:

- The solution must comply with the provisions of the Manifesto of the reference architecture for new initiatives and solutions in Health and in the characteristics of the HES architecture, referenced in 2.1 Reference architecture and 2.3 Characteristics of the architecture in all its terms, especially those indicated in the section that mentions the most relevant characteristics.
- The solution must comply with the supported product versions, available in the CTTI software roadmap (https://qualitat.solucions.gencat.cat/estandards/estandard-full-ruta-programari/) of its components throughout the life of the contract. The offer must indicate how all the components of the platform will be kept up to date (obsolescence management), indicating the proposed version and patch management process.
- The solution will have to be assimilated or integrated with the CTTI lifecycle tools, with regard to source code management, continuous integration, automatic deployment pipelines, code quality, automated testing and infrastructure as code. All these activities are framed by continuous deployment DevOps techniques and methodologies.
- The solution must be integrated with the control tools of the operation, with regard to:
    - Scaling matrix, offering 24x7 support at different levels of resolution
    - Incidental, requests and queries on the CTTI ticketing platform
    - Polling and monitoring with Control Center tools

  - Centralization of logs and observability of the platform with the tools of the Control Center
- The proposed solution will consist of 3 execution environments: Integration, Pre-Production and Production and a "sandbox" development environment that will be offered to developers in the application market in a packaged form. INT and PRE environments can be deployed in the same private virtual network, as long as they do not share resources in their different layers (balancers, containers, databases,..) to save redundant networking elements in a small environment like INT. The Pre-Production and Production environments must be identical in their architecture, except in the capacity which, in the case of the Pre-Production environment, may be between 70% and 100% of that of PRO. The Integration environment and the "sandbox" environment may have a different simplified architecture, but contemplating the same base products. The development environment within the service is not contemplated, and the characteristics of the service are at the discretion of the bidder. However, the products and tools used in this development environment must be the same in the same versions as those offered in the service.
- The new versions of the solution software must be deployed automatically with a single build step and passing the same artifact built by all INT, PRE, PRO environments. The maximum deployment time required between the time the source code is deposited in the code repository and its availability in production is one (1) hour. It is required that deployments can be carried out during service hours without interruption or degradation of the service perceptible by the end user. It is recommended to use the "feature toggles" technique to contemplate rapid reversals and selective deployments of the new versions. In the same way, the use of specific software is recommended to manage the versions of the databases and enable their automation in the deployment flows, in the same way as it is done with the business logic components.
- The management and operation of the platform's infrastructure will be carried out exclusively automatically, avoiding in any case manual operational tasks. Automation scripts will be considered as source code and will therefore be subject to all source code management considerations that are required for business components.
- All third-party products used will include business support services by the respective manufacturers, in 24/7 mode, with a response time of less than 1 hour in the event of incidents of critical severity that lead to interruption or degradation of the service. The offer must be accompanied by the details of the products and evidence of compliance with this requirement for each of them. In the event of using components without this type of support provided by the manufacturer, the successful bidder will assume this level of service and response time.
- All the APIs offered by the service will be given in three modalities:
  - Synchronous mode: REST API or GRAPHQL over HTTPS protocol (TLS1.3 or higher), published on the API Manager corporate platform.
  - Asynchronous modality: Apache Kafka topics published on the Kafka Corporate Messaging Platform service.
  - Microfrontend modality: web components that consume the service's business services and that can be embedded in container applications.

- Given the current trend in information systems, the system covered by this contract will have to run on cloud native platforms. All products and applications that are installed in the context of this tender will be ready to be migrated to another cloud provider with little effort and to be able to provide the service in two or more public cloud providers
    - Lowcode, SaaS or cloud native tools will be used in this order of preference
    - In the case of cloud native, container technology will be used in all software artifacts, preferably in serverless mode
    - MongoDB Atlas databases will be used that allow multi-vendor and multi-region execution in public cloud providers.

The databases used must be designed to contemplate different storage qualities depending on the function or validity of the data to be retrieved, to maximize the performance of the most common queries containing the TCO (Total Cost of Ownership) of the platform.

The service must include the performance of backups and the hardware components necessary to carry them out. These backups will have the following characteristics:

- Retrieval of data at a point in time in the last 48 hours
- Incremental daily withholding with 2 weeks of retention, full weekly withholding with 1 month retention, full monthly withholding with 3 months of retention, and full annual withholding with 1 year of retention

This backup must include the appropriate mechanisms to obtain the copy in the window indicated and to obtain a copy with the congruence and consistency required by the application and the data.

5.1.8 Description of the Architecture

The bidder must present the technological solution proposed to carry out the activities required in these specifications, detailing the different components and technologies that support it. Specifically:

- Description of the technological solution, indicating the different functional blocks that compose it, and the function of each of the blocks (e.g.: main execution platform, process engine, application market, homologation process, etc.).
- Detailed architectural design (including diagrams), the respective justifications for the architectural decisions made in the design and the adaptations made on the Health Reference Architecture Manifesto or the HES Architecture Characteristics Document, if applicable.
- High-level design of the technological solution for each functional block, including all the required technological components (e.g.: ETL, databases, application servers, container orchestration, etc.) and interactions with other functional blocks of the solution itself or external.
- Required Work Environments
- Product and version of each proposed technology

- SaaS products required in each component of the solution
- Sizing of the infrastructure necessary to provide the service broken down by environment and functional domain.

5.2 Installation, configuration and post-implementation support of the technological solution

The successful bidder will carry out the following activities related to the installation, configuration and operation of the technological solution, in the different environments agreed:

- Preparation of the necessary technical documentation according to the Health Solutions Quality Model (09_Annex_9_Model_Qualitat_Salut_WIP) to be able to proceed with the installation.
- Coordination with CTTI's Solution Integration and Cloud Support team, for the validation of the Architecture Document and for the provision of the necessary cloud infrastructure.
- Installation of all the components of the proposed technological solution with the necessary infrastructure scripts as code following CTTI's SIC+ indications.
- Configuration and integration of all the components of the solution.
- Certification of the quality of the installation:
  - Justification of the correct installation with specific evidence of each component.
  - Inspection of the installation by the respective manufacturers, or by their own staff duly certified and accredited by the manufacturer.
- Preparation of the technical documentation resulting from the installation.
- Updating the CMDB with all the components of the solution.
- Preparation of the operation documentation of the technological solution required by the Operations Area.
- Carry out the post-implementation support of the technological solution.
  - Incorporation of patches and management of technological obsolescence every six months.
  - Platform capacity and growth plan
  - Performance management.
  - Scheduling periodic disaster recovery tests and backup restoration.

Generalitat de Catalunya
Centre de Telecomunicacions
i Tecnologies de la Informació

/Salut

PRELIMINARY CONSULTATION ON THE MARKET FOR THE CONSTRUCTION OF AN OPEN PLATFORM IN HEALTH - ARCHITECTURE COMPONENTS, APPLICATION MARKET AND PLATFORM SERVICES

APPENDIX 3: APPLICATION MARKET

CTTI/2025/113

Barcelona, February 2025

Version history and contributions

Unió Europea
Fons Europeu
Next Generation

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD

Pla de Recuperació, Transformació i Resiliència

Next Generation Catalunya

Generalitat de Catalunya

Description of the review	Author	Date	Version
Initial draft		27/12/24	0.1
Revision and final version		08/02/25	0.2

Index

1. Introduction

This annex is dedicated to defining the main elements that should make up the market for applications of the open platform in health. The application market is one of the fundamental architectural components of the platform, as described in the technology architecture annex, while representing one of the critical services for the success of the new health information systems model.

This dual character, as an architectural and service component, places this annex on the border between technical and functional specifications. On the one hand, the application market must be integrated in a coherent way with the rest of the components of the open platform architecture, complying with the technical requirements and established design patterns. On the other hand, it must act as the catalyst that allows innovation and collaboration within the Catalan health ecosystem, facilitating that new actors can provide innovative solutions to the health system and that these can be adopted in an agile and safe way.

The application market must implement the necessary mechanisms to ensure that the solutions to be integrated comply with the technical, functional and security requirements demanded, while facilitating the integration and adoption processes. For this reason, it is structured in two differentiated but complementary parts:

1. Developer portal: Space that provides the tools, documentation and resources necessary to facilitate the development and integration of applications on the platform. It includes the development, testing and homologation environments.
2. Application portal: Catalogue that allows you to discover, evaluate and obtain the applications and services available. It includes the mechanisms of prescription and adoption by the different actors of the system.

The following chapters delve into the characteristics and components of each of these parts, defining the requirements they must meet to achieve the objectives established in the Digital Health Strategy of Catalonia 2024-2030 (Annex 1), always maintaining coherence with the global technological architecture of the open platform.

2. Developer portal

The developer portal is an essential element to ensure the success of the open platform, as it acts as the main entry point for all actors who want to develop or integrate solutions. This portal must implement the Platform *Engineering*[1] paradigm, which promotes self-service, autonomy and standardization, not only in the development of products but also in their operation and monitoring.

The success of an open platform depends largely on its ability to attract and retain developers and companies that provide innovative solutions. To achieve this, the portal must offer an optimal experience that reduces friction in the adoption of the platform and accelerates the development cycle. This involves providing tools, documentation and resources that facilitate both the first steps and the continuous development of complex solutions.

The portal also plays a key role in the technical governance of the platform, as it implements the mechanisms that ensure that all the solutions developed comply with the established technical, quality and security standards. This governance is implemented in such a way that it does not pose a barrier to innovation, but acts as a facilitator to guarantee the quality and interoperability of solutions.

2.1. Objectives

The main objectives of the developer portal are:

- Provide a complete environment for the development of applications and data products.
- Facilitate the adoption of the platform through high-quality tools and documentation.
- Automate development, testing, and deployment processes.
- Ensure compliance with technical and quality standards.
- Provide tools for monitoring and managing the lifecycle of applications.

The main objectives of the developer portal are grouped into four areas of action described in detail below.

2.2. Facilitation of adoption

[1] Platform engineering is a practice that relies on in-house platforms, enabling self-service capabilities for software engineering teams following a cloud-native approach. A platform encompasses a set of tools, services, and infrastructure that allows developers to build, test, deploy, and monitor software applications. These platforms are known as in-house developer platforms (IDPs) and are specifically tailored to an organization's needs, demands, and goals. Simply put, in a cloud-native world, *Platform Engineering* is the application of DevOps principles at scale.

The portal must minimize barriers to entry for new developers and companies, providing:

Guided and progressive onboarding process

- Structured training path that begins with basic concepts and evolves towards advanced functionalities.
- Interactive tutorials that allow you to experiment with APIs and services in a secure environment.
- Pre-configured templates for different types of applications and data products (clinics, management, monitoring, etc.).
- Role-specific guides (developer, architect, product manager, QA).

Documentation and learning resources

- Complete and up-to-date technical documentation of all services and APIs.
- Examples of code and commented and reusable tests.
- Best practice guides and recommended design patterns.
- Real-world use cases with implementation examples.
- FAQ and common problem solving.

Immediate development environments

- Instant access to pre-configured cloud development environments.
- SDKs and development tools ready to get you started.
- A set of representative test data for testing functionalities.
- Integration with the most common integrated development environments (e.g. Visual Studio Code and IntelliJ) through *plugins* and extensions.

Technical support and accompaniment

- Ticket system for technical consultations.
- Live chat to resolve urgent queries.
- Developer forum moderated by experts.
- Periodic training sessions and resolution of doubts.
- Support programme for strategic projects.

2.3. Acceleration of development

The portal must optimize the development cycle by:

Standardized environments

- Pre-configured Docker containers with all necessary dependencies.
- Virtual development environments based on Kubernetes.

- Integration with continuous integration/continuous deployment (CI/CD) tools (e.g. Jenkins, GitHub Actions, etc.).
- Automated management of development, testing and pre-production environments.

Reusable components

- Library of UI/UX components that follow the *design system* of the Catalan Health System.
- Pre-built plugins for integration with common services.
- Information models based on archetypes, templates and validated openEHR queries .according to the instance of the *Catalan Clinical Knowledge Manager* (CKM).
- Reference implementations of common integration patterns.

Process automation

- Continuous integration/continuous deployment (CI/CD) model pre-configured for different types of applications.
- Automation scripts for common tasks.
- Automatic code generation tools from specifications.
- Automated deployment systems with *rollback*.

Development and testing tools

- Test APIs that simulate the behavior of production services.
- Automated testing tools (unitary, integration, e2e).
- Code quality and security validators.
- Profiling and optimization tools.

2.4. Quality Assurance

The portal must implement mechanisms that ensure quality in accordance with the following characteristics:

Validation of standards

- Automatic verification of compliance with the platform's technical standards, through a series of "*fitness functions"* that validate the application's adherence to the standards both during deployment time and during the operation of the application, providing service to its users.
- Validation of compliance with openEHR specifications.
- Accessibility verification according to WCAG 2.1 (https://www.boe.es/eli/es/rd/2018/09/07/1112/con).
- Code quality analysis (cyclomatic complexity, duplication, etc.).

Automatic tests

- Automatic execution of security test suite.
- Performance and scalability tests.
- Accessibility and compatibility tests.
- Data integrity validation.

Verification of documentation

- Checking the completeness of the technical documentation.
- Validation of training and support materials.
- Review of user guides and operating manuals.
- API documentation verification.

Interoperability

- Integration tests with other components of the platform.
- Validation of data exchange formats.
- Check backward compatibility.
- Integration tests with external systems.

2.5. Technical governance

The portal must provide tools for effective governance in accordance with:

Life cycle management

- Version control of applications, data products and components.
- Management of dependencies and updates.
- Obsolescence policies.
- Monitoring of use and adoption.

Observability

- Real-time monitoring dashboard.
- Performance and availability metrics.
- Distributed traces for problem diagnosis.
- Automatic threshold-based alerts.

Change control

- Change review and approval flows.
- Management of branches and versions.
- Automation and conflict resolution.
- Traceability of modifications.

Incident management

- Centralised incident ticket system.
- Categorization and prioritization of incidents.
- SLAs according to type of incident.

3. Application portal

The application portal represents the main interface between the creators of digital solutions and the users of the health system. This portal must act as a modern and dynamic application marketplace that facilitates the discovery, evaluation and adoption of digital solutions, while ensuring that all available applications comply with the technical, functional and safety requirements established by the health system.

This portal must implement mechanisms that allow different adoption models, from self-service for simple applications to professional prescription processes for complex clinical solutions. It must also facilitate user feedback and evaluation, creating a continuous improvement cycle that benefits both developers and end users.

A distinctive feature of this portal is its ability to manage different types of applications with different distribution and monetization models, from free applications developed by the health system itself to third-party commercial solutions, to open-source applications developed by the community.

3.1. Objectives

The main objectives of the application portal are:

- Provide a unified catalog of applications and services.
- Facilitate the discovery and adoption of new solutions.
- Guarantee the quality and security of the applications.
- Manage administrative and commercial aspects.
- Provide usage and rating metrics.

The main objectives of the application portal are grouped into four areas of action described in detail below.

3.2. Discovery and adoption

The portal must facilitate the discovery and selection of suitable applications:

Organised and accessible catalogue

- Clear categorization by application type and use case.
- Advanced search system with relevant filters.
- Personalized recommendations according to profile and context.
- Featured new and popular apps.

Full information

- Detailed files of each application with screenshots and videos.

- Technical and functional documentation.
- Usage and compatibility requirements.
- Scientific evidence to support it.
- Information on costs and licensing model.
- Data necessary for its operation and data generated.

Rating system

- Verified user opinions and ratings.
- Scores for different aspects (usability, functionality, etc.).
- Statistics of use and adoption.
- Testimonials and success stories.

Guided adoption process

- Differentiated adoption flows according to the type of application.
- Implementation guides and best practices.
- Support for data migration if necessary.
- Initial training for users.

3.3. Prescription management

The portal must support the professional prescription of applications:

Prescription model

- Integration with existing prescription systems.
- Validation of eligibility criteria.
- Management of consents and authorizations.
- Monitoring of use and adherence.

Tools for professionals

- Specific search engine by prescription.
- Prescription guides by pathology/condition.
- Warnings and contraindications.
- Patient monitoring dashboard.

Access management

- Prescription-based access control.
- Management of licenses and subscriptions.
- Renewal and revocation of access.
- Usage audit.

Integration with clinical systems

- Connection with the Health Record of Catalonia and other electronic medical record systems.
- Integration of data and results.
- Clinical notifications and alerts.
- Monitoring of health outcomes.

3.4. Commercial and administrative management

The portal must manage the commercial and administrative aspects:

Marketing models

- Support for different pricing models.
- Management of subscriptions and licenses.
- Secure payment system.
- Turnover.

Supplier management

- Registration and validation of suppliers.
- Management of contracts and agreements.
- Data analytics.
- Support for the resolution of incidents.

Legal and regulatory aspects

- Management of terms and conditions.
- Compliance with the GDPR and other applicable regulations.
- Consent management.
- Audit and traceability.

Analytics

- Dashboards for use.
- Usage and adoption reports.
- Satisfaction metrics.
- Business KPIs.

3.5. Support and quality of service

The portal must ensure the quality of the service:

User support

- Multi-level ticket system.
- Knowledge base and FAQ.
- Chat and phone support.
- User community.

Incident management

- Incident notification system.
- Monitoring and resolution.
- Proactive communication.
- Impact analysis.

Quality monitoring

- SLA tracking.
- Satisfaction surveys.
- Trend analysis.
- Identification of improvements.

Continuous improvement

- Collecting feedback.
- Suggestion management.
- Roadmap for improvements.
- Communication of updates.

3.6. Types of applications and products

The portal must support different types of applications and products, each with its own specific characteristics and requirements. This diversity is key to meeting the different needs of the health system and promoting innovation in all areas.

3.6.1. Primary Use Applications

Applications aimed at providing direct support to healthcare processes and health management:

Clinical and care management applications

- Specialized clinical workstations.
- Healthcare process management systems.
- Clinical documentation applications.
- Tools for coordination between professionals.

Monitoring and Tracking Apps

- Vital signs monitoring systems.
- Chronic disease tracking apps.
- Tools for controlling adherence to treatment.
- Clinical alert and notification systems.

Telemedicine applications

- Medical videoconferencing platforms.
- Telemonitoring systems.
- Teleconsultation tools.
- Telerehabilitation platforms.

Mobile health applications (mHealth)

- Apps to promote healthy habits.
- Health and symptom diaries.
- Medication management tools.
- Self-care support apps.

Applications for medical devices and *wearables*

- Device data capture applications.
- Measurement interpretation systems.
- IoT device integration platforms.
- Calibration and maintenance tools.

3.6.2. Secondary use applications and/or data products

Products that generate value through the analysis and processing of clinical data:

Analysis and clinical research products

- Cohort analysis systems.
- Tools for epidemiological studies.
- Predictive and stratification models.
- Platforms for analysing health outcomes.

Management and planning products

- Dashboards for decision-making.
- Resource planning tools.
- Healthcare quality analysis systems.

- Population management platforms.

Clinical decision support products

- Diagnostic aid systems.
- Prescription support tools.
- Personalized medicine algorithms.
- Warning and prevention systems

Training & Simulation Products

- Clinical simulators with real data.
- Adaptive learning tools.
- Competency validation systems.
- Virtual practice environments.

3.6.3. Platform services

Transversal services that complement the applications and products:

Integration Services

- Connectors with external systems.
- Data transformation services.
- Standards adapters.
- Courier services.

Security services

- Identity and access management.
- Encryption and signature services.
- Audit and traceability.
- Consent management.

Infrastructure services

- Data storage.
- Distributed processing.
- Caching services.
- Load balancing.

Support services

- Notification management.

- Geolocation services.
- Document management.
- Translation services.

3.6.4. Distribution models

The portal must support different distribution models depending on the nature of the application or product:

Software as a Service (SaaS)

- Applications hosted and managed in the cloud.
- Access via the web or mobile application.
- Automatic updates.
- Pay per subscription.

On-premise *applications*

- Deployment in local infrastructure.
- Management and maintenance by the organization.
- Integration with local systems.
- Perpetual or temporary license.

Hybrid solutions

- On-premises and cloud components.
- Data synchronization.
- Offline operation.
- Mixed licensing models.

Open source

- Approved open source licenses.
- Accessible code store.
- Complete documentation.
- Developer community.

3.7. Main components

This section describes the fundamental elements that make up the structure of the application portal, including the catalogue of applications to organise and present the available solutions, the approval system to guarantee quality and safety, and the commercial management to manage the business aspects.

3.7.1. Catalogue of applications

- System of categories and tags.
- Advanced search engine.
- Detailed application sheets.
- Rating and comment system.
- Usage statistics.

3.7.2. Homologation system

- Homologation process.
- Verification of technical requirements.
- Security and privacy validation.
- Functional and usability validation.
- Version and update management.

3.7.3. Commercial management

- Subscription and licensing system.
- Payment and billing management.
- Consumption and usage analytics.
- Support for different business models.

4. Homologation process

The homologation process is a fundamental element in the ecosystem of the open health platform, acting as a guarantor of the quality, safety and technical adequacy of all the applications and services that are integrated into it. This process is inspired by leading European initiatives such as the German DIGA (*Digitale Gesundheitsanwendungen*) and the French PECAN (*Prise En Charge de l'ANimation numérique en santé*), which have been pioneers in the systematic integration of digital applications in their public health systems.

From the German experience with the DIGA, the Catalan model adopts rigor in the evaluation and focus on the evidence of health outcomes, as well as direct integration with the prescription and reimbursement systems. From the French PECAN model, the emphasis is on supporting professionals and patients in the adoption of digital solutions, as well as the gradual focus on the incorporation of new applications into the catalogue of services.

It is important to note that the homologation included in this tender focuses on technological aspects and integration with the platform. Evaluation from a health perspective, including scientific evidence, clinical validity and impact on health, is articulated through the channels established with the Agency for Health Quality and Assessment of Catalonia (AQuAS), which is the reference body in the evaluation of health technologies in the Catalan health system.

This technical approval process has been designed to balance two apparently opposing needs: on the one hand, the need to establish rigorous controls that guarantee the safety and technological quality of the solutions, and on the other, the need to offer an agile process that does not pose a barrier to innovation and the continuous development of new solutions.

Homologation is not conceived as a mere administrative procedure, but as a collaborative process between developers and the platform, which provides added value in the form of improvements in the quality, security and usability of the applications. The process incorporates accompaniment and support mechanisms that help developers to comply with the established technical requirements, thus turning the homologation into an opportunity for improvement and learning.

The coordination between this technical approval and the health assessment carried out by the AQuAS must guarantee a complete process that ensures both the technological soundness and the clinical validity of the solutions that are integrated into the platform, thus providing maximum value to the health system.

4.1. Objectives

The homologation process pursues the following strategic objectives:

- **Technical Quality Assurance**: Ensuring that all applications meet established technical standards and integrate correctly with the platform.
- **Agility and efficiency**: Provide an agile and predictable approval process that does not

pose a barrier to innovation.

- **Transparency and objectivity**: Establish clear and objective evaluation criteria, accessible to all developers.
- **Continuous improvement**: To promote the continuous improvement of applications through constructive feedback during the approval process.
- **Institutional coordination**: Ensure effective coordination with the AQuAS and TICSalut for the evaluation of health aspects.

4.2. Phases of the process

This section details the sequential stages of the approval process, starting with the registration and initial application, through the technical and functional validations, up to the final publication of the application in the catalogue. Each phase is designed to guarantee the quality and adequacy of the solutions.

It should be noted that this set of stages is an initial proposal. It is expected that the bidder will be able to propose improvements. The final version to be implemented will have to be agreed with the CTTI and CatSalut.

1. **Registration and application**
   - Developer/company registration.
   - Description of the application.
   - Technical and functional documentation.
   - Test plan.
2. **Technical validation**
   - Architecture review.
   - Security analysis.
   - Integration tests.
   - Performance verification.
3. **Functional validation**
   - Review of functionalities.
   - Usability validation.
   - User testing.
   - Accessibility verification
4. **Publication**
   - Final approval
   - Deployment to production
   - Publication in the catalogue
   - Commercial activation.

4.3. Homologation criteria

It establishes the requirements and standards that applications must meet in order to be approved, divided into three main areas: technical requirements to ensure compatibility and performance, security requirements to protect data and access, and functional requirements to guarantee usability and value for the user.

4.3.1. Technical requirements

- Compliance with architectural standards.
- Integration with platform services.
- Performance and scalability.
- Observability and monitoring.

4.3.2. Security requirements

- Compliance with GDPR and applicable regulations.
- Identity and access management.
- Encryption and data protection.
- Traceability and auditing.

4.3.3. Functional requirements

- Alignment with system needs.
- Usability and user experience.
- Accessibility.
- Documentation and support.

5. Application prescription

The prescription of applications represents a paradigmatic change in health care, introducing digital applications and services as a therapeutic complement within the health system. This innovative model allows healthcare professionals to recommend and assign applications to patients as an integral part of their treatment plan, similar to how medications or other healthcare interventions are prescribed.

This new digital prescription model requires a robust and secure system that guarantees the adaptation of the applications to the specific needs of patients, facilitates the monitoring of its use and allows its effectiveness to be evaluated. The prescription of applications is not limited to a simple recommendation, but involves a complete process that includes the initial evaluation, the selection of the most appropriate application, the personalized configuration according to the patient's needs, the monitoring of use and the evaluation of the results obtained.

A differential element of the Catalan model is its commitment to interoperability and open standards, which allows for deep integration of prescribed applications with existing health information systems. This integration is carried out both with current systems and, natively, with the future Health History of Catalonia, which will act as the backbone of all health information. This approach ensures that the data generated by the prescribed applications are naturally integrated into the patient's medical record, thus facilitating more effective follow-up and better coordination of care.

The prescription system integrates naturally into the workflow of healthcare professionals, providing decision support tools that facilitate the selection of the most appropriate applications according to the available evidence and the specific characteristics of each patient. In addition, it incorporates monitoring mechanisms that allow professionals to monitor adherence and the results obtained.

Key elements of this prescription include bidirectional integration with healthcare information systems, alignment with established healthcare processes, and consideration of the specific cultural and social aspects of our healthcare environment. The native integration with the Health History of Catalonia ensures that both the prescriptions and the data generated by the prescribed applications are an integral part of the patient's medical history, thus providing a holistic view of their health and their care process.

5.1. Objectives

The application prescription system is aimed at the following objectives:

- **Healthcare integration**: Incorporate the prescription of applications as one more therapeutic tool within the care process.
- **Interoperability**: Guarantee full integration with the Catalan Health Record and other healthcare information systems.
- **Clinical decision support**: To provide tools that facilitate the selection of the most

appropriate applications according to the available evidence.

- **Monitoring and evaluation**: To facilitate the monitoring of the use and the evaluation of the results of the prescribed applications.
- **User experience**: Ensure a seamless experience for both professionals and patients in the use of prescribed applications.

5.2. Prescription model

The system will support the prescription of applications by health professionals, following a model similar to pharmaceutical prescription:

- Identification of patient needs.
- Selection of suitable application.
- Specific parameterization.
- Monitoring and evaluation.

5.3. Components of the prescription system

It describes the elements necessary to implement the prescription model, including the catalogue of prescription applications, systems of criteria and recommendations, integration with existing systems, and monitoring and evaluation tools:

- Catalogue of prescriptible applications.
- System of criteria and recommendations.
- Integration with existing prescription systems.
- Monitoring of use and adherence.
- Evaluation of results.

6. Transversal services

Transversal services constitute the critical infrastructure that supports the entire ecosystem of the open platform in health, providing the fundamental capabilities necessary to guarantee the safe, efficient and reliable operation of all applications and services. These services are essential for maintaining the quality, safety, and performance standards demanded by a modern healthcare system.

The implementation of these services follows a modular and scalable approach, allowing their evolution and continuous improvement without affecting the operation of the applications that depend on them. Transversal services act as an abstraction layer that simplifies the implementation of complex functionalities, allowing developers to focus on the specific functionalities of their applications.

A key aspect of these services is their "as a service" nature, which allows them to be consumed flexibly according to the needs of each application, thus optimizing the use of resources and facilitating scalability. In addition, they incorporate resilience and high availability mechanisms to guarantee the continuity of the service at all times.

6.1. Objectives of the transversal services

The transversal services pursue the following objectives:

- **Operational reliability**: Ensure the continuous and reliable operation of all platform components.
- **Comprehensive security**: Provide a robust security framework that protects data and access.
- **Scalability**: Ensure that services can grow and adapt according to the needs of the system.
- **Observability**: Maintain complete visibility of the operation of all components.
- **Operational efficiency**: Optimize the use of resources and automate operational processes.

6.2. Observability

It details the platform's monitoring and follow-up mechanisms, including availability control, performance measurement, centralized log management, distributed traceability and alert system:

- Availability monitoring.
- Performance metrics.
- Centralized logs.
- Distributed traceability.

- Alerts and notifications.

6.3. Safety

It specifies the security components and measures implemented, covering identity management, access control, security auditing and incident and vulnerability management:

- Identity management.
- Access control.
- Security audit.
- Incident management
- Vulnerability management.

6.4. Support

It describes the structure and organization of the support service, including different levels of technical support, incident management, knowledge base, training and developer community:

- Multi-level technical support.
- Incident management.
- Knowledge base.
- Education and training.
- Developer community.

7. Key indicators (KPIs)

Key performance indicators (KPIs) constitute the reference framework for measuring and evaluating the success and impact of the open health platform in all its aspects. This system of indicators has been designed to provide a holistic view of the operation of the platform, covering both technical, functional and business aspects.

The selection and definition of these indicators has been carried out with the aim of providing meaningful and actionable metrics that allow informed decision-making at all levels. KPIs are not simple static measures, but are part of a dynamic system of continuous improvement that allows you to identify trends, anticipate problems and evaluate the impact of the different initiatives and changes implemented.

The KPI system is designed to be transparent and accessible to all actors in the ecosystem, providing different views and levels of detail according to the needs of each user profile. In addition, it incorporates automated data collection and analysis mechanisms that guarantee the objectivity and reliability of the measurements, as well as their availability in real time.

7.1. Objectives of the key indicators

The system of key indicators is established with the following objectives:

- **Comprehensive monitoring**: Provide a complete view of the operation of the platform in all its aspects.
- **Decision-making**: Facilitate informed decision-making based on objective data.
- **Continuous improvement**: Identify areas for improvement and measure the impact of corrective actions.
- **Transparency**: To offer visibility on the performance and impact of the platform to all the actors involved.
- **Impact assessment**: To measure the real impact of the platform on the health system and on the health of citizens.

7.2. Technical KPIs

It establishes the key indicators to measure the technical performance of the platform, including metrics such as availability, response time, error rate, and test coverage:

- Availability of the service.
- Response time.
- Error rate.
- Test coverage.
- Development cycle time.

7.3. Functional KPIs

It defines the indicators to evaluate the use and adoption of the platform, measuring aspects such as the number of published applications, active users, ratings and satisfaction:

- Number of published applications.
- Number of active users.
- Evaluation of applications.
- Adoption rate.
- User satisfaction.

7.4. Business KPIs

It specifies the metrics aimed at evaluating the commercial success and sustainability of the platform, including indicators such as the number of active developers, publication time, conversion rates and return on investment:

- Number of active developers.
- Time to publication.
- Conversion rate.
- Revenue generated.
- Return on investment.

Generalitat de Catalunya
Centre de Telecomunicacions
i Tecnologies de la Informació

/Salut

TENDER FOR THE CONSTRUCTION OF AN OPEN PLATFORM IN HEALTH - ARCHITECTURE COMPONENTS, APPLICATION MARKET AND PLATFORM SERVICES

APPENDIX 4: ORCHESTRATION AND PROCESSES

CTTI/2025/113

Barcelona, January 2025

Unió Europea
Fons Europeu
Next Generation

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD

Pla de Recuperació, Transformació i Resiliència

Next Generation Catalunya

Generalitat de Catalunya

Version history and contributions

Description of the review	Author	Date	Version
Initial draft		19/01/25	0.1
Final Version Review and Release		09/02/25	0.2
Simplification of the version		11/02/25	0.3

Index

1. Introduction

This annex is dedicated to defining the services and functionalities that will have to respond to the elements included in the proposal in the domain of orchestration and management of processes in the field of Health. The objective is to guarantee the integration of care processes, interoperability between applications and the traceability of clinical decisions through orchestration tools and process management systems that are reusable by all elements and actors of the platform.

The orchestration and process management component is a fundamental piece of the open platform, as it acts as a backbone that coordinates and integrates the rest of the components. Its ability to model, execute and monitor complex healthcare processes makes it a key element in achieving more integrated and people-centred healthcare.

The central element of this component is the process engine and a repository of states of the process instances, which must be able to govern both the presentation of each module through the different user interfaces (clinical, administrative or patient-oriented workstation), as well as the API contracts offered by each application and the processing of events generated in other applications approved on the platform. This engine must support the most relevant standards in business process modelling (BPMN), case management (CMMN) and decision rules (DMN), adapting them to the particularities of the healthcare sector and being able to interact with CDS and AI tools.

The critical nature of care processes requires this component to provide the highest levels of reliability, performance, and safety. It must guarantee the continuity of the service 24/7, ensure the integrity and confidentiality of clinical information, and provide robust traceability and audit mechanisms. At the same time, it must be flexible enough to adapt to different needs and contexts of use, allowing the personalization and evolution of processes according to the changing needs of the health system.

Although the tender asks for support for specific standards, the environment must be able to handle decision rule definitions in other standards and interconnection with external engines through events and APIs.

1.1. Purpose and scope

This functional, technical and governance annex details the specific requirements for the system of orchestration and management of care processes that is part of the open health platform. The main objective is to establish a technological framework that allows:

- To model and execute care processes in a flexible and adaptable way.
- Coordinate the execution of activities between different actors in the health system.
- Integrate different applications and systems under a cohesive process model.
- Monitor and analyse the execution of processes for continuous improvement.

The scope of the orchestration system includes:

- Process execution engine.
- Declarative rules engine
- Modeling and design tools.
- Platform integration components.
- User interfaces and monitoring.
- Governance and control systems.
- Repository of process definitions.
- Interoperability with CDS tools and other AI modules and agents

1.2. Context within the open platform

The orchestration system is a central component of the open platform that acts as an integration layer between:

- The openEHR-based clinical data repository.
- The native forms tool of openEHR (in the bidding process).
- Apps in the app market.
- Existing corporate systems.
- The user interfaces of professionals and patients to be developed in the context of the Health History of Catalonia.

Its main function is to coordinate the execution of the defined care processes, ensuring that:

- The activities are carried out in the right order and at the right time.
- Information flows correctly between systems.
- The traceability and audit of the actions is maintained.
- Business rules and clinical decisions are correctly applied.

The processes of construction and homologation of developments that make use of orchestration and processes must be integrated into the development and homologation models of the open platform as a whole.

1.2.1. Process Modeling Standards

The complexity of care processes requires the combined use of different modeling standards that allow capturing both structured workflows and the most dynamic and adaptive aspects of healthcare. The complementarity between BPMN, CMMN and DMN, unified under the umbrella of BPM+ Health, provides the necessary framework to accurately and comprehensively model the different aspects of care processes.

BPMN provides the ability to define structured and predictable workflows, such as clinical protocols or standardized clinical pathways. CMMN allows you to manage more dynamic and adaptive situations, typical in the care of complex or chronic patients. DMN facilitates the formalization of clinical decision rules, allowing their automation and ensuring consistency in their application. The integration of these standards under the specifications of BPM+ Health guarantees their specific applicability in the healthcare field.

BPMN 2.0 (Business Process Model and Notation)

- Full support for all elements of the BPMN 2.0 specification.
- Implementation of advanced workflow patterns.
- Specific elements for clinical processes:
    - Clinical registration tasks.
    - Clinical events.
    - Collaboration between professionals.
    - Management of healthcare resources.
- Extension capacity for specific needs.
- Syntactic and semantic validation of models.

CMMN 1.1 (Case Management Model and Notation)

- Modelling of dynamic clinical cases.
- Management of clinical stages and milestones.
- Adaptive task planning.
- Elements of document management.
- Definition of roles and authorizations.
- Activation and termination rules.
- Integration with clinical indicators.

DMN 1.3 (Decision Model and Notation)

- Modeling of complex clinical decisions.
- Integration with clinical guides.
- Support for evidence-based rules.
- Rule versioning.
- Traceability of decisions.
- Validation of coherence.
- Reuse of components.

BPM+ Health

- Implementation of health profiles.
- Harmonization between BPMN, CMMN and DMN.
- Support for clinical process libraries.
- Validation according to GMP+ Health specifications.
- Exchange of models between platforms.
- Semantic integrity of models.

1.2.2. Interoperability standards

Interoperability is a fundamental requirement for the success of the open platform. The interoperability standards selected must guarantee not only the technical exchange of information, but also the preservation of its clinical significance throughout the care process. The adoption of internationally recognized standards is key to ensuring the sustainability and scalability of the platform.

The combination of HL7 FHIR, openEHR and IHE provides a comprehensive interoperability framework covering different aspects and levels of integration. FHIR provides a modern and agile model for clinical data exchange, openEHR provides a robust model for clinical knowledge management, and IHE defines the integration profiles necessary to ensure interoperability in specific use scenarios. The correct implementation of these standards is essential to achieve true integration of systems and processes.

Access to clinical and demographic data from the open platform

For CRUD information actions, data access interfaces must be accessed and used, incorporating security management and ensuring consistency and integrity

openEHR

- Integration with openEHR repository.
- Access to archetypes and templates.
- Management of AQL queries.
- Persistence of clinical data.
- Versioning of compositions.
- Management of terminologies.
- Semantic validation.
- SMART authentication and authorization on openEHR.

HL7 FHIR

- Implementation of FHIR R4 and R5 resources.
- Support for on-premises FHIR extensions.
- Validation of FHIR profiles.
- Management of FHIR terminologies.
- SMART on FHIR authentication and authorization.
- Subscriptions and notifications.
- Search and filter resources.

IHE

- Support for IHE integration profiles.
- Implementation of IHE flows.
- Management of actors and transactions.
- Conformity validation.
- Audit log.
- Safety according to ATNA.
- Identifier management.
- Documentation according to XDS

1.2.3. Flexibility and adaptability

In the healthcare environment, the ability to adapt to changing situations and specific needs is critical to the success of any information system. Care processes, by their very nature, require a high degree of flexibility to respond to the particularities of each patient, the preferences of professionals and the local characteristics of each healthcare organization. The platform must provide this flexibility without compromising the consistency and traceability of processes.

Flexibility must be manifested both in the initial design of the processes and in their execution, allowing real-time modifications to adapt to unforeseen situations or changes in the patient's condition. This adaptability must be supported by robust version control and traceability mechanisms that allow the changes made to be understood and audited.

Modification of processes in real time

- Dynamic changes in workflows.
- Adaptation to unforeseen situations.
- Exception management.
- Versioning of modifications.
- Rollback of changes.
- Traceability of modifications.
- Analysis of trends in the use of alternative paths to those initially established in the original process

Contextual personalization

- Adaptation by centre/service.
- Configuration by professional role.
- Local variations of processes.
- Management of specific resources.
- Parameterization of interfaces.
- User preferences.

2. Process Orchestration System Architecture

The architecture of the orchestration system constitutes the backbone on which all the care processes of the open health platform will be implemented. This architecture has been designed following principles of modularity, scalability and resilience, with the aim of supporting the inherent complexity of healthcare processes while maintaining the flexibility necessary to adapt to the changing needs of the healthcare system.

The proposed architectural design is inspired by reference architectures from other sectors that have demonstrated success in managing complex processes on a large scale, but adapting them to the particularities of the healthcare sector. Safety, traceability and availability are critical considerations that have influenced all design decisions, recognizing the sensitive nature of health information and the criticality of care processes.

2.1. Main components

The orchestration of care processes requires a modular and robust architecture that guarantees both flexibility in execution and the consistency and traceability of all operations. The main components of this architecture have been selected and designed specifically to respond to the unique challenges of the healthcare sector, such as the need to maintain continuity of care, the management of complex cases that require dynamic decisions, and coordination between multiple professionals and levels of care.

Each component fulfills a specific and critical function within the system, but it is their coordinated interaction that allows the complexity of care processes to be effectively managed. The modularity of the architecture facilitates not only the maintenance and evolution of individual components, but also the incorporation of new functionalities and adaptation to future needs of the health system.

The proposal must identify the elements that make up the architecture of the environment in the following points. The elements may be common to the rest of the platform's architecture, but it is requested that their functionality be specified in relation to the scope of the annex.

Process Execution Engine

Core component that implements the BPM+ Health standards (BPMN, CMMN, DMN):

- **Execution core**: Interprets and executes process definitions.
- **Status Manager**: Maintains the status of running instances.
- **Queuing system**: Manages asynchronous communication between components.

- **Transaction Manager**: Ensures consistency in execution.
- **Scheduler**: Manage scheduled tasks and timers.

Repository of definitions

Store and manage the definitions of processes and related elements:

- **Version Manager**: Version control of processes and rules.
- **Category system**: Organization and classification of definitions.
- **Validator**: Verifies the correctness of the definitions.
- **Search engine**: Facilitates the location of definitions.
- **Tag system**: Allows you to classify and relate definitions.

Rules engine

Manage the execution of business rules and decisions:

- **Rule interpreter**: Evaluates conditions and executes actions.
- **Rule caching**: Optimizes access to frequent rules.
- **Tracer**: Records the decisions taken and their justification.
- **Conflict Manager**: Resolves conflicts between rules.
- **Predicate evaluator**: Processes complex expressions.

Event system

Manage communication between components through events:

- **Event bus**: Integration with the platform bus
- **Filters**: Allows selective subscription to events.
- **Router**: Directs events to the right subscribers.
- **Persistence**: Stores events for auditing.
- **Monitor**: Monitors the flow of events.

2.2. Data model and integration

The effective management of care processes requires a robust data model that can capture both the structure of the processes and their state of execution, maintaining the consistency and traceability of the information at all times. This model must be flexible enough to adapt to the variety of healthcare processes, but at the same time rigorous enough to guarantee the integrity and security of clinical data.

Integration with other systems is a critical aspect of this architecture, as care processes often involve multiple information systems, both internal and external. The integration model has been designed to facilitate interoperability while maintaining the autonomy of the participating systems, using recognized standards in the healthcare sector and proven integration patterns.

The data model of the orchestration system must be designed to guarantee the consistency and traceability of all processes:

Persistence model (canonical model)

- **Definition data**: Stores definitions of processes and rules.
- **Execution data**: Maintains the status of active instances.
- **Historical data**: Records the history of complete executions.
- **Audit data**: Map out all actions and decisions.
- **Monitoring data**: Performance metrics and indicators.

Integration layer

- **Standard** adapters: Connection with common systems.
- **Custom plugins**: Integration with specific systems.
- **Transformers**: Conversion between data formats.
- **Validators**: Integrity verification in integrations.
- **Monitors**: Supervision of integrations.

2.3. Operating environments

The complexity of care processes and the criticality of clinical information make it essential to have a clear management strategy for operating environments. This strategy must allow the development and testing of new processes and functionalities without putting healthcare operations at risk, while guaranteeing the quality and security of all updates before they are deployed in production.

The segregation of environments is not only a good technical practice, but a fundamental requirement to ensure continuity of care and the protection of clinical data. Each environment is designed for a specific purpose and has the appropriate controls and security measures for its use, from development environments with synthetic data to the production environment with the highest levels of protection and monitoring.

The system includes several environments to guarantee quality and safety:

Development environment

- **Individual Sandbox**: Isolated space per developer.
- **Development tools**: IDEs and utilities.
- **Synthetic data**: Generation of test data.

- **Version control**: Source code management.
- **Continuous integration**: Test automation.

Integration environment

- **Complete system**: Replica of existing components in production.
- **Anonymized data**: Minimum set of real data.
- **Integration tests**: End-to-end validation.
- **Functional tests**: Internal functional validation.
- **Deployment testing**: Assessment that the application can be deployed in a productive environment.

Pre-production environment

- **Complete system**: Production replica with 50%-70% of the planned capacity in production.
- **Anonymized data**: Secure copy of real data.
- **Exploratory end-user testing**: End-to-end validation of the complete solution.
- **Performance tests**: Capacity evaluation.
- **Security tests**: Validation of protections.

Production environment

- **High availability**: Complete redundancy.
- **Advanced monitoring**: 24x7 supervision.
- **Automatic scaling**: Dynamic adjustment of resources.
- **Continuous backup**: Real-time backups.
- **Automatic recovery**: Self-recovery of errors.

3. Specific requirements

The requirements for which your support is specifically requested to be described are:

3.1. Functional requirements

3.1.1. Process design using BPMN 2.0

Full support for BPMN 2.0 is essential to model the sequential and structured aspects of care processes:

- **Intuitive visual editor**
    - Drag-and-drop interface.

    - Real-time validation.
    - Contextual suggestions.
    - Predefined templates.
    - Customization of styles.
- **Advanced BPMN elements**
    - Complex events.
    - Subprocesses.
    - Pools and lanes.
    - Conditional flows.
    - Error management.
- **Health extensions**
    - Specific clinical elements.
    - Integration with terminologies.
    - Care patterns.
    - Clinical indicators.
    - Safety rules.

3.1.2. Clinical Decision Modeling Using DMN

DMN support allows you to formalize and automate complex clinical decisions:

- **Decision tables**
    - Multiple inputs/outputs.
    - Complex rules.
    - Priorities.
    - Conflicts.
    - Validation.
- **Requirements Diagrams**
    - Sources of information.
    - Dependencies.
    - Impact.
    - Justification.
    - Traceability.
- **Clinical integration**
    - Clinical guides.
    - Protocols.
    - Alerts.
    - Contraindications.
    - Recommendations

3.1.3. Case-based process management using CMMN

Support for CMMN is crucial to manage more dynamic and adaptive aspects of care processes:

- **Case modeling**
  - Adaptive stages.
  - Dynamic planning.
  - Entry/exit criteria.
  - Roles and authorisations.
  - Clinical milestones.
- **Discretionary elements**
  - Optional tasks.
  - Human planners.
  - Activation rules.
  - Flexible dependencies.
  - Temporary restrictions.
- **Knowledge management**
  - Experience capture.
  - Case patterns.
  - Best practices.
  - Continuous learning.

3.1.4. Reusability. Importing BPMN, DMN and CMMN layouts

The tool must allow the import of BPMN, DMN and CMMN designs created in external tools. This functionality will ensure compatibility with other platforms used in the healthcare field and facilitate the transition to the new solution. The import must be accurate and maintain the logic and semantics of the processes.

3.1.5. Process Instance Management

The tool must provide tools to manage the different instances of a running process. This includes monitoring the status of each instance, identifying anomalies, and the possibility of manual intervention when necessary. It must guarantee the persistence of data and its integrity in real time.

- **Life cycle**
  - Creation.
  - Activation.
  - Suspension.
  - Finalization.
  - Filed.
- **Status check**
  - Persistence.
  - Consistency.
  - Recovery.
  - Versions.
  - Historical.
- **Operations**

    - Consultation.
    - Modification.
    - Cancellation.
    - Migration.
    - Filed.
- **State Machine**
    - Defined states.
    - Valid transitions.
    - Validations.
    - Actions.
    - Notifications.
- **Monitoring**
    - Current state.
    - Progress.
    - Alerts.
    - KPIs.
    - Trends.
- **Historical**
    - Transitions.
    - Decisions.
    - Modifications.
    - Interventions.
    - Audit.

3.1.6. Rule management

The management of business rules in the healthcare field requires a balance between the formalization of protocols and clinical guidelines and the flexibility necessary to adapt to specific cases. The system must allow the definition, maintenance and execution of complex rules while guaranteeing their traceability and justification.

- **Defining Rules**
    - Expressions.
    - Conditions.
    - Actions.
    - Priorities.
    - Versions.
- **Rule execution**
    - Evaluation.
    - Chaining.
    - Conflict resolution.
    - Cache.
    - Performance.
- **Life cycle management**

  - Versions.
  - Activation.
  - Deactivation.
  - Tests.
  - Deployment.

3.1.7. Access control and security

It must have a robust authentication system based on the standards defined in the platform's architecture. Additionally, it must include a granular permissions management mechanism to determine what actions each user can take within the platform.

3.1.8. Integration with third-party systems

The tool must be able to integrate with other hospital information systems and platform components through standardized APIs. This includes synchronization with the Electronic Medical Record, interaction with notification systems and the exchange of information with data analytics platforms to improve decision-making.

3.1.9. Generation and reception of events

The platform must allow the generation and reception of events that facilitate the automation of processes. These events must be managed by an orchestration system that allows them to be monitored and recorded to ensure transparency in the execution of the processes.

3.1.10. Flexibility and restrictions on process modification

On-the-fly composition of process variants must be allowed at runtime and a process must be marked as non-modifiable according to usage policies related to the user profile. It must be possible to prevent immutable processes from being cloned and creating variants.

3.1.11. Process monitoring and analytics

Process monitoring and analytics are essential to ensure quality of care and continuous improvement. The system must provide real-time visibility into the execution of processes and advanced analytics capabilities to identify patterns and opportunities for improvement.

- **Real-time monitoring**
  - Dashboards.
  - Alerts.
  - KPIs.
  - Trends.
  - Predictions.

- **Advanced analytics**
  - Process mining.
  - Patterns.
  - Bottlenecks.
  - Simulation.
  - Optimization.
- **Reports and dashboards**
  - Performance.
  - Quality.
  - Efficiency.
  - Costs.
  - Clinical results.

3.2. Usability requirements

3.2.1. Features of Process Designer

The process designer is a critical tool that must allow users to model care processes in a visual and intuitive way. The interface needs to strike the balance between the power needed to model complex processes and the simplicity required to make it accessible to users with varying levels of technical expertise.

The tool implements multiple levels of abstraction that allow users to work with the appropriate level of detail for their task, from high-level views to detailed technical specifications.

Visual Editor

- **Interactive canvas**
  - Zoom & pan.
  - Grid & snap.
  - Multi-select.
  - Alignment.
  - Guides.
- **Palette of elements**
  - BPMN elements.
  - CMMN elements.
  - DMN elements.
  - Personalized elements.
  - Templates.

Advanced features

- **Real-time validation**
  - Syntactic validation.
  - Semantic validation.
  - Good practices.
  - Notices..
  - Suggestions.
- **Collaboration**
  - Multi-user editing.
  - Guest reviews.
  - Version control.
  - Change control.
  - Sharing.

3.2.2. Training and support for users

It should include guides, tutorials, and interactive support mechanisms to facilitate user adoption of the platform.

This document establishes the specific requirements for the tender, ensuring that the tool meets the functional and technical needs required for its implementation in the health field.

3.3. Requirements for the canonical model

The canonical model to be managed must be linked to no specific technology and allows the management of processes through standardized entities. Through APIs, it facilitates the interoperability of designed processes and rules with other orchestration engines and systems.

This model must allow the monitoring and analysis of process activity.

Minimally:

3.3.1. Entities of the Model

- **Processes**: They represent workflows and constitute the core of management. They can be created, updated, completed or canceled.
  - Created with new definitions.
  - Updated as needed.
  - Completed when they achieve their goals.
  - Cancelled when necessary

- **Activities**: Subunits within a process, corresponding to specific tasks. They can be created, completed or canceled.
  - Created as part of a process.

  - Completed when the objectives are achieved.
  - Cancelled if necessary.
  - Monitored by follow-up.

- **User Tasks**: Actions assigned to users, managed by creating, assigning, completing or canceling.
  - Creation and assignment.
  - Status tracking.
  - Completion or cancellation.
  - Notifications and reminders.
- **Incidents**: Registration of unwanted events or errors within processes. They can be created and solved.
  - Detailed record.
  - Classification by type.
  - Assignment of managers.
  - Follow-up until resolution.
- **Control Commands**: Commands to trigger actions within the system, such as posting messages or sending signals.
  - Posting messages.
  - Sending signals.
  - Activation of flows.
  - Status control.

3.3.2. Models and Attributes

The canonical model defines the following main data structures:

Process definitions

- **Definition of process**:
  - Unique identifier.
  - Descriptive name.
  - Version.
  - Associated metadata.
  - Validations required.
- **Instance of process**:
  - Execution status.
  - Start date.
  - Last updated.
  - Base definition.
  - Affected subjects.
  - Specific details.

  - Associated resources.

Operational elements

- **Subject of the process**:
  - Unique identifier.
  - Scope of application.
  - Specific properties.
  - Relationships with other elements.
- **Functional status**:
  - Name of the state.
  - Start timestamp.
  - Transition conditions.
  - Validations required.

Support elements

- **Metadata**:
  - Key-value pairs.
  - Background information.
  - Classification data.
  - Traceability elements.
- **Activities** (within a process instance)
  - Key
  - Description
  - Type
  - State
  - Start time
- **Comments**:
  - Process identifier.
  - Text of the comment.
  - Date and time.
  - Author.
  - Associated metadata.
- **External references**:
  - Unique identifier.
  - URI of the resource.
  - Reference type.

- **Input variables**: Subject Proxy of the activity related to each step of the process

- **Policies**: Rules for accessing or restricting a resource. (Resource, permissions, effect)

3.3.3. Activity Events

- Cancellation of an activity.
- Completion of an activity.
- Creation of a new activity.

3.3.4. Process Events

- Creation of a new process instance.
- Completion of a process instance.
- Cancel a process instance.
- Updating a process instance.

3.3.5. User Task Events

- Assigning a user task.
- Completion of a user task.
- Canceling a user task.
- Creating a user task.
- Notify a person of a task.
- Expiration of the term of a user task.
- Update a user task.

3.3.6. Incident Events

- Create an incident.
- Resolution of an incident.

3.3.7. Execution Commands

- Command to cancel a process instance.
- Command to start a process instance.
- Command to update a process instance.
- Command to assign a task to a user.
- Command to complete a user task.
- Command to indicate that the time to run a task has expired.

3.4. Technical requirements

In addition to the general technical requirements of the platform included in Annex-2 Architecture and Annex-8 Execution Conditions, due to their relevance, it is requested that the support elements for this module be explicitly described by:

3.4.1. Integration with openEHR using the clinical data access module

The effective integration of clinical information with a process orchestration system requires special care to ensure that care processes can access and manipulate this information consistently and securely.

To manage this integration, the following is required:

- Read operations
  - AQL consultations.
  - OpenEHR templates.
  - Versions of compositions.
- Write operations
  - Access to APIs and clinical data access services
  - Traceability
- Access to the CKM repository and the clinical data access module
- Access to ontology servers
  - Mappings
  - Subsets

3.4.2. Integration with forms and apps

It must allow the call and response to components developed or executed with these tools, maintaining the management of interactions between them.

Integration with forms and applications represents the layer closest to the end user, where care processes materialize in specific interfaces and interactions. This integration should provide a smooth and consistent experience, hiding the underlying complexity while maintaining all quality and security guarantees.

Form integration

- **Dynamic Rendering**

  - Real-time validation.
  - Automatic calculations.
  - Contextual help.
  - Responsive design.
- **Status management**
  - Local persistence.
  - Synchronization.
  - Undo/Redo.
  - Self-saved.
  - Conflict resolution.

Application integration

- **Micro-frontends**
  - Dynamic composition.
  - Isolation.
  - Communication between modules.
  - Management of dependencies.
  - Versioning.
- **Frontend APIs**
  - Shared context.
  - Events.
  - State management.
  - Routing.
  - Telemetry.

3.4.3. Interoperability

Interoperability with external systems is essential in an increasingly interconnected healthcare ecosystem. This interoperability must be guaranteed both at a technical and semantic level, ensuring that the information shared maintains its meaning and context.

The execution of processes must allow interoperability through recognized standards in the health sector, providing the necessary mechanisms to guarantee the security and traceability of information exchanges.

- **Health standards**
  - HL7 v2.
  - HL7 FHIR.
  - DICOM.
  - IHE.
  - CDA.
- **Technical standards**
  - REST.

  - SOAP.
  - WebSocket.
  - JMS.
  - AMQP.

3.4.4. Version control

Version control in a healthcare process orchestration system goes beyond typical source code management. It must consider all the artifacts that are part of the processes, from flow definitions to decision elements, business rules and integrations. It is crucial to maintain consistency between all these elements while allowing their independent evolution.

The version control system must implement mechanisms that guarantee the complete traceability of all changes, allowing us to understand who made each modification, why it was made and what its impact was.

Version management

- **Semantic versioning**
  - Major versions.
  - Minor versions.
  - Patches.
  - Branching.
  - Merging.
- **Versioned artifacts**
  - Processes.
  - Rules.
  - Forms.
  - Integrations.
  - Configurations.

Change control

- **Approval workflow**
  - Request.
  - Review.
  - Approval.
  - Implementation.
  - Verification.
- **Documentation**
  - Changelog.
  - Release notes.
  - Impact.
  - Rollback.

  - Dependencies.

3.4.5. Specific monitoring and dashboards

Dashboards and monitoring tools are essential to provide visibility on the execution of care processes. These interfaces must present complex information in a clear and comprehensible way, allowing users to quickly identify situations that require their attention.

The design of dashboards prioritizes clarity and visual hierarchy, ensuring that the most important information is immediately visible while maintaining access to more granular details when needed.

Operational dashboards

- **Real-time views**
  - General situation.
  - Active processes.
  - Alerts.
  - Performance.
  - Resources.
- **Detailed analysis**
  - Drill-down.
  - Filtering.
  - Comparatives..
  - Trends.
  - Export.

Views

- **Graphics**
  - Process map.
  - Temporary views.
  - Indicators.
  - Heat maps.
  - Network graphics.
- **Tables and lists**
  - Listed.
  - Tasks.
  - Event logs.
  - Reports.
  - Exports.

3.4.6. Repository of processes and rules

Managed environment for developments with service characteristics similar to that of the platform's repository of elements.

The module must have repository functions that provide service to the canonical data model that allows the management of definitions and management of the execution of processes and rules.

It will be necessary to uniquely identify the development, the standard in which it is defined and its interfaces with other systems and with users in the form of "user proxy".

Version: 0.0

ANNEX 5 TO THE SPECIFIC TECHNICAL SPECIFICATIONS FOR THE CONSTRUCTION OF AN OPEN HEALTH PLATFORM – USE CASES

File no.: CTTI/2025/113

Annex I. Use cases of the open platform for evaluation

The objective of this annex is to propose 3 use cases that capture most of the main functionalities that the open platform architecture must provide and a series of objective indicators to evaluate each use case.

1. Use case 1: Vaccination card

1.1 Overview

Application that shows the immunisation data of a specific citizen and their family members of whom they are the authorised guardian and that is integrated into the "La Meva Salut" application.

1.2 Evaluation objective

It is an application whose main functionality is the reading of clinical data from the clinical data repository and the demographic data service to establish the relationship between the index citizen and the potential citizens of the legal guardian.

1.3 Basic and deliverable functionalities

The application must comply with the following functional requirements that are specified by points:

- Frontend that can be integrated into the "La Meva Salut" application (as a citizen portal) where, based on the information of the citizen who is authenticated (information available in a token), it is possible to select the data of the citizen himself or his tutors.
- The following relevant data for each immunisation received will be displayed: Name of the vaccine, protected disease (disease or pathogen that it prevents), date of administration, number of doses (1st dose, booster dose, etc.), batch of the vaccine, route and place of administration, administration centre and name of the healthcare professional who has administered.
- Deployment of backend microservices (if necessary) on the open platform for data ingestion/modification.
- Development of the solution in the development, pre-production and production environments provided by the open platform architecture.

This translates into the following deliverables for this use case:

- Source code of the solution developed in the development sandbox saved in the official CTTI repository.
- Functional manual of the basic functionalities of the application.
- Proposal for a continuous monitoring service to evaluate the operation in production.

- Technical manual on its deployment in the architecture of the open platform according to guidelines.

2. Use case 2: Third-party application integration

2.1 Overview

This use case consists of the integration of a *full stack* application developed in another environment but which consumes, writes and updates data from the platform's services. The integration of a critical workstation developed within the framework of a project is proposed as a use case.

2.2 Evaluation objective

The effective integration of an application developed in another environment (Critical Workstation) with the architecture of the open platform will be evaluated, including data services (write, read, update, delete) and the consumption of other necessary services (terminology server, demographic server, etc.).

2.3 Basic and deliverable functionalities

The use case must meet the following requirements that are specified by points:

- Testing of the APIs of the different services (data services and others) in a pre-production environment to facilitate integration.
- The integration of the APIs must require the authentication method (JWT) specified in the architecture annex.
- Testing of frontend injection in other applications (e.g. Historial de Salut de Catalunya) in a pre-production environment.
- Putting the application integration into production.

This translates into the following deliverables for this use case:

- Pre-production environments for testing the different integrations (including frontend injection).
- Putting into production the effective integration of the critical station (where its default, another third-party application).
- Continuous monitoring services to evaluate effective integration into production.
- Technical manual on the integration of a third-party solution with the open platform architecture, including pre-production functionalities.

2.4

3. Use case 3: Development of a support application for healthcare pathways

3.1 Overview

This use case consists of developing an end-to-end application using all the available services of the open platform. The implementation of a clinical route for low back pain, a very common pathology in the population, is proposed, based on a published clinical guideline (

https://ics.gencat.cat/web/.content/Assistencia/esquena/guia-lumbalgia.pdf). The application provides technological support from the first contact of the patient with low back pain in primary care to the development of a therapeutic plan that may include the intervention of other health actors and/or care resources.

3.2 Evaluation objective

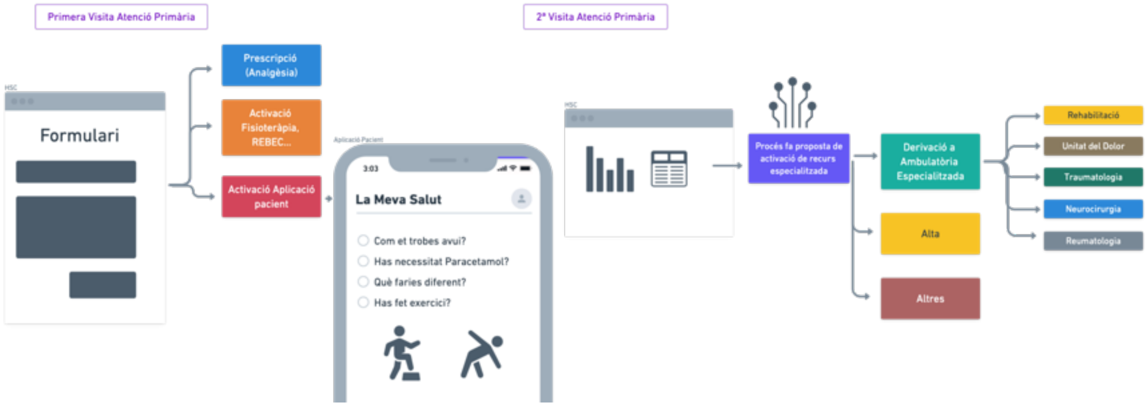
It is an application that requires the use of the main components of the open platform: data services (writing, reading and updating), process engine, development and testing environments, execution core and application market. It is necessary to demonstrate how the process engine orchestrates the different services and how it consistently applies clinical guidance.

3.3 Basic and deliverable functionalities

The application must respond to the following functional requirements to support the low back pain care process in accordance with the clinical guidelines mentioned above:

- Modeling the openEHR elements that are part of the use case
- BPMN/CMMN/DMN modeling and/or decision rules to be used in the use case
- Activation of a data entry form within the work environment based on an event corresponding to a diagnosis.
  This form will incorporate information obtained from access to clinical data in openEHR format and must allow the entry of clinical data to be updated.
- From the complete form, a process will be instantiated (modelled using BPMN) that will activate a therapeutic plan that includes different actions: Medication prescriptions, PROMa and sequence of follow-up visits.
- Submission of a form to consult the status of the process with the possibility of consulting the initial form
- Submission of a form to define the result of a follow-up visit allowing the professional to change the timing of the next visit

Figure 1 shows a possible functional definition of the low back pain process.


Primera Visita Atenció Primària
2ª Visita Atenció Primària
HSC
Formulari
Prescripció (Analgèsia)
Activació Fisioteràpia, REBEC...
Activació Aplicació pacient
Aplicació Pacient
3:03
La Meva Salut
Com et trobes avui?
Has necessitat Paracetamol?
Què faries diferent?
Has fet exercici?
HSC
Procés fa proposta de activació de recurs especialitzada
Derivació a Ambulatòria Especialitzada
Alta
Altres
Rehabilitació
Unitat del Dolor
Traumatologia
Neurocirurgia
Reumatologia

This translates into the following deliverables for this use case:

2 Models used in the use case

3 Overview of the solution with identification of the elements of the platform that interact.

4 Source code of the solution.

5 Self-installing environment to check the proposal.

6 Proposal for a functional and technical manual.

ANNEX 8 OF CONDITIONS OF EXECUTION OF THE SERVICE

BUILDING AN OPEN PLATFORM IN HEALTH - ARCHITECTURE COMPONENTS, APPLICATION MARKETPLACE AND PLATFORM SERVICES

Unió Europea
Fons Europeu
Next Generation

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

Pla de Recuperació,
Transformació
i Resiliència

Next Generation
Catalunya

Generalitat
de Catalunya

TABLE OF CONTENTS

1 CONDITIONS OF EXECUTION OF THE SERVICE

1.1 ACTIVITIES ASSOCIATED WITH THE MANAGEMENT OF THE APPLICATION SERVICE

The management of the application service must be adapted to the processes and sub-processes established by the CTTI in force at the time of the execution of the service, when these are based on classic service management cycles (adaptation of good practices of the ITIL methodology).

These processes and sub-processes establish the appropriate mechanisms to maintain an ideal level of quality of the services that the CTTI offers to its customers, including all the management activities of the different services offered:

- Registration, analysis and resolution of incidents, requests, changes, problems
- Knowledge management related to these services.
- Satisfactory deployment of the new services to be incorporated.
- Establishment of the appropriate mechanisms for continuous monitoring of services.

Currently, the processes that are considered within the scope of Application Service Management are:

- Request Management Process
- Incident Management Process
- Knowledge Management Process
- Problem Management Process
- Event Management Process and Monitoring
- Change Management Process
- Configuration and Inventory Management Process
- Delivery and Deployment Management Process
    - Prepare the Service Subprocess
- Capacity and Availability Management Process

For each of the processes, apart from the activities of the process, the successful bidder must:

- To provide a contact matrix and a single contact channel (mailbox and telephone) for each process, and to keep the information updated and published in the KMDB of the CTTI, following the procedures established by the CTTI.
- Provide at least one person responsible for each process, with responsibility for dialogue with the head of the area and the head of the CTTI service in relation to all the activity carried out by the successful bidder in the process.
- Hold periodic follow-up meetings with those responsible for solving problems and establishing continuous improvement actions.

Within the continuous improvement, the successful bidder may make proposals to the CTTI related to the management of the processes detailed below, always focused on the optimization and efficiency of the process/procedures end to end.

The *"Processes, activities and documentation associated with service management" section* of the applications detail, for each process, the objective, the responsibilities of the successful bidder, the activities to be implemented and the associated documentation.

The successful bidder must also bear in mind that, in all service management processes and/or procedures linked to the CTTI Control Centre, it must carry out all the activities framed in the corresponding section.

1.2 ACTIVITIES ASSOCIATED WITH THE METHODOLOGY, STANDARDS AND DELIVERABLES

The organization of the work and execution of the service must be adapted to the methodologies, standards and deliverables established by the CTTI in force at the time of the execution of the service, with the deliverable quality plan in its Traditional and/or Agile aspect being the document that will detail how the process that guarantees the quality of the projects should be.

In all services, the application of the defined Quality Gates mechanisms will be mandatory.

Reference information can be found on the website: https://qualitat.solucions.gencat.cat

1.3 ACTIVITIES ASSOCIATED WITH QUALITY CERTIFICATION

The objective of quality certification is to guarantee that the quality of the service, process or product meets the established requirements. This evaluation must allow those involved to make decisions to continue, stop or cancel an activity, process, project or service.

Prior to the start-up of a service, or the closure of a phase of the life cycle, it is important to ensure that the service or phase meets the established requirements and standards (functional, quality, architecture, security, etc.).

The CTTI will validate that the requirements have been met, the controls have been complied with and will make a formal certification. You will be responsible for:

- Check that all parties have completed the established phases and requirements.
- Analyse the risk of the start-up and include the necessary recommendations.

Validate that all parties have made their approval for the deployment of the service. If the certification process does not end satisfactorily, but the parties have given their approval, they will have to sign a document accepting the exception.

Reference information can be found on the website: https://qualitat.solucions.gencat.cat

1.4 ACTIVITIES ASSOCIATED WITH CARRYING OUT TESTS WITH DEDICATED TEAMS

In applications of Very High or High criticality, the activities related to the tests must be carried out by a group independent of the maintenance team, with experience in carrying out these types of activities.

The CTTI or the area will be able to interact directly with this group.

These independent teams will be responsible for the following set of activities, without limitation:

- Definition of test plans
- Specification, execution and evaluation of the results of the integration tests between systems
- Specification, execution and evaluation of the results of system tests, in all its aspects, both functional and non-functional (performance tests, usability tests,...)
- Automation of tests (performance test scripts, functional regression tests, ...)
- Source code quality review

Unit tests and integration between system components will be carried out, in general, by the project and/or maintenance team.

1.5 ACTIVITIES ASSOCIATED WITH SAFETY

In terms of information security, it is essential that the successful bidder achieves, among others, the following objectives:

- Guarantee an adequate level of security of the applications. The successful bidder must consider security at different times in the life cycle of an application. These actions will make it possible to manage the security risks of any application at all times, and to make the decisions that are considered appropriate.
- The correct implementation of information security throughout its life cycle.
- Guarantee the correct implementation of the security model in the development of applications, set by the Cybersecurity Agency of Catalonia, involving the security teams from the beginning of the development projects, carrying out the necessary tests, guaranteeing in all cases the deployment of cybersecurity services and following the guidelines set in general.
- The monitoring of the policy set by the Cybersecurity Agency of Catalonia to guarantee the correct implementation of the security model in the maintenance of applications, involving the security teams from the beginning of the service, carrying out the necessary tests and following the guidelines set in general.

- To contemplate the classification of application information, carried out by the business, in order to correctly apply the regulatory and legal framework of the Generalitat in matters of security.
- The implementation of the necessary measures for compliance with current legislation on security based on the classification of information in the applications.
- The implementation of security controls that mitigate the risks to which the application is exposed and all the assets on which it depends.
- Comply with all applicable legal frameworks on cybersecurity (e.g., National Security Scheme, data protection legislation, legislation regulating identity systems and electronic signatures, where applicable, legislation applicable to critical infrastructures or essential services, etc.).
- Comply with all applicable requirements in accordance with the Information Security Regulatory Framework of the Government of Catalonia (Regulatory Framework) and any subsequent updates that may occur. The current standards of the Regulatory Framework can be consulted on the security portal of the Cybersecurity Agency of Catalonia.
- To have the appropriate resources to carry out the tasks that correspond to it related to regulatory compliance, responding to requests related to regulatory compliance verifications or other related requests, within the deadlines, through the channels and formats set by the Cybersecurity Agency of Catalonia and the CTTI.
- Comply as a data processor with the provisions of data protection legislation. With regard to the security of the processing of the same, the successful bidder will implement the security measures established in the Cybersecurity Framework for Data Protection.
- Assume the correction of all those security vulnerabilities to comply with the thresholds requested by the Cybersecurity Agency of Catalonia, from which the application may be promoted to production.
- Assume the correction of all those security vulnerabilities detected in the security analyses. The Cybersecurity Agency of Catalonia may carry out the security analyses it deems appropriate at any time during the life cycle of the application.
- To guarantee the effective deployment of the cybersecurity strategy determined by the Cybersecurity Agency of Catalonia, ensuring the effective implementation of the different services, processes and technologies that comprise it.

Given the changing nature of security threats, the technological evolution itself and the changes that may occur, the successful bidder must adapt the controls and security measures during the execution of the service if necessary. In general, it is essential that the security measures to be deployed by the successful bidder make it possible to deal with, at least, threats such as:

- Information theft, with the subsequent impact on business and legal (such as the GDPR).
- Intrusion into equipment, configuration/security changes to take control.
- Theft of user credentials.
- Exploitation of vulnerabilities in developed or evolving applications.
- Intercept network traffic by capturing information (DNS spoofing, HTTPS spoofing, among others).
- Legal breach. For example, non-compliance with the GDPR for access to users' personal data.
- Causing a denial of service.
- Access by unauthorized administrators/developers or by illegitimate use. Unauthorized use of resources.
- Errors of the administrators/developers of the service. For example, misconfigurations, poorly applied security measures, among others.
- Uncontrolled remote access. Attackers could take advantage of weak remote access mechanisms (e.g., VPNs with weak passwords).
- Social engineering to access confidential information of the personnel who provide the service.

The current standards can be consulted on the security portal of the Cybersecurity Agency of Catalonia (https://ciberseguretat.gencat.cat/ca/inici).

The details of the requirements and security model are described below:

1.5.1 Requirements and security model in development activities

1.5.1.1 Security requirements

The successful bidder must comply with the current security regulatory framework of the Generalitat de Catalunya. However, this section highlights those security aspects considered to be of greater relevance within the scope of the service.

Information Security Classification

- The successful bidder must take into account the classification of the information of the applications/projects to be developed in the contract, carried out by the business, in order to correctly apply the regulatory and legal framework of the Generalitat de Catalunya in terms of security.

Inventory

- To report and update the information linked to the applications (especially URLs, digital certificates and classification level of the application data) in the repository determined by CTTI and the Cybersecurity Agency of Catalonia.

Regulatory and Legal Compliance

- The successful bidder must comply with all the applicable legal framework on cybersecurity. In relation to compliance with the National Security Scheme (ENS), without prejudice to the required compliance with all applicable measures:
  - It must also comply with the regulations and technical guides that develop it.
  - It must include in its offer a declaration of responsibility obliging itself to comply with the ENS at the time of the start of the execution of the contract and to have the Declarations or Certifications of Conformity with the ENS or comparable accreditations, as appropriate, for the category of security required, of the systems, as well as maintaining the conformity in force during the term of the contract. This Declaration or Certification of Conformity or certifications or accreditations of compliance must include in their scope, at least, the scope of the contract. In the event that the CTTI requests it during the execution of the contract, it must submit the documentation accrediting compliance, such as the conformity badge, the security policy, the audit report or the self-assessment statement (as applicable) and the declaration of applicability relating to the compliance process. In the event that it is an accreditation of compliance other than the Declaration or Certification of Conformity, this documentation must include a risk assessment report prepared by the successful bidder's Safety Manager that determines the risks and their treatment.
  - They must communicate the name and details of the person designated as a security contact point (POC), as established in article 13.5 of the ENS or, where appropriate, the justification required by this provision for not appointing them and which must include an alternative proposal to make up for this lack of designation. This person will have to channel and supervise compliance with information security requirements and the management of incidents that occur during the execution of the contract. As provided for in the ENS, the person designated as a POC may be the person who holds the role of Security Manager of the successful bidder, someone who is part of their area or who has direct communication with it.
  - The POC must notify any security incident that may result, directly or indirectly, in the security of the information systems, within the deadlines and by the means determined by the CTTI, the Cybersecurity Agency of Catalonia or the established procedures. The successful bidder must provide all the information necessary for its management and notification to the competent bodies by the responsible entity. If necessary, the successful bidder must

collaborate with any of the tasks required by the CTTI or the Cybersecurity Agency of Catalonia for the identification, containment, eradication, recovery and collection of evidence of security incidents.

  - It must train, raise awareness and inform its staff about their duties, obligations and responsibilities in terms of security, reminding them of the possible disciplinary measures applicable and their duty of confidentiality with respect to the data to which they have access.

- The successful bidder must comply with all the requirements that are applicable in accordance with the Regulatory Framework of the Generalitat de Catalunya and all subsequent updates that may occur.

- The successful bidder must be incorporated into the regulatory compliance model of the Generalitat de Catalunya, carried out by the Cybersecurity Agency of Catalonia. This model will include the possible audits that the CTTI or the Cybersecurity Agency of Catalonia determine to carry out, as well as the subsequent implementation of the action plans derived from them. The successful bidder must have the appropriate resources to carry out the tasks that correspond to it in the compliance model, responding within the deadlines set by the Cybersecurity Agency of Catalonia and the CTTI. Compliance management will be carried out with the tool determined by the Cybersecurity Agency of Catalonia.

- The successful bidder must guarantee access to security and compliance information (procedures, incident logs, traces, among others) for authorised staff of the CTTI and the Cybersecurity Agency of Catalonia. All safety information must always be available to these authorised and previously identified personnel. The CTTI, the Cybersecurity Agency of Catalonia and the successful bidder will jointly establish the mechanisms to facilitate access to this information by authorised personnel, establishing the minimum security controls.

- In relation to the processing of personal data, the successful bidder will comply with the provisions of the General Data Protection Regulation as a data processor. With regard to the security of the processing of the same, the successful bidder will implement the security measures established by the Cybersecurity Agency of Catalonia in the Cybersecurity Framework for Data Protection. This implementation and level of compliance will be incorporated into the regulatory compliance model of the Generalitat de Catalunya.

- In the event of carrying out audits and monitoring the derived action plans, these must be carried out with the methodology and tools established by the Cybersecurity Agency of Catalonia.

Security exception management

The successful bidder must:

- Process a security exception for each control defined in the Security Regulatory Framework that is not complied with, including a mitigation plan and compensatory measures.
- Continuously monitor the security exceptions to which the services covered by the contract are affected.
- Raise risks to the Monitoring Committees in relation to exceptions considered to be of high risk, to ensure their management and monitoring.
- Ensure that once the exceptions have expired, the exception measure is eliminated. The CTTI and the Cybersecurity Agency of Catalonia must expressly authorise these removals.

Identification and Electronic Signature Systems

- When developing a new solution, the GICAR platform should be used, whenever possible, to authenticate users, considering in the case of critical applications the use of captcha and two-factor authentication.
- Likewise, the catalogue of electronic identification and signature systems of the Generalitat de Catalunya and the user guide that develops it will preferably be taken into consideration to propose identification and signature solutions to be integrated into the procedures and procedures of the Administration of the Generalitat de Catalunya in its relationship with citizens.

Trace Management:

- The successful bidder must comply with the current track management standard. The successful bidder must ensure that the application stores all the traces that are applicable to it in accordance with its classification of information and the applicable regulatory and legal framework.
- The traces must be accessible in reading mode and the marking of the traces will be ensured with specific conservation requirements according to the applicable legislation.
- The successful bidder, taking into account the level of security classification of the application, must provide the mechanisms for the traces of the application to be accessible and integrated with the corporate repository of traces of the Generalitat de Catalunya.

  Among others, these traces must allow:

  - The identification and access of the different types of users and the actions carried out with date and time (successful and failed connection attempts, administration tasks within the application, traces of the processing of administrative files (who and when have done what), consultation of specially protected data, among others).
  - The detection/solution of incidents.

  - The detection of possible security incidents.

- In the case of Devops applications, the successful bidder must guarantee the configuration of the infrastructure security logs in accordance with the applicable regulations.

Secure Communications:

- The successful bidder must ensure that the applications, whether published on the internet or on the intranet, use secure communication channels (HTTPS/TLS) in their user interface and in the interconnection with other applications, configuring robust cryptographic protocols and algorithms in accordance with the indications of the Cybersecurity Agency of Catalonia.

Architecture, disaster recovery tests and backup recovery tests

The successful bidder must:

- Ensure that the design of the solution/application architecture allows the required availability/continuity requirements to be achieved.

- Participate in the preparation and execution of continuity/disaster recovery tests (PRDs) and backup recovery tests, carrying out tests that certify that the application is operational and the recovered information is accessed correctly.

Signing the code of the applications:

- Signing of applets for any information system. The code that is the subject of the applets must be signed with a digital certificate from the Generalitat de Catalunya in order to guarantee integrity.

Management of administrator/developer users:

- The successful bidder must comply with the Guide to the Management of Administration Accounts of the Generalitat de Catalunya.

Among other measures, the successful bidder must:

- Users with high privileges will have to be limited as much as possible. It must always be done with nominal accounts. In the event that a privileged user is required by the developers, this fact must be notified to the Cybersecurity Agency of Catalonia for its authorisation and assessment of the associated risk.

- Recertify privileged users on a semi-annual basis, and will have to establish and implement action plans to correct the identified deficiencies.

Security in the provision of the service:

The successful bidder must:

- All administrators/developers' computers must comply with the security measures established by the Cybersecurity Agency of Catalonia and the CTTI (EDR, antivirus, for example) in order to access the equipment and network of the Generalitat de

Catalunya. Under no circumstances will equipment that the Government of Catalonia (CTTI and the Catalan Cybersecurity Agency) has not authorised be used.

- In case of remote access, all administrators/developers will need to access through the corporate VPN solution and have a second factor authentication (MFA) to minimize the risk of credential theft. Likewise, if corporate tools allow it, any access by an administrator/developer from within the corporate network must also have a two-factor authentication.
- In general, apply prevention and information protection measures in accordance with the standards of the Generalitat de Catalunya.
- The successful bidder may be audited periodically to assess the degree of compliance and identify security risks.

1.5.1.2 Description of the security model in application development

To guarantee an adequate level of security of the applications, the successful bidder must consider security at different times in the life cycle of an application. These actions will make it possible to manage the security risks of any application at all times, and to make the decisions that are considered appropriate.

The supplier must:

- In the phase of collecting functional requirements:
    - The supplier must take into account the functional and non-functional security requirements so that the solution meets these requirements. If you do not know them, you must request them from the person in charge of the system or Solutions Manager or, failing that, from the Cybersecurity Agency of Catalonia.
- In the application development phase:
    - Complete and submit to the Cybersecurity Agency of Catalonia the Architecture Document (DA) including the following information:
    - Type of information processed.
    - Proposed solution to respond to the requirements, functional and non-functional, previously defined.
    - Develop and implement all those security measures defined in the DA.
    - Provide all the documentation or information related to the solution that the Cybersecurity Agency of Catalonia may require.
    - The successful bidder must apply the best security practices in the development by producing secure applications by design.
    - The successful bidder must carry out the necessary security tests in order to validate that the applications developed are secure in all their

  components and the results of the technical tests that demonstrate this must be delivered to the Cybersecurity Agency of Catalonia.

  - For web applications, the successful bidder must perform dynamic security analysis (OWASP) on all published interfaces, whether web front-ends or APIs. These tests must be carried out in non-productive environments.
  - For all the code used, the successful bidder will have to carry out static code analysis. It will also be necessary to ensure the security of the code of the libraries used.
  - For container-based applications, these will also need to be scanned with specific security vulnerability tools.
  - It will be a requirement to pass the application to production that the results of the security tests are within the thresholds established by the Cybersecurity Agency of Catalonia.
  - The Cybersecurity Agency of Catalonia may carry out any type of technical security analysis it deems appropriate at any time to check whether the security level of the application meets the established security requirements. In these cases, the successful bidder must provide a test user for the complete execution of the analyses.

- In the service phase (production)
  - To provide all the necessary support and information to the Cybersecurity Agency of Catalonia to be able to carry out the technical security analyses that the Cybersecurity Agency of Catalonia deems appropriate.
  - The provider must carry out security analyses periodically to validate that the system does not have new vulnerabilities.
  - The Cybersecurity Agency of Catalonia may carry out any type of analysis it deems appropriate at any time and may require the correction of those vulnerabilities that are considered necessary depending on the business criticality of the information system.
  - Correct all those security vulnerabilities to comply with the thresholds requested by the Cybersecurity Agency of Catalonia.
  - Ensure cybersecurity throughout the software development lifecycle. This means that development tools, such as version control or continuous integration, are aligned with the required security controls at all times.
  - Provide the data required for the development of cybersecurity indicators, which allow the performance of the supplier to be measured, with respect to compliance with security policies, directives and controls (for example, frequency of incidents, response time, vulnerabilities detected, etc.).

1.6 ACTIVITIES ASSOCIATED WITH CORPORATE ARCHITECTURE

The successful bidder must comply with the regulatory framework and the processes and procedures of the corporate architecture in force of the Generalitat.

Apart from the architectural requirements detailed in this document, as additional requirements of mandatory compliance, the architecture principles are available at the link https://canigo.ctti.gencat.cat/arquitectura/principis/principis_arq/ and in the same way the cloud manifesto is available at the link https://canigo.ctti.gencat.cat/arquitectura/manifest-cloud/

1.6.1 Corporate Architecture Regulatory Framework

The successful bidder must be aware of and guarantee compliance with the regulatory framework and principles of corporate architecture of the Generalitat de Catalunya in the performance of the services covered by these specifications. All the information and associated prescriptions are published on the Arquitectura http://canigo.ctti.gencat.cat website and on the Quality and Models for the Delivery of IT solutions to the Generalitat de Catalunya website, in its Standards section https://qualitat.solucions.gencat.cat/estandards/

For illustrative purposes and as a minimum, a list of the most common standards of use in the provision of the tendered service is presented:

- Principles of Information Systems Architecture
- Software Roadmap
- DNS Domain Standard
- Standard for the nomenclature of IT infrastructures
- Document architecture and datasets according to requirements corporate technical data architecture
- Standard for Web Interface Software Development
- Standard for mobile software development

1.6.2 Architectural processes and procedures

The successful bidder must know and execute the corporate architecture processes as appropriate in the life cycle of the services covered by these specifications.

In the CTTI process map (which can be consulted in http://ctti.gencat.cat/ca/serveis/governanca_tic/desenvolupament_manteniment_aplicacions/), among others, you can find the description of the demand management processes and projects as well as their link with the Solution Integration and Corporate Architecture units.

For illustrative purposes and as a minimum, a list of the most relevant processes in the provision of the tendered service is presented below:

- Architecture Conformance Process (certification)
- Process of Management of technological obsolescence
- Process of Dissemination of Regulations and Architectural Processes
- Architecture Exception Management Process
- Infrastructure Procurement Process (PAI)

1.6.3 Corporate architecture frameworks and tools

The successful bidder must use the different frameworks (e.g. Canigó, EIXAM) and corporate platforms (Canigó, Cloud, SIC/SIC+, SGDE, LowCode, interoperability solutions, among others) as long as they apply to the technological architecture of the application.

The detailed definition of each of them is published on the Arquitectura http://canigo.ctti.gencat.cat/platforms website. The use of the different tools and frameworks will be done according to the guidelines and instructions published on the aforementioned website.

The successful bidder must use the functionalities offered by each tool or framework, as a transversal platform, and not use its own development or that of other third parties to cover the same function. The different tools and frameworks will incorporate more functionalities to cover the new requirements (functional and technological) of the applications of the Generalitat de Catalunya. If the current functionalities do not meet the business needs, the corresponding change request must be requested to incorporate the new functionality into the transversal tools and frameworks, or an architectural exception must be processed for not using the corporate tool.

1.6.4 Requirements for solutions with cloud-native architectures

Accompanying the technological evolution of ICT, the CTTI is progressively incorporating both new work methodologies and expanding the catalog of technological services of CPD to incorporate technologies and working methods that facilitate the improvement of productivity and efficiency in the process of maintenance of applications.

These methodologies and the expansion of CPD's catalogue of technological services mean that, in addition to the general capacities requested in the other sections, the successful bidder must have specific capacities in the following areas:

- Agile and DevSecOps methodologies and tools that support their implementation (Github, Workflows, Gitflow, JIRA, ...).

- Distributed architectures, containerization and interoperability (APIs, event driven architectures, synchronous and asynchronous communications)
- Infrastructure as Code (IaC), following the specifications of SIC/SIC+.
- FinOps and calculation of cloud architectures by design.
- Observability from design to end of life cycle.

For those new projects or maintenance services that are developed with these methods and solutions, the successful bidder must define and operate the end-to-end application architecture in hybrid environments and in all its dimensions. The CTTI will provide, for the different aspects, the self-service mechanisms that allow the successful bidder to be autonomous in the operation, governance and visibility.

Specifically, in these cases, the successful bidder must contemplate, among others, the following obligations in the different aspects of the life cycle of the application:

App Design:

- The solutions defined must be oriented to cloud deployment and therefore modular and each module scalable horizontally.
- Cloud-based solutions will include the definition and configuration of infrastructure as code (IaC). The successful bidder must know the IaC standards defined by CTTI and that apply to both computing infrastructure, managed cloud services as well as network services and provide the configuration of all of them together with the application code.
- The solution must include by design multi-AZ high availability, horizontal scaling according to load, backup and recovery forecasting. Most of these aspects are included in CTTI's IaC blueprints, but in case of modifying or adapting the templates, these requirements must be maintained.
- The architecture of the solution must take into account the volatile nature of the containers, and therefore without a session and maintaining the principle of resilience of its components.
- Regardless of whether images provided by CTTI or others are used, the deployment of new solutions implies the adoption of responsibilities by the successful bidder in the maintenance processes of the application. Including:
  - Maintain container images as well as application code without security alerts, depending on the checkpoints that SIC/SIC+ will execute.
  - Definition of alarms and probes and integrate them with corporate monitoring and/or observability systems
  - Incorporation of observability following the section *"Activities associated with observability and monitoring".*

Availability, backup and recovery of the application

- The solutions that make up our information systems must allow the coexistence of distributed systems, that is, they can be made up of different technological stacks, clouds and with variable availability while maintaining the level of service and security.
- The successful bidder will have to assume the necessary operations to persist the data adapted to the functional and confidentiality requirements using the mechanisms that make available the different hyperscales and pieces of the catalogue.
- The successful bidder will carry out and guarantee the health of the information system by monitoring the different parts that compose it as well as the functional monitoring that responds to the business use cases.
- The successful bidder will guarantee the health of the information system by building and maintaining its observability and monitoring throughout its life cycle (from design to decommissioning), following the guidelines in the section *"Activities associated with observability and monitoring".*
- As with traditional development, the successful bidder is the first contact in the event of an incident or request, although in this development model the successful bidder must be able to resolve it autonomously. If it is necessary to carry out any action on the application or its configuration elements, the successful bidder will be responsible for responding to the request (stop application, stop container, etc.).

  In the event that the application is part of a Critical Business Process, the successful bidder and the Control Centre will work in a coordinated manner, following what is described in the section *"Activities associated with the Control Centre".*

Application capacity management.

The successful bidder is solely responsible for the sizing and forecasting the growth needs of the solution in terms of:

- Performance, power, memory and storage. In the specific case of storage and in accordance with business requirements, it will propose information historicization policies (different types of "cold" storage), also taking into account the economic aspects of the solution as a whole.
- Bandwidths
- Vegetative growth
- Detection of bottlenecks taking into account user journeys and the distributed architecture of the solutions.

Finops Indicators

The architecture of the solution or product must contemplate the traceability necessary to allow the automation of:

- The generation of alarms and self-management of costs of the platform.
- Cost control indicators in items based on usage billing.
- The successful bidder will monitor costs and implement the necessary alarms by integrating them into the CTTI tools.

App security

- The solutions will be integrated with the transversal elements of the communications node (Net0 in the case of public cloud) in terms of incoming, outgoing, intranet communications, as well as with the implemented perimeter security elements.
- The architecture of the solution will have to consider security at the network level and communication between the different components and clouds, both public and private, and therefore, where communication between layers of the application will not be executed within the XCAT or Net0 node.
- The successful bidder must apply the security measures identified for each cloud element according to the level of security of the data managed by the application.
- The successful bidder is responsible for applying security patches to the different components that make up the solution or product.

Updates

- The successful bidder will have to update the solutions to minimize security risks, technological obsolescence, as well as adapt to the Roadmap, whether of CTTI or public clouds.
- Not using CTTI images will not exempt you from keeping the software up to date and without known security holes.

Application deployment

- It will manage the automated deployment process in all work environments, compulsorily using the SIC/SIC+ platform as a code repository and parameterization, construction and automated deployment in all environments, both of the infrastructure when we work in the cloud, and of the application.
- The definition and configuration of all components will be included in the deployment

With regard to the projects and maintenance carried out with the DevSecOps method, it should be considered that the implementation of DevSecOps in the CTTI is mainly based on the automation and code management tools currently in place, and that they are progressively equipped with more functionalities to have an increasingly programmable and dynamic infrastructure from a solution life cycle perspective. These automation tools cover two broad disciplines:

- Development and deployment, in order to provide maximum speed from the conception of an idea until it is in production, minimizing manual intervention but maintaining the required quality guarantees.
- Monitoring and diagnosis, in order to give visibility to those responsible for the applications of all those indicators that allow them to anticipate any problem that affects the application and to be able to diagnose its causes. This visibility must be through the CTTI's Corporate Observability Platform. The discipline will be carried out following the guidelines of the section *"Activities associated with observability and monitoring".*

New evolutionary maintenance projects or services that are determined to be managed under DevSecOps concepts must contemplate from the outset, at least, the following working premises, premises that are also of progressive application in traditionally managed maintenance:

In the construction stage with DevSecOps, the successful bidder must:

- Based on the continuous delivery and construction of the application code, and the infrastructure when we work in the cloud.
- Incorporate observability and monitoring following the guidelines in the section "Activities associated with observability and monitoring".
- Make automatic deployments of the application.
- Integrate with service management tools that allow monitoring the activity of changes and deployments of applications
- Carry out the tasks that allow the execution of the different aspects of testing included in the CTTI Quality methodology, which must cover, among others: unit tests, regression tests, static code quality, functional testing, security (static and dynamic) and performance and capacity.

A release candidate will be considered ready when it has successfully passed all the stages. In this sense, CTTI will establish the compliance thresholds from which each of the tests will be considered passed.

- For monitoring and diagnosis, the successful bidder of the development must follow the guidelines of the section *"Activities associated with observability and monitoring".*

The CTTI will provide the tool that allows the orchestration of all the automations described (SIC/SIC+) as well as the integration with the service management tools that allow monitoring the activity of changes and deployments of the applications.

1.6.5 Application identity management and access control model

The Government of Catalonia has a transversal identity management and access control model to resources managed by a platform called GICAR.

During the term of the contract, the applications that are part of the scope of the contract must be integrated with this platform in accordance with the regulations and procedures described in https://canigo.ctti.gencat.cat/plataformes/gicar/

1.6.6 Source code management

The source code of the applications is an asset of the Generalitat and as such it must be properly protected.

In the management of the source code of the applications and the code of the infrastructures and other artifacts necessary for the operation of the applications for which the successful bidder is responsible, the successful bidder will have the following obligations:

- The successful bidder is obliged to deposit the source code and the rest of the artifacts of the applications in the SIC, or failing that in one of the other repositories authorized by CTTI.
- The successful bidder is obliged to carry out the compilation automation tasks in those applications where the technology is supported by SIC, as well as the automation of deployments in the different environments. The scope will be delimited in the special cases that are so declared, and they will be made explicit by the successful bidder in the corresponding architecture exception (see processes of the Architecture area).
- The source code must be labeled with the corresponding associated version code.
- For business-critical applications, the code must be signed.

The management of the source code and its associated processes must be considered as one more task to be carried out within the scope of this service, and consequently it must have its corresponding planning and allocation of resources. The use of unjustified manual deployments will be penalized.

No module/evolution of an application that does not have deployment automation will not come into service, except for that in which it has been stated in an architectural exception, which cannot be automated, in whole or in part.

1.6.7 Development environments

The successful bidder will be responsible for acquiring, deploying and properly operating the different development environments that are required for the provision of the service.

The configuration of these development environments must comply with the current architecture and security standards and requirements of the service management model. Any change or exception must be expressly authorised by the CTTI. An extraordinary exception will be allowed during the transition phase of the service.

The successful bidder must have all the development infrastructures, located in its premises, including the communication lines with the CPDs of the Generalitat de

Catalunya that are necessary for the provision of the services and for the internal management of the services themselves.

The successful bidder must submit a document describing the technical architecture and configuration of the development environment, which must be aligned with the base software and the configuration, among others, of the DPC environments.

The CTTI reserves the right, for a specific technological environment or highly critical application, to decide to directly provision and manage the development environment. In these cases, the supply and management of the communication lines will continue to be the responsibility of the successful bidder.

In the event that there are integration environments in the corporate DPC, the successful bidder must integrate its development environments.

1.6.8 Data management

1.6.8.1 Technical data governance

Within the framework of technical data governance (https://canigo.ctti.gencat.cat/dadesref/gestiodades/) the successful bidder must:

- Identify the reference entities that are needed by the applications under their responsibility, and use the published reference entities in the design of the information system without creating new equivalents.
- Identify new entities to add to the set of published entities.
- In the event of being required by the technical data management office, which is the internal body of CTTI that is responsible for the management and maintenance of the information of the reference entities, the successful bidder must deliver the information with the structure and values of the new entities in the format indicated (usually, it is the delivery of an extract from the table(s) containing the information in DDL and DML format).

The identification of the reference entities that are in use and the new entities to be added will be done by updating the architecture description document, informing the section provided for this purpose (*Information view – Reference entities*) and specific information collection forms managed by the technical data governance team.

1.6.8.2 Open Data Model

The Generalitat has an open data portal (dadesobertes.gencat.cat). In the event that it is decided that the data involved in the tender can be opened by the area, the successful bidder must provide support to be able to open them. However, the successful bidder will have to internalize the architecture of the open data platform and propose solutions that use this architecture, especially in cases where the publication is aimed at the public and does not involve data that cannot be published in open access (personal data, for example).

All the information, regulations and procedures of the open data service of the Government of Catalonia are published at: http://dadesobertes.gencat.cat

1.7 ACTIVITIES ASSOCIATED WITH OBSERVABILITY AND MONITORING

Observability is defined as the ability to measure, monitor and understand the state of a system through the collection of relevant data, its processing and analysis, allowing in-depth knowledge of its present behavior and the ability to predict its future behavior.

An "observable" ICT solution is one that allows you to determine your health index and provides all the necessary data, end to end, to cover 4 layers of analysis: preventive, predictive, reactive and forensic.

As a result of new trends, the CTTI is immersed in an initiative to shift from traditional monitoring and operations to observability and intelligent control of services.

1.7.1 Observability standards

The implementation of the Observability of an ICT Solution takes the form of different measurement elements, such as, for example, having a standardised and adequate LOG level in specific locations, efficiently designed queries to obtain data, installation of agents in the infrastructures, design of appropriate functional probes, users of fictitious navigation and/or execution and non-consolidatable transactions, etc.

This instrumentation of the Observability of ICT Solutions and its implementation must follow the standards and guidelines of the CTTI set out in **the CTTI Observability White Paper**.

The **observability axes** established in this CTTI White Paper and which must allow the calculation of the health index of an ICT Solution are the following:

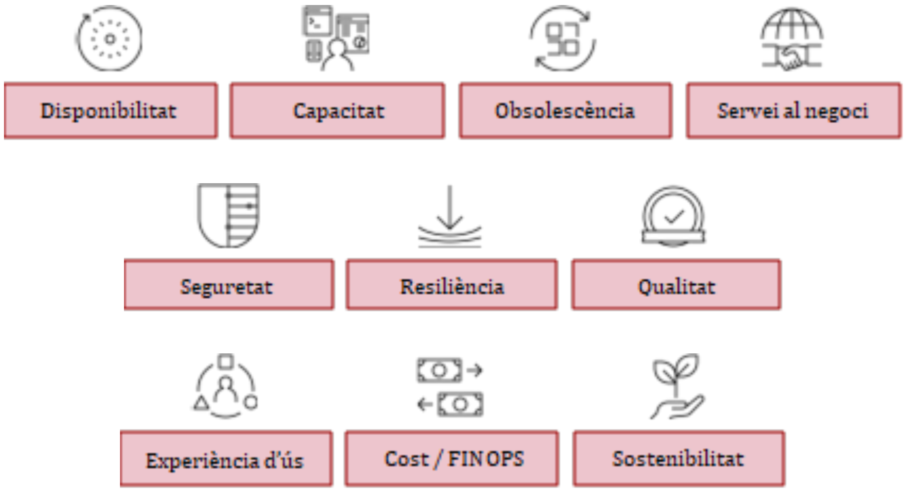


Illustration 1: Observability axes of the health index of a system

- Availability: The Solution is serving.
- Capacity: The Solution is sized to provide service. A lack of capacity could lead to an availability incident in the short or medium term.
- Obsolescence: The Solution has technological wear and tear.
- Service to the business: The Solution is providing a correct service to the business for which it is designed.

- Quality. The Solution complies with the quality standards established by CTTI.
- Safety. The Solution complies with the security standards established by CTTI and the Cybersecurity Agency of Catalonia.
- Resilience: The Solution is competent to recover in the event of failures or system outages.
- User experience (UX): The satisfaction of the use of the Solution by end users.
- Cost / FINOPS. The cost and finances of the operation of the Solution.
- Sustainability. The environmental impact of the Solution.

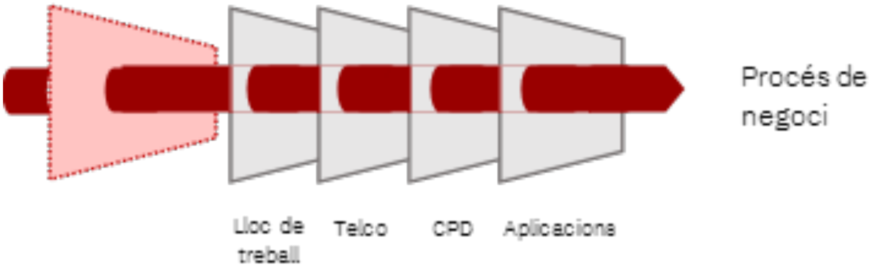
These axes are based on the collection of outstanding information, its processing and evaluation. This is based on the collection of different **types of data**, which are detailed below:

- Metrics: A metric is a quantitative value of a characteristic that allows you to evaluate the operation of a system. For example, metrics are understood to be data on the utilization of the infrastructure and performance of a system (such as CPU usage, memory, etc.).
- Logs: Records of the events that affect a particular process, evidencing the behavior of the systems. For example, logs are understood to be the set of logs generated by the infrastructure of a router, of an application during its operation.
- Traces: Information about how services interact with each other (e.g., response time).
- User or technical probes: navigations or checks necessary for the evaluation of the operation of the Solution
- Other information elements: context information, static parameters, attributes, etc.

It is important to know that the business processes of the CTTI are formed, end to end, by components of different families of services, understood as different groupings according to technological-functional criteria.

The current service families are:

- Jobs (LldT).
- Telecommunications (Telco).
- Data and Cloud Processing Center (DPC).
- Apps.



Map of the business process involving CTTI's service families

The CTTI's Observability standards will be updated over time through continuous improvement processes and adaptation to new technologies and technological paradigms.

1.7.2 Monitoring availability and capacity

The monitoring of an ICT Solution is part of its Observability. We define availability and capacity monitoring as the process of continuously monitoring and verifying whether an ICT Solution is accessible and functioning properly to avoid interruptions in its use by users and has sufficient resources to manage the workload and demand with optimal performance. This implies that monitoring also covers the 4 layers of analysis: preventive, predictive, reactive and forensic.

Currently the monitoring of availability and capacity is developed in 7 levels of measurement:

Measurement levels

- **Level 1: Functional or synthetic measurement**
  - Simulation of one or more transactions of an application with a virtual user in 24/7 hours that inform of its availability.
  - Simulation of one or more transactions of an application with a virtual user on a 24/7 schedule, collecting the execution times of each transaction.

- **Level 2: Technical measurement and dependencies**
  - Measures to control or check the services provided by the Solution: back-office services, APIs, or other technical elements.
  - Evaluation of the dependencies of other Systems for the proper functioning of the Solution (authentication services, third-party APIs, integrations, etc.).

- **Level 3: Infrastructure measurement**
  - **Level 3.1 Basic Infrastructure Measurement**
    - Basic data related to the infrastructure such as, for example, CPU, memory, disk, disk partition space, etc., of any type (containers, virtual machines, physical machines, cloud services, etc.)
    - Basic data relating to the network infrastructure, communications, workplace, security elements, etc., of any type (WAN, LAN, SDWAN, SDLAN, Communications Towers, RESCUE, etc...)

  - **Level 3.2 Advanced Infrastructure Measurement**
    - Advanced infrastructure data related to the platform, such as, for example, data from application servers, databases, web servers, etc., of any type (containers, virtual machines, physical machines, etc.).
    - Advanced data relating to network platforms, communications, workplace, security elements, etc. of any type (WAN, LAN, SDWAN, SDLAN, Communication Towers, RESCUE, etc...)

- **Level 4: Performance Measurement**
  - Metrics and traces of the transactional performance of all service activity: APM (Application Performance Monitoring) and others, depending on the service family.

- **Level 5: User Experience Measurement**
  - User interaction with the ICT Solution in real time: RUM (Real User Monitoring).

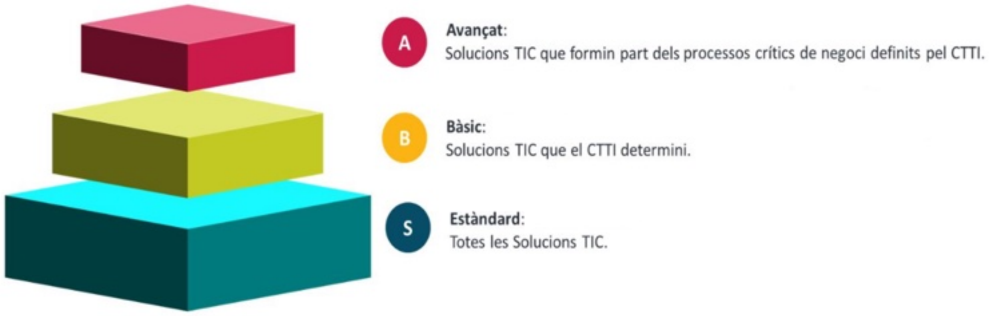
- **Level 6: Measurement of business data**:
  - Business-specific information, such as users who use an ICT Solution by time slot, procedures registered by the hour, erroneously signed documents, correct school pre-registrations, etc.

- **Level 7: Procedure and management**:
  - Information on indicators related to the associated procedures and management, are indicators for monitoring aspects such as the existence of a capacity plan, the performance of periodic load tests, etc.

1.7.3 Construction of the measurement of ICT Solutions

As not all ICT Solutions have the same relevance at the business level, the successful bidder will have to participate in the construction of the necessary information to ensure the level of observability and measure that the CTTI determines, taking into account this importance.

This participation will be regulated based on three observability packages, according to the importance of each ICT Solution:


A
Avançat:
Solucions TIC que formin part dels processos crítics de negoci definits pel CTTI.
B
Bàsic:
Solucions TIC que el CTTI determini.
S
Estàndard:
Totes les Solucions TIC.

- **Advanced Package**: It will be used to observe and measure all ICT Solutions that are part of the critical business processes defined by the CTTI. In this case, the information collected on the corporate observability platform will correspond to:
    - Observability : all axes
    - Availability and capacity monitoring: the 7 levels of measurement described must be incorporated.
- **Basic Package**: It will be used to observe and measure the ICT Solutions that the CTTI determines to be considered important, even though they are not part of the critical business processes. In this case, the information collected on the corporate observability platform will correspond to:
    - Observability : all axes
    - Availability and capacity monitoring: Levels 1, 2, 3.1 and 6 must be incorporated.
- **Standard Package**: It will be used to observe and measure all ICT Solutions. In this case, the information collected on the corporate observability platform will consist of:
    - Observability: the Observability axes will be defined ad-hoc according to the case
    - Availability and capacity monitoring: there is no aggregation by levels, only the LOGs need to be incorporated.

As part of the required service, the successful bidder must actively participate in the observability of the ICT Solutions for which it is responsible and must carry out all the necessary tasks to be able to design, build, facilitate, incorporate and deploy these observability and measurement packages following the observability and deployment policies and standards set by the CTTI.

The design of ICT Solutions must intrinsically and natively carry the Observability of all its components and cover its entire life cycle.

As an example, some of the tasks that the successful bidder must perform:

- Design, build, maintain and evolve a monitoring module adapted to each ICT Solution that allows, throughout its life cycle, to provide all the observability information under the responsibility of the successful bidder to incorporate it into the corporate platform, following the standards defined by the CTTI.
- Actively participate in the process of coding, registration, maintenance and versioning, and decommissioning of the functional measurement (e.g. synthetic probes) of the ICT Solutions under their responsibility with the aim of having reliable and uninterrupted monitoring.
- Design, build and facilitate the business indicators of the ICT Solution (for example, consumption of the service in volume of users or use, number of files managed, number of accesses, etc.) always following the indications of the CTTI, with regard to the indicators to be measured and the format for integrating the data.
- Design, build, facilitate and maintain the technical and dependency indicators of the ICT Solution together with the CTTI Service Managers.
- The traces and logs that are generated from the ICT Solution itself and the elements that it may use, provide the sufficient level of detail for the management

of the service (monitoring of the execution of its components, performance records to observe deviations in the expected performance, incidents, etc. and following the standards of the CTTI.

- Access to the LOGS and/or sending them, integration of the Observability and monitoring tools of the winning company with those of the CTTI
- Actively participate in the process of building, modifying and decommissioning the observability indicator tables of the applications, under their responsibility.
- Work together with the maintenance team of the Corporate Observability Platform to ensure the incorporation of information from the services for which it is responsible.
- Incorporate the software elements associated with Observability into the different templates of the infrastructure services as code.
- If necessary, sending alerts from the tools of the winning company to the CTTI's corporate monitoring tools.
- If necessary, enable queries for technical or business information (for example, via API) from the CTTI's corporate monitoring tools to the winning company's own tools.
- Where appropriate, installation of information collection agents in the infrastructures following the guidelines determined by the CTTI (installation of agents linked to the CTTI's corporate tools).
- Others that may arise as a result of the technological evolution of the service of the successful bidder or of the corporate observability and monitoring tools of the CTTI and/or the successful bidder.
- Collaborate with the CTTI in the improvement of Observability standards and work for the excellence of services.

These tasks, among others, must allow, throughout the life cycle of the ICT Solution, to provide the observability information under the responsibility of the successful bidder to incorporate it into the corporate platform.

In all cases, the cost of implementing the observability policies of the awarded services and their incorporation into the CTTI's corporate observability platform, following the CTTI model, will be borne by the winning company.

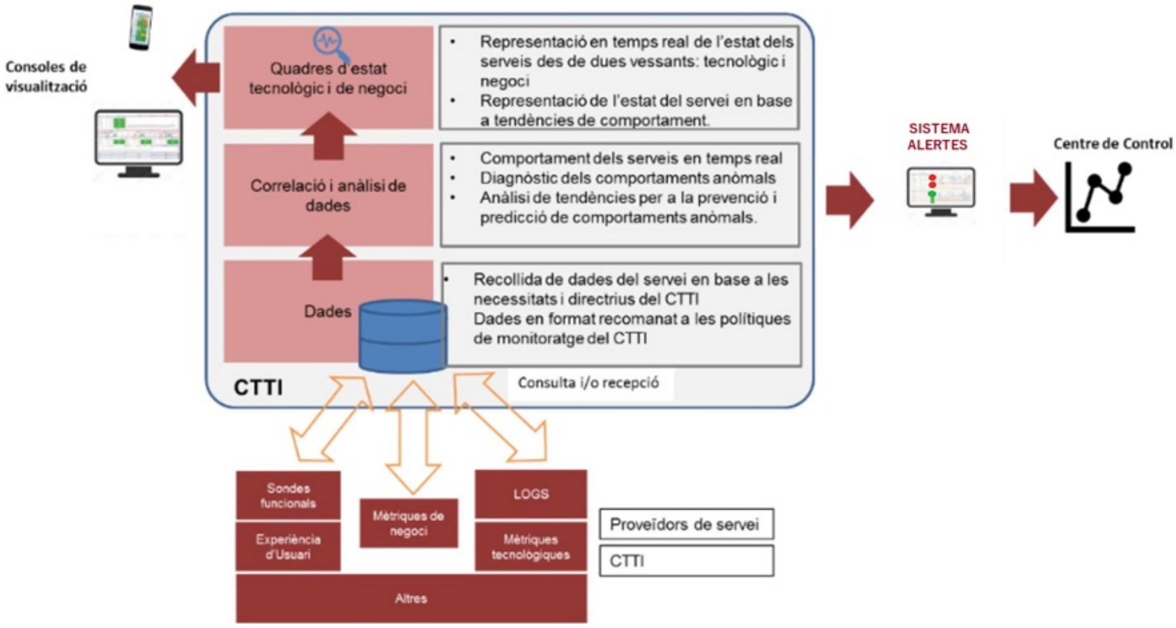
In addition to the Observability policies required by the CTTI, the provider would define, develop, implement and maintain all the additional mechanisms it deems necessary to guarantee excellent service delivery.

1.7.4 CTTI Corporate Observability Platform

All the data corresponding to the observability axes, measurement levels and types of data are collected and correlated in **the CTTI Corporate Observability Platform**, with the aim of having an end-to-end vision of the ICT Solutions that can be offered to all interlocutors according to their needs (Suppliers, Areas, Control Centre, Direction). This vision, end to end, must cover the 4 axes of analysis: preventive, predictive, reactive and forensic.

That is why it is essential to implement ICT solutions to collect data (in real time and in history) and establish behavioral parameters to evaluate the present state and have the ability to predict their future behavior covering the 4 layers of analysis: preventive, predictive, reactive and forensic.

The current functional architecture of the CTTI's corporate observability platform includes the following parts:



- Representació en temps real de l'estat dels serveis des de dues vessants: tecnològic i negoci
- Representació de l'estat del servei en base a tendències de comportament.

- Comportament dels serveis en temps real
- Diagnòstic dels comportaments anòmals
- Anàlisi de tendències per a la prevenció i predicció de comportaments anòmals.

- Recollida de dades del servei en base a les necessitats i directrius del CTTI
Dades en format recomanat a les polítiques de monitoratge del CTTI

The CTTI's Corporate Observability Platform is mandatory for use by the successful bidder. The CTTI reserves the right to allocate the cost of the licenses that the winning company needs to provide the service.

In addition to the CTTI Corporate Observability Platform, the provider will define, develop, implement and maintain the additional tools it deems necessary to guarantee excellent service provision and will provide/integrate all the information required on the CTTI Observability Platform to obtain a centralised and shared end-to-end view and will facilitate access to the CTTI and the Control Centre for integrated consumption.

In the event that licenses are required for the implementation of the own Observability tools or specific complements to be added to the CTTI Observability Platform, these will be the responsibility of the successful bidder.

The CTTI will determine the measurement criteria and policies that are required in any of the observability tools that are implemented.

1.8 ACTIVITIES ASSOCIATED WITH THE OPERATIONS OF THE CONTROL CENTRE

The CTTI Control Centre is responsible for ensuring the maximum availability of the ICT Solutions of the Government of Catalonia by performing the following functions:

- **CONTROL** the health status of all ICT Solutions in real time and end to end and **LEAD** the recovery of the service in the shortest possible time, in the event of relevant incidents. In this sense, the Control Centre is responsible for:

  Establish policies and methodologies for action in the face of this type of incident. The successful bidder must know and apply them appropriately, following their guidelines. More specifically, and as an example, the successful bidder must:

  - To attend on a mandatory basis and within the established deadlines all the crisis committees convened by the Control Centre of the Generalitat, applying its methodology, tools and procedures.
  - To participate actively in all the POST-MORTEM analysis committees of incidents that the Control Centre of the Generalitat determines.
  - Implement and monitor all action plans derived from the resolution of an incident, especially those that have caused a high impact on the business (public administration and/or citizen and/or business fabric).
  - Execute the action plan necessary for the restoration of the service with the direct collaboration of the successful bidder who will be responsible for its design and execution. The successful bidder must also actively collaborate with other service providers when the incident requires it.
- **KNOW** the detailed operation of services classified as critical (or those that have a direct relationship with them). In this sense, the successful bidder will be responsible for:

  - To provide and keep updated information on the technical and functional architecture of the services for which it is responsible and with which it is related. The successful bidder must provide this information, following the CTTI guidelines and applying the methodologies of the Control Centre (publication in the tools determined by the CTTI, access to the supplier's tools that the CTTI needs, formats and conditions for updating, etc.).
  - Carry out the necessary training for the Control Centre team to ensure knowledge of the service and its evolution in terms of technology and projects that can be developed.
- **DETECT** anomalous behavior of the services and **ESTABLISH** corrective actions before they have an impact on the business. In this area, the Control Centre is responsible for:

  - Establish policies and methodologies for the analysis of historical data and trends. The successful bidder must be aware of them and apply their execution appropriately, following their guidelines.
  - Lead the analysis of significant and historical data of the service in different axes (for example, availability, performance, quality, changes, etc.) to detect anomalous behaviors that may negatively impact the provision of the service in the short, medium or long term (capacity, repetitive errors, increase in response

time, etc.). The successful bidder will be responsible for actively participating in this analysis and providing access to the historical data of the service (e.g., infrastructure metrics, consumption metrics, LOGs, and any other that may be necessary) following the CTTI guidelines and assuming the cost of integrations with the CTTI tools (e.g., those of the Control Center).

- **ASSESS** the RISK of IMPACT on the BUSINESS of the actions carried out on ICT Solutions. Within this environment, the Control Centre is responsible for:
  - Establish policies and methodologies for risk analysis and assessment of relevant actions in ICT Solutions. The successful bidder must be aware of them and apply their execution appropriately, following their guidelines.
  - Lead the Evaluation Committees of the relevant actions on ICT Solutions. The successful bidder will be responsible for determining, together with him, the impact on the business and will have to design and execute, when appropriate, the test plan to guarantee the result of a relevant action and provide evidence of its results. In addition, the successful bidder must provide access to all the tools that allow changes in equipment to be determined in real time or others that the CTTI determines.

- **COMMUNICATE** the state of health of all the ICT Solutions of the Government of Catalonia to all the actors involved, according to their role and responsibility, in real time. The Control Centre must guarantee that the CTTI's communication policies related to the processes in which it participates or is responsible for them are correctly applied. In this sense, the successful bidder will be responsible for providing, with quality, all the important information to be communicated that the Control Center requires within the deadlines and format and with the tools that the CTTI determines. Likewise, the successful bidder must provide the reports in the required time and form in relation to any of the processes or interactions with the Control Centre (actions and status of relevant incidents, post-mortem reports, planning and detailing of important changes or any other required deliverable).

Due to the importance of the Control Centre as responsible for the availability of the ICT Solutions of the Generalitat de Catalunya, the successful bidder must provide at least one person responsible for guaranteeing the correct functioning and evolution of all the processes of the Control Centre.

1.9 ACTIVITIES ASSOCIATED WITH THE ACCESSIBILITY OF WEBSITES AND APPLICATIONS FOR MOBILE DEVICES IN THE PUBLIC SECTOR

The successful bidder must comply with all the regulations and requirements indicated in the web interface development standard described in https://qualitat.solucions.gencat.cat/estandards/estandard-desenvolupament-web/ as well as the rest of the axes to be considered in the application interface:

In particular, it will take into account all the provisions of RD 1112/2018, of 7 September, on accessibility of websites and applications for mobile devices in the public sector and therefore will apply the standard "UNE-EN 301 549. Accessibility requirements for ICT products and services". This standard is the Spanish version of EN 301 549 V3.2.1 (2021-03) Accessibility requirements for ICT products and services, declared as a harmonised standard in Commission Implementing Decision (EU) 2021/1339 of 11 August 2021, and which is equivalent to meeting all level A and AA requirements of WCAG 2.1.

In line with Royal Decree 1112/2018, of 7 September, on the accessibility of websites and applications for mobile devices in the public sector, an Accessibility Review Report (IRA) must be submitted. For more information, please consult the following link: (https://atenciociutadana.gencat.cat/ca/serveis/webs/accessibilitat/avaluacio-de-laccessibilitat/informes-de-revisio-de-laccessibilitat-ira/)

Below is described as a summary of the contents of the website: https://qualitat.solucions.gencat.cat where these activities to be carried out in the project are detailed, as well as their context of application:

Accessibility compliance

Applies to websites, web apps, intranets, extranets, and mobile web apps regardless of platform

The content, which must be accessible, regardless of the technological platform used to make it available to the public, is as follows:

a. Textual and non-textual information.

b. The documents and forms that can be downloaded.

c. Time-based pre-recorded multimedia content.

d. The forms of bidirectional interaction.

e. The processing of digital forms.

f. The execution of the identification, authentication, signature and payment processes.

Accessible content must comply with Standard EN 301 549 V3.2.1 (2021-03)

Both in new information systems or applications, as well as in evolutionary ones with a frontal impact: in the design, development and validation phase, accessibility criteria must be taken into account from the design itself, during development and testing, and to the delivery of the product to install it in environments to carry out validations.

- In the design phase: a report on the accessibility of the prototype must be submitted. This report evaluates the accessibility criteria that apply to the design.
- In the development phase, it is necessary to submit a report on the accessibility of the built front-end. This report includes the accessibility criteria that apply to the mockup.

- In the implementation and testing phase in the pre-production environment, accessibility must be evaluated:
  - with automatic tools if the environment allows access to tools such as siteimprove and the Observatory tool
  - with manual review

  NOTE: In the event that the pre-production environment does not have visibility on the internet, and no internal automatic validation tool is available, automatic evaluation will not be carried out in this phase.

  A report must be submitted that accredits the pages and tools used, accessibility criteria that apply to each case, as well as the result of the evaluation.

- After deployment in the production environment: if manual and automatic validations have been carried out in the pre-production environment and this environment is equivalent to the production environment, these validations can be skipped in production. In any other case, it will be necessary to do both and submit the report described above.

Multi-device adaptation

Applies to interfaces and web applications aimed at citizens and internal users

Procedure for selecting the multi-device test matrix

A representative selection of browser versions, operating systems, devices and screen resolutions most used in the last 6 months and covering 85-95% of users must be made.

- Digital products aimed at citizens:
  - For an existing website/application, usage data and thresholds can be extracted from analytics (Piwik Pro or analytics service that you have implemented).
  - For a newly created website/application or where we do not have usage data, take the data from Statcounter GlobalStats for the last 6 months in Spain.
- Digital products aimed at internal users:
  - For an existing website/application, usage data and thresholds can be extracted from analytics (Piwik Pro or analytics service that you have implemented).
  - Portability with browsers and versions that remain in force under the Software Roadmap Standard must also be guaranteed.
  - If you don't have analytics data, grab data from other apps used by a group of similar users.

It will be necessary to submit a report indicating the matrix of devices used (indicate OS version, browser and resolutions) and confirm that it is displayed correctly by complementing some representative screenshots in illustrative mode.

Corporate Design System

The design system is the standard for creating and designing information systems and applications. It applies to both public and internal digital services with the aim of building homogeneous experiences based on our own identity that defines our digital personality.

The design system of the Government of Catalonia is based on the simplification of elements, their reuse and the commitment to functional, meaningful and accessible solutions.

Its design principles are focused on five fundamental aspects:

1. Accessibility
2. Prioritization of user needs
3. Intuition and functionality
4. Consistency
5. Sustainability

The design system offers design components and libraries for use in the conceptualization and prototyping of digital products. It also offers tools and frameworks for front-end code developers.

sistemadedisseny.gencat.cat is the space that brings together all the documentation and information on the design system of the Generalitat de Catalunya, from how to install it, how to use it, good practices, consultation of planned versions and support mechanisms.

In the area of Health, the specific design system for this area must be followed: https://zeroheight.com/12913d2f0/p/645635-sistema-de-disseny-de-salut

Application interface design methodology

The design of services and the definition of the UI of digital products must be approached with design thinking methodologies. Consult the Digital Services Guide which provides information on the methodology for designing, implementing, maintaining and evaluating digital services (https://administraciodigital.gencat.cat/ca/actualitat/publicacions/guia-serveis-digitals/).

The interface of the application must be defined with an iterative process that allows you to address everything from the architecture of the information to the detail of the representative screens. In this design process, the end users of the product must be involved to ensure that the approaches made fit their needs and facilitate an efficient and usable interaction.

It applies to the tasks and deliverables required in the design of the application interface to be executed with profiles specialized in UX/UI design:

Design phase:

- Information architecture, navigation menus and transversal elements of the application.
- Elements and components available on each screen.
- Navigation flows (screens, modals, components, actions, messages or any other element of the interface that may appear due to a functional condition).
- Literals: field labels, literals specific to the interface, warnings and messages (correctly completed actions, errors, statuses, blocks, etc.), contextual helps, etc.
- The display of the screens in desktop resolution and/or in mobile resolution
- Define and document the behavior of the interface according to the different use cases or variants that may occur as a result of the functional definition of the product.

Construction phase:

- Support during product development to respond to new needs or adapt elements to adjust them to technical constraints that arise in this phase.

Testing phase

- The UX/UI profiles involved in the design phase must review the correct implementation of all the elements defined in that phase and determine the adjustments to be made to ensure the UX quality of the final product.

1.10 ACTIVITIES ASSOCIATED WITH THE AUDITS

The CTTI, the Cybersecurity Agency of Catalonia and any competent body may review or audit the correct execution of the processes (including quality assurance and security) as often as they deem necessary, of the aspects of these specifications that are determined and of the results obtained in an application.

The execution of the audits must be carried out in coordination with the CTTI.

In all cases in which it is decided to carry out an audit, the successful bidder must guarantee total, unconditional and irrevocable access to existing documents and tools that are related to the provision of services.

The successful bidder will provide the assistance and information required by the audits, at no additional charge to the CTTI. The information will be provided in the form and time required.

Carrying out the audit at no time will exempt the successful bidder from complying with the commitments arising from the provision of the services.

At the end of the audit, the parties will review the deviations and/or observations detected, drawing up an action plan. The result as a whole will be signed by both parties.

The successful bidder, in accordance with the calendar established in the action plan, undertakes to report on the status and to carry out the activities established in the action plan. The CTTI will be able to verify that the action plan has been implemented correctly.

The performance of the audits does not exempt them from their responsibility to carry out the audits to which they are obliged by current legislation. The audit reports linked to the services covered by this contract will also be submitted to the CTTI for its information.

1.11 TEAMS AND ROLES

The teams that provide the service covered by this contract must have specific functional and technological knowledge related to the functional context of the lot as well as the technological platforms they use, the life cycle management tools and the regulations and standards of the CTTI.

For the provision of services, the following profiles will be considered and the main functions under their responsibility will be determined:

- **Project manager.**
    - Plan the activities of the evolutionary
    - Carry out the analysis of deviations from the development/project (scope, cost and time)
    - Manage and monitor the development/project
    - Manage the resources assigned to the development/project
    - Manage and coordinate with the suppliers of other systems of the Generalitat that have dependencies with the development/project
    - Manage changes
    - Manage risks
    - Responsible for coordinating and directing the project.
    - Main point of contact for communications.
    - Risk and dependency management.
    - Coordination with all the actors involved.
    - Quality assurance of deliverables.

- **Software Architect.**
    - Responsible for the conceptual design of the solution and the architecture of the technological components necessary to cover the needs of the development/project.
    - Define the different possible technical alternatives to cover the development/project, determining the best possible solution of all those available, always with the aim of keeping the application as parameterizable, flexible and efficient as possible.
    - Carry out the sizing of the technological platform as well as the proposal of technical configuration of each of the components of the platform to optimize the operation of the application.

  - Update the architecture document when necessary.
  - Design of the overall architecture of the platform.
  - Definition of standards and development patterns.
  - Technical validation of components.
  - Ensuring architectural coherence.
  - Technical guidance from the development team.

- **Senior Developer**
  - Put into practice the knowledge of the techniques and resources, focusing mainly on the programming languages existing in the environment they use, as well as taking advantage of the facilities and aids that the software provides for the development of the development
  - Study the complex problems defined by consultants and analysts, diagramming the flow of detailed treatment programming.
  - Write programs in the programming language indicated.
  - Evaluate the deliverables and establish what tests to be carried out
  - Design and implement test cases
  - Automate test cases
  - Prepare your test environments and datasets
  - Run test cases and log found defects
  - Implementation of the core components of the platform.
  - Development of integration services.
  - Implementation of security mechanisms.
  - Development of APIs and web services.
  - Testing and resolution of incidents.

- **Experts en UX/UI**
  - Design of the user interface of the application market.
  - Definition of the user experience for the different profiles.
  - Creation of prototypes and wireframes.
  - Carrying out usability tests.
  - Preparation of style guides and visual components.

- **Consultant / Business Analyst Specialist in Health**
  - Taking requirements, identifying business needs and defining proposals for functional solutions
  - Give the functional specifications of the integration services with other systems with which the evolutionary is related
  - Carry out the preliminary analysis to determine the needs of new evolutionaries
  - Define and participate in communication and support plans.
  - Perform the version management of the application and the control and supervision of its deployment on the data centers in coordination with the test managers

  - Define, design, maintain and monitor the data model and its implementation
  - Support the definition of the quality plan
  - Define, document, and update test plans
  - Monitor and control testing activities. Continuously report on their progress.
  - Making test result reports
  - Coordinate the tests with the rest of those involved (project manager, responsible for solutions, operations, ...)
  - Specialized in Health
  - Analysis of functional requirements.
  - Modelling of healthcare processes.
  - Specification of use cases.
  - Validation with end users.
  - Functional documentation.

- **Cloud Security Engineer.**
  - Stay up to date with the latest security threats and also the latest updates and developments presented by public cloud providers in the field of security.
  - Implement and maintain the security policies, procedures and controls of the new system that must guarantee the integrity of the data and the security of the applications.
  - Design, execute and periodically audit the backup plan of the new system
  - Ensure that the new system complies with current rules and regulations (especially ENS high level and GDPR).
  - Conduct regular security audits and risk assessments to identify security threats and correct vulnerabilities.
  - Design the security architecture.
  - Implement access controls.
  - Management of identities and authorizations.

- **Experts in health interoperability**
  - Implementation of health standards (HL7, FHIR, etc.).
  - Integration with external systems.
  - Mapping of clinical terminologies.
  - Interoperability validation.
  - Technical documentation of integrations.

- **Experts in change management:**
  - Design and execution of the change management plan
  - Analysis of the impact on the different groups
  - Development of communication strategies

  - Coordination with the different stakeholders
  - Monitoring and evaluation of adoption

- **Training experts**
  - Design of the training plan
  - Development of training materials
  - Execution of training sessions
  - Evaluation of the effectiveness of the training
  - Adaptation of content according to feedback

For technical specificities, equivalent profiles may be taken into consideration.

Taking into account the specific needs of each contract, the teams and profiles necessary for its execution will be defined.

1.12 ACTIVITIES ASSOCIATED WITH CTTI'S GOVERNANCE TOOLS

The CTTI will determine and/or provide the tools that support the processes to manage and govern ICT services. The following conditions must be met:

- The successful bidder must use the tools proposed by the CTTI under the conditions established by it.
- The successful bidder will be responsible (if any) for the costs associated with the use of these tools (access, licensing, integration, etc.). In order to ensure the operation of the governance processes, the CTTI may establish minimum volumes of licenses to be acquired by certain of the tools.
- The successful bidder may propose modifications to the tools to obtain better efficiency and quality in the service, provided that the continuity of the service level agreements is ensured. Any request for change must be documented in advance so that the CTTI can analyse and authorise the advisability of its implementation.
- The successful bidder may make use of additional tools, with the prior authorisation of the CTTI. This does not exempt them from complying with and using the tools determined by the CTTI. The use of these additional tools may not deteriorate the service or entail an additional cost to the CTTI. The use of these additional tools may not jeopardize the continuity of the service after the end of the contractual relationship.
- The CTTI may evolve the chosen tools at any time during the duration of the contract.
- The CTTI reserves the right to incorporate new tools. In any case, a minimum of 2 months' notice will be given to suppliers before its implementation.

- The information contained in the tools must coincide with the reality of the execution of the services and the established processes and procedures. The CTTI will not take into consideration information regarding processes and procedures supported by tools that is not contained in the tools determined by the CTTI.
- The correct updating of the information in the tools is a requirement of the service, processes and solutions. Any defect in the information of the tools that is the responsibility of the successful bidder will be considered a defect in the service itself.
- The successful bidder undertakes to use them properly within a period of 2 months from the start of the service. For the new tools, the CTTI will communicate their roadmap, and the successful bidder will adapt in a planned period of 2 months, from the date of the formal communication of the implementation.
- The list of the tools and products that support them, as well as the necessary licensing to be provided by the successful bidder is as follows:

Tool group	Tool	Product	Required license from the successful bidder
CTTI documentation repository	MS Sharepoint	MS Sharepoint	N/A
Demand and project governance	AkisTIC	CA Clarity	Access to the tool
Service governance			
Self-service portal	PauTIC-Portal	BMC Remedy	N/A
Ticket management tool	PauTIC-Console	BMC Remedy	Ticket Update Creating and updating changes
Observability tools	WATCHTOWER	ELASTIC	Access to the tool, according to profile
Monitoring tools	MonTIC	HP BSM	N/A
Control Center Tools	SOSTIC	-	N/A
	Webex	CISCO	N/A
Configuration database	PauTIC-CMDB	BMC Atrium	Updating inventory items
Compliance with service	COSTIC	Digital Fuel Service Intelligence	N/A

Tool group	Tool	Product	Required license from the successful bidder
level agreements			
Knowledge management	PauTIC-KMDB	BMC KMDB	Updating knowledge articles
Security Governance			
Application security analysis	Security Analysis Source Code	Fortify - HP	N/A
	Dynamic application security analysis	ZAP - Free Software	N/A
	Dynamic application security analysis	WebInspect – HP	License of use
Management, assurance and quality control of applications			
Application development governance	Software lifecycle management	ALM-Octane	Yes
Running the tests	Running performance tests	Load Runner	N/A
	Execution of acceptance or exploratory tests	Sprinter	N/A
	Web Test Automation	Selenium	N/A
	Execution of mobile device tests	UFT Mobile	Yes
	Functional Test Automation	UFT One	Yes
	Performance Test Automation	VuGen	N/A
Quality review and/or certification	Code Review	Sonarqube	N/A
	Review of the adaptability of web pages	Crossbrowsertesting	Yes
App development lifecycle support	Continuous Integration Systems	SIC	N/A

Tool group	Tool	Product	Required license from the successful bidder
Support for the invoicing process	Verv - Navision	Web	N/A

Below, in a generic way, the types of tools to be used in the contract are detailed.

1.12.1 CTTI documentation repository

The CTTI will make available to the successful bidder a repository where they can exchange with the CTTI the documentation regarding the provision of the service and its governance processes. In this tool, the successful bidder will also save the deliverable documents resulting from the execution of the service and related projects.

This repository will be the single source of deliverable documents, and the rest of the governance tools will have to reference this repository. The successful bidder will be responsible for keeping the information updated and following the policies, nomenclature and version control determined by the CTTI.

1.12.2 **Demand and project governance tools**

The CTTI has tools to manage the demand for projects and control and monitor projects.

The successful bidder must use this tool in conjunction with the CTTI to carry out the tasks related to the following processes and procedures related to the requests for services on demand of the contract:

- Control and management of the project portfolio
- Submission and acceptance of proposals
- Formalization of the order
- Planning and acceptance of billing milestones
- Project control and monitoring

The degree of control and monitoring of the projects will be stipulated according to the criticality of the project for the business and the provisions of the CTTI methodology.

The successful bidder will be able to carry out detailed monitoring of the projects in their own tools, ensuring that the required information is reported in the CTTI tools.

1.12.3 **Service management tools**

Currently, the CTTI has several tools that support the governance processes of the services.

Below are the tools available to the CTTI for the management and operation of the service:

- **Self-service portal:** Entry point for the end user and/or supplier equipment for the management of incidents, requests, queries, complaints, problems and others that CTTI decides.
- **Ticket management tools**: Tool that supports ITIL processes for managing incidents, requests, queries, complaints, changes, problems, configuration, deployments and versions. All these processes will be managed through this tool, so the successful bidders will have to monitor them in the CTTI tool.
- **Configuration Database** (CMDB): The successful bidder must keep the inventory and status information of the services in the CTTI configuration database up to date as determined by the CTTI. The integration between the CTTI database and those of the suppliers may be carried out through a federation of databases if the CTTI considers it appropriate, therefore, the successful bidder must facilitate this integration.
- **Tool for managing compliance with service level agreements:** The CTTI has a tool to record service indicators, aggregate the information, calculate the performance target based on the established service level agreements and calculate the associated penalty, if applicable.

  This tool is the benchmark for monitoring compliance with the service level agreements established with the successful bidder, in the event that the information does not come automatically from other CTTI tools, the successful bidder will be responsible for providing it in the format determined by the CTTI.
- **Knowledge Management Tool** (KMDB). The knowledge management tool will become the information database to speed up the resolution of incidents, problems, queries or complaints, both by the CTTI user service and by the service providers themselves or the end user. The successful bidder must have access to the knowledge management tool as an information reference, and it will be part of their responsibilities to publish content that may serve as a reference in the future by the successful bidder itself, end users, the CTTI or other suppliers.

The CTTI may incorporate other tools that it considers necessary for Service Management, such as log correlation tools or tools for diagnosing application problems. It may also require systematic information on the activity of the service.

1.12.4 **Security governance tools**

In order to respond to the application security model defined by the Catalan Cybersecurity Agency, the set of tools to be used by the successful bidder is as follows:

- **Source Code Security Analysis:**
  - Tool for executing analysis of the source code of the application.

- **Dynamic Code Analysis (OWASP):**
  - Tool for the execution of dynamic analysis of Web applications.

These tools must be used by the provider in development environments by submitting the reports resulting from their execution to the Cybersecurity Agency of Catalonia.

1.12.5 Tools for the management, assurance and quality control of applications

In order to respond to the application quality model defined by the CTTI, the set of tools that the successful bidder must use as applied is as follows:

- **Test management**
  - Repository in which the different types of tests to be carried out are planned, defined and executed to validate that the solution is ready to be implemented, check compliance with the acceptance criteria and that it has no defects
- **Running the tests**
  - Repository for the definition and execution of performance tests on information systems
  - Tool for running acceptance tests and/or exploratory tests.
- **Test Automation Tools**
  - Web Test Automation Tool
  - Tool for automating functional tests in all technologies
  - Tool for automating performance tests
- **Quality review/certification tools**
  - Source code review tool for different technologies (SAP, .NET, Java, ...) and layers of the architecture.
  - Web page adaptability review tool (responsive)

1.12.6 Tools to support the application development lifecycle

To reduce the lifecycle time of application development and the protection of software assets owned by the Generalitat de Catalunya, the CTTI has tools that provide the following functionalities:

- Source code version custody service.
- Automation of the construction and deployment of applications with tasks of:
  - Repository of authorised common libraries
  - Construction of artifacts to be deployed
  - Code analysis
  - Automatic deployments
  - Automated request for deployments in PRE/PRO, with registration in Change Management - Remedy

- Management of users, accesses and roles in the aforementioned applications

1.12.7 **Tools to support the invoicing process.**

The CTTI has a portal that allows the validation of the service actually received and that allows suppliers to start the billing process for the services delivered to the CTTI.

The successful bidder will be able to consult the validation status of the service delivered and, once validated by the CTTI, retrieve the delivery note code that must appear on the invoice.

1.12.8 **Observability and monitoring tools**

The CTTI Observability platform and monitoring tools provide a centralized view of the health of ICT Solutions by measuring the different axes according to the CTTI Observability standards. The successful bidder must implement the ICT Solutions in order to incorporate observability and monitoring into the CTTI Corporate Observability Platform as set out in the section *"Activities associated with observability and monitoring".*

Each provider will additionally use its own management tools for the Observability and monitoring of the ICT Solutions under its responsibility to guarantee the Service over time and evolved according to the needs at all times. For those ICT Solutions that the CTTI considers, the successful bidder must provide access to its monitoring tools.

In the event that licenses are required for the implementation of the Observability tools, these will be the responsibility of the successful bidder.

1.12.9 **Reporting-Reporting**

For control and monitoring, periodic metrics and reports will be used to support the established management bodies and which are, as a whole, the mechanism for monitoring and evaluating the service.

The successful bidder is responsible for generating and delivering the reports and reporting metrics (hereinafter information) that the CTTI determines, using the CTTI tools and data. These must allow the CTTI to govern, control and manage the services provided by the successful bidder, from an individual (application), scope, transversal and global perspective.

Among others, the following reports will be requested:

Report	Periodicity
Application Service Management Report	Monthly
Service Level Agreement Report	Monthly
Security Vulnerability Report	Quarterly
Obsolescence management plan follow-up report	Quarterly
Capacity Plan Monitoring Report	Quarterly

Monitoring report of the quality and continuous improvement plan	Quarterly
Version Change Plan Tracking Report	Quarterly
Observability Management Plan Follow-up Report	Quarterly

The exact format and detailed content of the information to be prepared by the successful bidder in all areas will be defined by the CTTI. The CTTI may request, during the term of the contract, changes in the structure and content of the information to adjust to the needs of monitoring the services.

In the event that the CTTI requests information, the successful bidder will deliver it, complying, if applicable, with the SLAs defined by the service.

The successful bidder undertakes to deliver the information in electronic format and subsequently processable by the CTTI within the deadlines established by the CTTI.

The successful bidder must have the necessary mechanisms to guarantee that the metrics and measurement indicators are correct, and the CTTI may carry out the audits it deems necessary for their verification.

1.13 CALENDAR AND SCHEDULES

The successful bidder must cover the calendar and schedules described below. The services will be provided according to the official work calendar published by the Generalitat de Catalunya, and those that are in any of the work centres of the Generalitat that make use of the ICT services subject to this tender will be considered as Working Days. **Normal Hours** will be considered between 8:00 a.m. and 6:00 p.m.

Service Level	Timetable
Labour	Weekdays from 8 a.m. to 6 p.m.
Extended Labor	Weekdays from 8 a.m. to 10 p.m.
Continuous	Every day from 8 a.m. to 10 p.m.
Extended Continuum	24 hours x 7 days

The services must be sized to be able to absorb the load curves according to the timetable of the departmental area, and the successful bidder undertakes to provide the services as required by the ANS for each of the services.

Outside the hours of execution of the service, and for the applications that require it according to the level of support, the successful bidders must organize a system of on-call or equivalent system that allows them to have the required personnel locatable and available to carry out interventions, whether remote or face-to-face in less than 1 hour.

Some of the services will require that certain activities, in order to avoid impact on the continuity or availability of the application, be carried out on public holidays and/or outside normal hours. These activities are understood to be included within the scope of the service to be provided by the successful bidder and will not be subject to additional billing or rate changes. In these cases, and regardless of the level of support, a certain flexibility in the schedule is required for the performance of extraordinary activities that must be carried out outside the hours established in the provision of any of the services within the scope of the contract. This point affects the recurring technological services of:

- Operational Management
- Platform management
- Support (all support services)
- Corrective Maintenance
- Technical Offices

Some examples of situations in which it is applicable are, among others:

- Support for periods of high activity that require the extension of the usual hours (calls, campaigns, ...)
- Support associated with critical business process milestones
- Extraordinary functional support for occasional extension of the public employee's working day

If, during the execution of the contract, the CTTI or the successful bidders detect the need to modify the service schedule of any of the services, the CTTI and the successful bidders will jointly agree on the modification.

1.14 PHYSICAL LOCATION AND NECESSARY RESOURCES

The professionals who are part of the service will be located for the most part in the facilities of the successful bidder, and all costs associated with their jobs and their operation and maintenance will be borne by the successful bidder: office space, furniture, personal computers, technical and communications infrastructure, consumables and the like.

The facilities, buildings and dependencies used for the location of the service must comply at all times with all the requirements of construction, habitability, safety and ergonomics stipulated by the current regulations of the Generalitat and the State in their most demanding expression.

The conditions that the successful bidder must meet with regard to infrastructure and connection in order to optimally carry out all the activities related to the provision of the service are as follows:

Premises: it must be able to isolate the communications infrastructure (local area networks or Internet connection equipment) with other premises within the same building or office building.

Communications: The successful bidder must have a high-capacity Internet connection at their headquarters, depending on the number of concurrent connections and the type of protocols they use to run the service. As well as having a main line and a backup line.

With the exception of the own infrastructure that the Generalitat has to provide to facilitate the access of the successful bidder, the provision, installation and all associated expenses of installation and support of the WAN and LAN infrastructure necessary to connect to the work environments in the Generalitat and carry out the provision of the service (communication lines, physical cabling and the necessary communications devices: routers, switches, firewalls, etc.) will be the responsibility of the successful bidder, who will be solely responsible for their conservation and support.

Security : The bidder must guarantee the following aspects:

- Access to Networks. The successful bidder must implement access control mechanisms through accounts or electronic certificates of personal users to guarantee the security, integrity and confidentiality of the data contained in the company's equipment affected by the service. The successful bidder must maintain audit files with detailed information (user, date, date and time, resources accessed, etc.) of the accesses to the equipment, which may be audited.
- Physical access. The company will have premises with restricted access by fingerprint, card or similar control, in which all the computers from which it is possible to access the Applications of the Generalitat must be located. The successful bidder must keep the necessary information so that the Generalitat can, at any time, verify that only duly authorised personnel access these areas.
- Job Security. It must be guaranteed that each job of the successful bidder is updated at the level of operating system, service pack and antivirus. The successful bidder's workstations that connect to the Generalitat may be subject to the security policy agreed by the Generalitat to ensure that the work session with the Generalitat is reliable.
- Tools: The bidder must guarantee the use of the tools, proposed by the CTTI, that support the processes to manage and govern ICT services.

It should be borne in mind that, due to the needs of the service, the transfer of certain personnel responsible for the successful bidder to the premises determined by the CTTI may be requested, either during specific periods, for project coordination or resolution of critical incidents, or on a more continuous basis, for the operation of the service itself. In these spaces, the Generalitat will provide the furniture of the workplace and connection to the LAN network and Internet access, and the successful bidder will be responsible for the provision of the rest of the necessary equipment (desktop computers/laptops, tablets, mobile phone terminals, etc.) for the development of the tasks.

At any time during the execution of the contract, the CTTI reserves the right to request the successful bidder to provide the service in person at the facilities of the Generalitat de Catalunya. The successful bidder must adapt to these agreed changes within the agreed period.

Likewise, the successful bidder will assume, at no additional charge, any travel costs that, due to the need for the service, are required to be carried out within the Catalan territory.

The workplace of the "core" team defined in section 4.11 Teams and roles of the PPTP must be the CatSalut facilities. If necessary, the successful bidder must also be available to travel to the facilities of the different actors in order to obtain the information in person.

1.15 ROTATION CONTROL

The stability of the resources of the service with knowledge and commitment is very important for the correct provision of the service.

The winning company may make changes to the work team during the execution of the contract, but must notify the CTTI in writing at least 14 calendar days in advance, justifying the change and informing of the profile and characteristics of the person who joins. The CTTI will check that the person to be incorporated complies with the curricular conditions of the team member they are replacing.

The winning company will assume the selection and training of new incorporees and will carry out the necessary controls to ensure the correct transfer of knowledge, thus guaranteeing that the quality of the service provided and perceived is maintained.

Under no circumstances will the replacement of staff entail an additional cost, and it must be guaranteed that the service is not affected by this change

1.16 GUARANTEE

During the period of validity of the contract, the successful bidder will maintain a 12-month guarantee on the results of the work delivered, counted from the date of acceptance of the delivery (or up to a maximum of 6 months once the contract has ended), ensuring that they comply with the specifications previously established by the CTTI, and undertakes to correct any error that may appear during the same period at no additional charge. Hidden defects or errors that are detected during the warranty period, and refer to the services provided or their results, will be corrected by the supplier at no cost for the necessary intervention, within the maximum period established in the SLAs.

In those applications in which the guarantee is required from a third party other than the successful bidder (for example, a corrective maintenance action on an application that has been developed by a third party), the successful bidder will be responsible for the management of this guarantee, and it is therefore their responsibility to apply the guarantee for the resolution of incidents and support without any cost being passed on to the CTTI.

3-month service return phase guarantee. The provider must provide the CTTI with additional assistance services at no cost during the guarantee period of the return of the service, if requested.

1.17 CONFIDENTIALITY

The successful bidder undertakes not to disseminate and to keep the most absolute secrecy of all the information to which it has access and to supply it only to authorised personnel indicated by the CTTI or by the body promoting the tender.

The successful bidder is expressly obliged to maintain absolute confidentiality and reserve regarding any data that may become known as a result of participation in this tender, or, on the occasion of the fulfilment of the contract, especially personal data, which may not be copied or used for any purpose other than that for which the information has been designated.

When the object of the contract is the construction of Information Systems and/or Technological Infrastructures, the duty of secrecy includes the technological components and technical security measures implemented in them.

The successful bidder will be responsible for any violations of the duty of secrecy that may occur on the part of the staff in their charge. Likewise, it is obliged to apply the necessary measures to guarantee the effectiveness of the principles of minimum privilege and need to know, on the part of the personnel participating in the execution of the contract.

Once the contract has ended, the successful bidder undertakes to destroy with sufficient security guarantees and/or return all the information provided by the CTTI or the body promoting the tender, as well as any other product obtained as a result of it.

2 SERVICE LEVEL AGREEMENTS (SANS)

The objective of this section is to describe the SLS model, which defines the **indicators** and **levels of service** required, and establishes an objective and measurable basis that reflects the commitment between the successful bidder and the CTTI to provide the required services in a satisfactory manner, vis-à-vis the Generalitat de Catalunya.

The CTTI aims to obtain a high quality level of service, as well as a high degree of satisfaction on the part of users, based on:

- The establishment of service indicators, so that the CTTI can carry out an objective evaluation of the service and its deliverables, and that the successful bidder has a basis for correcting any deficiencies in the provision, and for the improvement of its processes and organization.
- The establishment of a penalty model that relates the level of service provision to its billing.

For these reasons, the following SLA structure is defined:

- ANS of Application. These are the indicators that measure the level of service of the applications individually for each of them.

- ANS of Scope. These are the indicators that measure the overall level of service for each area.
- YEARS of Contract. These are the indicators that measure the degree of achievement of administrative agreements and the overall management of the contract.

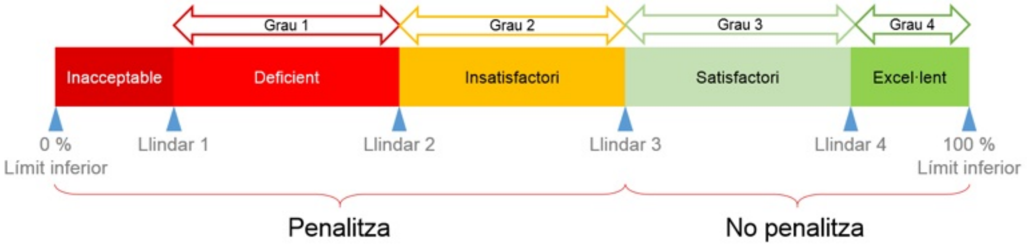
2.1 CHARACTERISTICS OF INDICATORS

The indicators will have the following characteristics:

- Code. Unique identifier of the indicator.
- Name. Defines the measurement object of the indicator.
- Description. Description of the indicator and its objective. The restrictions necessary to carry out the calculation of the value of the indicator are included (e.g. time restrictions, classification of incidents,...).
- Service. Determine the technological service to which the SLA is applied.

Abbreviation	Service
GN	General, applies to all services
GO	Operational management
SU	User support
GP	Platform management
MC	Corrective maintenance
MP	Preventive, perfective and adaptive technical maintenance
EV	Evolutionary maintenance

- Obtaining formula/tool. Formula to be applied for the calculation of the value of the measurement indicator, identifying the variables involved in the calculation (metrics) and, where appropriate, the reference to the tool that allows the automation and extraction of the data.
- Periodicity. Frequency of measurement of the indicator value.
- Degree thresholds for the definition of the brackets. Values that define the degree of compliance with the required level of service. For each indicator, 4 degree thresholds will be defined. Depending on the band, the indicator will present the following values:



- Maximum penalty. Determines the maximum value that the penalty can reach in the event of non-compliance with the defined target threshold.

Degree of the indicator

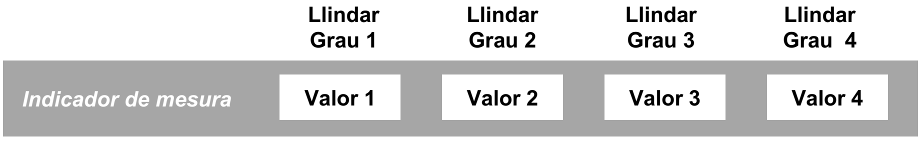
The grade of the indicator can take the following values:

- Grade 1: Deficient or Unacceptable
- Grade 2: Unsatisfactory
- Grade 3: Satisfactory
- Grade 4. Excellent

Grade 4 will be the target level, while grade 3 will be the minimum performance level to consider the indicator to be satisfactory.

2.2 CALCULATION OF INDICATORS

For each indicator, 4 thresholds are established to define the **linear sections** that must allow the obtaining of the associate **degree**.



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

For the value measured by an indicator (indicator value), it will be necessary to search for the thresholds between which it is located and apply the following procedure, taking into account whether the values defined by the thresholds (Value 1 – Value 4) are increasing or decreasing:

- For increasing threshold values (Grade 1 Threshold value < Grade 4 Threshold value)
  1) If the value is below the threshold of 1, the degree will be 1.
  2) If the value is equal to or greater than threshold 4, the degree will be 4.
  3) In all other cases, the Degree calculation formula will be applied.
- For decreasing threshold values (Grade 1 Threshold value > Grade 4 Threshold value)

1) If the value is above the threshold of 1, the degree will be 1.

2) If the value is equal to or less than threshold 4, the degree will be 4.

3) In all other cases, the Degree calculation formula will be applied.

Calculation formula of the Degree:

Grade = $\frac{(\text{Valor indicador} - \text{Valor llindar inferior})}{Valor\ llindar\ superior\ - Valor\ llindar\ inferior}$+ Grade corresponding to the lower threshold

When applying the Bachelor's degree calculation formula, the following considerations must be taken into account:

- When two or more thresholds take the same value, the value of the *"Degree corresponding to the lower threshold"* corresponds to that of the upper coincident threshold.

  For example, when the *Grade 1 Threshold* and the *Grade 2 Threshold* take the same value, the "*Grade corresponding to the lower threshold"* corresponds to the *Grade 2 Threshold*, i.e., it takes a value of 2.

- When the value measured by an indicator (*indicator value*) coincides with any of the values defined by the thresholds (Value 1, Value 2, Value 3), the value corresponding to the matching threshold will be taken as the "Lower threshold value". When two or more thresholds take the same value, the value corresponding to the upper matching threshold will be taken as the "Lower threshold value".

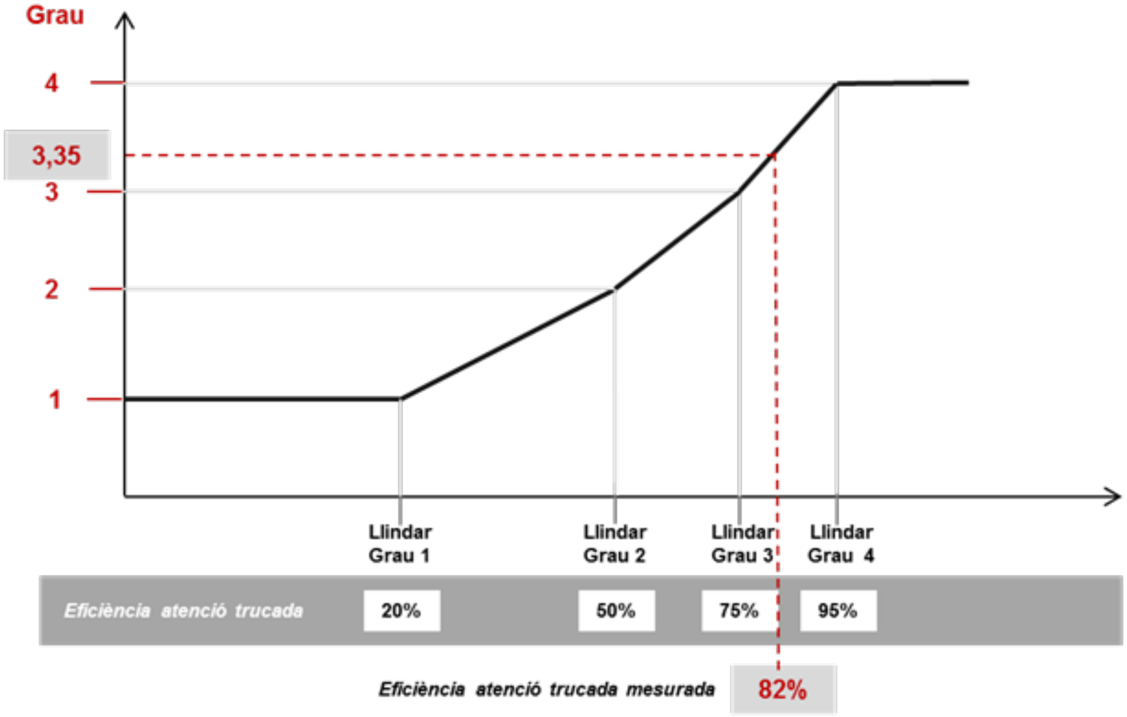
  For example, assuming the following threshold values: *Grade 1 Threshold* and Grade 2 *Threshold* take the same value, 20%, *Grade 3 Threshold* takes 75% and *Grade 4 Threshold* takes 95%; when the value measured by the indicator takes 20%, the "*Lower Threshold Value" takes 20%, the* "*Upper Threshold Value" takes 75% and* the "*Degree corresponding to the lower threshold"* takes value 2.

Example of calculation:

Let's assume that we have the indicator "Call service efficiency" that can take percentage values between 0% and 100% and that the target value is 95%. If the following thresholds have been defined:

- *Threshold Grade 1. The value of the indicator is 20%*
- *Threshold Grade 2. The value of the indicator is 50%*
- *Threshold Grade 3. The value of the indicator is 75%*
- *Threshold Grade 4. The value of the indicator is 95%*

If the value measured in a period by the indicator "Call service efficiency" has been 82%, the calculated degree is: ((82-75)/(95-75))+3=3.35.



This model is dynamic, as it allows adaptation over time to new objective levels and minimum levels, without varying the possible degrees.

We could determine, for example, that during the transition phase of the service the threshold of grade 3 is 85%, while in the execution phase the second year it is already 95% and the threshold of grade 4 increases to 98%.

2.3 SOURCES OF INFORMATION FOR OBTAINING SERVICE LEVELS

The CTTI will use the CONTIC (ICT Service Level Agreement Control) information system for the calculation, analysis and storage of service and process indicators. Although at the beginning of the service the CONTIC information system is not able to calculate all the defined indicators, they will be progressively incorporated into its catalogue. The supplier must provide the indicators that are under its responsibility through the enabled interfaces.

Whenever possible, the source of the data used for the calculation of the indicators will be the ticket management and monitoring tools of the CTTI. For those indicators that the CTTI is not able to obtain autonomously, it will be the responsibility of the successful bidder to calculate and report them with the established periodicity and the detail and format required by the CTTI, which may reach the level of service instance or ticket.

The CTTI will use the service indicators to carry out the calculations of compliance with the SLAs and to generate the corresponding reports.

2.4 MODIFICATION OF INDICATORS AND SERVICE LEVELS

Throughout the provision of the service, in the event of any modification of the indicators and service levels with the aim of providing a better service, the CTTI together with the provider will agree and plan its modification.

Some of the causes that may lead to these modifications are, among others, variations in the functional environment and business conditions, changes in scope and volume, innovations and improvements in the service.

2.5 APPLICATION OF SERVICE LEVEL AGREEMENTS

The Service Level Agreements defined for each service will be mandatory throughout the contract, except for the transition phase of the service.

For each service, the successful bidder must fully comply with the Service Level Agreements defined once the transition provision phase has ended.

3 RELATIONSHIP MODEL

The relationship model defines the functions and responsibilities of the supplier and the CTTI in a common framework of action, to ensure compliance with the obligations of each of the parties.

The relationship model is based on establishing the committees and their operation, to ensure compliance with the requirements of the conditions of execution of the services described in these specifications.

The successful bidder may expand, improve and detail, based on the guidelines set out herein, the proposed organisation and the specific scheme of the relationship with the CTTI, as well as the control mechanisms specific to each service and transversal function. The successful bidder's work team must have the appropriate sizing, training and means to carry out the assigned tasks.

The relationship model is based on a structure of competencies and functions that fall on a skeleton of those responsible for the supplier, who will relate to the CTTI based on 2 levels (management and operational).

The successful bidder will assign to the CTTI the managers who will support the Relationship Model. The team of managers must also have the appropriate size, training and means to carry out the functions and responsibilities assigned.

3.1 LEVELS OF THE RELATIONSHIP MODEL

The functional levels of the relationship model are the strategic and operational levels.

Both the successful bidder and the CTTI undertake to ensure that decisions taken at one level flow to the later or earlier level.

Management Level

The main objective of this level is to establish the guidelines of the contract and to monitor the set of activities carried out in the period, especially aimed at achieving the objectives and efficiencies proposed by the supplier.

Attendees on behalf of the successful bidder in committees at this level (steering committee) must have decision-making capacity on service commitments.

It is the maximum level of monitoring of the contract and the provision of the service. From this level, proposals for action in those aspects that may lead to the modification of the contract will be submitted to the contracting authority.

Operational Level

This level aims at the daily operation of the service according to the procedures developed and to deal with specific problems that affect the service provided.

3.2 MANAGEMENT BODIES (COMMITTEES)

The composition of the different committees between the CTTI and the successful bidder is described below, and their operation, to ensure compliance with the requirements of the conditions for the execution of the services described in these specifications. These committees will also have the function of executing the mechanisms to adjust these conditions in accordance with the evolution of service needs.

The bidder must make explicit the structure and functioning of the Relationship and Coordination Committees that are necessary to maintain a permanent dialogue with the actors involved in the process.

If it deems it appropriate, the CTTI may demand changes in the frequency of meetings, as well as request extraordinary follow-up meetings.

Extraordinarily, a temporary work team may be formed with specific objectives previously agreed.

Both the provider and the CTTI will commit to ensuring that decisions made at one level flow to the later or earlier level.

The different committees identified above are described below with the following structure by way of example, without prejudice to the fact that throughout the execution of the service the characteristics of each committee may be adjusted (Participants, Objectives, Entries, Exits, etc.).

In this sense, the supplier must incorporate the people responsible for each area of execution into the different committees according to the specific issues to be dealt with in the committee.

3.2.1 Management Committee

The frequency of this committee is expected to be quarterly, but this period may be modified according to the needs of the service.

<table>
<tr><td colspan="4">Title
Management Committee</td></tr>
<tr><td colspan="4">Participants</td></tr>
<tr><td>***CTTI***</td><td colspan="2">***Generality***</td><td>***Provider***</td></tr>
<tr><td>- Service Manager
- Other attendees (if applicable)
- Contract Manager (if applicable)</td><td colspan="2">- Head of the Cybersecurity Agency of Catalonia (if applicable)</td><td>- Service Manager
- Project Manager
- Account Manager (if applicable)</td></tr>
<tr><td colspan="4">Objectives</td></tr>
<tr><td colspan="4">- Marking Tactical Guidelines
- To monitor the set of activities carried out in the period, especially aimed at achieving the objectives and efficiencies proposed by the supplier.
- Review and status of the most relevant security aspects (risks, incidents of the period, ongoing developments)
- Inform and propose to the contracting authority any possible modifications to the contract that must be carried out.
- Approve increases and decreases in the volume of recurring service.
- Review and propose penalties for non-compliance with the service and escalate them to the contracting authority.
- Agree on the contract's dashboards.
- Transfer tactical guidelines to the operational level.
- Plan, prioritise and review activities with a cross-cutting impact.
- Monitor contractual obligations.
- Carry out financial monitoring.
- Development of innovation proposals in line with the transversal strategy of the CTTI.</td></tr>
<tr><td colspan="2">Entries</td><td colspan="2">Departures</td></tr>
<tr><td colspan="2">- Monitoring reports and dashboards
- Minutes of the contract operating committee.
- Decisions to be made</td><td colspan="2">- Minutes (signed between the parties)
- Decisions made
- Proposals to the Contracting Authority</td></tr>
<tr><td colspan="4">Periodicity</td></tr>
<tr><td colspan="4">Quarterly or at the request of the CTTI</td></tr>
</table>

3.2.2 Operational Committee

The frequency of this committee is expected to be monthly, but this period may be modified according to the needs of the service.

Title **Operational Committee**
Participants

<table>
<tr><th><em>CTTI</em></th><th><em>Generality</em></th><th><em>Provider</em></th></tr>
<tr><td>- Service Manager
- Other attendees (if applicable)</td><td>- Head of the Cybersecurity Agency of Catalonia (if applicable)</td><td>- Service Manager
- Project Manager</td></tr>
<tr><td colspan="3">Objectives</td></tr>
<tr><td colspan="3">- To carry out the monitoring and global control of the operation and provision of services in accordance with the SLAs of departmental application defined and with the specific needs within the scope of the department or entity
- Plan, prioritise and review ongoing activities
- Monitor the planning of the project, and verify the correct execution of the planned activities.
- Monitor the daily operation of the service and verify the correct management of requests, changes, problems and incidents.
- Develop and maintain the operational procedures necessary for the proper functioning of the services.
- Analysis of requests and/or situations of change in services.
- Scaling of possible improvements detected in the service
- Treatment of specific problems
- Development of innovation proposals in line with the strategy and business needs of the department or entity</td></tr>
<tr><td>Entries</td><td colspan="2">Departures</td></tr>
<tr><td>- Analysis and proposals for improvement
- Decisions to be made</td><td colspan="2">- Minutes (signed between the parties)
- Proposals to the steering committee
- Service monitoring reports and dashboards that are determined by service management.
- New operating procedures
- Decisions made</td></tr>
<tr><td colspan="3">Periodicity</td></tr>
<tr><td colspan="3">Monthly or at the request of the CTTI</td></tr>
</table>

3.3 STRUCTURE OF RESPONSIBILITIES

The following specifications identify the roles responsible for the CTTI and the successful bidder for ensuring compliance with this relationship model.

The roles that will participate in the different committees with the specific functions and responsibilities for the services subject to this tender are indicated below.

CTTI Roles

- **Contract promoter area:** This is responsible for defining the need for the contract, generating all the necessary documentation for the processing of the file and monitoring its execution.

- **Service manager:** This is responsible for monitoring and executing the services covered by the contract, aligning the business needs of the contracted services, as well as partial and final acceptance of the solution.

Supplier Roles

- **Account manager:** This figure is unique per supplier. It is the reference figure for all contracts between the CTTI and the supplier and the ultimate responsible for the provision of all the services and projects of the supplier. The account manager must have a decision-making authority on the service, especially in the case of joint ventures. This figure will be maintained throughout the life of the contract or contracts between the CTTI and the supplier, in commercial management, during the provision of the service and until its return. They must be guarantors of the existence of relationship mechanisms in their organisation to carry out the agreements made between CTTI and the supplier. In the event of changes in the scope and/or cost of the services that imply a contractual modification, it is responsible for conveying it.
- **Service managers:** The provider will assign a person responsible for each of the services provided. His main responsibilities are:
  - The daily management and monitoring of the service, as well as the resolution of conflicts and temporary or permanent resizing of the same.
  - Maintenance of the record of the evolution of the service in order to subsequently be able to prepare service reports and justify compliance with the SLAs.
  - Monitoring and control of the resources assigned to the service(s)
  - They will analyse any deviations and serious situations within the quality, deadlines or scope of the service
  - At a transversal level, they will carry out cost control, effort estimation and monitoring.
  - At a transversal level, they will analyse the modifications in the scope and cost of the service that may arise, and will interpret these modifications with respect to the contracts in force. In the event that they do not involve a contractual modification, they must be the guarantor of formalising and implementing the agreements made internally in their organisation.
  - They will ensure good collaboration between the different successful bidders with whom it must relate in order to improve the final business service.
- **Functional Manager:** This is responsible, in development services (on-demand projects), for the analysis of the solution in order to align the needs of the business with the development and implementation, as well as the final acceptance of the solution prior to its delivery to the client.

- **Head of Management Control:** This is the figure who will consolidate and provide the CTTI with both objective and subjective information; valued (reliable and quality information and analysed based on knowledge of the model); that allow operational and strategic decisions to be made throughout the life of the contract.

  It will be responsible for ensuring that the CTTI receives the agreed management reports, both with economic-financial indicators and others, as well as monitoring the economic model agreed with the successful bidder.

- **Legal Responsible:** This will be the main interlocutor with the CTTI in legal-legal matters for all the services/contracts provided by the successful bidder. It will be responsible for formalising the interpretations made with respect to the contracts in force, when these involve contractual modifications.

- **Invoicing Manager:** They must provide information regarding the invoicing process, according to the model and format defined by the CTTI, as well as collaborate in the reconciliation process. It will ensure and ensure that the supplier:

  - Provide information on the invoicing process, according to the model and format defined by the CTTI:

    - Present the invoice, and the detail for each element/concept of the amounts invoiced, adapting to the following criteria:

      a) Complete detail of all invoiced cost elements, identifying the minimum cost units.

      b) Classification and coding of invoiced cost elements:

      c) The coding format and typing criteria will be validated together.

  - Collaborate in the conciliation process.

- **Architecture Manager:** This is responsible for coordinating and harmonizing the application of the corporate architecture in the information systems and services to be built or maintained by the supplier.

  His main responsibilities are:

  - To ensure compliance with the principles associated with the different domains, and compliance with ICT corporate architecture standards.
  - Propose and incorporate new ICT architectures while maintaining and/or evolving existing ones.
  - To ensure consistency in the application of the ICT corporate architecture.
  - Identify reusable components and promote both their generation and use.

- Provide a control mechanism, which is essential to ensure effective compliance with ICT corporate architecture standards.

- **Head of Innovation:** He is responsible for managing and directing the internal innovation process in his organization designed and oriented to the needs of the CTTI, becoming the head of the bidding company in the field of innovation before the CTTI.

  His main responsibilities are:

  - Propose, systematically and proactively, innovative ideas, opportunities and challenges and PoCs and pilot projects to the CTTI.
  - Design, manage and implement a model of relationship with the innovation ecosystem focused on its organization that connects it with the innovation ecosystem of the CTTI.
  - Monitor the innovation process and evaluate its results.

- **Project Manager:** This is responsible for ensuring the overall vision of the monitoring of the projects awarded to the supplier. It will be the responsibility of this figure to transmit and coordinate the application of the methodology established by the CTTI for the management of projects in the supplier.

- **Responsible for Support Operation and Service Provision:** It is responsible for compliance with the processes of managing requests, incidents, knowledge, problems, events and monitoring (support) and management of configuration and inventory, changes, deliveries and deployments, capacity and availability (provision).
- **Quality Manager**: You will be responsible for:
  - Ensure the existence of a quality plan for projects, services and applications.
  - Quality assurance.
  - Verification of the execution of quality control.
- **Security Manager:** You will be responsible for:
  - Act as a link between the application provider and the different agents involved (CTTI, Cybersecurity Agency of Catalonia) when security issues are discussed
  - Guarantee, lead and promote compliance with the security regulatory framework of the Generalitat de Catalunya within its organisation, ensuring the correct implementation of security levels and their corresponding measures (technical, organisational, and legal); as well as the security guidelines established by the Cybersecurity Agency of Catalonia.
  - Coordinate regular follow-up meetings with CTTI and the Cybersecurity Agency of Catalonia to report on the degree of adequacy of applications to the security model of the Generalitat de Catalunya, identify the most relevant risks and propose action plans for their mitigation.

  - That all the staff of the successful bidder who will provide services to the CTTI and the Generalitat, go through an awareness and training plan on security matters, focusing on the regulatory framework of the Generalitat and the security procedures that apply to it.
  - Ensure regular information to the CTTI and the Cybersecurity Agency of Catalonia according to the deadlines set, of everything related to security (incidents, corrective measures, risks, new projects, initiatives, etc.).
  - Ensure that all the provider's personnel who have to process data or data processing systems of a sensitive level or higher sign an Individual Confidentiality Agreement. The CTTI and the Cybersecurity Agency of Catalonia will be able to audit this aspect.
  - Operational coordination with the incident response team and with the SOC of the Cybersecurity Agency of Catalonia in the event of incidents or possible cybersecurity threats (Delivery of evidence for the management and investigation of security incidents, support for the rapid application of protection and containment measures against threats or cyber incidents, having information linked to the application (URLs, application user, logs, etc.))
  - Use the Security Portal on a regular basis to keep track of all information related to the security of the applications.

- **Head of Continuity:** He will be responsible for:
  - Guarantee and lead within their organisation the correct implementation of the continuity and availability plans (both technological and business services) agreed with the CTTI.
  - Ensure regular information to the CTTI according to the deadlines set, of everything related to Continuity and Availability (incidents, corrective measures, risks, new projects, initiatives, etc.

- **Head of Observability and Monitoring**
  - It will be responsible for the correct incorporation of observability and monitoring into the ICT Solutions under the responsibility of the successful bidder as set out in the section *"Activities associated with observability and monitoring*. Among its functions, it will have to ensure a correct implementation in time and form of the Observability necessary for the excellence of the services provided, guaranteeing continuous improvement. He is in charge of implementing the Observability standards within his organization, always in relation to the service object of the contract, and working in close collaboration with the corresponding head of the CTTI.

- **Responsible for the processes of the Control Center**
  - The person responsible for the processes of the Control Centre on the part of the successful bidder is responsible for guaranteeing the application of the policies and methodologies of the Control Centre with regard to the management of critical business processes. They must work in close collaboration with the corresponding Head of the Control Centre

for the services covered by these specifications. This collaboration must guarantee the following:

- Carrying out monthly operational monitoring of the Control Centre's key indicators (for example: response time to critical incidents, modifications in monitoring based on changes in the infrastructure, quality of participation in Technical Rooms or Crisis Committees, etc.) to detect shared points for improvement.
- Guarantee, in a manner and in a timely manner, the implementation of the improvements detected based on operational monitoring or the evolution of the DPC service and/or the Control Centre.
- To guarantee that the people assigned to the processes managed by the Control Centre respond in a timely manner.

4 DEFINITIONS, MODELS AND PROCESSES

4.1 CLASSIFICATION OF APPLICATIONS.

4.1.1 Business criticality

Every application has an associated business criticality according to the following scale:

- **Very high.** This includes applications that:
  - **Business criticality Level 0:** They support processes on which people's safety depends (emergency care, eCAP, ...)
- **High.** This includes applications that:
  - **Business criticality Level 1:** They support processes on which the subsistence of third parties depends (RMI, Welfare subsidies, ...)
  - **Business criticality Level 2:** They support processes related to the essential functioning of the Government (press room, tax management, DOGC, ATRI, ...)
- **Stocking.** This includes applications that:
  - **Business criticality Level 3:** They support processes with legal requirements (for example: judicial notifications, GIP-SIP, ...)
  - **Business criticality Level 4:** They support other processes considered critical but that are not included in any of the above groups (impact on reputation or media)
- **Low:** All other apps

4.1.2 **Quality characteristics**

The CTTI establishes how the health of applications should be measured and evaluated according to different quality characteristics.

More information can be found at:

- Quality characteristics of a solution (https://qualitat.solucions.gencat.cat/glossari/caracteristica_qualitat/)
- Quality characteristics of deliverables (https://qualitat.solucions.gencat.cat/glossari/caracteristica_qualitat_lliurables/)

4.1.3 Information Security Classification

The classification of the information of an application in terms of security (considering confidentiality, integrity, availability, authenticity and traceability) is made according to the following scale of levels:

- **Very critical.** Applications are included with:
  - Highly confidential information, accessible by a very limited number of individuals, with very high integrity, authenticity and traceability requirements, through the use of certified products.
  - Systems classified as high level according to the requirements of the National Security Scheme.

  Examples: Applications related to cryptographic key management, applications with information from the Security Forces

- **Criticism**. Applications are included with:
  - High-level personal data.
  - Confidential information restricted to a small circle of people, with encryption and traceability requirements.
  - Its dissemination or lack of integrity could lead to serious damage to the Department/Body: non-legal non-compliance that cannot be remedied, significant damage to an individual, political repercussions,...
  - Systems classified as medium level according to the requirements of the National Security Scheme.

  Examples: Applications with data on gender-based violence and abuse, trade union management systems, health data, work-related injuries and accidents, management and processing of judicial files, management of files in prisons or juvenile centres.

- **Sensitive**. Applications are included with:
  - Medium-level personal data.
  - Information restricted to areas or units, with advanced access control requirements and guarantees of integrity and authenticity. Its dissemination or lack of integrity could have an impact on the

Department/Agency: legal non-compliance that can be remedied, minor damage to an individual, illicit profits of third parties, limited disrepute of reputation,...
  - Systems classified as low level according to the requirements of the National Security Scheme.

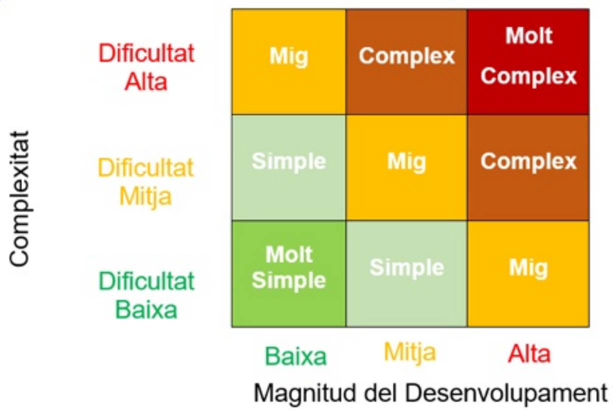
- **Internal**. Applications are included with:
  - Data that must remain within the Department/Body, perhaps shared with third parties who provide services or with whom there are collaboration agreements (suppliers, local bodies, associations, other bodies,..) exclusively for the performance of the functions entrusted to them.
  - Non-critical reliability information; deficiencies in their entirety may result in slight or no damage, although they require the application of basic access control guarantees.
- **Public**. Applications with public information are included, with no restrictions on the dissemination of their content.

4.2 EVOLUTIONARY DEVELOPMENTAL CLASSIFICATION MODEL

The classification of evolutionary development services will be carried out taking into account their complexity determined by the activities to be carried out and the magnitude of the development to be carried out on the application.

Taking into account these two dimensions, 5 types of small evolutionaries are defined:

- **Very Simple Project**
- **Simple Project**
- **Middle Project**
- **Complex Project**
- **Very complex project**



Complexitat	Baixa	Mitja	Alta
Dificultat Alta	Mig	Complex	Molt Complex
Dificultat Mitja	Simple	Mig	Complex
Dificultat Baixa	Molt Simple	Simple	Mig

Magnitud del Desenvolupament

This classification combines the following types of complexity and magnitudes of development:

Levels of **Complexity**:

1. **Low difficulty technique:**
   a. Closed solution projects or integration of SaaS services.
   b. Application of simple algorithms.
   c. Modest data processing.
   d. Proofs of concept.

2. **Medium difficulty technique:**
   a. Projects that require complex algorithms.
   b. Functional requirements of medium difficulty.
   c. Data processing with rules of medium complexity.
   d. There may be data in unstructured and/or non-standard formats.
   e. Productive pilots.
   f. Partially complete data.

3. **High difficulty techniques:**
   a. Projects that need ad-hoc development.
   b. They may require highly complex algorithms.
   c. Business consultants may be required for functional requirements.
   d. Highly complex data processing is required.
   e. Incomplete data.

Levels of **Magnitude of Development**:

1. **Low Magnitude:**
   a. A development of minimal dimensions is planned.
   b. Short-term developments.
   c. Small-scale data processing.
   d. The data are complete.

2. **Average Magnitude:**
   a. Developments that may take weeks.
   b. The collection of requirements can take weeks.
   c. Obtaining the data may not take an immediate time.

3. **High Magnitude:**
   a. Large developments.
   b. The analysis, design, and development phases may require several weeks or months.
   c. Data processing can take many hours, due to the magnitude of the development.

4.3 MODEL FOR QUANTIFYING MAINTENANCE SERVICES

4.3.1 On-demand services

A standard valuation method is established for each of the services and what data is required to estimate the work, including the tasks or dedications necessary to execute the requested orders with an end-to-end view.

The estimation model establishes the necessary mechanisms to objectify the effort assessment process within demand management. The on-demand services to be developed within the framework of the provision of the service require an initial estimate of efforts by the successful bidder, in order to analyse their feasibility and be able to plan the resource needs to be used. As well as the validation of the CTTI of the proposal made.

The objectives to be achieved are:

- Ensure that the successful bidders undertake to comply with the actions and minimum quality criteria for each of the evolutionary / projects according to their nature.
- Unify the way of assessing, standardising work tools and establishing common compliance criteria through a standard method.
- To make the review of the estimate and its justification more effective, limiting the validation effort to minimum criteria, limited within the evaluations of the activities, obliging the successful bidder to comply with them.
- To allow the costs of each activity and phase of the evolution/project to be quantified automatically, calculating the cost of the task according to the elements of the service, technological environment (ET) and Lot to which it belongs.

A method is established to assess and quantify the cost and effort of evolutions and projects, based on the classification of tasks, types and level of difficulty:

- The tasks to be carried out in each of the on-demand services.
- The required deliverables defined in the corresponding sections of chapter 3. Conditions of execution of the services .
- The technical and functional knowledge necessary to carry out these tasks of the teams.
- The timetable for their execution.

The CTTI will provide the templates or files, and when a tool is developed, they will be introduced into it, to price the needs of the service, which serve to calculate the effort and cost involved, indicating and assessing certain predetermined tasks, allowing, at the same time, the personalization of the data according to the possible casuistry of each application and giving importance to security and quality.

It will therefore be necessary to make a template or introduce it in a tool, the assessments for the development and deployment, if applicable, in the different environments, to evaluate the costs involved in the different evolutions/projects, where the following are available:

- Calculation based on the construction elements of the different evolutions or use cases built in the description of development tasks.
- Automatic calculation of the tasks to be done during deployment according to the selected application, forcing to justify the creation of new tasks and the elimination of the default ones.

- Predefined calculation of the effort involved in doing each task, giving the possibility of readjustment (+/-), due to the complexity or difficulty of the task, always with justification
- It will be necessary to easily parameterize the deployment tasks included in each module. Table where it is easy to define which activities correspond to each module.

As a summary, this template or the tool that will be made available to the successful bidders is based on the quantification of expenditure by service element awarded, based on the Lot and Technological Environment (ET) of the application evaluated and awarded.

It is assumed that the calculation is automatic of the effort involved in doing each task and the service element that is necessary, giving the possibility of readjustment (+/-), always with justification. From this information it is possible to have the total calculation (breakdown of each of the phases of the work to be carried out)

It will be necessary for the CTTI and the successful bidder to parameterize the tool, when it is available, in a simple and understandable way, allowing the customization of the data according to the possible casuistry of each application, giving importance to security, and defining minimum quality conditions.

4.3.2 Recurring services

The causes that can increase or decrease the volume of recurrences are the following:

- Variation in the number of users and their turnover rate
- Change of service schedule
- Change in the criticality of the service level
- Incorporation of a new evolutionary
- Change of a technological platform
- Evolution of functionalities and/or incorporation of new technologies (e.g. robotics)

A review of the appellant may be carried out by the CTTI, through the presentation of the corresponding justifying report to the executive committee, taking into account, in order to assess and quantify the cost and effort of evolutions and projects, based on the classification of the tasks, types and level of difficulty. The templates will be available or the tool to price the needs of the service, the templates are used to calculate the effort and cost involved, indicating and evaluating certain predetermined tasks, allowing, at the same time, the customization of the data according to the possible casuistry of each application and giving importance to security and quality.

In the event that the small maintenance evolutions on demand may cause a recurring variation, it must be proposed by the successful bidder and approved by the CTTI at the time of acceptance of the offer of the evolutionary on demand. In the case of major evolutions of new functionalities, prepared by a third party, the possible variation of the appellant must be approved by the CTTI prior to its commissioning, based on the proposal made with the template or on the tool with the details of the tasks and efforts to be made according to the detail of the maintenance service.

A maximum annual recurring increase is established equivalent to 18% of the cost of the evolutionary rate, taking into account that not every evolution necessarily has an impact on the recurring one. The increase in recurring costs may decrease as time goes by, as a result of the stabilization of the service.

It should be noted that the cost of corrective maintenance will not be incorporated until the end of the warranty period.

4.4 PROCESSES, ACTIVITIES AND DOCUMENTATION ASSOCIATED WITH SERVICE MANAGEMENT

The purpose of service management is to control and ensure that services are available, accessible, maintained, updated, informed, disseminated and governed and meet the quality objectives of the CTTI.

The processes of the CTTI are defined and approved by the Management and published for the performance of all the actors involved.

The details of the processes are published at:

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

These processes are mostly supported by a single management tool in order to streamline, document and control any event, incident, problem, known error or data necessary for each service and give the best possible response to any request for the service. This tool is owned by the CTTI and determines its use. It may be used by the SAU, CTTI and any approved service company involved in the management of service processes.

In addition, each successful bidder may make proposals to the CTTI of the data to be incorporated in order to improve the management of requests, incidents, changes and service problems under their responsibility.

All the information, linked to each element of the processes detailed below, must be able to be consulted by any agent participating in this process (Users, UAS, CTTI, Control Centre, suppliers and other agents).

4.4.1 REQUEST MANAGEMENT

In this process, the successful bidder is specifically responsible for the following aspects:

- To participate proactively with the CTTI in the definition of requests for the services for which it is responsible, including the other providers involved in the provision of the end-to-end connectivity service.

- Ensure the use of requests and follow the established Operating Instructions.
- Document and provide Level 1.5 procedures for the UAA or automations with the aim of decreasing the time to resolve requests to the end user.

4.4.2 INCIDENT MANAGEMENT

The main objective of Incident Management is to recover the normal operation of the service in the shortest possible time, minimizing the impact on business operations, ensuring that the service remains at the level of quality and availability associated with the business criticality of the service provided by the successful bidder.

The Incident Management process supports all the services that CTTI provides to the user and therefore its scope is the resolution of all incidents that may affect these services. An incident is understood to be any event that is not part of the normal operation of a service and that causes, or may cause, the interruption, malfunction or degradation in the quality of the service.

In this process, it is important to note that, depending on the business criticality of the service that the successful bidder maintains, it assumes responsibility for applying the procedures that the CTTI determines for each of the cases. These procedures establish who to relate to, such as the User Support Service, the Control Centre and any other supplier involved in the process.

With regard to the Incident Management process, the successful bidder will be responsible for:

- Participate in the Incident Management process, actively and with the necessary technical knowledge, end to end, for all the services provided to the CTTI.
- Document in the tool that the CTTI determines all the actions carried out to solve the incidents.
- Record and communicate the incidents that the successful bidder detects (via monitoring or analysis of patterns/trends) using the communication channels and procedures determined by the CTTI.
- Promote and monitor actions throughout the life cycle of an incident, collaborating with the rest of the approved companies involved in it, to guarantee the restoration of the service in the shortest possible time.
- Carry out specific reports for:
  - High-impact incidents in all the services it provides to the CTTI, differentiating delivery times according to the criticality marked by the business.
  - To respond to certain business needs whenever the CTTI requires it.
  - The successful bidder must make use of the templates provided by the CTTI.

- To attend on a mandatory basis and within the established deadlines all the crisis committees, technical rooms and control rooms, that the CTTI requires to carry out the treatment of incidents of the services maintained by the successful bidder.
- Keep the data stored in the KMDB up to date and accessible.
- To propose the information to be incorporated into the KMDB in order to improve the responses to incidents of services under its responsibility.
- Lead the dialogue with manufacturers, if necessary, and especially in the case of product-based solutions. The successful bidder must have support contracts with the manufacturers of the infrastructure platforms on which the applications are run, with the appropriate conditions to provide the service for which the successful bidder is responsible (among others, timetable and SLA).
- Ensure the relationship with the rest of the processes involved in incident management, focusing above all on the management of problems, changes and events and monitoring, without forgetting the rest that may be necessary (for example, configuration management, capacity and availability management and those determined by the CTTI).

4.4.3 KNOWLEDGE MANAGEMENT

The main objective of Knowledge Management is to define the strategy, protocols and type of documents that the KMDB must store and to verify that the information delivered is adequate when it goes into production, or an evolution of an existing solution. He will also be responsible for implementing and controlling the KMDB's feeding and operating mechanisms.

The successful bidder must participate in the Knowledge Management process, actively and with the necessary technical knowledge, end to end, for all the services it provides to the CTTI.

In this process, the successful bidder is specifically responsible for the following aspects:

- Incorporate and publish the documents determined by the CTTI as well as all the documentation that the successful bidder considers necessary for the comprehensive management of the services for which it is responsible, in the KMDB that the CTTI determines.
- Prepare and keep updated all the documentation necessary to support the processes of the management of services of the CTTI, according to the established templates. Especially with regard to the necessary functional documentation of the services that facilitate the action of the Control Centre.

4.4.4 PROBLEM MANAGEMENT

The main objectives of Problem Management are to reduce the impact of detected incidents on the business, prevent their recurrence and identify possible points of failure. To achieve this, the successful bidder must proactively participate in the Problem Management process, in order to:

- Analyse incidents without an established root cause to establish patterns and points of failure and then analyse them taking into account the level of risk to the business and propose the necessary corrective actions.
- To be a promoter in the opening of possible problems after the analysis of incidents specific to the service (trends and patterns).
- Document information on known errors, the solution implemented, the actions carried out as well as information on possible temporary solutions that may have been implemented, ensuring that the information is collected in the tool determined by the CTTI.
- Analyse the economic impact of the implementation of the temporary or definitive solution to a problem to help in decision-making.
- Draw lessons learned from problem-solving.
- Carry out the analysis of trends and patterns of incidents or problems in order to improve their identification and be able to prevent risk situations that may lead to unavailability of services.

4.4.5 EVENT MANAGEMENT AND MONITORING

The main objective of Event Management is to act as one of the input sources of the Incident Management and Problem Management processes, and will be fundamentally supported by the use of the different monitoring and observability tools.

The CTTI will be responsible for defining the monitoring and observability policies and the successful bidder will ensure and actively collaborate with all the tasks that may be necessary to carry out this activity.

The successful bidder will be responsible for providing all the information, scripts and/or other necessary elements, in the format requested by the CTTI, so that this monitoring can be applied and/or integrated into the CTTI tools. In this sense, the successful bidder must have the necessary tools to carry out these actions and make the necessary developments to guarantee it at no additional cost to the service itself.

More specifically, with regard to the Event Management and Monitoring process, the successful bidder will be responsible for:

- Carry out functional monitoring of the service, which must be consistent throughout its life cycle, in each of the different environments (non-productive and productive). To bring this end-to-end functional monitoring in an automated way to the CTTI tools. This activity will apply to those services that the CTTI deems appropriate.
- Actively collaborate in the implementation of real user experience monitoring or other market trends.
- Occasionally, and in agreement with the CTTI, the performance of this monitoring may be transferred to the CTTI, leaving the successful bidder responsible for preparing the necessary documentation to carry out this monitoring.
- In the event of substantial changes or new functionalities of the services, it will be necessary for them to facilitate their monitoring and observability. This implies that a series of criteria must be taken into account, such as:
    - Security: Possibility of creating users with specific profiles so that they cannot access sensitive data and that they cannot be intrusive.
    - Functional: That this user can access the main functionalities as a user would, in order to test/validate their operation.
    - Statistical: Avoid false indicators, for example of consumption of the service as a real user, given that it is a synthetic user.
- In addition, it must be taken into account that the successful bidder must implement the monitoring that the CTTI requires as a result of the need for the rest of the management processes (incidents, problems,... etc.)
- Prepare and keep updated all the documentation necessary to support the processes of the management of CTTI services.
- Follow the management procedures associated with the process, defined by the CTTI.
- Ensure the relationship with the rest of the processes involved in event management and monitoring, such as: Incident management, change management, capacity and availability management, request management, problem management and the rest that may be necessary.
- Ensure end-to-end control of the process by generating follow-up reports in the established format. It is important to know that the successful bidder must carry out specific reports in the face of a business problem or need, whenever the CTTI requires it. The successful bidder makes use of the templates provided by the CTTI.

The successful bidder must have access to the monitoring consoles, which are determined in accordance with the CTTI, and have them available and monitored, at least during the established service hours of the applications in order to ensure the proper functioning of their services as well as to be proactive in the different operational procedures such as incident management, problems, events and monitoring, etc...

4.4.6 CHANGE MANAGEMENT

A change is any necessary action to be performed, whether for the maintenance, updating, improvement or implementation of a service, which may affect the configuration elements that make up the service, and which is supported.

The main objective of Change Management is to ensure the use of standardized methods and procedures with efficient and timely management of all changes, guaranteeing the quality and availability of the service at all times.

Changes can be initiated either proactively by providing some improvement to the service or reactively to resolve errors in the service, but in any case it will be necessary to analyze the suitability of making a first execution of the same in the pre-production environment.

The successful bidder must participate in the Change Management process, actively and with the necessary technical knowledge, end to end, for all the services it provides to the CTTI.

In this process, the successful bidder is specifically responsible for the following aspects:

- Rigorously apply the management procedures associated with the change management process, defined by the CTTI.
- Make use of the tools for the management/execution of changes determined by the CTTI.
- Determine and communicate the risk and impact on the business of the execution of each of the changes, reviewing interactions with other services. For this reason, the successful bidder is responsible for:
  - Know the architecture of the services end-to-end
  - Coordinate with the rest of the suppliers involved in the service (SHOCK or others) in order to be able to correctly determine the impact of the change and ensure its correct execution.
  - Communicate the implementation of the changes to the agents involved.
- Ensure, when possible, the execution of changes in the Production environment once they have been validated, exhaustively, in non-production environments and have been correct.
- Ensure that the different non-production environments available are aligned with the production environments and are suitable to guarantee prior testing before going into production.

- Perform/design/automate validation tests after the execution of the changes.
- Plan with the business the execution of the different changes, according to their needs and the existing execution windows.
- Ensure that change management maintains the relationship with the rest of the processes involved in the maintenance of the applications (for example, configuration management, problem management, event management, capacity management, availability management, continuity management, incident management and the rest that may be necessary).
- Propose the creation of standard change models to increase the degree of automation of tasks, always subject to assessment and approval by the CTTI
- Ensure control of the end-to-end change management process by generating follow-up reports in the established format. It is important to know that the successful bidder must make specific reports in the face of a business problem or need, whenever the CTTI so requires. The successful bidder will make use of the templates provided by the CTTI.

4.4.7 DEMAND MANAGEMENT

The objective of demand management is to understand, anticipate, influence customer demand and provide the necessary capacities to meet it.

According to the types of elements, demand is classified into:

- **Regular demand**, in the case of devices or services present in the Catalogue.
- **New Demand**, if new devices or services are requested in the Catalogue. Any new application will have to go through a specific approval and validation process at the central services of the CTTI and the ICT managers of the affected areas. The successful bidder of the service, with their contact with users and knowledge of the service, will help to capture the demand and needs of the customer. They will do so through:
    - The communication of the inputs received to those responsible for the Generalitat, following the relationship model defined by CTTI.
    - The preparation of activity studies, determining seasonalities, trends and patterns of use.

The results will be reflected in the corresponding service and activity reports, to be generated monthly.

4.4.8 CONFIGURATION AND INVENTORY MANAGEMENT

The main objective of Configuration and Inventory Management is to provide accurate and reliable information on all the elements that make up the CTTI's ICT services to support the rest of the procedures that require it. For this reason, the successful bidder will be responsible for registering the information required and defined by the CTTI for each Configuration Element (CI) in the Configuration Management Database (CMDB) of the CTTI, as well as ensuring that it is kept up to date according to the processes defined by the CTTI.

In addition, each approved company can maintain its own CMDB with necessary and detailed technical information on the services it provides to the CTTI. The CTTI may request the connection and/or consultation between the CMDB of the successful bidder and the CMDB of the CTTI.

Global responsibilities of the successful bidder:

- Prepare and keep updated all the necessary documentation to support the processes of the management of the CMDB of the CTTI.
- Ensure end-to-end control of the process by generating follow-up reports in the established format. It is important to know that the successful bidder must carry out specific reports in the face of a business problem or need, whenever the CTTI requires it. The successful bidder makes use of the templates provided by the CTTI.
- To carry out periodic audits of the information of the CMDB of the CTTI, following the procedures and deadlines established by the CTTI:
    - The successful bidder will be responsible for making the necessary modifications to the CMDB's CIs in order to regularise the inconsistencies detected through the audits.

The successful bidder must facilitate and give access to audits of its CMDB's where the CI's that make up the CTTI services are registered, under the same parameters described above.

4.4.9 DELIVERY AND DEPLOYMENT MANAGEMENT

The main objective of Delivery and Deployment Management is to help in the construction, execution of tests and delivery of services, so that the specifications set out in the design of the service are met, as well as the requirements of the users.

The successful bidder will be responsible for:

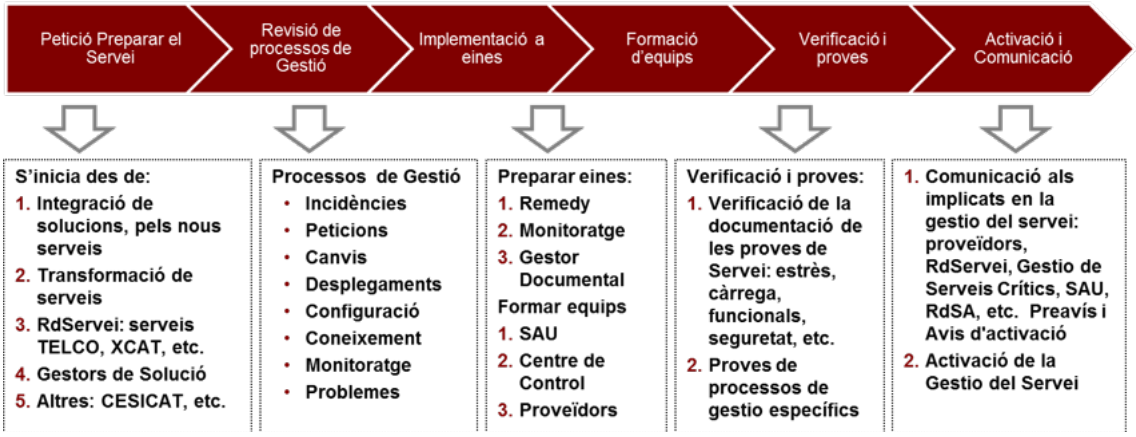
- Plan and control the implementation of new hardware and software versions of existing services.
- Communicate and manage customer expectations during the planning and production of new versions.
- Ensure that all master copies of the software and configurations in production and all their associated documentation are in the information repository defined by the CTTI for this purpose, and that the CTTI CMDB is up to date.

- It will be essential to use the tools defined by the CTTI for deployment automation and custody of configurations and code.
- Incorporate and publish the documents that the CTTI determines, as well as all the documentation that the successful bidder considers necessary for the comprehensive management of the services for which it is responsible, in the KMDB of the CTTI.
- Prepare and keep updated all the necessary documentation to support the processes of the management of the CMDB of the CTTI.
- Follow the management procedures associated with the process, defined by the CTTI.
- Ensure the relationship with the rest of the processes involved in the management of deliveries and deployments, such as: Incident management, change management, capacity and availability management, request management, problem management and the rest that may be necessary.
- Ensure end-to-end control of the process by generating follow-up reports in the established format. It is important to know that the successful bidder must carry out specific reports in the face of a business problem or need, whenever the CTTI requires it. The successful bidder makes use of the templates provided by the CTTI.

4.4.9.1 Prepare the Service Subprocess

Preparing the Service groups together the necessary activities to ensure that the teams that manage the operation and exploitation of the services have all the necessary information to be able to carry it out with the expected quality.

The activities included are the following:



Petició Preparar el Servei

Revisió de processos de Gestió

Implementació a eines

Formació d'equips

Verificació i proves

Activació i Comunicació

S'inicia des de:
1. Integració de solucions, pels nous serveis
2. Transformació de serveis
3. RdServei: serveis TELCO, XCAT, etc.
4. Gestors de Solució
5. Altres: CESICAT, etc.

Processos de Gestió
- Incidències
- Peticions
- Canvis
- Desplegaments
- Configuració
- Coneixement
- Monitoratge
- Problemes

Preparar eines:
1. Remedy
2. Monitoratge
3. Gestor Documental

Formar equips
1. SAU
2. Centre de Control
3. Proveïdors

Verificació i proves:
1. Verificació de la documentació de les proves de Servei: estrès, càrrega, funcionals, seguretat, etc.
2. Proves de processos de gestio específics

1. Comunicació als implicats en la gestio del servei: proveïdors, RdServei, Gestio de Serveis Crítics, SAU, RdSA, etc. Preavís i Avis d'activació
2. Activació de la Gestio del Servei

Illustration 2: Activities included in the preparation of the service

Once the process begins, a meeting is convened with all those involved in the management of the service determined by the CTTI.

At this meeting, the management processes of the service are reviewed and the documents and delivery deadlines for each involved and the delivery deadlines are determined.

The successful bidder must attend this meeting and submit the documentation within the deadlines determined in each case.

It is imperative that all tasks are completed in order to activate the service to end users.

Below is an example of the documents requested from the successful bidder:

Process	Template	Description
Management of incidents and requests	02. Template Components Resolution Groups	Members of the Resolution Groups of the successful bidder and responsible for the management of the service.
	03. Template Matrix of Escalats (KBA00000692)	Escalation Matrix with those responsible for attending to the escalation of incidents and requests for the service by the successful bidder
	04. Support SAU Template 1.5 (KBA00000052)	Detailed information so that the SAU can directly resolve the incidents and queries of the users that are agreed in each case
	09. SAU Training Template	Training in the SAU on the main functionalities of the service, managers involved, etc.
Configuration management	08. Template Modelat_CMDB.pptx (KBA00000181)	Inform the Remedy CMDB with details of the applications and modules that make up the service. The successful bidder must report on the relationships with the infrastructures that support the applications.
Monitoring Management	10. Monitoring template (mandatory in a critical service)	Detail the steps to be followed by the functional probe that will simulate the user's activity.
Critical Services Management	11. Critical Service Template	Detail the functional and technical architecture to facilitate the management of incidents in critical services

Table 1: Example documents

These documents will be adapted and completed with the evolution of the CTTI's management requirements.

4.4.10 MANAGEMENT OF AVAILABILITY, CAPACITY AND CONTINUITY

The management of availability, capacity and continuity are three of the axes of observability, where the availability of the system refers to the fact that the system is operating and providing the service effectively, while in the case of capacity, the sizing is important to meet the demand for the required service, mentioning that a lack of capacity can lead in the short or medium term to an incidence of system availability.

The capacity management function must be led by the successful bidder, who must optimise the management of resources and forecast the evolution of consumption, notifying sufficiently in advance of situations where there may be a lack of resources or surplus resources.

It is the responsibility of the successful bidder to generate and review the architecture document with the details of the configuration of each element and the initial sizing. Based on the initial architecture of the services, they evolve and it will be necessary for the successful bidder to analyze and understand the load impact of the resources and/or infrastructures of the demand of the current Business and how it will evolve or behave over time.

The necessary action plans must be planned to ensure that the needs of the Business are covered and at the same time manage the possible associated risks (e.g. saturation of systems).

In addition, the successful bidder must:

- To guarantee leadership in the diagnosis and improvement of the performance of services by the successful bidder.
- Carry out periodic tests of the availability of the services it provides.
- Ensure the relationship with the rest of the processes involved in the management of Capacity and Availability, such as: Incident management, change management, request management, problem management and the rest that are necessary.
- Ensure end-to-end control of the process by generating follow-up reports in the established format. It is important to know that the successful bidder must carry out specific reports in the face of a business problem or need, whenever the CTTI requires it. The successful bidder will make use of the templates provided by the CTTI.

The purpose of continuity management is mainly focused on guaranteeing the continuity of services and processes in the face of any adverse situation, avoiding a significant impact on the organization.

The objectives pursued are:

- Have Continuity Plans that allow an emergency situation to be managed efficiently.
- Guarantee the continuity of processes and services considered critical, the unavailability of which may have an irreversible impact.
- To test the Continuity Plans as a measure to guarantee their effectiveness in a real contingency situation.
- Focus efforts on mitigating relevant risks.
- Coordinate all the key people to deal with a contingency situation.

- Comply with legal/regulatory requirements in terms of business continuity.
- Align with the CTTI methodology and good market practices (ISO 27002, ISO22301 shortly), NIST sp 800-30.34, STEP 77, ITIL, ISO/PAS 22399:2007).

The supplier must:

- Deliver your continuity policy.
- Have a continuity plan for the services covered by the contract (and keep it up to date) and carry out recovery tests at least annually to achieve the required availability/continuity requirements. Prioritize testing over the most critical environments. Simulate different types of scenarios: massive infection of equipment, denial of service, etc.
- Draw up the test plan and execute them on the day of the test, in coordination with the teams that carry out the continuity tests of the Generalitat.
- Participate in the preparation and execution of continuity/disaster recovery tests (PRDs) and backup recovery tests, carrying out tests that certify their correct implementation.
- Submit to CTTI a service plan, as well as the reports and evidence that demonstrate the execution of the tests carried out.
- All PRD information must always be available to authorized and previously identified CTTI personnel.
- Document, develop and implement the availability measures necessary to cover the availability service level indicators.
- The management of availability, capacity and continuity are three of the axes of observability, where the availability of the system mentions that the system is operating and providing the service effectively, while in capacity it is important to size to meet the demand for the required service, mentioning that a lack of capacity can lead in the short or medium term to an incidence of system availability.

4.4.10.1 Business Continuity Plan of the Generalitat

The approved body must develop and implement a continuity plan for its staff and for the facilities from which it operates. The contingency plan will be validated by the CTTI, and must include at least:

- The recommendations of the ISO-22301 standard in order to guarantee the correct size of the proposed solution.
- The definition of a team of people, teams and organisation, detailing their individual roles and responsibilities as well as their hierarchy.
- An operation plan in alternative facilities (secondary management centre) owned by the winning company, which will include all the necessary means to carry out

the service, in the event that it is not possible to operate normally in the main management facilities. You will have to consider different contingency scenarios (pandemic, massive infection/encryption of the provider's equipment, the need to provide all services remotely, among others).

- Contingency infrastructures must consider all the systems necessary to provide the service, including physical work facilities, and must be fully detailed (location, information systems, communications, etc.).
- A plan of periodic testing of the designed plan and audit processes.

This contingency plan must guarantee that the restoration of the service is:

- 50% within 2 hours, from the start of the contingency plan.
- 100% within 4 hours, from the start of the contingency plan.

The CTTI will participate in all the tests of this supplier business continuity plan that it deems appropriate.

4.4.10.2 Business Continuity Plans of the Generalitat

The approved person will participate, when required, in the business continuity tests of ICT services carried out by the Generalitat de Catalunya coordinated by the CTTI and which may involve the participation of several suppliers.

4.4.10.3 Infrastructure Services of Interest

Given that these infrastructures are considered of interest by the CTTI and the Cybersecurity Agency of the Generalitat de Catalunya, the successful bidder must:

- Document the Single Points of Failure of all the infrastructures that serve the Generalitat and their degree of impact in the event of a failure. In addition, the successful bidder must prepare a risk analysis and ensure that there are no single points of failure (SPOFs) in critical system architectures (classified as essential, strategic or important).
- Develop correctly documented "fail-over" procedures (manual or automatic), which also include the "fail-back" process or return to the normal situation before the incident. All procedures must always be accessible by authorized CTTI personnel.
- Draw up an annual plan to test equipment in a Spare situation (equipment ready to operate in the event that assets are affected by an incident), to ensure that they work when necessary. The successful bidder will deliver to CTTI, every six months, a report on the results of the tests in these equipment.
- Make up-to-date backups of the base software used, configurations and data to ensure rapid location in the event of an incident. Backups must be available in two locations, one primary and one alternate. Version control must be guaranteed, which must be accessible by authorized CTTI personnel. Every six

months, the supplier will deliver a report that reflects the backups made as well as the details of the restorations that have had to be carried out in the period as a result of an incident. The OSEG may request proof of recovery of the backup copies. Adhere to a data recovery test plan planned in coordination with CTTI and those responsible for the applications/information systems. To comply with the LOPD, environments with Medium or High level personal data may undergo a six-monthly data recovery test. The rest of the files (low level LOPD and files without personal data) will follow an annual review/restoration plan. In this plan, an annual data recovery test may be requested for each different technology/system and different copy system, as a mechanism to verify the correct data recovery

4.4.11 RECONCILIATION, SERVICE ACCEPTANCE AND BILLING

The CTTI has established procedures for reconciling costs, accepting the service received and invoicing it. The successful bidder must follow these procedures and use the tools that the CTTI has in place.

The costs that may arise from the adaptation of the successful bidder's information systems to the formats requested by the CTTI will be borne by the contractor. It will also be responsible for providing technical support to the CTTI in any doubts related to the invoiced items and the formats of cost and billing items.

At a high level and with approximate dates, a billing cycle is subdivided into the following steps:

- Receipt of the cost and upload files to the CTTI tools (from the 1st to the 5th of each month).
- Reconciliation of costs received and identification of non-inventoried services (costs that will not be accepted) and deadline for the supplier to solve them (up to the 10th of each month).
- Process of passing on costs to the customer and publication of reports (until the 20th of each month).
- Acceptance of the service received through the approval of the delivery note(s) of the supplier (20th of each month).
- Issuance of the supplier invoice to CTTI (from the 20th of each month).
- Publication and review of discrepancies (from the 20th of each month).

4.4.11.1 Receipt of Service Costs

The approved party must provide the CTTI with a detail of the costs of the services provided by means of a csv file in the format established by the CTTI.

This cost detail will contain the necessary information to be able to correlate with the inventory the cost elements attributable to individual resources, regardless of the technical solution on which the service is based. The costs must be aligned with the inventory information that the successful bidder will have entered into the management tool during the service provision process (identification data of the elements, date of registration, date of cancellation, among others).

The incorporation of cost elements that imply a new classification in the cost file must be notified by the successful bidder, at least thirty (30) calendar days in advance of the implementation of the affected services.

The CTTI may make changes to the format of the file during the execution of the contract to adapt it to other services or cost elements, and the successful bidder must apply them within a maximum period of two months.

4.4.11.2 Reconciliation of Received Costs

The CTTI will reconcile the data received, requiring support from the winning company if necessary. In the event of discrepancies or inconsistencies in invoicing, during the reconciliation process these will be dealt with jointly between the CTTI and the successful bidder.

If the responsibility for the discrepancy lies with the successful bidder, in addition to the return of the value of the discrepancy, the CTTI may request the successful bidder to assume the management cost that the CTTI has entailed for the treatment of said discrepancy.

In general terms, the conciliation rules implemented analyse the following points:

- That the rates are correct: correct amounts, current rate, application of tariff bands according to volume, among others.
- That the inventory is correct: the service exists and is active in inventory, the invoiced and inventoried volumes coincide, among others.
- That the billing logic is followed: no duplicates, no incompatible charges, among others.

4.4.11.3 Acceptance of the Service Received

The invoicing process considers, prior to sending the invoice to the CTTI, an agreement of the provision of the service through a document or delivery note, following the procedures, tools and standards of the CTTI.

The CTTI will validate only the cost that can be confirmed as a service provided.

The service provided specifically includes the final inventory of this service in the CTTI tools. The lack of inventory of services prevents the CTTI from passing on its cost to its customers and, therefore, has a great internal impact. Therefore, services that are not inventoried in the CTTI tools with a minimum of necessary information will not be validated and will not be included in the amount of the supplier delivery note. By way of example, the minimum requirements would be: identification of the service code (subscribed number), identification of the service (catalogue service), identification of the provider, information on the area that has requested it, and that the service is not duplicated. The CTTI will clearly establish these minimums and may modify them if necessary by informing the supplier in advance.

The CTTI will also not assume any imputed costs on elements that are erroneously coded/typed in the electronic file, until the error is corrected.

4.4.11.4 Invoicing of the Services Received

The invoice finally issued by the supplier will indicate the validation delivery note code and will be broken down by the different groups of technological elements or services that make it up. The invoice will be issued in accordance with the provisions of the billing plan detailed in the administrative specifications.

The CTTI may change, during the term of the contract, the current invoicing model to a self-invoicing model.

4.4.11.5 Budget function

The successful bidder will prepare the budget reports on the contracted services, initially on an annual basis, in accordance with the calendar established by the CTTI.

The budget reports prepared must provide sufficient information for the annual forecast of expenditure or for the planning of new implementations, changes, among others, both globally by the Generalitat, and in terms of department, body, etc.

4.5 FUNCTIONS OF THE CYBERSECURITY AGENCY OF CATALONIA

The Cybersecurity Agency of Catalonia is the competent body responsible for planning, managing and controlling the ICT security of the Administration of the Generalitat and its public sector, as established in the government agreement LAW 15/2017, of 25 July, on the Cybersecurity Agency of Catalonia. In this regard, the Cybersecurity Agency of Catalonia will supervise compliance with security requirements by the successful bidder in the exercise of its functions.

The functions and services of the Cybersecurity Agency of Catalonia are published at: https://ciberseguretat.gencat.cat/ca/agencia/que-fem/