Análisis técnico

Oficina Técnica Únicas

Octubre 2025

Histórico de versiones:

Versión	Realizado por:	Fecha
1.0	Minsait	05/06/2025
1.1	Minsait ajustes en versiones y despliegue en cloud	10/06/2025
1.2	Minsait reincorporar dimensionamiento	20/06/2025
1.3	Minsait validación de la plataforma	30/06/2025

Contenido

Introducción y objetivo

Este documento constituye el Análisis Técnico de la Plataforma ÚNICAS, y tiene como objetivo proporcionar una visión clara, detallada y estructurada de los componentes técnicos que forman parte del sistema, su arquitectura, sus capacidades de integración y sus requerimientos de despliegue.

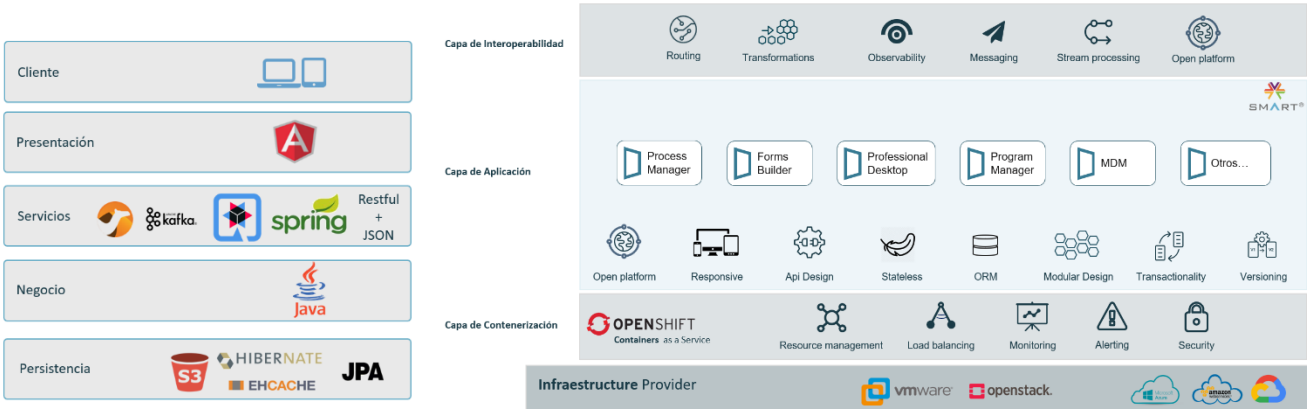
Está dirigido a los equipos técnicos de las Comunidades Autónomas (CCAA) y a los responsables del Nodo Central (NC), con el fin de facilitar la planificación, instalación, operación y mantenimiento de los Nodos Autonómicos (NA), y de asegurar la interoperabilidad con el resto de la Red ÚNICAS.

En particular, este documento busca:

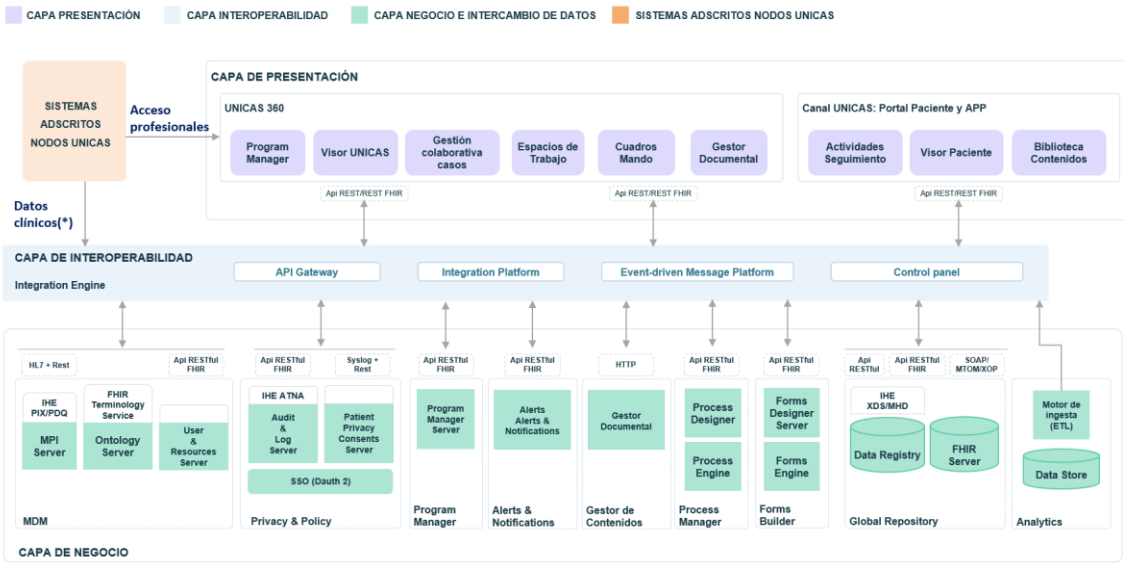
- Describir la **arquitectura de referencia** para los distintos escenarios de despliegue (on-premise, cloud, híbrido), con énfasis en escalabilidad, seguridad y modularidad.
- Documentar las **capas tecnológicas** (presentación, negocio, persistencia, contenerización, interoperabilidad) y las tecnologías empleadas en cada una de ellas.
- Explicar la **organización funcional y técnica** de los 22 módulos principales, incluyendo lógica de negocio, servicios, integraciones, reglas y controladores.
- Definir los **requisitos técnicos mínimos** para cada CA: infraestructura, comunicaciones, alta disponibilidad, configuración por entorno.
- Detallar los **mecanismos de seguridad, auditoría y trazabilidad** que aseguran el cumplimiento normativo y el alineamiento con los estándares del SNS.
- Servir de base para generar documentos específicos de despliegue y validación por parte de cada CA, facilitando la **homogeneidad técnica** y la integración con sistemas sanitarios locales (HIS/HCE).

Arquitectura general

La arquitectura de la Plataforma ÚNICAS está diseñada bajo un enfoque modular, escalable y seguro, fundamentado en el uso de microservicios desplegados sobre contenedores orquestados con Kubernetes. Esta arquitectura permite su despliegue flexible en múltiples entornos tecnológicos y su adaptación a las capacidades específicas de cada CA.



A. Capas tecnológicas y responsabilidades
   a. Capa de presentación
      - Interfaces web desarrolladas con Angular y Web Components.
      - Diseño 100% responsivo y stateless.
      - Comunicación vía APIs REST estandarizadas bajo FHIR®.
      - Módulos: Professional Desktop, Patient Portal, myHealth, Visor de Historia Clínica, MDT Meeting.
   b. Capa de negocio
      - Microservicios Java/Spring Boot v2.7.1.
      - Exposición de servicios vía APIs REST (FHIR® R4/R5).
      - Integración con perfiles IHE: PDQm, PIXm, ATNA.
      - Implementación modular que facilita la evolución de componentes sin afectar al sistema completo.
   c. Capa de interoperabilidad
      - Integration Engine para transformación y enrutado de mensajes.
      - Microservicios basados en Quarkus (3.15.x y 3.20.x) y Camel K (2.6.x).
      - Kafka para mensajería orientada a eventos.
      - API Gateway para control de acceso, trazabilidad y monitorización.
      - Conexiones seguras con HIS, otros Nodos Autonómicos y el NC.
   d. Capa de persistencia
      - Bases de datos relacionales: MySQL 8+ o Oracle 19c.
      - DAO con Hibernate y JPA.
      - Almacenamiento adicional para logs, métricas, trazas de auditoría, streams.
      - Soporte opcional para almacenamiento S3 (30-50% adicional para informes no estructurados).
      - Uso de Ehcache para mejora de rendimiento.
   e. Capa de contenerización
      - Contenedores Docker orquestados con Kubernetes.
      - Uso de Rancher (sin licencias) u OpenShift, para instalaciones on-premise o cloud. En proceso de certificación para el Clúster cloud provisto AWS-EKS.
      - Alta disponibilidad (auto-escalado, auto-curación, despliegues blue-green).
   f. Capa de infraestructura
      - Compatible con entornos on-premise, nubes privadas y públicas (AWS, Azure, GCP, OpenStack, VMware).
      - Permite despliegues híbridos, adaptables a las capacidades técnicas de cada CA.



B. Infraestructura de despliegue

La solución debe desplegarse sobre un Clúster Kubernetes, que actuará como plataforma base para los componentes del NA. Este apartado proporciona las instrucciones y consideraciones necesarias para su correcta implementación en cada CA.

Para evitar incurrir en costes de licencias adicionales, el Clúster Kubernetes propuesto se basa en Rancher que no requiere de las mismas, no obstante aquellas CCAA que lo deseen también podrán optar por instalar la solución sobre un Clúster Kubernetes tipo Openshitf, eso sí, tendrán que tener en cuenta que deberán sufragar los costes de las licencias de dicha plataforma, normalmente dependiente del número de CPUs o vCPUs dispuestas para el trabajo, es decir, en nodos Worker, así como el tipo de soporte que se desea Premium (entorno Productivo) o Estándar (entornos no productivos). Para entorno cloud también se certificará la opción de desplegar el NA sobre infraestructura AWS basada en EKS.

a. Modalidades de despliegue:
   - Cada CA podrá optar por una de las siguientes modalidades según sus capacidades:
     - Infraestructura propia (On-Premise): el clúster se instala sobre servidores físicos o virtuales.
     - Infraestructura Cloud: el clúster se implementa sobre servicios de nube pública, privada o híbrida[1].

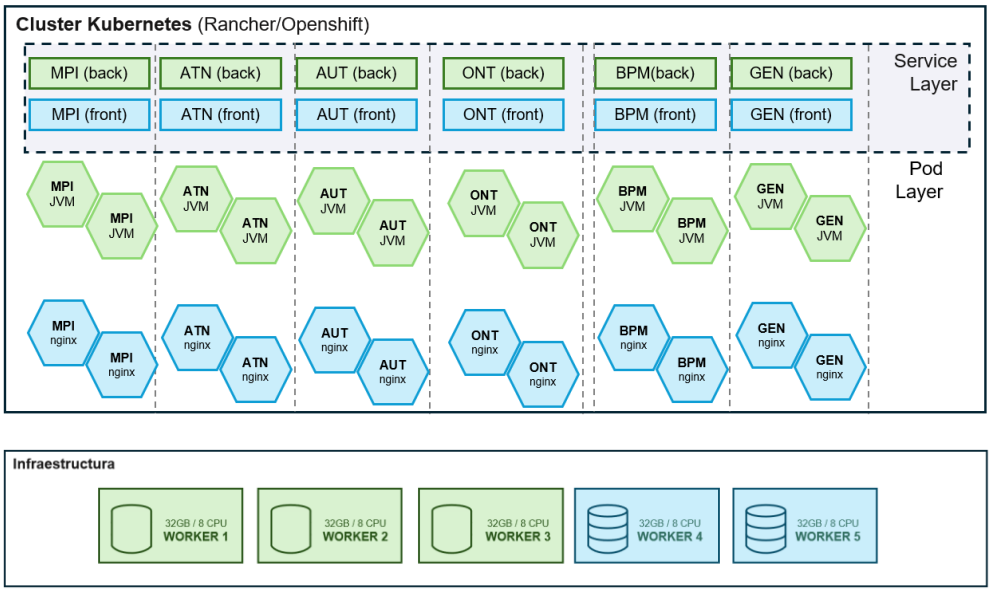
b. Requisitos de alta disponibilidad:
   - El clúster debe desplegarse en modo Alta Disponibilidad (HA). Esto implica:

[1] La instalación en proveedores Cloud Google y Azure, de momento sólo está certificada sobre despliegues del clúster Kubernetes en la plataforma de forma no gestionados, de forma que las opciones GKE y AKS respectivamente no están por el momento certificadas

- Tres nodos Master: responsables del control del clúster (etcd, kube-apiserver, kube-scheduler, kube-controller-manager).
- N nodos Worker: ejecutan los servicios y pods de la plataforma. Su número dependerá del escenario de carga asignado a la CA.

C. Entornos de despliegue:

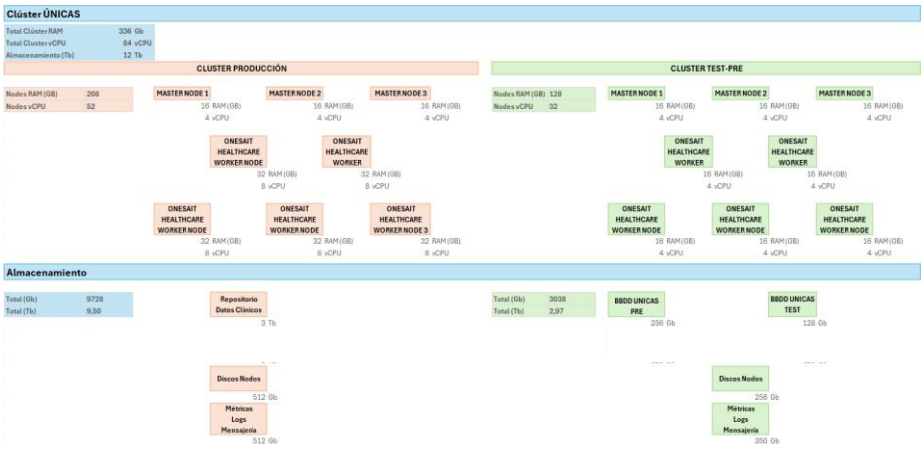
- La solución debe presentar dos entornos: clúster de producción y Test-Preproducción.
- Para determinados escenarios se plantean soluciones “single instance” para los clústeres no productivos, dado su menor volumen de necesidad, aconsejamos, en la medida de lo posible, que se provea de un entorno HA también para los preproductivos, con una dotación menor, lo que facilita tanto la extrapolación de comportamientos cara a la puesta en producción, así como la escalabilidad cara al futuro de estas
- Diagrama de despliegue en Kubernetes, donde los diferentes componentes de la solución se distribuirán a lo largo del clúster, asegurando la alta disponibilidad, a modo ejemplo, el siguiente esquema presenta una posible distribución de los servicios y pod, en los que se puede diferenciar la existencia independiente de los que sirven la capa front de los que proveen el back



D. Escenarios de despliegue

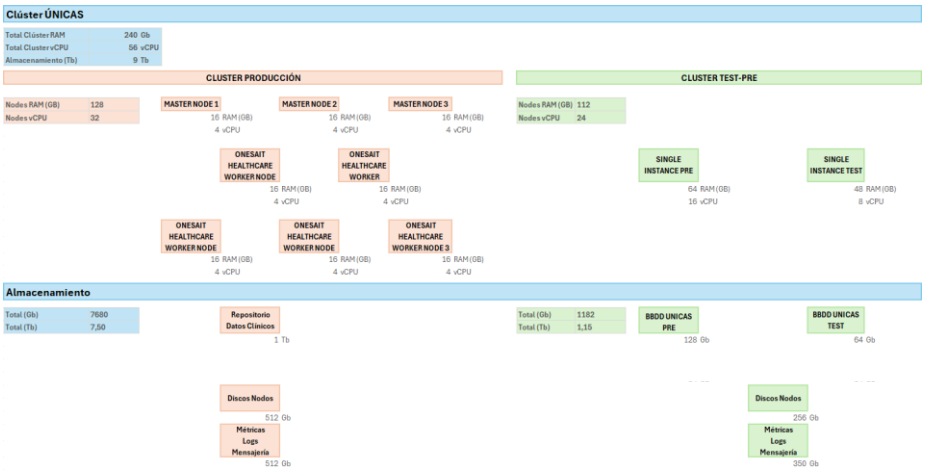
En función de la volumetría de pacientes a gestionar por la CA, se definen tres escenarios de despliegue que sirven como base para el dimensionamiento de la infraestructura del NA, cada uno con una configuración técnica de referencia que incluye recursos de cómputo y almacenamiento para los entornos de producción y test-preproducción.

Hasta 150.000 pacientes a cinco años (Grande)



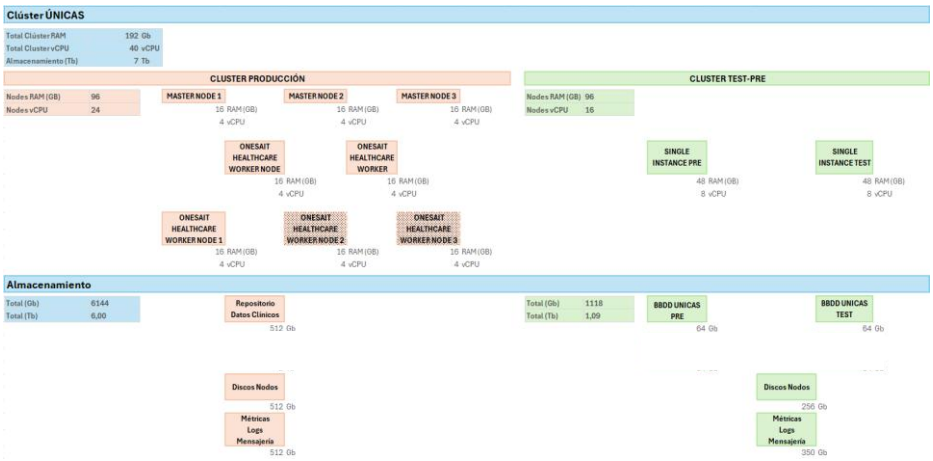
Este escenario está orientado a aquellas CCAA con un volumen elevado de pacientes y mayor exigencia en términos de concurrencia y rendimiento. La configuración recomendada incluye un clúster de producción con 3 nodos *master* y al menos 5 nodos *worker*, permitiendo garantizar la alta disponibilidad y el procesamiento de grandes volúmenes de datos desde el inicio. El entorno de test-preproducción también se despliega en alta disponibilidad, replicando las condiciones del entorno productivo.

Hasta 30.000 pacientes a cinco años (Mediano)



El escenario mediano ofrece una configuración equilibrada para CCAA con cargas intermedias. Se contempla un clúster de producción con 3 nodos *master* y entre 3 y 4 nodos *worker*. Para el entorno de test-preproducción, se recomienda una arquitectura en modo instancia única, suficiente para validar flujos y realizar pruebas funcionales, manteniendo controlado el consumo de recursos.

Hasta 5.000 pacientes a cinco años (Pequeño)



En este último escenario se plantea la opción de emplear 3 *nodos master* y 3 *nodos worker* en lugar de 5, considerando que los dos *nodos worker*, entramados en el esquema del Clúster de Producción como parte de una arquitectura escalable, representan una posibilidad de crecimiento futuro, aunque no es necesario proveerlos inicialmente. El entorno de test-preproducción puede instalarse en instancia única.

E. Persistencia

- El NA debe disponer de una capa de persistencia robusta y dimensionada correctamente para garantizar la disponibilidad, rendimiento y escalabilidad de la plataforma ÚNICAS en cada CA.
- Esta capa está formada por la base de datos, el almacenamiento general para datos operacionales y el almacenamiento opcional de informes no estructurados.

a. Base de datos:

- La base de datos se utiliza para almacenar los datos estructurados del repositorio clínico. Se deberá elegir entre:
  - MySQL 8 o superior, o bien
  - Oracle 19c o superior

b. Sistema de almacenamiento:

- Este sistema debe proporcionar soporte a:
  - El volumen operativo del clúster (almacenamiento para los nodos y servicios en ejecución).
  - La base de datos.
  - El almacenamiento de:
    - Streams.
    - Trazas de auditoría.
    - Métricas del rendimiento del sistema.
    - Logs técnicos y funcionales.
- El dimensionamiento del sistema de almacenamiento variará de acuerdo con el escenario de despliegue al que cada CA quiera adherirse, en función del volumen estimado de pacientes UNICAS y carga, se han establecido tres grandes escenarios.

c. Almacenamiento de informes no estructurados (opcional):
   - En caso de que se decida persistir los informes no estructurados fuera de la BBDD, se recomienda utilizar un sistema de archivos basado en protocolo S3.
   - El volumen requerido para estos informes representará entre un 30% y 50% del volumen previsto para el repositorio estructurado, en función del escenario de pacientes previsto por cada CA. Este volumen se descontará del almacenamiento total de BBDD si se opta por esta vía.

F. Organización modular
   - Espacio Profesional: Visor, Program Manager, MDT Meeting.
   - Espacio Paciente: myHealth (app), Patient Portal (web).
   - Backoffice Técnico: Auditoría, Ontología, Consentimientos, Repositorio, SSO, Terminología, Analytics.

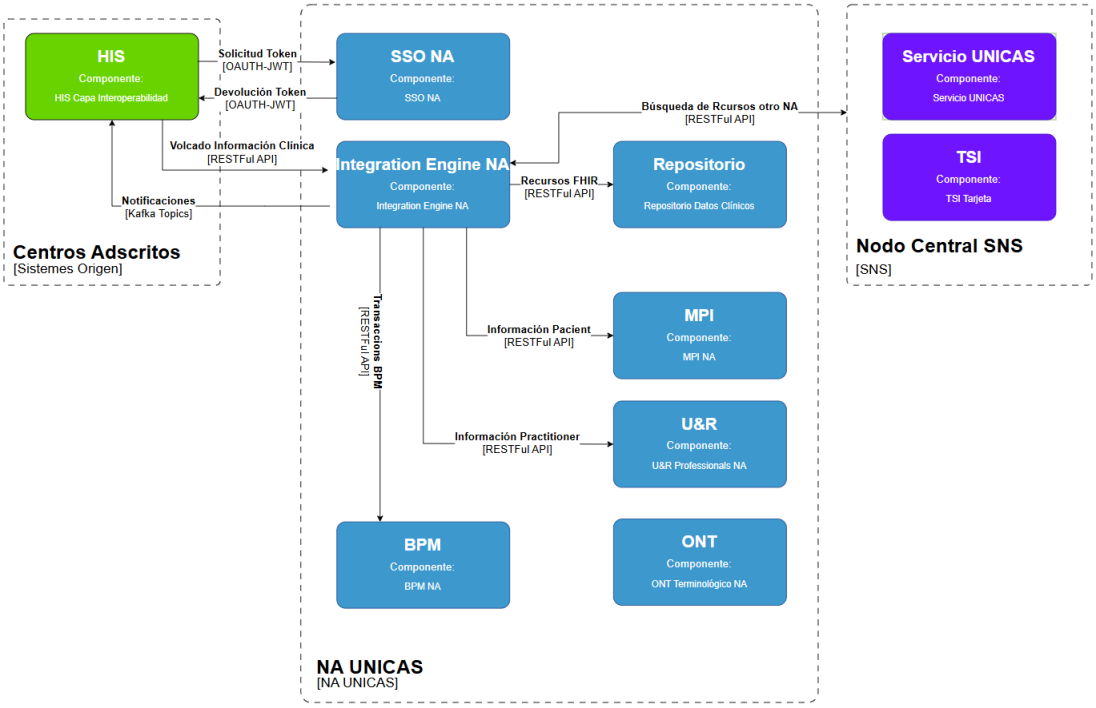
G. Seguridad y auditoría
   - Seguridad de comunicaciones basada en TLS y mTLS.
   - Autenticación con Cl@ve, LDAP, SAML v2 y AD.
   - Trazabilidad completa de eventos mediante servidor ATNA.
   - Interoperabilidad segura con el Nodo Central mediante certificados cliente.

Interoperabilidad de datos NA

La interoperabilidad de datos permite que toda la información clínica generada en los centros adscritos al NA se integre de forma estructurada, segura y estandarizada en la plataforma UNICAS. Este flujo está diseñado para facilitar la integración con los sistemas existentes (HIS) de cada CA. El proceso se articula de la siguiente forma:

- El HIS del centro, a través de su capa intermedia, solicita autenticación al componente SSO NA.
- Una vez autenticado, el HIS envía los datos clínicos existentes al Integration Engine NA, que enruta toda la información que se va generando hacia su destino funcional. Esta información puede ir al:
  - Repositorio
  - MPI
  - Usuarios y Recursos
  - BPM

También se dispondrá de un mecanismo de suscripción que permitirá a los orígenes recibir notificaciones sobre determinados eventos que se produzcan en el Repositorio. Estas notificaciones se articularán a través de topics Kafka.



Interoperabilidad de la interfaz de usuario NA

La interoperabilidad de la interfaz de usuario (UI) permite que el profesional sanitario acceda a los componentes visuales del NA directamente desde su estación clínica habitual, a través del HIS correspondiente al centro adscrito. Esta integración no requiere duplicidad de accesos ni modificación estructural de los sistemas locales, y puede ser orquestada mediante el SSO corporativo.

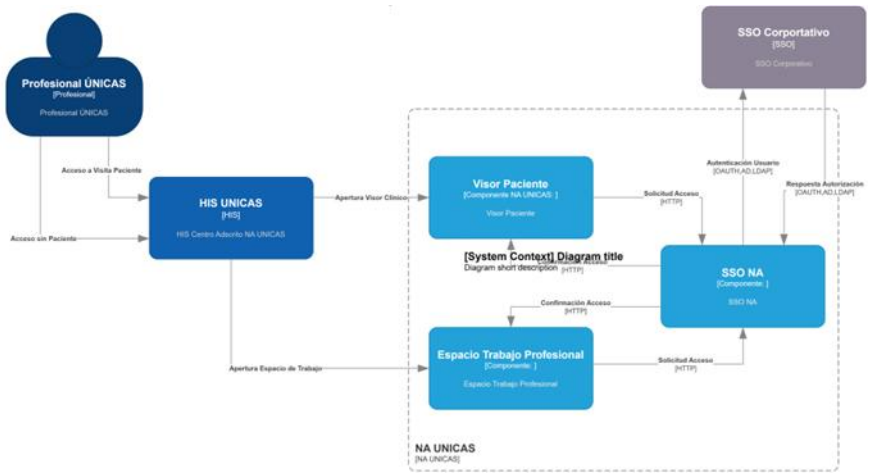
El acceso puede realizarse de dos formas:

- **Acceso a Visita de Paciente**: lanza el Visor del Paciente, permitiendo acceder al historial clínico estructurado.
- **Acceso sin Paciente**: lanza el Espacio de Trabajo Profesional, donde el usuario gestiona programas, tareas y colaboración asistencial.

Ambos accesos se redirigen a los módulos correspondientes del NA, y requieren autenticación previa. Esta se gestiona mediante el componente SSO NA, el cual:

> Recibe las solicitudes de acceso desde el Visor del Paciente y el Espacio de Trabajo Profesional.
> Puede delegar la autenticación en el SSO Corporativo de la CA.
> Recibe la respuesta de autorización y permite el acceso a los módulos visuales del NA, sin necesidad de introducir credenciales adicionales.

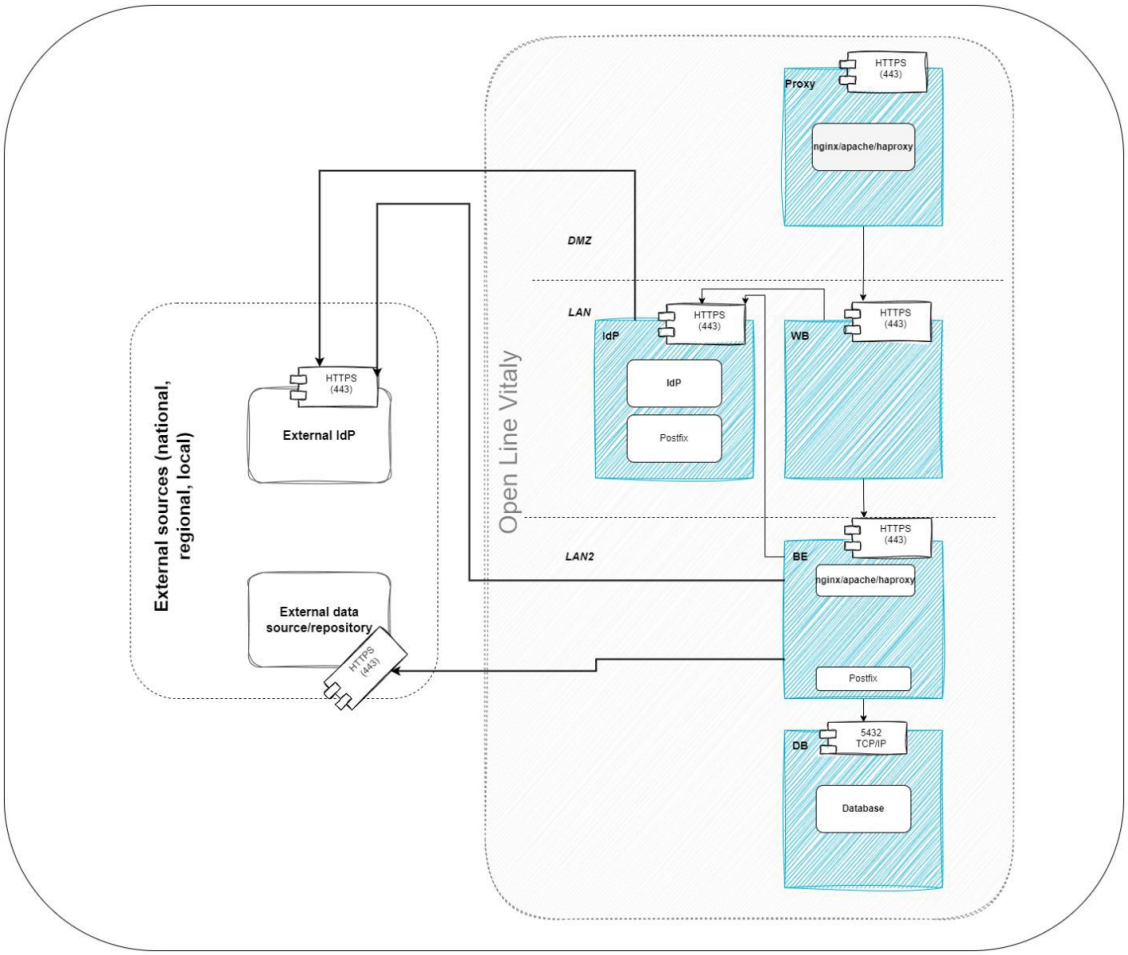
La capa de presentación del NA actual como una capa visual supraprofesional que puede ser levantada desde cualquier HIS que disponga de la integración correspondiente. Esto permite al profesional trabajar sobre los servicios de UNICAS sin abandonar su entorno habitual.



La arquitectura descrita busca garantizar una base tecnológica sólida, interoperable, extensible y adaptable, que permita a las CCAA una implementación sostenible y alineada con los requisitos del Sistema Nacional de Salud.

1.1. Plataforma Colaborativa (MDT Meeting)

Para el caso particular de este componente la instalación también es posible realizarla en infraestructura on-prem o cloud, pero en este caso sus componentes se desplegarán directamente sobre VM según el siguiente esquema:



Y bajo acorde a la siguiente tabla de necesidades, para cada entorno:

No.	Descripción	CPU [#]	Persistencia [GB]		RAM [GB]	OS
			OS	No OS		
1	Proxy server	2	8	32	2	Rocky Linux 9+ / RHEL 9+
2	Web portal	4	8	92	8	Rocky Linux 9+ / RHEL 9+
3	Middleware server	4	8	92	8	Rocky Linux 9+ / RHEL 9+
4	Database server	4	8	30 (/opt) + 300 (/var)	2	Rocky Linux 9+ / RHEL 9+
5	Identity provider	2	8	32	2	Rocky Linux 9+ / RHEL 9+

La capa “Proxy server” puede ser provista por balanceadores externos que gobiernen el acceso a las diferentes capas según el esquema.

Por lo que respecta al “Database server”, debe ser un PostgreSQL 15 o superior.

Para soluciones basadas en cloud, se debe proveer una infraestructura análoga que permita albergar las diferentes capas, a continuación, mostramos las necesidades propias para una infraestructura provista por AWS[2]:

- 1x m7i.large EC2 instance + 100GB EBS volume
- 2x m7i.xlarge EC2 instance + 2x 100GB EBS volume
- 1x db.m7i.xlarge RDS instance with 300GB of storage
- 3x AWS ELB instance
- 1x AWS SES instance
- DNS in AWS Route 53

1.2. Validación de la plataforma

Con el objetivo de verificar que el Nodo Autonómico se ha desplegado correctamente y cumple con los requisitos funcionales y de comunicación definidos en la arquitectura, se han definido una serie de pruebas de validación básicas del despliegue que permiten comprobar los aspectos clave del entorno. A continuación, se describen los casos de prueba ejecutados:

- **DEP-01** Verificación de visibilidad entre capas
- **DEP-02** Verificación de pods en Kubernetes
- **DEP-03** Acceso vía HTTPS a la interfaz web
- **DEP-04** Registro de eventos en servidor ATNA

[2] Puede consultarse el detalle de esta infraestructura a través del siguiente enlace https://calculator.aws/#/estimate?id=b73860555677b049c6e81db1aa00aafa0a6a7954

- **DEP-05** Despliegue correcto a base de datos
- **DEP-06** Comunicación con Nodo Central

<Nombre caso prueba> Verificación de visibilidad entre capas	**<Código del CP>**	DEP-01
Descripción: Verificar que existen canales de comunicación activos entre los distintos componentes de la infraestructura: desde el clúster Kubernetes a la base de datos, desde los sistemas origen (HIS) al clúster Kubernetes, y desde los equipos cliente al ingress del clúster. Esta visibilidad garantiza que todos los servicios pueden comunicarse entre sí como se espera.		
Prerrequisitos • Clúster Kubernetes desplegado y operativo. • Base de datos accesible desde el clúster. • Equipos cliente y sistemas origen con acceso habilitado al entorno. • Servicios expuestos correctamente en ingress.		
Pasos: 1. Validar conectividad desde el clúster Kubernetes a la base de datos ejecutando una consulta simple desde un pod de backend. 2. Confirmar que los sistemas origen pueden realizar peticiones al ingress del clúster y reciben respuesta. 3. Comprobar que los equipos cliente acceden correctamente a la interfaz web expuesta en el ingress accediendo a la URL del entorno.		
Resultado esperado: Se verifica la conectividad en los tres sentidos: el clúster puede acceder a la base de datos, los sistemas externos pueden comunicarse con el clúster, y los equipos cliente acceden correctamente al punto de entrada web del entorno**.**		
Resultado obtenido: La visibilidad entre capas es correcta. Las conexiones entre los distintos componentes se establecen sin errores, permitiendo el funcionamiento esperado de la plataforma.		

<Nombre caso prueba> Verificación de pods en Kubernetes	**<Código del CP>**	DEP-02
Descripción:		

Verificar que los contenedores (pods) correspondientes a los servicios de la plataforma están desplegados, activos y en estado Running en el clúster Kubernetes.
Prerrequisitos • Acceso al entorno de orquestación Kubernetes (dashboard o terminal). • Permisos de consulta en namespace del entorno desplegado.
Pasos: 1. Ejecutar kubectl get pods -n <namespace>. 2. Comprobar que todos los pods aparecen en estado Running y sin reinicios inesperados. 3. Verificar que no existen errores en logs iniciales.
Resultado esperado: Todos los pods desplegados visibles con kubectl get pods, sin reinicios ni errores en logs.
Resultado obtenido: Todos los servicios están activos y en estado Running. Sin errores de despliegue ni alertas críticas.

<Nombre caso prueba> Acceso vía HTTPS a la interfaz web	**<Código del CP>**	DEP-03
Descripción: Validar que la interfaz web principal de la plataforma (escritorio profesional) está accesible mediante protocolo HTTPS con certificado válido.		
Prerrequisitos • URL habilitada de acceso a la plataforma. • Navegador actualizado con conexión al entorno.		
Pasos: 1. Abrir la URL de la plataforma en el navegador. 2. Verificar presencia de candado SSL indicando conexión segura. 3. Acceder a la plataforma con un usuario habilitado.		
Resultado esperado: La interfaz web se carga correctamente vía HTTPS y no se generan advertencias de seguridad por parte del navegador.		

Resultado obtenido: El acceso a la plataforma mediante HTTPS funciona correctamente. Certificado reconocido como válido. No se presentan bloqueos o alertas de seguridad.

<Nombre caso prueba> Registro de eventos en servidor ATNA	**<Código del CP>**	DEP-04
Descripción: Validar que los accesos y acciones del usuario se registran correctamente en el sistema de auditoría conforme al perfil IHE ATNA (Audit Trail and Node Authentication).		
Prerrequisitos • Usuario de pruebas realizando acciones en la plataforma. • Acceso a interfaz de consulta del servidor ATNA.		
Pasos: 1. Acceder a la plataforma con un usuario habilitado que tenga acceso a los módulos. 2. Realizar acciones típicas (acceso a MPI, apertura de formulario, etc.). 3. Consultar eventos en servidor de auditoría.		
Resultado esperado: Los eventos aparecen registrados: login, consulta de recursos, navegación por módulos. Incluyen timestamp, usuario, acción, IP, resultado.		
Resultado obtenido: El servidor ATNA registra correctamente los eventos generados por los usuarios. Todos los accesos están trazados con su información correspondiente.		

<Nombre caso prueba> Despliegue correcto a base de datos	**<Código del CP>**	DEP-05
Descripción: Validar que la base de datos asociada al entorno de la plataforma está accesible, activa y permite consultas básicas sin errores ni tiempos de espera anómalos.		
Prerrequisitos		

• Usuario con permisos de lectura sobre la base de datos. • Conexión estable desde la infraestructura a los servicios de base de datos.
Pasos: 1. Conectarse al gestor de base de datos (MySQL, Oracle) con credenciales que permitan la lectura de los esquemas y tablas creadas. 2. Ejecutar consulta básica: SELECT COUNT(*) FROM us_ohmpi.persona. 3. Validar conexión y retorno sin error.
Resultado esperado: La base de datos responde correctamente a las consultas. Tiempo de respuesta aceptable y sin errores de conexión o permisos.
Resultado obtenido: Acceso validado. Se verificó integridad de las tablas principales y disponibilidad total de la base de datos sin errores ni latencias elevadas.

<Nombre caso prueba> Comunicación con Nodo Central	**<Código del CP>**	DEP-06
Descripción: Verificar que el Nodo Autonómico dispone de visibilidad de red hacia el Nodo Central y que se ha instalado correctamente el certificado necesario para establecer la comunicación segura. Comprobar que, utilizando dicho certificado, se puede realizar una petición al Nodo Central y se obtiene una respuesta válida, lo que confirma que la autenticación mutua está configurada correctamente.		
Prerrequisitos • Nodo Central accesible en entorno de preproducción. • Certificados válidos instalados y configurados. • Servicio operativo en ambos extremos.		
Pasos: 1. Confirmar que existe visibilidad y conectividad hacia el Nodo Central. 2. Verificar que el certificado está instalado en el entorno del Nodo Autonómico y configurado en el componente que establece la conexión. 3. Realizar una petición desde el Nodo Autonómico al Nodo Central utilizando dicho certificado. 4. Revisar la respuesta de la petición y validar que no se producen errores de autenticación o de conexión TLS.		

Resultado esperado: La plataforma alcanza el Nodo Central, el certificado está correctamente instalado y configurado, y la petición se completa con éxito, estableciendo una conexión segura sin errores.
Resultado obtenido: La comunicación con el Nodo Central se establece correctamente. La petición fue aceptada y no se han detectado errores de conexión ni autenticación.

Capa de presentación

La capa de presentación de la plataforma ÚNICAS engloba los componentes visuales utilizados por los diferentes perfiles de usuario (profesionales sanitarios, pacientes, cuidadores) para interactuar con los servicios disponibles a través del NA. Esta capa se caracteriza por su diseño responsivo, usabilidad avanzada y cumplimiento de los principios de accesibilidad y seguridad.

Todos los módulos de presentación han sido desarrollados siguiendo una arquitectura stateless, desacoplada del backend, y consumen exclusivamente APIs REST basadas en FHIR®, lo que permite un despliegue flexible, escalabilidad horizontal y consistencia funcional entre entornos.

Tecnologías empleadas

- Framework principal: Angular 15+.
- Estilo visual: Web Components, TailwindCSS, Material Design.
- Internacionalización: i18n (múltiples idiomas configurables).
- Seguridad: OAuth 2.0, JWT, integración con Cl@ve, AD, LDAP.
- Auditoría: Integración con servidor ATNA para trazabilidad de accesos y acciones.
- Soporte multiplataforma: Web responsive, app nativa (Android/iOS).

1.3. Módulos y estructura funcional

1.3.1. Onesait Healthcare Professional Desktop

- Plataforma web que actúa como punto de entrada para los profesionales.
- Presenta un escritorio dinámico con accesos modulares a los servicios habilitados según el perfil.
- Incluye sistemas de validación de entrada, control de sesión y auditoría en tiempo real.

- Estructura: menú lateral de navegación, dashboard principal, área de trabajo central.

1.3.2. Onesait Healthcare myHealth.

- Aplicación nativa (iOS/Android) diseñada para pacientes y cuidadores.
- Estructura basada en tres zonas funcionales: barra superior de navegación, cuerpo de pantalla para contenido, menú lateral para funciones rápidas.
- Soporte multidioma y actualizaciones OTA (over-the-air).
- Funcionalidades: acceso a historia clínica, tareas, mensajería, citas, gestión de consentimiento.

1.3.3. Onesait Healthcare Patient Portal.

- Versión web responsive que replica las funcionalidades de la app myHealth.
- Acceso mediante Cl@ve.
- Diseño consistente con la app para una experiencia de usuario unificada.
- Especialmente optimizado para navegadores web de escritorio y dispositivos móviles.

1.3.4. Onesait Healthcare Visor de Historia Clínica.

- Aplicación Smart on FHIR® para visualización de historia clínica longitudinal.
- Interfaz cronológica interactiva con filtros por episodio, profesional, servicio o tipo de documento.
- Integración directa con el repositorio clínico FHIR®.
- Componentes configurables según organización: tabs, columnas, filtros, secciones desplegables.

1.3.5. Plataforma Colaborativa (MDT Meeting)

- Aplicación colaborativa para la gestión de reuniones multidisciplinares.
- Estructura de pantallas: listado de reuniones, vista detallada, tareas asociadas, área de notas clínicas.
- Funcionalidades: agenda compartida, notificaciones, generación de informe clínico estructurado accesible desde el repositorio FHIR®.
- Soporte para flujos asíncronos de preparación y consulta post-reunión.

Esta capa está diseñada para ser desacoplada de su capa de backend, permitiendo su actualización y despliegue independiente, existiendo al igual que para el Visor dos modos de acceso en función del contexto con y sin pacientes, ambos estando siempre disponibles a través del Visor y Profesional Desktop respectivamente.

Capa de negocio

La capa de negocio de la Plataforma ÚNICAS contiene la lógica funcional y los servicios que orquestan el comportamiento de los diferentes módulos. Está implementada en microservicios desarrollados en Java con Spring Boot y organizados por dominios funcionales. Estos microservicios exponen APIs REST que cumplen con los estándares FHIR® R4/R5, e integran reglas de negocio, validaciones, controladores y gestión de excepciones.

Cada microservicio está diseñado para ser independiente, escalable y desplegable de forma modular, lo que facilita la evolución, el mantenimiento y la integración con los sistemas locales de cada CA. La gestión de errores se basa en controladores centralizados con códigos de error estructurados y trazabilidad mediante logs y eventos.

1.4. Módulos y lógica funcional

1.4.1. Onesait Healthcare Professional Desktop

Escritorio profesional que gestiona el acceso único para profesionales sanitarios, centralizando módulos según rol.

- Servicios expuestos: gestión de sesión, recuperación de menú personalizado, visualización de tareas, navegación por módulos.
- Reglas de negocio: validación de permisos de acceso por tipo de usuario y centro; sesiones activas únicas por profesional.
- Excepciones: acceso denegado por rol; expiración de token; errores en carga de servicios asociados.
- Interacciones: Users & Resources, SSO, Alerts, Forms, Program Manager.

1.4.2. Onesait Healthcare myHealth

App móvil, permite que pacientes y cuidadores accedan a información clínica, mensajería y tareas desde un entorno móvil.

- Servicios expuestos: Consulta de episodios, tareas pendientes, mensajería, consentimientos, documentación.
- Reglas de negocio: Visibilidad limitada por edad, tutor legal, ámbito asistencial y estado del consentimiento.
- Gestión de excepciones: Token inválido, paciente sin vínculo activo, error en integración con Consent Manager.
- Interacciones: Patient Portal, Consent Manager, Alerts, Global Repository.

1.4.3. Onesait Healthcare Patient Portal

Versión web responsive del canal paciente con las mismas funcionalidades que myHealth.

- Servicios expuestos: Mismos endpoints de consulta, adaptados a interfaz web.
- Reglas de negocio: Mismas que myHealth, con posibilidad de uso compartido (madres/padres).
- Gestión de excepciones: Control de sesión doble vía navegador; trazabilidad duplicada corregida.
- Interacciones: Chat, Gestor Documental, myHealth.

1.4.4. Onesait Healthcare Visor de Historia Clínica

Aplicación Smart on FHIR® para visualizar la historia clínica longitudinal del paciente desde fuentes locales y remotas.

- Servicios expuestos: Carga de recursos FHIR® (Observation, Encounter, DocumentReference, …), filtros, visualización por fechas.
- Reglas de negocio: Ordenamiento cronológico, acceso limitado por rol y alcance de derivación.
- Gestión de excepciones: Falta de datos, error de integración con FHIR® Server, falta de autorización.
- Interacciones: Global Repository, Ontology Server.

1.4.5. Plataforma Colaborativa (MDT Meeting)

Herramienta de Onesait Healthcare que facilita la coordinación entre profesionales mediante reuniones colaborativas sobre casos clínicos complejos.

- Servicios expuestos: Gestión de agendas, actas, asistentes, tareas asociadas y generación de informes clínicos.
- Reglas de negocio: Control de acceso por especialidad, validación de quorum mínimo, firma digital del informe.
- Gestión de excepciones: Cancelación de reunión sin quorum, error al generar PDF estructurado, conflictos en tareas cruzadas.
- Interacciones: Professional Desktop, Visor, Alerts, Consent Manager, Global Repository.

1.4.6. MPI Server

Gestión de la identidad única del paciente. Garantiza la unicidad y trazabilidad de la identidad del paciente a través de la Red ÚNICAS.

- Servicios expuestos: Búsqueda, alta, actualización y fusión de identidades; exposiciones de servicios IHE PIXm y PDQm.
- Reglas de negocio: Detección de duplicados, normalización de identificadores, resolución de conflictos de identidad.
- Gestión de excepciones: Rechazo por duplicado, error en reglas de fusión, incoherencias de atributos.
- Interacciones: Integration Engine, SSO.

1.4.7. Users & Resources

Gestión del ciclo de vida de los usuarios y sus roles profesionales dentro del NA. Basado en FHIR®.

- Servicios expuestos: Alta, baja y modificación de usuarios, asignación de roles, integración con LDAP y sistemas federados.
- Reglas de negocio: Validación de estructura organizativa, compatibilidad de roles, sincronización con directorios externos.
- Gestión de excepciones: Usuario no autorizado, conflicto de perfiles, error en sincronización con IdP.
- Interacciones: SSO, Professional Desktop, Consent Manager.

1.4.8. Módulo de Autenticación y Autorización (SSO)

Gestiona el acceso seguro a la Plataforma. Proporciona autenticación federada y control de acceso único a toda la plataforma.

- Servicios expuestos: Login SAML/OIDC, generación de tokens JWT, verificación de sesión, logout.
- Reglas de negocio: Asignación de permisos según claims del token, validación de sesiones activas, caducidad segura.
- Gestión de excepciones: Token expirado, usuario no autorizado, fallos de federación.
- Interacciones: Users & Resources, Professional Desktop, API Gateway.

1.4.9. Servidor de Auditoría

Registro de accesos, cambios y eventos de seguridad en la plataforma. Cumple con el perfil IHE ATNA y expone API FHIR® AuditEvent.

- Servicios expuestos: Registro de eventos (access, update, delete), exposición de logs vía FHIR® AuditEvent.
- Reglas de negocio: Captura obligatoria de eventos sensibles, persistencia en tiempo real, integración con sistema ATNA.
- Gestión de excepciones: Fallos en la escritura, eventos mal formateados, inconsistencias de origen.
- Interacciones: Todos los microservicios, Servidor ATNA, Integration Engine.

1.4.10. Onesait Healthcare Ontology Server

Servidor de vocabularios controlados y catálogos maestros. Cumple con el estándar HL7 FHIR® y permite mapeo y validación semántica entre terminologías

- Servicios expuestos: Consulta, mapeo y validación semántica de SNOMED CT, LOINC, CIE-10.
- Reglas de negocio: Relación semántica entre conceptos, versiones compatibles, consistencia entre módulos.
- Gestión de excepciones: Código no reconocido, ambigüedad de mapeo, conflictos en actualización de versiones.
- Interacciones: Global Repository, Integration Engine, Visor Historia Clínica.

1.4.11. Integration Engine

Motor de integración que permite la interoperabilidad entre la plataforma y los sistemas externos de las CCAA (HIS, HCE, LIS, RIS, etc.). Basado en eventos.

- Servicios expuestos: Transformación de mensajes (HL7 v2, FHIR®, CDA), enrutamiento, gestión de colas Kafka, servicios REST.
- Reglas de negocio: Validación de estructura de mensaje, mapeo semántico, gestión de reintentos y colas de errores.
- Gestión de excepciones: Fallo en transformación, timeout de conectores, errores en enrutamiento.
- Interacciones: Global Repository, Ontology Server, HIS externos.

1.4.12. Onesait Healthcare Global Repository

Repositorio clínico FHIR® centralizado para almacenar y consultar datos clínicos y administrativos.

- Servicios expuestos: Create, Read, Update, Delete sobre recursos clínicos FHIR® (Patient, Encounter, Observation, ...).
- Reglas de negocio: Validación semántica mediante Ontology Server, consistencia de episodios, control de versiones.
- Gestión de excepciones: Recurso mal formado, conflictos de versión, fallos de persistencia.
- Interacciones: Visor Historia Clínica, Consent Manager, Integration Engine, Forms Builder.

1.4.13. Onesait Healthcare Consent Manager

Gestión de consentimientos informados del paciente para el acceso, uso y compartición de a su información clínica.

- Servicios expuestos: Alta y revocación de consentimientos, consulta de estado, firma electrónica, auditoría de uso.
- Reglas de negocio: Restricción de acceso por ámbito, caducidad automática, validación por CA.
- Gestión de excepciones: Firma fallida, estado inconsistente, falta de autorización.
- Interacciones: myHealth, Patient Portal, Visor Historia Clínica, Alerts.

1.4.14. Onesait Healthcare Alerts & Notifications.

Gestión de alertas y notificaciones a pacientes, cuidadores y profesionales. Soporta múltiples canales.

- Servicios expuestos: Alta de plantillas, envío en tiempo real o programado, registro de entregas.
- Reglas de negocio: Prioridad del mensaje, canal preferido (push, email, in-app), reglas de redifusión.
- Gestión de excepciones: Falla de entrega, formato inválido, colas saturadas.
- Interacciones: Professional Desktop, myHealth, Patient Portal, Process Manager.

1.4.15. Process Manager.

Modelado y ejecución de procesos asistenciales clínicos o administrativos. Incluye motor BPM y diseñador visual.

- Servicios expuestos: Alta, activación y seguimiento de procesos; integración con tareas y eventos del sistema.
- Reglas de negocio: Control de estado de procesos, condiciones de activación, relaciones entre eventos.
- Gestión de excepciones: Interrupciones por fallo de tareas, flujos inconsistentes, errores de temporización.
- Interacciones: Forms Builder, Alerts, Consent Manager, Professional Desktop.

1.4.16. **Onesait Healthcare Forms Builder.**

Diseño visual de formularios clínicos para recoger información durante los procesos asistenciales.

- Servicios expuestos: Diseño visual, renderizado dinámico, carga de datos, almacenamiento de respuestas.
- Reglas de negocio: Validaciones personalizadas, compatibilidad con recursos FHIR®, control de versiones.
- Gestión de excepciones: Errores en esquema, fallos de carga, conflicto de versiones.
- Interacciones: Global Repository, Process Manager, Consent Manager.

1.4.17. **Onesait Healthcare Analytics.**

Solución de analítica con BI, dashboards y cuadros de mando sobre los datos clínicos de la plataforma.

- Servicios expuestos: Dashboards, informes, exportación de datos, agregación OLAP.
- Reglas de negocio: Control de acceso por rol, niveles de agregación, filtros dinámicos.
- Gestión de excepciones: Errores de conexión con fuentes, datos incompletos, fallos de visualización.
- Interacciones: Global Repository, Settings Manager, Users & Resources.

1.4.18. **Gestor Documental.**

Gestión de contenidos y documentos que los profesionales pueden compartir con los pacientes.

- Servicios expuestos: Subida, descarga, versión, permisos, indexación y clasificación.
- Reglas de negocio: Control de acceso, versionado automático, conservación mínima requerida.
- Gestión de excepciones: Documento corrupto, conflicto de versión, error de permisos.
- Interacciones: MDT Meeting, Patient Portal, myHealth, Chat.

1.4.19. **Onesait Healthcare Program Manager.**

Gestión de programas asistenciales mediante planificación de tareas y seguimiento de indicadores.

- Servicios expuestos: Alta de programa, asignación de pacientes, generación de tareas, monitorización.
- Reglas de negocio: Reglas por perfil clínico, validaciones por protocolo, vinculación con consentimientos.
- Gestión de excepciones: Paciente fuera de criterios, tarea fallida, desincronización con Forms Builder.
- Interacciones: Professional Desktop, Forms Builder, Alerts, Consent Manager

1.4.20. Onesait Healthcare Settings Manager.

Gestión de parámetros de la configuración técnica y funcional de la plataforma a nivel de entorno y nodo.

- Servicios expuestos: Gestión de parámetros, variables de entorno, rutas de servicios y flags.
- Reglas de negocio: Validación de parámetros críticos, auditoría de cambios, configuración segura.
- Gestión de excepciones: Valores fuera de rango, errores de validación, conflicto entre nodos.
- Interacciones: Integration Engine, Analytics, Program Manager.

1.4.21. Onesait Healthcare Chat.

Módulo de mensajería asíncrona que facilitar la comunicación asíncrona entre pacientes, cuidadores y profesionales. Soporta conversaciones bidireccionales, generación de notificaciones automáticas y consulta del historial de mensajes

- Servicios expuestos: Envío y recepción de mensajes, gestión de conversaciones, almacenamiento cifrado.
- Reglas de negocio: Autorización por perfil, cifrado extremo a extremo, notificaciones automáticas.
- Gestión de excepciones: Usuario no disponible, fallo de entrega, conflictos de conversación.
- Interacciones: Patient Portal, Professional Desktop, Alerts, Gestor Documental.

Integraciones externas: Servicios consumidos o expuestos, protocolos, seguridad.

1.5. Comunicaciones

La arquitectura de red del Nodo Autonómico debe diseñarse para garantizar una comunicación segura, eficiente y trazable. A continuación, se describen los canales de comunicación que deben ser habilitados y configurados durante la instalación.

1.5.1. Comunicación Cliente → Front del Nodo Autonómico

Los profesionales sanitarios y usuarios acceden al sistema a través de una interfaz web desplegada en el clúster Kubernetes. Esta comunicación debe realizarse de forma segura mediante HTTPS.

- Se recomienda el uso de certificados TLS válidos emitidos por una autoridad de confianza.
- El sistema debe registrar todas las peticiones mediante trazas accesibles desde el servidor ATNA.

1.5.2. Comunicación Sistemas Origen → Clúster del NA

Los sistemas de información clínica (HIS, LIS, RIS, etc.) deben poder enviar datos al Nodo Autonómico.

- La integración se realiza a través de servicios REST API bajo estándar FHIR® R5 siguiendo las especificaciones publicadas en la IG de UNICAS .
- Securización basada en OAUTH 2 y token JWT.
- Comunicación encriptada por TLS.

1.5.3. Comunicación Clúster NA → Capa de persistencia

El clúster Kubernetes debe mantener una conexión segura y estable con la capa de persistencia, tanto para acceder a la base de datos como al sistema de archivos asociado (incluido el almacenamiento opcional S3). Esta comunicación es crítica para el funcionamiento de la plataforma y debe cumplir con los siguientes requisitos:

- Para la conexión con la base de datos, será necesario habilitar el puerto específico según el motor utilizado:
  - Puerto 3306 si se utiliza MySQL.
  - Puerto 1521 si se utiliza Oracle.
  - Puerto 5432 para PostgreSQL (Sólo Plataforma Colaborativa MDT Meeting)
- En caso de emplear un sistema de almacenamiento tipo S3 para informes no estructurados, se debe permitir la comunicación con los servicios correspondientes. El puerto requerido dependerá del proveedor de la solución.

1.5.4. Comunicación Clúster NA → Nodo Central

La solución requiere interoperabilidad entre los nodos autonómicos y el Nodo Central gestionado por el Ministerio de Sanidad, esta debe regirse por:

- Las comunicaciones se realizan exclusivamente por HTTPS.
- Comunicación encriptada por mTLS.
- El acceso debe estar protegido mediante certificados cliente, que identifican a la CA de forma única ante los servicios del Nodo Central.

Contemplará todas las necesidades de sincronización, notificación, gobierno y consulta de la información generada desde los nodos autonómicos, o bien gobernada por el Nodo Central.

1.6. Seguridad y certificados

Para garantizar la seguridad en todas las comunicaciones, se deben implementar certificados digitales que protejan las conexiones y autentiquen tanto a servidores como a clientes.

- Se deben generar certificados de servidor para proteger las capas Front y Back del Nodo Autonómico. Estos certificados aseguran que tanto los usuarios como los sistemas origen se conecten a una fuente confiable mediante HTTPS.
- Para las comunicaciones entre el Nodo Autonómico y el Nodo Central, puede ser necesario disponer de un certificado de cliente. Este certificado identifica de forma única a cada Comunidad Autónoma frente a los servicios del Nodo Central, garantizando que solo los nodos autorizados puedan acceder a sus interfaces.

Anexo I – FAQ

¿Es posible instalar el NA sobre un Clúster Kubernetes no gestionado por Rancher?

Sí, el NA podrá desplegarse sobre un Clúster Kubernetes basado en Openshift, pero deberá tenerse en cuenta que este tipo de Clúster requerirá de un licenciamiento adicional no incluido. También está certificado el uso sobre el clúster EKS provisto on-cloud por AWS.

¿Puede instalarse el NA sobre infraestructura provista en Cloud?

Sí, la instalación del NA en cada CA puede realizarse sobre infraestructura propia o sobre infraestructura Cloud.

¿Los entornos no productivos pueden instalarse sobre instancias Kubernetes basadas en un único nodo?

Sí, para los escenarios mediano y pequeño, sí que se prevé que estos entornos se puedan desplegar en infraestructuras más sencillas, no obstante, habrá que tener en cuenta que estos entornos serán más complejos de escalar, si fuera necesario, así como que tampoco proporcionarán capacidades HA, y difieren con respecto al entorno productivo, lo que podría complicar determinados tipos de prueba en los que se requiera extrapolar comportamientos en este.

¿Pueden mezclarse escenarios de despliegue?

Sí, los escenarios propuestos se calcularon en base al potencial volumen de pacientes en cada NA en función de su población pediátrica, pero cada CA puede optar por utilizar un esquema para el entorno de Producción y otro para los pre-productivos, por ejemplo, para el caso de querer dotar a estos últimos de capacidades HA, podría optarse del esquema inmediatamente inferior y así mantener las características como se indicaba en la pregunta anterior.

¿Para la persistencia en Base de Datos existe otra alternativa que no sea MySQL u Oracle* para los componentes No colaborativos*?

No, el NA debe ser instalado sobre un motor base de datos MySQL 8 o superior, o en un Oracle 19c o superior.

¿Para la persistencia en Base de Datos existe otra alternativa que no PostgreSQL* para la Plataforma Colaborativa (MDT Meeting)*?

No, la plataforma colaborativa del NA debe ser instalada sobre un motor base de datos PostgreSQL 15 o superior.

¿Es necesario tener un sistema de almacenamiento S3 para la persistencia de Informes?

No, estos se pueden almacenar directamente sobre la base de datos, no obstante, se aconseja disponer de este sistema adicional basado en S3, para evitar el crecimiento de la BBDD derivado de la inclusión de este tipo de información que por su naturaleza en muy pesada.

¿Es necesario que los equipos cliente de los usuarios de los HIS tengan acceso al NA?

Sí, es necesario que desde estos equipos se pueda acceder a los componentes Front del NA, de forma que desde los propios HISs se pueda invocar a las funcionalidades que ofrece el NA tanto en el contexto de profesional, como en el contexto de paciente.

¿Se puede reutilizar el certificado cliente con el que se accede al SNS desde la CA para otras funcionalidades?

Sí, siempre y cuando este siga vigente, podrá reutilizarse el certificado cliente de la CA para comunicar con el NC situado en el Ministerio. Esto además facilitará la gestión de este, ya que ante renovaciones sólo será necesario renovar un único certificado y desplegarlo en todas las soluciones que requieran este tipo de autenticación con el SNS.

¿Los sistemas de información Origen deben tener conexión con el NA?

Sí, ya que será necesario que desde estos se remita toda la información que se disponga de los pacientes que se adhieran al Proceso UNICAS, en el formato indicado en la IG[3], tanto en la admisión a modo de volcado de toda la información histórica, como a partir de ese momento toda aquella información que se vaya generando del mismo. No obstante, pueden darse escenarios donde la información no se vuelque directamente desde este, sino que exista una capa intermedia que los proporcione, en cuyo caso deberá ser esta la que disponga de dicha visibilidad, sin perjuicio de que pudieran existir escenarios mixtos, donde parte podría venir directamente de los HISs y otra parte de estos elementos intermedios, en cuyo caso deberemos habilitar la visibilidad desde ambos elementos.

[3] https://unicas-fhir.sanidad.gob.es/