Documento de Arquitectura de Software
Grupo 09 - 2025

Taller de Sistemas Empresariales
Taller de Sistemas de Información Java EE

German Rodao 4.796.608-7

Agustin Silvano 5.096.964-8

Piero Santos 6.614.312-9

Tabla de Contenido

1. Introducción

Este documento presenta la arquitectura de la plataforma de gestión de historias clínicas electrónicas normalizadas (HCEN), la cual fue desarrollada como trabajo de laboratorio para la edición 2025 de los cursos Taller de Sistemas Empresariales (Ingeniería y Licenciatura en Computación) y Taller de Sistemas de Información Java EE (Tecnólogo en Informática) de la Facultad de Ingeniería, Universidad de la República.

El objetivo del proyecto fue diseñar e implementar una solución orientada a la gestión de documentación médica, que permitiera a distintos actores del sistema de salud (pacientes, profesionales, clínicas) compartir, acceder y controlar el acceso a dicha información de forma segura, trazable y flexible.

La arquitectura fue concebida tomando en cuenta los distintos aspectos funcionales y no funcionales planteados en el enunciado del proyecto, con especial énfasis en el manejo de identidades, control de accesos, interoperabilidad, escalabilidad y mantenibilidad del sistema.

Este documento describe las diferentes vistas arquitectónicas de la solución, siguiendo una estructura estándar que abarca desde el modelo conceptual hasta los aspectos de implementación y despliegue.

1.1. Objetivo del Documento

El objetivo de este Documento de Arquitectura de Software (Software Architecture Document, SAD) es brindar una visión comprensible de la arquitectura general de la plataforma de gestión de historias clínicas electrónicas normalizadas (HCEN).

Este documento tiene como propósito servir como una guía para comprender las decisiones arquitectónicas tomadas durante el desarrollo del sistema, facilitar la comunicación entre los distintos actores involucrados en el proyecto (estudiantes, docentes y posibles evaluadores externos), y sentar las bases para futuras extensiones, mantenimiento o implementación real de la solución.

A lo largo del documento se presentan las distintas vistas arquitectónicas requeridas, abarcando aspectos conceptuales, casos de uso, restricciones, atributos de calidad, diseño lógico, distribución e implementación.

1.2. Representación de la Arquitectura

La arquitectura de la plataforma «HCEN» está representada por diferentes vistas que permiten visualizar, entender y razonar sobre los elementos significativos de la arquitectura, así como identificar áreas de riesgo que requieren mayor elaboración [**Kruchten1995**][**Perovich2003**]. En particular, las vistas utilizadas para representar la arquitectura de la plataforma son:

1. **Vista Conceptual:** Describe a alto nivel los conceptos principales del sistema y sus relaciones. Incluye una descripción general de la plataforma y el modelo conceptual que guía el diseño.

2. **Vista de Casos de Uso:** Representa las funcionalidades más relevantes del sistema desde el punto de vista de los distintos actores. Esta vista describe el comportamiento esperado del sistema ante diferentes escenarios de interacción.

3. **Vista de Restricciones:** Detalla las restricciones tecnológicas, regulatorias o de otro tipo que deben ser consideradas en el diseño e implementación del sistema.

4. **Vista de Atributos de Calidad:** Enumera los atributos relacionados a requerimientos no funcionales (como seguridad, escalabilidad, mantenibilidad o interoperabilidad) que guían las decisiones arquitectónicas.

5. **Vista Lógica:** Describe los componentes principales del sistema, sus responsabilidades y las relaciones entre ellos. Incluye diagramas de componentes y refinamientos necesarios para entender la estructura interna del sistema.

6. **Vista de Distribución:** Representa la disposición física del sistema en un entorno productivo. Muestra cómo los distintos elementos del sistema se distribuyen entre los nodos físicos o virtuales de la infraestructura.

7. **Vista de Implementación:** Presenta las decisiones tecnológicas adoptadas para llevar a cabo la solución, incluyendo frameworks, lenguajes y herramientas utilizadas. Se justifica la elección del estilo arquitectónico y se discuten alternativas consideradas.

8. **Vista de Decisiones de Arquitectura:** Resume las decisiones arquitectónicas clave tomadas durante el proyecto, así como el razonamiento detrás de ellas, considerando posibles alternativas.

1.3. Partes Interesadas (i.e. *stakeholders*)

Las partes interesadas en la plataforma hcen.uy son:

1. **Ciudadano:** persona física con derechos y obligaciones que interactúa con la plataforma para acceder a los servicios ofrecidos.

2. **Equipo de Desarrollo:** profesionales encargados de implementar, mantener y evolucionar la plataforma, quienes necesitan comprender la arquitectura para tomar decisiones técnicas informadas.

3. **Administrador del Sistema:** responsable de la configuración, monitoreo y operación del sistema en el entorno productivo.

4. **Profesionales de Salud:** usuarios especializados que utilizan la plataforma para gestionar y acceder a la información clínica.

La Tabla 1 indica a qué parte interesada está orientada cada una de las vistas de la arquitectura.

Tabla 1: Partes Interesadas y Vistas

	Vista de Casos de Uso	Vista de Restricciones	Vista de Calidad de Servicio	Vista Lógica	Vista de Procesos	Vista de Implementación	Vista de Datos	Vista de Servicios	Vista de Distribución	Vista de Decisiones de Arquitectura
Ciudadano	✓	✓		✓						
Equipo de Desarrollo	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Administrador del Sistema		✓	✓	✓	✓	✓	✓		✓	✓
Profesionales de Salud	✓			✓			✓	✓		

1.4. Organización del Documento

El resto del documento se organiza en ocho secciones, cada una de las cuales describe una de las vistas que representan la arquitectura:

- Sección 2: Vista Conceptual
- Sección 3: Vista de Casos de Uso
- Sección 4: Vista de Restricciones
- Sección 5: Vista de Atributos de Calidad
- Sección 6: Vista Lógica
- Sección 7: Vista de Distribución
- Sección 8: Vista de Implementación
- Sección 9: Vista de Decisiones de Arquitectura

2. Vista Conceptual

La Vista Conceptual brinda una descripción general de la plataforma y presenta los principales conceptos asociados a la misma.

2.1. Descripción General de la Plataforma

La plataforma hcen.uy es un sistema integral diseñado para gestionar de manera segura y eficiente la información clínica y administrativa en el ámbito de la salud. Su arquitectura modular permite la interoperabilidad entre diferentes actores, incluyendo pacientes, profesionales de la salud, y administradores de clínicas. La plataforma se centra en garantizar la confidencialidad, integridad y disponibilidad de los datos mediante un modelo robusto de control de acceso, así como en facilitar la trazabilidad y auditoría de las acciones realizadas.

El sistema soporta funcionalidades esenciales tales como la gestión de usuarios y roles, administración de sesiones y tokens de autenticación, manejo de documentos clínicos con versiones, así como políticas de acceso y consentimiento explícito de los pacientes. Además, la plataforma incluye una configuración multi-inquilino para adaptar las necesidades particulares de cada clínica, asegurando personalización y escalabilidad.

En la Figura 1 se presenta una visión general de la plataforma, mostrando sus principales componentes y la interacción entre ellos.

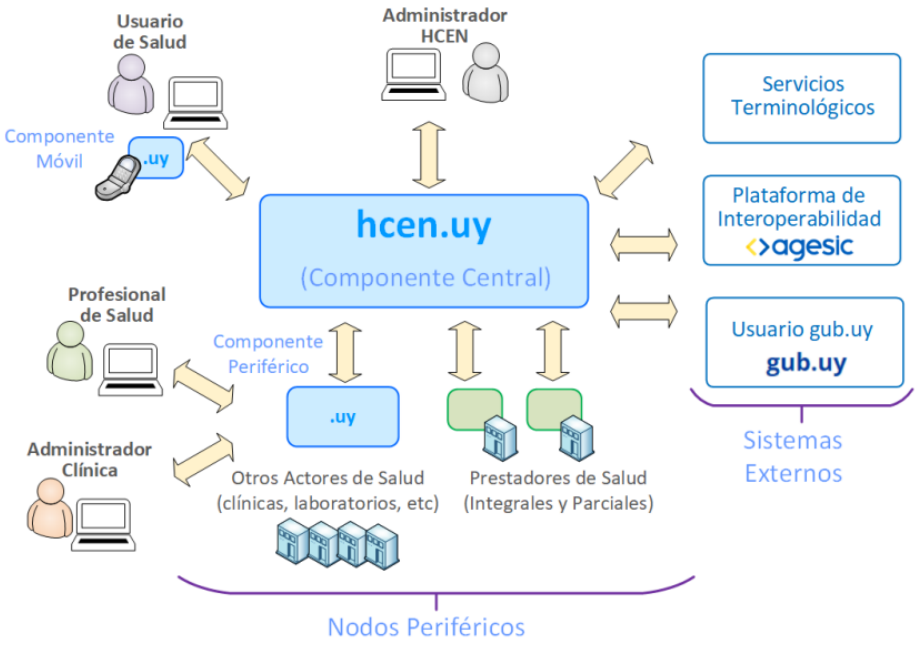


Figura 1: Descripción General de la Plataforma

2.2. Modelo Conceptual

El modelo conceptual de la plataforma hcen.uy presenta los principales componentes del sistema y sus relaciones, permitiendo visualizar las funciones clave y cómo interactúan entre sí.

La arquitectura se compone de tres grandes dominios: un **componente central**, un **componente móvil**, y un conjunto de **nodos periféricos multi-tenant**, donde operan las clínicas. Además, se contemplan integraciones con sistemas externos como la Plataforma de Interoperabilidad (PDI) y Gub.uy para autenticación.

- El **componente central** incluye funcionalidades como el portal de administración, el portal ciudadano, los servicios de auditoría, el índice único de usuarios (INUS), los metadatos del repositorio nacional de documentos clínicos (RNDC), y el motor de políticas de acceso.
- El **componente móvil** está compuesto por la aplicación móvil y el servicio de notificaciones push.
- Los **nodos periféricos multi-tenant** contienen portales para clínicas y profesionales, almacenamiento local de documentos, y APIs que exponen la funcionalidad clínica.
- Las **integraciones externas** permiten a los usuarios autenticarse mediante Gub.uy y acceder a sistemas clínicos mediante PDI.

La Figura 2 presenta gráficamente este modelo conceptual de alto nivel.

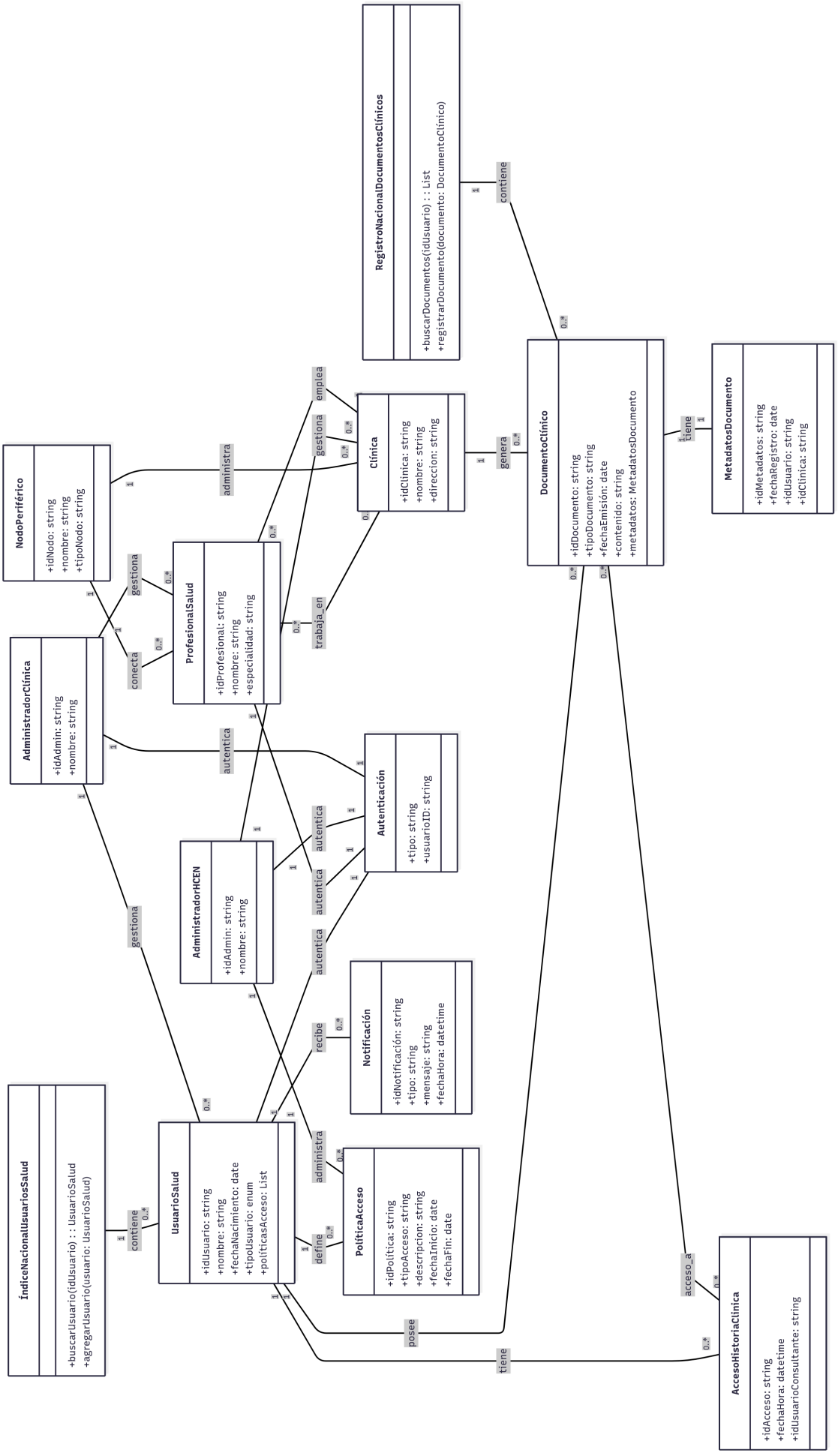


Figura 2: Modelo Conceptual

3. Vista de Casos de Uso

La Vista de Casos de Uso se centra en los aspectos funcionales de la plataforma. En esta sección se identifican los actores que interactúan con el sistema y se presentan los casos de uso principales, modelando cómo los distintos perfiles de usuario acceden a las funcionalidades del sistema.

Además, se identifican los casos de uso que se consideran críticos desde el punto de vista arquitectónico, ya sea por involucrar múltiples componentes, representar funcionalidades centrales del sistema, o requerir integraciones complejas con servicios externos.

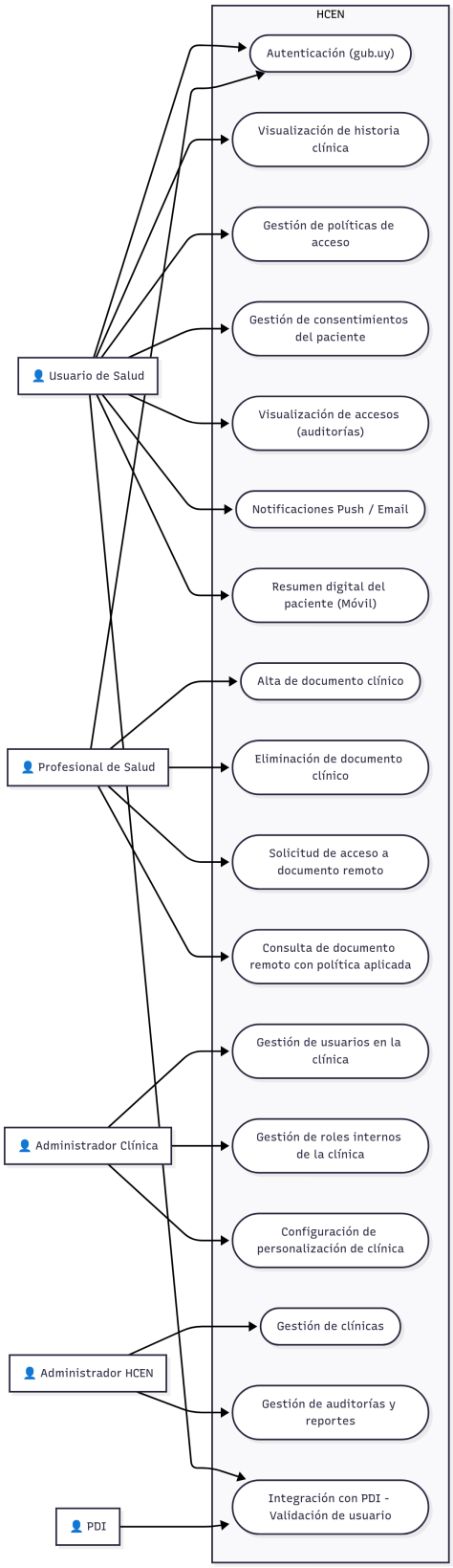
3.1. Actores

A continuación se presentan los actores identificados en la plataforma:

- **Usuario de Salud:** Persona que accede a su historia clínica electrónica a través del portal web o la aplicación móvil. Puede configurar políticas de acceso, recibir notificaciones y visualizar accesos realizados a sus datos clínicos.
- **Profesional de Salud:** Médico u otro profesional habilitado por una clínica para registrar documentos clínicos, consultar la historia clínica de pacientes, y solicitar acceso a documentos remotos.
- **Administrador de Clínica:** Usuario responsable de la gestión operativa de una clínica dentro del sistema. Puede administrar usuarios de salud, profesionales, roles internos, y configurar la personalización del portal de la clínica.
- **Administrador HCEN:** Encargado de gestionar clínicas registradas en la plataforma desde el componente central. Puede generar reportes, analizar auditorías, y administrar el sistema a nivel global.
- **Plataforma PDI (externa):** Sistema externo del Estado uruguayo utilizado para validar la identidad y edad de los usuarios a través del Servicio Básico de Información.
- **Sistema gub.uy (externo):** Plataforma nacional de autenticación utilizada para validar la identidad de los usuarios mediante OIDC/OAuth2.

3.2. Diagrama de Casos de Uso

A continuación se presenta el Diagrama de Casos de Uso general de la plataforma, donde se incluyen los principales casos de uso identificados. En el mismo se destacan los casos de uso considerados críticos para la arquitectura.


HCEN
Autenticación (gub.uy)
Visualización de historia clínica
Gestión de políticas de acceso
Gestión de consentimientos del paciente
Usuario de Salud
Visualización de accesos (auditorías)
Notificaciones Push / Email
Resumen digital del paciente (Móvil)
Alta de documento clínico
Profesional de Salud
Eliminación de documento clínico
Solicitud de acceso a documento remoto
Consulta de documento remoto con política aplicada
Gestión de usuarios en la clínica
Administrador Clínica
Gestión de roles internos de la clínica
Configuración de personalización de clínica
Gestión de clínicas
Administrador HCEN
Gestión de auditorías y reportes
Integración con PDI - Validación de usuario
PDI

3.3. Caso de Uso Crítico 1: Autenticación con gub.uy

Descripción

El usuario de salud o profesional accede al sistema mediante el servicio de autenticación centralizado gub.uy, que utiliza el protocolo OIDC/OAuth2. El sistema valida la identidad, crea la sesión y registra el evento en la auditoría.

Pre-condiciones

- El usuario debe estar registrado en el sistema gub.uy.
- La aplicación móvil o portal web debe estar en línea y conectada con el Portal Central.

Flujo de Eventos

1. El usuario inicia el login en la App móvil o el Portal web.
2. El Portal Central redirige al usuario hacia gub.uy con una solicitud de autenticación (OIDC).
3. gub.uy autentica al usuario y devuelve al Portal Central un código o token.
4. El Portal Central valida el token recibido y obtiene los claims asociados al usuario.
5. Si corresponde, el Portal Central consulta al INUS para validar/obtener información adicional del usuario.
6. El Portal Central establece la sesión del usuario (JWT o cookie de sesión) y lo notifica a la App/Portal.
7. El Portal Central envía un registro del evento de login al sistema de Auditoría.

Post-condiciones

- El usuario queda autenticado en la aplicación móvil o portal web.
- El evento de login queda registrado en el sistema de auditoría.

3.4. Caso de Uso Crítico 2: Visualización de Historia Clínica

Descripción

El usuario de salud accede a la plataforma (Portal o App móvil) y solicita visualizar su historia clínica. El sistema central obtiene la información del paciente desde INUS, recupera los metadatos de documentos clínicos desde el RNDC y, en caso de ser necesario, consulta documentos específicos en los nodos periféricos. Finalmente, la historia clínica es presentada al usuario y el acceso queda registrado en la auditoría.

Pre-condiciones

- El usuario debe estar autenticado en la aplicación (Portal o App móvil).
- El usuario debe estar registrado en INUS.
- Los sistemas INUS, RNDC y los nodos periféricos deben estar disponibles.

Flujo de Eventos

1. El usuario solicita visualizar su historia clínica en el Portal Central.
2. El Portal Central consulta al INUS para verificar y obtener la información del paciente.
3. INUS devuelve los datos del paciente al Portal Central.
4. El Portal Central solicita al RNDC la lista de documentos clínicos asociados al paciente.
5. El RNDC devuelve la lista de metadatos de documentos clínicos.
6. Por cada documento cuyo contenido esté alojado en un nodo periférico:
   a) El Portal Central solicita el documento a la API de la clínica correspondiente, verificando las políticas de acceso.
   b) El nodo periférico devuelve el documento o redirige hacia su acceso.
7. El Portal Central presenta al usuario la historia clínica (metadatos y documentos obtenidos).
8. El Portal Central registra el evento de consulta de historia clínica en el sistema de auditoría.

Post-condiciones

- El usuario puede visualizar su historia clínica (metadatos y documentos).
- El acceso a la historia clínica queda registrado en el sistema de auditoría.

3.5. Caso de Uso Crítico 3: Alta de Documento Clínico

Descripción

Un profesional de salud registra un nuevo documento clínico en el sistema a través del portal de la clínica. El sistema valida si el paciente existe en INUS, guarda el documento en el repositorio local de la clínica y registra los metadatos en el RNDC. Finalmente, se notifica al profesional sobre la creación del documento y el evento queda registrado en el sistema de auditoría.

Pre-condiciones

- El profesional debe estar autenticado en el portal de la clínica.
- El paciente debe estar registrado en INUS o se debe permitir el alta de un nuevo usuario en caso de no existir.
- Los servicios de INUS, RNDC y almacenamiento local deben estar disponibles.

Flujo de Eventos

1. El profesional envía al sistema de la clínica un documento clínico con su archivo y metadatos.
2. La clínica verifica si el paciente está registrado en INUS:
   a) Si no existe, la clínica registra al paciente en INUS.
   b) INUS devuelve el identificador del paciente.
3. La clínica guarda el documento en su repositorio local, obteniendo un localizador y un hash del archivo.
4. El sistema de la clínica registra en el RNDC los metadatos del documento, incluyendo identificador, localizador y hash.
5. El RNDC confirma el registro de los metadatos.
6. El sistema de la clínica registra el evento de alta en el sistema de auditoría.
7. La clínica confirma al profesional la creación del documento (201 Created).

Post-condiciones

- El documento clínico queda almacenado en el repositorio local de la clínica.
- Los metadatos del documento quedan registrados en el RNDC.
- El evento de alta del documento queda registrado en la auditoría.

3.6. Caso de Uso Crítico 4: Solicitud y Otorgamiento de Acceso a Documentos Clínicos

Descripción

Un profesional de la salud solicita acceso a un documento clínico remoto de un paciente a través del sistema de la clínica. El sistema central consulta al motor de políticas para evaluar si la solicitud puede ser permitida, denegada o requiere aprobación del paciente. En caso de requerir aprobación, el paciente recibe una notificación para otorgar o rechazar el acceso. Finalmente, el resultado se comunica al sistema de la clínica y el evento queda registrado en el sistema de auditoría.

Pre-condiciones

- El profesional debe estar autenticado en el sistema de la clínica.
- El paciente debe estar registrado en INUS y vinculado con el documento clínico al que se desea acceder.
- El motor de políticas debe estar disponible para evaluar solicitudes de acceso.
- El sistema de notificación al paciente debe estar operativo en caso de que se requiera su aprobación.

Flujo de Eventos

1. El profesional solicita acceso a un documento remoto asociado a un paciente desde el sistema de la clínica.
2. El sistema de la clínica envía la solicitud de acceso al portal central.
3. El portal central consulta al motor de políticas (ABAC/RBAC) para evaluar la solicitud.
4. El motor de políticas devuelve una decisión inicial: permitir, denegar o pendiente de autorización del paciente.
   a) Si la decisión es **permitir**, se concede acceso inmediato.
   b) Si la decisión es **denegar**, se informa al profesional sin acceso.
   c) Si la decisión es **pendiente**, el sistema central notifica al paciente vía push o correo electrónico:
      1) El paciente responde otorgando o rechazando el acceso.
      2) El portal central actualiza el estado de la solicitud en el motor de políticas.
5. El portal central notifica al sistema de la clínica el resultado de la solicitud, incluyendo en caso de ser aprobado un token temporal o permiso.
6. El portal central registra la solicitud y la decisión en el sistema de auditoría.

Post-condiciones

- El profesional puede acceder al documento clínico si la solicitud fue permitida o aprobada por el paciente.
- Si la solicitud fue denegada, el acceso queda restringido.
- El evento de solicitud y su resultado quedan registrados en el sistema de auditoría.

3.7. Caso de Uso Crítico 5: Gestión de usuarios en la clínica

Descripción

El Administrador de la clínica gestiona los usuarios de salud asociados a la clínica. Esto incluye la creación de profesionales de salud, registrando sus datos personales y su especialidad. Al crear un usuario, el sistema actualiza el índice nacional de usuarios de salud (INUS) si corresponde, y mantiene un registro de auditoría de las acciones realizadas para garantizar trazabilidad y cumplimiento de políticas internas.

Pre-condiciones

- El Administrador de la clínica debe estar autenticado mediante el mecanismo interno del componente periférico.
- La clínica debe estar registrada en el sistema y habilitada para gestionar usuarios.
- Se debe disponer de conectividad con el INUS para registrar usuarios que lo requieran.

Flujo de Eventos

1. El Administrador de la clínica solicita la creación de un profesional de salud ingresando nombre, correo electrónico y especialidad.
2. El componente periférico (ClinicAPI) recibe la solicitud y valida los datos.
3. Si corresponde, se registra al usuario en el INUS y se obtiene un identificador único (inusid).
4. ClinicAPI confirma al Administrador que el profesional ha sido creado correctamente.
5. El sistema registra en el módulo de Auditoría la acción de alta del profesional.
6. El flujo finaliza con la disponibilidad del nuevo profesional en el portal de la clínica para su gestión.

Post-condiciones

- El nuevo profesional de salud queda registrado en la clínica y, si aplica, en el INUS.
- La acción queda registrada en el sistema de Auditoría, garantizando trazabilidad.
- El profesional puede acceder a los portales correspondientes según su rol y especialidad.

3.8. Caso de Uso Crítico 6: Gestión de políticas de acceso

Descripción

El Administrador del portal HCEN gestiona las políticas de acceso sobre la información clínica de los usuarios. Esto incluye la creación y modificación de políticas, definiendo alcance, tipos de sujetos y condiciones. Cada cambio realizado se registra tanto en el historial de políticas como en el sistema de auditoría, garantizando trazabilidad y cumplimiento de las normas de seguridad y acceso establecidas por la plataforma.

Pre-condiciones

- El Administrador del portal HCEN debe estar autenticado mediante Usuario gub.uy.
- El motor de políticas debe estar operativo para procesar las solicitudes.
- El sistema debe contar con disponibilidad para registrar cambios en el historial de políticas y en auditoría.

Flujo de Eventos

1. El Administrador crea o edita una política de acceso especificando el alcance (scope), tipo de sujeto (subject_type) y condiciones.
2. El Motor de Políticas recibe la solicitud y valida la información ingresada.
3. El Motor de Políticas registra los cambios en el Historial de Políticas.
4. El Motor de Políticas devuelve una confirmación al Administrador indicando que la operación se completó exitosamente.
5. El Motor de Políticas registra el evento en el sistema de Auditoría para asegurar trazabilidad.

Post-condiciones

- La nueva política de acceso queda activa y disponible para ser evaluada en solicitudes de acceso futuras.
- Los cambios quedan registrados en el Historial de Políticas.
- El evento queda registrado en el sistema de Auditoría, garantizando trazabilidad y cumplimiento normativo.

3.9. Caso de Uso Crítico 7: Gestión de consentimientos del paciente

Descripción

El paciente gestiona sus consentimientos sobre el acceso a su historia clínica a través del portal central. Esto incluye la creación, edición y revocación de consentimientos, los cuales definen las condiciones bajo las cuales los profesionales de salud pueden acceder a sus documentos clínicos. El sistema aplica automáticamente las políticas correspondientes, actualiza el RNDC según el alcance del consentimiento y registra la acción en el sistema de auditoría para garantizar trazabilidad.

Pre-condiciones

- El paciente debe estar autenticado en el portal central mediante Usuario gub.uy.
- El Motor de Políticas debe estar disponible para evaluar y aplicar las condiciones del consentimiento.
- El RNDC debe estar operativo para asociar o bloquear documentos clínicos según el consentimiento.

Flujo de Eventos

1. El paciente crea, edita o revoca un consentimiento para el acceso a su historia clínica.
2. El portal central envía la acción al Motor de Políticas para evaluar y aplicar las condiciones definidas.
3. El Motor de Políticas devuelve confirmación de la correcta aplicación de la política.
4. Dependiendo del tipo de acción:
   a) Si es revocación, el portal central indica al RNDC bloquear el acceso a los documentos asociados.
   b) Si es creación o edición, el portal central indica al RNDC asociar los documentos correspondientes según el alcance definido.
5. El portal central registra la acción en el sistema de Auditoría.
6. El portal central confirma al paciente que su acción fue registrada exitosamente.

Post-condiciones

- Los documentos clínicos del paciente quedan asociados o bloqueados en el RNDC según el consentimiento.
- La acción queda registrada en el sistema de Auditoría, asegurando trazabilidad.
- El paciente puede verificar que sus consentimientos fueron aplicados correctamente.

3.10. Caso de Uso Crítico 8: Consulta de documento remoto con política aplicada

Descripción

Un profesional de salud o usuario de salud solicita acceso a un documento clínico remoto. El sistema central evalúa las políticas de acceso correspondientes mediante el Motor de Políticas. Dependiendo de la decisión, el acceso puede ser permitido, denegado o pendiente de aprobación. En caso de permiso concedido, se recuperan los metadatos desde el RNDC y el documento real desde el nodo periférico correspondiente. Todos los eventos quedan registrados en el sistema de auditoría.

Pre-condiciones

- El usuario o profesional debe estar autenticado en el sistema (Portal Central o nodo periférico).
- El documento clínico solicitado debe estar registrado en el RNDC.
- El Motor de Políticas debe estar operativo para evaluar solicitudes de acceso.
- Los nodos periféricos deben estar disponibles para entregar los documentos solicitados.

Flujo de Eventos

1. El usuario solicita un documento remoto proporcionando un token de acceso.
2. El Portal Central envía la solicitud al Motor de Políticas para evaluar las políticas de acceso.
3. El Motor de Políticas devuelve una decisión: permitir, denegar o pendiente.
4. Dependiendo de la decisión:
   a) **Permitir**:
      1) El Portal Central solicita los metadatos del documento al RNDC.
      2) El RNDC devuelve la lista de metadatos del documento.
      3) El Portal Central solicita el documento real al nodo periférico correspondiente (ClinicAPI).
      4) El nodo periférico devuelve el documento o un redireccionamiento para su descarga.
   b) **Denegar**: El Portal Central informa al usuario que el acceso fue denegado.
5. El Portal Central registra el evento de acceso en el sistema de Auditoría.

Post-condiciones

- El usuario obtiene el documento si la política de acceso lo permite.
- Si la política lo deniega, el usuario no puede acceder al documento.
- Todos los eventos de acceso quedan registrados en el sistema de Auditoría.

3.11. Caso de Uso Crítico 9: Gestión de roles internos de la clínica

Descripción

El Administrador de la clínica gestiona los roles internos de los usuarios de la aplicación de la clínica. Esto incluye la creación y modificación de roles, definiendo los permisos asociados a cada uno. Una vez actualizados, los cambios se reflejan en los usuarios correspondientes y se registran en el sistema de auditoría para garantizar trazabilidad y cumplimiento de las políticas internas.

Pre-condiciones

- El Administrador de la clínica debe estar autenticado mediante el mecanismo interno del componente periférico.
- El Portal Central y el módulo de Roles deben estar operativos para recibir y almacenar la información.
- El sistema de notificaciones debe estar disponible para informar a los usuarios sobre cambios de rol, si aplica.

Flujo de Eventos

1. El Administrador solicita la creación o modificación de un rol interno, incluyendo los permisos asociados.
2. El Portal Central recibe la solicitud y valida la información.
3. El módulo de Roles guarda la información del rol y sus permisos.
4. El módulo de Roles confirma al Portal Central que la operación se realizó correctamente.
5. El Portal Central notifica a los usuarios afectados por cambios en roles, si corresponde.
6. El Portal Central registra la acción de gestión de roles en el sistema de Auditoría.

Post-condiciones

- Los roles internos quedan actualizados con los permisos correspondientes.
- Los usuarios afectados son notificados sobre cambios en sus roles.
- La acción queda registrada en el sistema de Auditoría, asegurando trazabilidad.

3.12. Caso de Uso Crítico 10: Gestión de auditorías y reportes

Descripción

El Administrador del portal HCEN solicita reportes de auditoría para analizar accesos y actividades sobre la información clínica. El sistema recopila los metadatos de documentos desde el RNDC y los datos de usuarios desde el INUS, generando un reporte compilado que permite evaluar la trazabilidad, cumplimiento de políticas de acceso y detectar posibles incidencias o irregularidades.

Pre-condiciones

- El Administrador debe estar autenticado mediante Usuario gub.uy.
- El sistema de Auditoría debe estar operativo para procesar solicitudes de reportes.
- RNDC y INUS deben estar disponibles para proporcionar la información requerida.

Flujo de Eventos

1. El Administrador solicita un reporte de accesos desde el Portal Admin HCEN.
2. El sistema de Auditoría consulta los metadatos de documentos en el RNDC.
3. El sistema de Auditoría consulta los datos de usuarios en el INUS.
4. El sistema de Auditoría compila la información en un reporte consolidado.
5. El sistema entrega el reporte al Administrador.

Post-condiciones

- El Administrador recibe el reporte compilado con la información de accesos y actividades.
- Todos los eventos de generación de reportes quedan registrados en el sistema de Auditoría.
- Se garantiza la trazabilidad y posibilidad de análisis sobre el uso de la plataforma.

3.13. Caso de Uso Crítico 11: Eliminación de documento clínico

Descripción

Un profesional de salud solicita la eliminación de un documento clínico. El sistema central y el nodo periférico coordinan la acción para marcar el documento como inactivo en el RNDC, eliminar el archivo físico en el almacenamiento local de la clínica y registrar la acción en el sistema de auditoría. Finalmente, el profesional recibe la confirmación de la eliminación exitosa.

Pre-condiciones

- El profesional debe estar autenticado en el sistema mediante el mecanismo interno de la clínica.
- El documento clínico debe existir y estar registrado en el RNDC.
- El RNDC y el almacenamiento local deben estar operativos para procesar la eliminación.

Flujo de Eventos

1. El profesional solicita la eliminación de un documento clínico desde el sistema de la clínica.
2. El nodo periférico (ClinicAPI) marca el documento como inactivo en el RNDC.
3. El nodo periférico elimina el archivo físico correspondiente en el almacenamiento local.
4. El nodo periférico confirma al profesional que el documento fue eliminado correctamente.
5. El nodo periférico registra la acción de eliminación en el sistema de Auditoría.

Post-condiciones

- El documento clínico queda marcado como inactivo en el RNDC.
- El archivo físico del documento queda eliminado del almacenamiento local de la clínica.
- La acción queda registrada en el sistema de Auditoría, asegurando trazabilidad.

3.14. Caso de Uso Crítico 12: Notificaciones Push / Email

Descripción

El Portal Central envía notificaciones a los usuarios o pacientes sobre eventos relevantes, como accesos a su historia clínica, cambios en consentimientos o alertas importantes. Las notificaciones se envían mediante servicios Push y correo electrónico según corresponda, garantizando que el usuario reciba la información en tiempo y forma.

Pre-condiciones

- El usuario o paciente debe estar registrado y contar con credenciales válidas en el sistema.
- El Portal Central debe estar operativo y poder comunicarse con los servicios de Push y Email.
- Los servicios de Push y Email deben estar disponibles para entregar las notificaciones.

Flujo de Eventos

1. El Portal Central detecta un evento relevante (acceso a historia clínica, cambio de consentimiento, alerta, etc.).
2. El Portal Central envía la notificación correspondiente al servicio Push.
3. El servicio Push entrega la notificación al usuario o paciente.
4. Si aplica, el Portal Central envía un correo electrónico mediante el servicio Email.
5. El servicio Email entrega el correo al usuario o paciente.

Post-condiciones

- El usuario o paciente recibe la notificación en su dispositivo mediante Push.
- Si corresponde, el usuario o paciente recibe un correo electrónico con la información del evento.
- Se asegura la trazabilidad de los envíos de notificaciones.

3.15. Caso de Uso Crítico 13: Integración con PDI - Validación de usuario

Descripción

El Portal Central valida la información de un usuario mediante la Plataforma de Interoperabilidad (PDI). La consulta incluye datos básicos y fecha de nacimiento para verificar que el usuario sea mayor de edad. Posteriormente, el usuario se registra o actualiza en INUS y la acción de consulta queda registrada en el sistema de Auditoría, asegurando trazabilidad y cumplimiento normativo.

Pre-condiciones

- El Portal Central debe estar operativo y tener acceso a la PDI.
- El usuario debe estar identificado mediante su cédula de identidad.
- La PDI y el INUS deben estar disponibles para recibir y procesar las solicitudes.

Flujo de Eventos

1. El Portal Central consulta a la PDI los datos del usuario mediante su cédula de identidad.
2. La PDI devuelve información básica del usuario, incluyendo fecha de nacimiento.
3. El Portal Central valida que el usuario sea mayor de edad.
4. El Portal Central registra o actualiza al usuario en INUS.
5. El Portal Central registra la consulta realizada a la PDI en el sistema de Auditoría.

Post-condiciones

- El usuario queda registrado o actualizado en INUS con la información validada.
- La consulta a la PDI queda registrada en el sistema de Auditoría.
- Se garantiza la trazabilidad de la validación del usuario y cumplimiento de políticas de edad mínima.

3.16. Caso de Uso Crítico 14: Configuración de personalización de clínica

Descripción

El Administrador de la clínica configura elementos de personalización del portal, tales como logos, colores y otros aspectos visuales. El Portal Central recibe la configuración, la guarda en el sistema de configuración clínica y registra el cambio en el sistema de Auditoría, garantizando trazabilidad y coherencia visual del portal para la clínica.

Pre-condiciones

- El Administrador debe estar autenticado mediante el mecanismo interno de la clínica.
- El Portal Central y el sistema de Configuración Clínica deben estar operativos.

Flujo de Eventos

1. El Administrador configura el branding del portal (logo, colores, etc.) desde el Portal de la clínica.
2. El Portal Central recibe la configuración y la envía al sistema de Configuración Clínica para su almacenamiento.
3. El sistema de Configuración Clínica confirma que la configuración fue guardada correctamente.
4. El Portal Central registra la acción de cambio de configuración en el sistema de Auditoría.

Post-condiciones

- La configuración personalizada de la clínica queda almacenada y activa en el portal.
- La acción de cambio de configuración queda registrada en el sistema de Auditoría.
- Se garantiza consistencia en la personalización visual del portal para la clínica.

3.17. Caso de Uso Crítico 15: Gestión de clínicas (Portal Admin HCEN)

Descripción

El Administrador del Portal HCEN crea o activa una clínica dentro del sistema. El Portal Central registra la clínica en INUS, configura el nodo periférico correspondiente y registra la acción en el sistema de Auditoría. Finalmente, el Administrador recibe confirmación de que la clínica fue creada exitosamente.

Pre-condiciones

- El Administrador del Portal HCEN debe estar autenticado.
- El Portal Central, INUS y el nodo periférico deben estar operativos.
- La información de la clínica (nombre, RUC, contacto) debe estar disponible.

Flujo de Eventos

1. El Administrador del Portal HCEN solicita la creación o activación de una clínica proporcionando nombre, RUC y contacto.
2. El Portal Central registra la clínica en INUS.
3. INUS devuelve el identificador generado para la clínica (clinic_id).
4. El Portal Central configura el nodo periférico correspondiente a la clínica.
5. El nodo periférico confirma que la configuración fue realizada correctamente.
6. El Portal Central registra la alta de la clínica en el sistema de Auditoría.
7. El Portal Central notifica al Administrador que la clínica fue creada exitosamente.

Post-condiciones

- La clínica queda registrada y activa en INUS con su nodo periférico configurado.
- La acción de creación queda registrada en el sistema de Auditoría.
- El Administrador recibe confirmación de la creación exitosa de la clínica.

3.18. Caso de Uso Crítico 16: Resumen digital del paciente (Componente Móvil)

Descripción

La aplicación móvil solicita al Portal Central un resumen digital del paciente siguiendo el estándar IPS-FHIR. El Portal Central obtiene los datos básicos del paciente desde INUS y los metadatos de documentos recientes desde RNDC. Posteriormente, recupera el contenido de cada documento desde los nodos periféricos, genera un resumen digital estructurado y lo entrega a la aplicación móvil. Toda la operación queda registrada en el sistema de Auditoría.

Pre-condiciones

- El paciente debe estar registrado en INUS y sus documentos deben estar disponibles en RNDC y nodos periféricos.
- La aplicación móvil debe estar autenticada y autorizada para solicitar el resumen digital.
- El Portal Central, INUS, RNDC y nodos periféricos deben estar operativos.

Flujo de Eventos

1. La aplicación móvil solicita el resumen digital del paciente al Portal Central utilizando IPS-FHIR.
2. El Portal Central obtiene los datos básicos del paciente desde INUS.
3. INUS devuelve los datos del paciente al Portal Central.
4. El Portal Central solicita a RNDC los metadatos de documentos recientes del paciente.
5. RNDC devuelve la lista de metadatos al Portal Central.
6. Por cada documento relevante:
   a) El Portal Central solicita el contenido del documento al nodo periférico correspondiente.
   b) El nodo periférico devuelve el contenido del documento.
7. El Portal Central genera el resumen digital del paciente siguiendo el estándar IPS-FHIR.
8. El Portal Central entrega el resumen digital estructurado a la aplicación móvil.
9. El Portal Central registra la consulta del resumen en el sistema de Auditoría.

Post-condiciones

- El paciente dispone de un resumen digital estructurado accesible desde la aplicación móvil.
- Toda la operación de consulta queda registrada en el sistema de Auditoría.
- Se garantiza la integridad y consistencia de los datos mostrados en el resumen digital.

4. Vista de Restricciones

La Vista de Restricciones describe limitaciones que deben respetarse tanto en el proceso de desarrollo como en el producto final [**Perovich2003**]. Estas restricciones pueden ser de naturaleza técnica o no técnica, e imponen condiciones que el equipo de desarrollo debe considerar al diseñar e implementar la solución. El objetivo de esta vista es explicitar las limitaciones que afectan el proyecto *hcen.uy*, a fin de diseñar la mejor arquitectura posible dentro de los márgenes establecidos [**Cervantes2016**].

Tabla 2: Restricciones del sistema hcen.uy

Id	**Descripción**
R001	Los portales del sistema (Administrador HCEN, Usuarios de Salud, Administrador de Clínica y Profesionales de Salud) deben ser aplicaciones web accesibles mediante navegador.
R002	La autenticación de usuarios debe realizarse mediante *Usuario gub.uy* para los roles que acceden al componente central (Administrador HCEN y Usuario de Salud).
R003	El componente central debe desplegarse en *Elastic Cloud* de ANTEL, utilizando los códigos promocionales provistos por el curso.
R004	Los componentes periféricos deben ejecutarse en una solución *PaaS* o *IaaS* gratuita (por ejemplo, Railway, Render o Heroku).
R005	La comunicación entre el componente central y la Plataforma de Interoperabilidad (PDI) debe realizarse mediante *Web Services SOAP*.
R006	La comunicación entre el componente móvil y el componente central debe realizarse mediante servicios *REST*, utilizando *JSON* como formato de intercambio.
R007	Todas las comunicaciones entre componentes (central, periféricos, móviles y PDI) deben realizarse sobre *HTTPS*, garantizando la seguridad de los datos en tránsito.
R008	Las contraseñas de usuarios deben almacenarse utilizando funciones *hash* con *salt*, siguiendo buenas prácticas de seguridad.
R009	La plataforma debe cumplir con la Ley N° 18.331 de Protección de Datos Personales y las normativas vigentes de AGESIC sobre seguridad de la información.
R010	El sistema debe implementar la integración con los componentes INUS y RNDC, respetando los lineamientos del modelo de referencia de los Servicios HCEN publicados por AGESIC.
R011	El diseño del sistema debe permitir escalabilidad horizontal, evitando el almacenamiento de estado en los servidores web o de aplicación.
R012	Los tiempos de entrega del proyecto son no negociables y están definidos por el cronograma oficial del laboratorio.
R013	El componente periférico debe soportar el modelo *multi-tenant*, permitiendo la personalización visual por clínica (logos, colores, etc.).
R014	El sistema debe utilizar el estándar *IPS-FHIR* para representar el resumen digital del paciente.
R015	Los servicios deben ofrecer interfaces públicas bien definidas que permitan la integración bidireccional entre nodos periféricos y el componente central.
R016	El sistema debe contar con pruebas automatizadas que cubran al menos el 80 % de la lógica del sistema.
R017	La solución debe desarrollarse utilizando software de código abierto o con licencias gratuitas, conforme a las políticas del curso.

5. Vista de Atributos de Calidad

La Vista de Atributos de Calidad se centra en los requerimientos de atributos de calidad de la plataforma.

Los atributos de calidad identificados para la plataforma hcen.uy abordan aspectos críticos del sistema que garantizan su correcto funcionamiento en el contexto del Sistema Nacional Integrado de Salud. Estos atributos se organizan en las siguientes categorías:

Seguridad: Dada la naturaleza sensible de los datos de salud, se establecen requisitos estrictos para el almacenamiento seguro de credenciales, la protección de las comunicaciones mediante protocolos cifrados, y el control de acceso basado en políticas definidas por los usuarios.

Escalabilidad: Para soportar el crecimiento del sistema y la incorporación de nuevos prestadores de salud, se requiere que la arquitectura permita escalar horizontalmente sin mantener estado local en los servidores de aplicación.

Performance: El sistema debe mantener tiempos de respuesta aceptables incluso durante períodos de uso intensivo, identificando y documentando los límites operacionales de la plataforma.

Interoperabilidad: Como sistema integrador del ecosistema de salud, se definen interfaces y protocolos estándar (SOAP, REST) para la comunicación entre todos los componentes, permitiendo la interacción fluida entre el componente central, los nodos periféricos, y sistemas externos como la PDI y Usuario gub.uy.

Testabilidad: Para garantizar la calidad del software y facilitar su mantenimiento, se establece un objetivo de cobertura de pruebas automatizadas que asegure la correcta funcionalidad de la lógica de negocio y los servicios expuestos.

Disponibilidad: Se especifican las plataformas de despliegue (Elastic Cloud de ANTEL para el componente central, y soluciones PaaS/IaaS para componentes periféricos) que garantizan la disponibilidad continua del sistema.

Usabilidad: La integración con Usuario gub.uy simplifica la autenticación, mientras que la personalización del look & feel permite a cada clínica adaptar la interfaz a su identidad institucional.

Multi-tenancy: El componente periférico debe soportar múltiples clínicas de forma aislada, optimizando recursos mientras mantiene la segregación de datos entre organizaciones.

Privacidad: Los usuarios de salud mantienen control sobre su información clínica mediante la configuración de políticas de acceso y la auditoría de consultas a su historia clínica.

Notificaciones: El componente móvil mantiene informados a los usuarios sobre eventos relevantes relacionados con el acceso a su información de salud.

Tabla 3: Atributos de Calidad

Id	Tipo	Descripción
AC001	Seguridad	Las contraseñas de los usuarios deben ser almacenadas utilizando funciones hash con salt.
AC002	Seguridad	La comunicación entre el componente central y los componentes periféricos debe realizarse utilizando HTTPS.
AC003	Seguridad	La comunicación entre el componente central y la PDI debe realizarse utilizando HTTPS.
AC004	Seguridad	La comunicación entre el componente móvil y el componente central debe realizarse utilizando HTTPS.
AC005	Seguridad	El acceso a documentos clínicos debe respetar las políticas de acceso definidas por los usuarios de salud.
AC006	Escalabilidad	El sistema debe ser escalable horizontalmente a nivel de servidor Web y servidor de aplicaciones.
AC007	Escalabilidad	Los servidores Web y de aplicación no deben mantener estado de sesión de forma local para facilitar la escalabilidad horizontal.
AC008	Performance	Los tiempos de respuesta del sistema no deben degradarse durante situaciones de uso pico.
AC009	Performance	El sistema debe soportar el uso concurrente de múltiples usuarios sin degradación significativa del tiempo de respuesta.
AC010	Performance	Se debe identificar y documentar el punto de quiebre del sistema mediante pruebas de carga.
AC011	Interoperabilidad	La comunicación entre el componente central y la PDI debe realizarse mediante Web Services SOAP.
AC012	Interoperabilidad	La comunicación entre el componente móvil y el componente central debe realizarse mediante Web Services REST.
AC013	Interoperabilidad	El componente central debe exponer una interfaz bien definida para que los nodos periféricos puedan registrar usuarios en el INUS.
AC014	Interoperabilidad	El componente central debe exponer una interfaz bien definida para que los nodos periféricos puedan registrar documentos clínicos en el RNDC.
AC015	Interoperabilidad	Los componentes periféricos deben exponer una interfaz bien definida para permitir al componente central recuperar documentos clínicos.
AC016	Interoperabilidad	El componente periférico debe exponer una interfaz para recibir información de alta de clínicas desde el componente central.
AC017	Testabilidad	Al menos el 80 % de la lógica del sistema debe estar cubierta por pruebas automatizadas.
AC018	Testabilidad	Cada servicio del sistema debe contar con al menos una prueba automatizada.
AC019	Disponibilidad	El componente central debe estar desplegado en Elastic Cloud de ANTEL.
AC020	Disponibilidad	Los componentes periféricos deben estar desplegados en soluciones PaaS o IaaS con cuentas gratuitas.

Tabla 4: Atributos de Calidad

Id	Tipo	Descripción
AC021	Usabilidad	Los usuarios de salud deben poder autenticarse mediante Usuario gub.uy.
AC022	Usabilidad	Los administradores HCEN deben poder autenticarse mediante Usuario gub.uy.
AC023	Usabilidad	Las clínicas deben poder personalizar el look & feel y logos de sus portales.
AC024	Multi-tenancy	El componente periférico debe soportar múltiples clínicas operando de forma aislada en la misma instancia.
AC025	Multi-tenancy	Cada clínica debe tener acceso exclusivo a sus propios datos de usuarios y profesionales de salud.
AC026	Privacidad	Los usuarios de salud deben poder visualizar quién accedió a su historia clínica y cuándo.
AC027	Privacidad	Los usuarios de salud deben poder configurar políticas de acceso sobre su historia clínica.
AC028	Notificaciones	Los usuarios de salud deben poder configurar qué notificaciones recibir en el componente móvil.
AC029	Notificaciones	El componente móvil debe recibir notificaciones de nuevos pedidos de acceso y nuevos accesos a historia clínica.

6. Vista Lógica

La Vista Lógica describe la arquitectura lógica de la plataforma hcen.uy, presentando la organización conceptual del sistema mediante múltiples niveles de refinamiento. Esta vista permite comprender los principales componentes lógicos del sistema, sus responsabilidades, dependencias e interacciones, proporcionando una visión estructurada que da soporte a los requerimientos funcionales identificados. Se utiliza un enfoque top-down, comenzando con una descomposición de alto nivel del sistema en sus tres componentes principales (Componente Central, Componente Móvil y Componente Periférico), para luego profundizar en subsistemas que presentan mayor complejidad arquitectónica o que son críticos para el cumplimiento de los atributos de calidad del sistema. En particular, se detallan tres refinamientos clave: la arquitectura en capas del Componente Central, que separa las responsabilidades de presentación, lógica de negocio, integración y persistencia; la arquitectura multi-tenant del Componente Periférico, que permite el aislamiento entre clínicas; y la Capa de Integración con Sistemas Externos, que encapsula la comunicación con gub.uy, PDI y servicios de notificaciones.

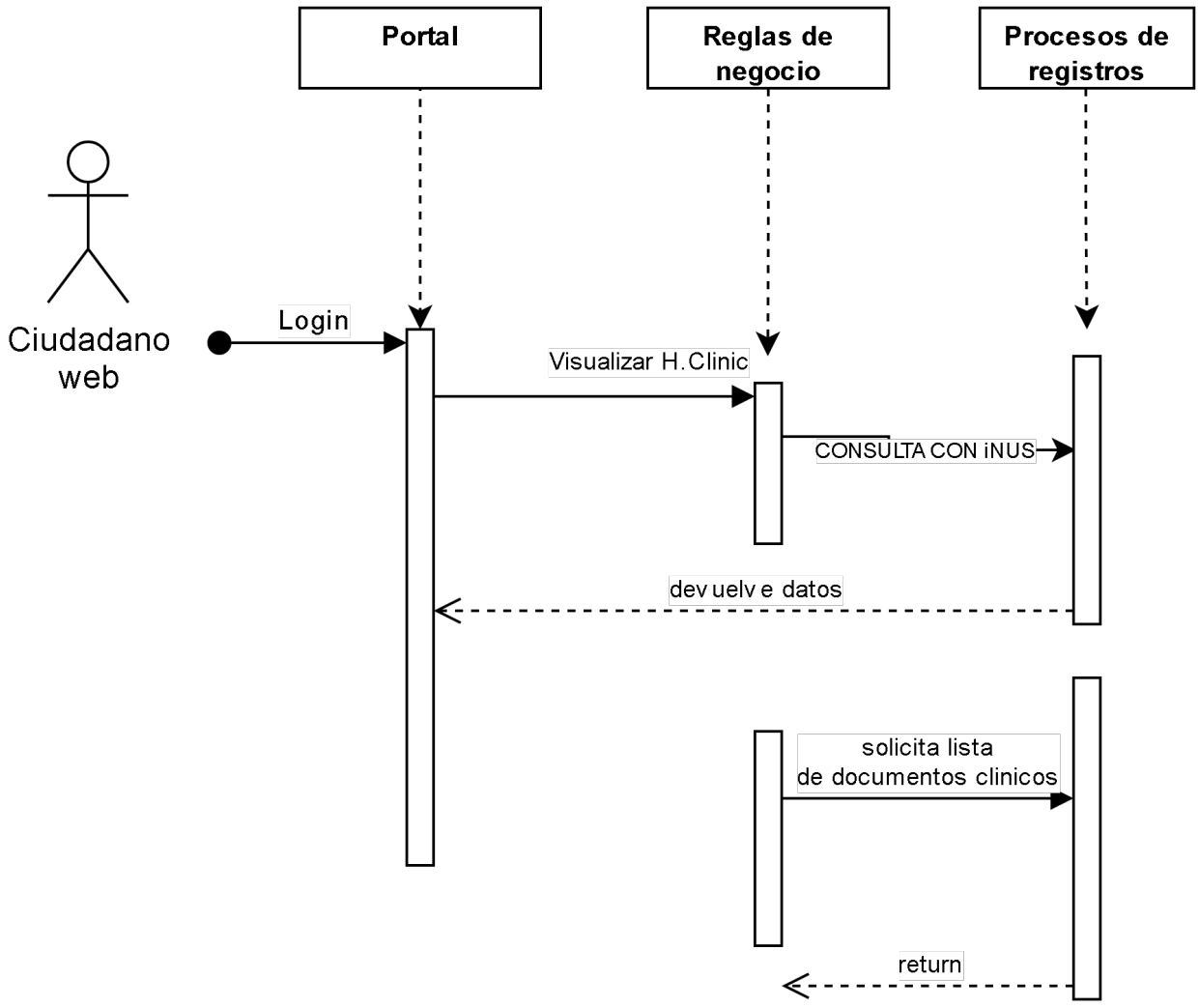


Figura 3: Enter Caption

6.1. Arquitectura General del Sistema

Vista de alto nivel de la arquitectura lógica del sistema.

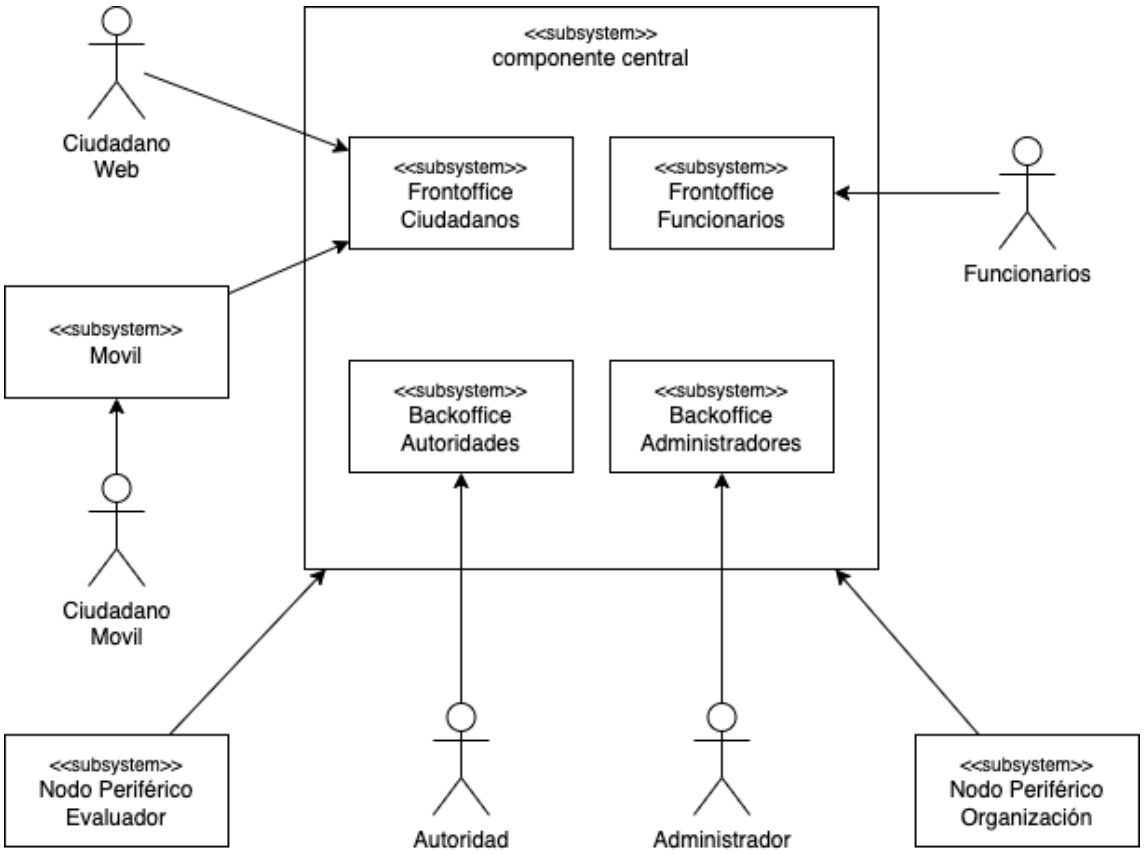


Figura 4: Vista Lógica

6.2. Refinamiento Componente Central - Arquitectura en Capas

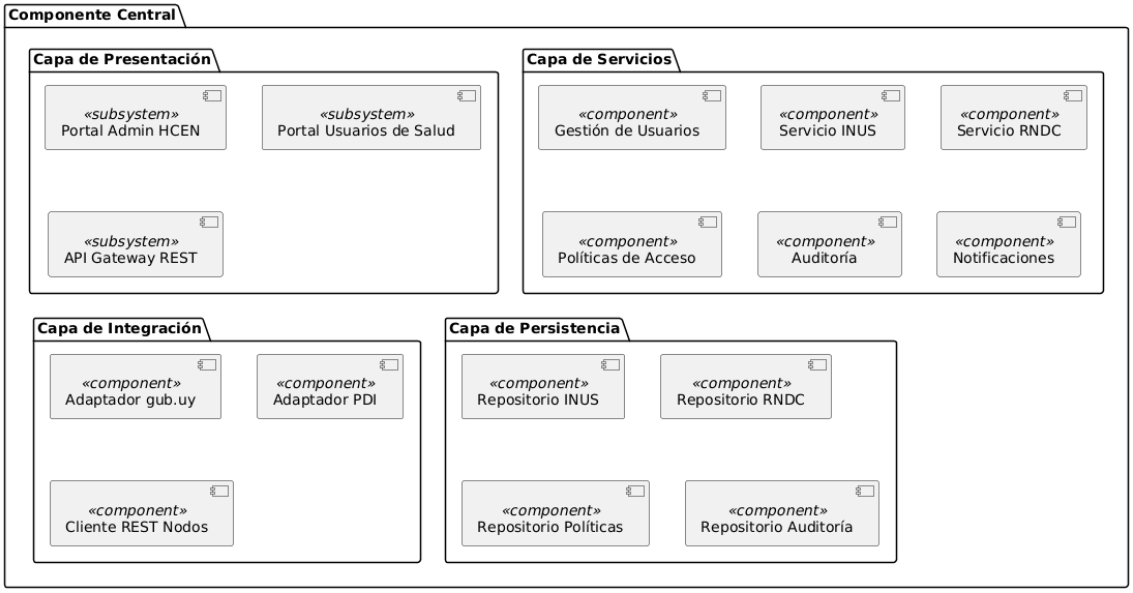


Figura 5: Vista Lógica Refinamiento Componente Central - Arquitectura en Capas

6.3. Refinamiento Componente Periférico Multi-tenant

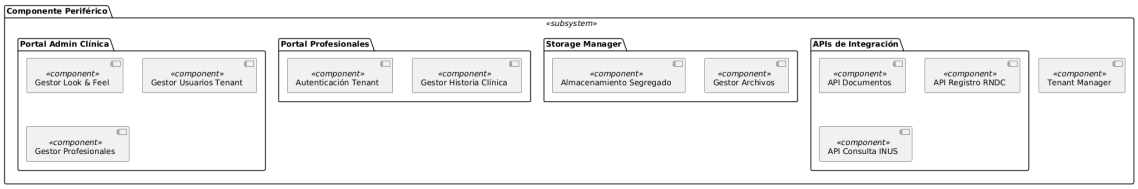


Figura 6: Vista Lógica Refinamiento Componente Periférico Multi-tenant

6.4. Refinamiento Capa de Integración con Sistemas Externos

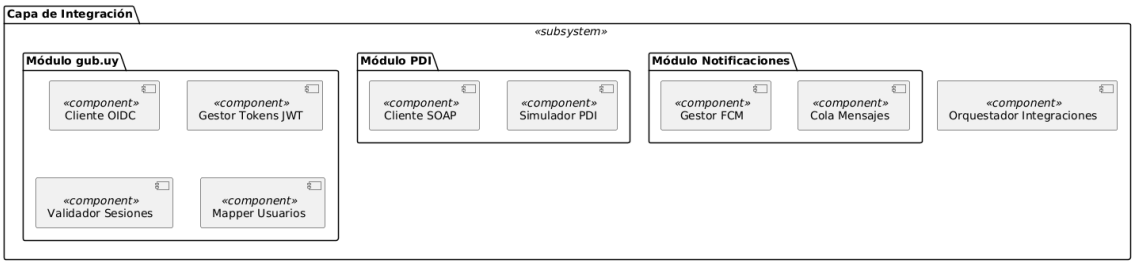


Figura 7: Vista Lógica Refinamiento Capa de Integración con Sistemas Externos

6.5. Diagramas de Interacción

En esta sección se presentan los Diagramas de Secuencia UML a nivel de componentes, correspondientes a los casos de uso críticos identificados para el sistema *hcen.uy*. Estos diagramas ilustran el flujo de mensajes y las interacciones entre los distintos componentes del sistema, tanto internos como externos, permitiendo comprender la dinámica del comportamiento distribuido.

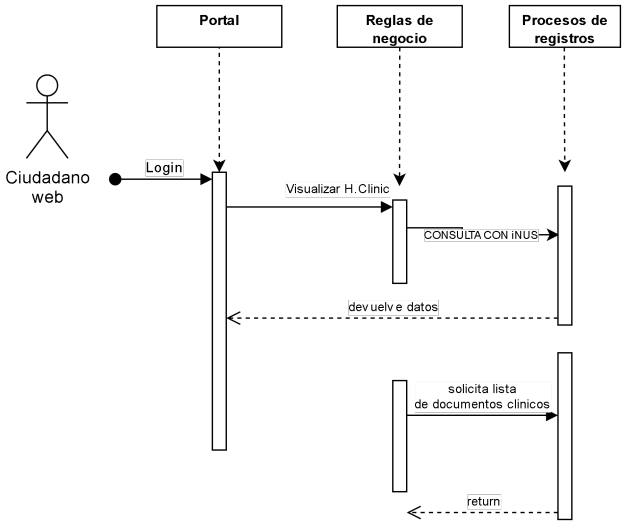


Figura 8: Enter Caption

6.6. CU01 – Autenticación de usuario ciudadano

Este caso de uso describe el proceso mediante el cual un ciudadano se autentica en el sistema utilizando su identidad digital a través del servicio PDI. El flujo involucra a la aplicación móvil,

el componente central y el servicio externo de autenticación. La comunicación con el PDI se realiza mediante servicios *SOAP*, mientras que entre el móvil y el central se utilizan servicios *REST*. Este caso es crítico por su relevancia en la seguridad y el acceso al sistema.

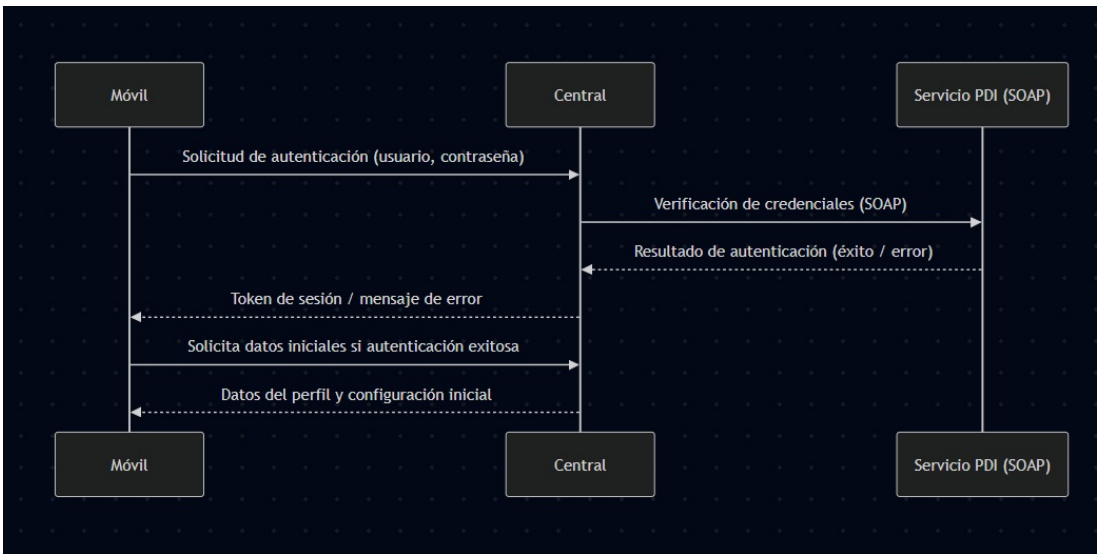


Figura 9: Diagrama de secuencia – CU01 Autenticación de usuario ciudadano

6.7. CU02 – Registro de atención médica / consulta

Este caso representa la creación de un nuevo registro de atención médica desde la aplicación móvil. El flujo incluye la comunicación del componente móvil con el central, y de este con los servicios externos RNDC e INUS, encargados del almacenamiento y actualización de información clínica. Es un caso crítico por la necesidad de mantener la integridad, consistencia y trazabilidad de los datos clínicos.

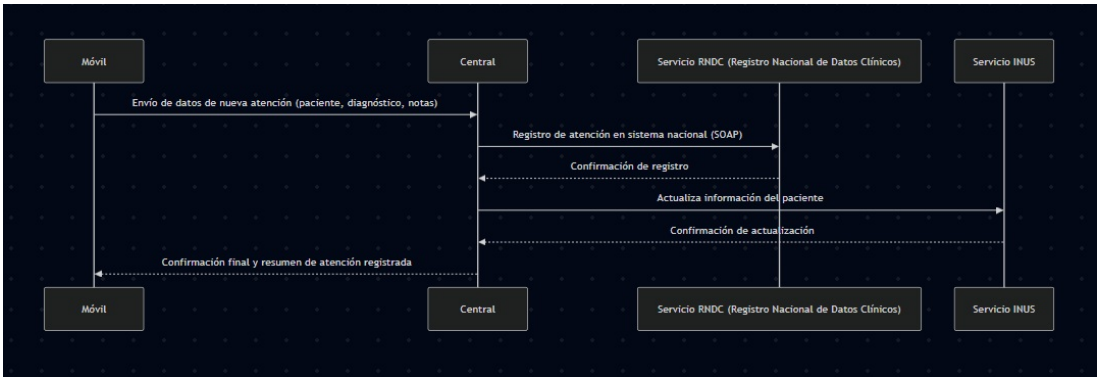


Figura 10: Diagrama de secuencia – CU02 Registro de atención médica / consulta

6.8. CU03 – Sincronización de datos entre aplicación móvil y sistema central

Este caso describe el proceso de sincronización de datos entre la aplicación móvil y el componente central del sistema. La interacción asegura que los datos locales del dispositivo se mantengan coherentes con los del servidor central, incluso cuando la aplicación opera parcialmente en modo offline. Es crítico por su impacto en la disponibilidad y consistencia del sistema distribuido.

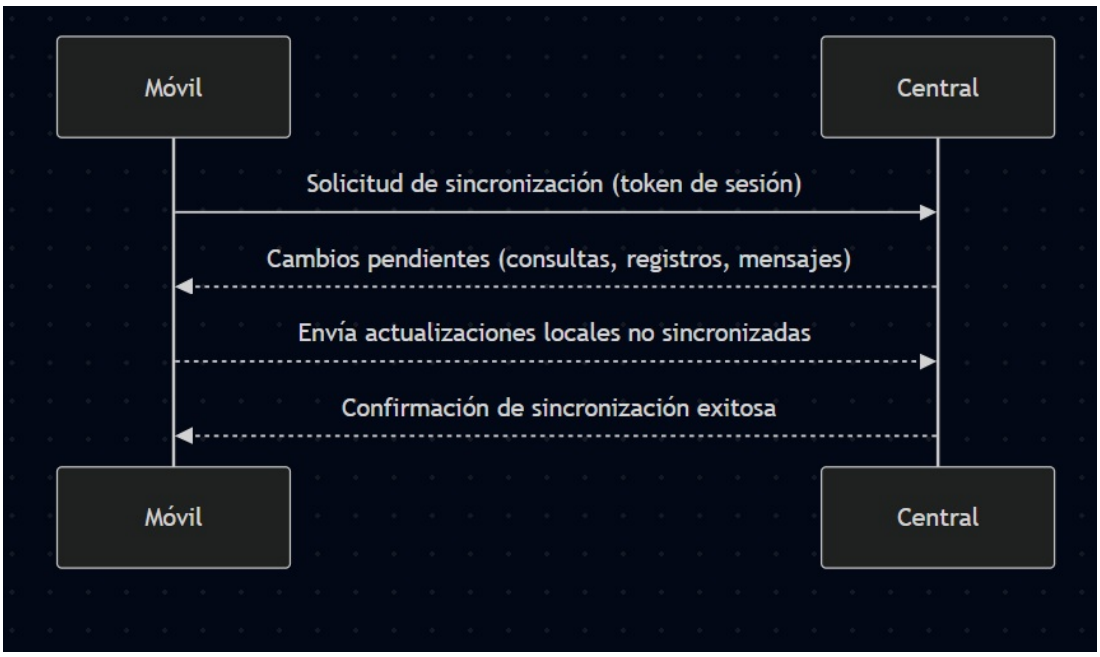


Figura 11: Diagrama de secuencia – CU03 Sincronización de datos entre aplicación móvil y sistema central

6.9. CU04 – Consulta de historial clínico

Este caso permite a un usuario (paciente o profesional) consultar el historial clínico almacenado en el sistema. El flujo de interacción incluye la solicitud desde el componente móvil, la intermediación del componente central y la consulta al servicio INUS, que devuelve la información consolidada. Es un caso crítico por su relación con la confidencialidad y la protección de los datos personales.

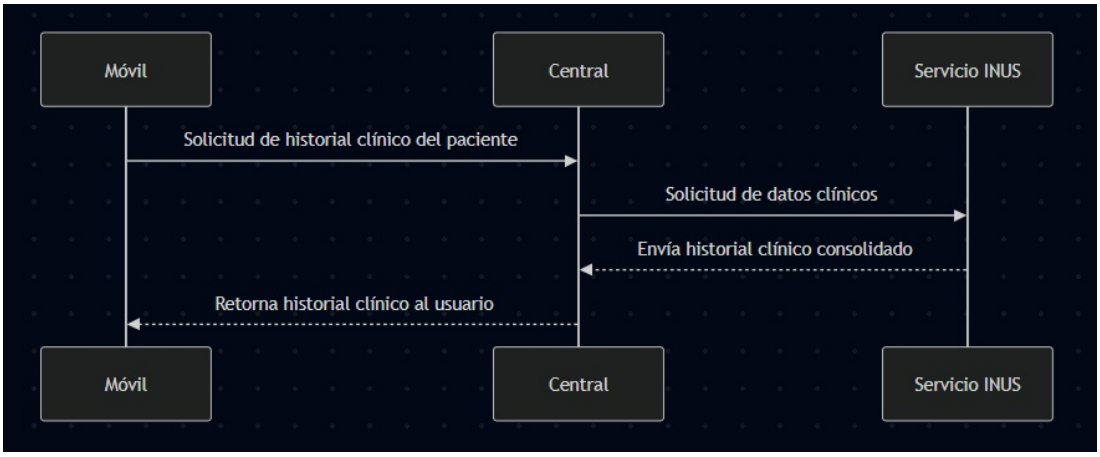


Figura 12: Diagrama de secuencia – CU04 Consulta de historial clínico

6.10. CU05 – Notificación de eventos relevantes al usuario

Este caso representa el envío de notificaciones desde el componente central hacia los usuarios, informando sobre eventos relevantes como turnos, resultados o recordatorios. La comunicación puede realizarse mediante notificaciones *push* o consultas periódicas (*polling*). Es un caso crítico por su importancia en la experiencia del usuario y la confiabilidad del sistema de comunicación.

Figura 13: Diagrama de secuencia – CU05 Notificación de eventos relevantes al usuario

7. Vista de Distribución

La plataforma hcen.uy se distribuye en múltiples nodos físicos y lógicos para garantizar escalabilidad, disponibilidad y seguridad. La arquitectura contempla tres escenarios principales de distribución que reflejan la separación entre el componente central, los componentes periféricos y las integraciones con sistemas externos.

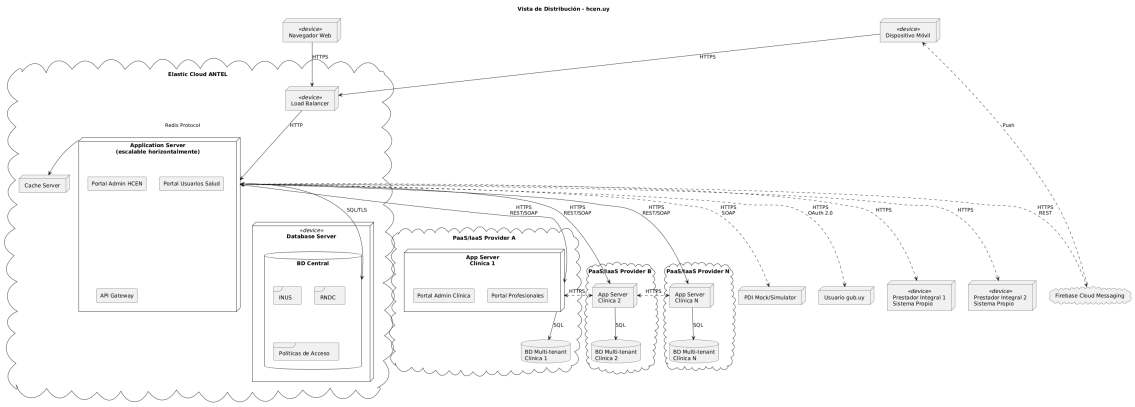


Figura 14: Vista Distribución - Escenario General

7.1. Escenario 1: Despliegue del Componente Central

Este escenario describe la distribución del componente central de hcen.uy en la infraestructura de Elastic Cloud de ANTEL. La arquitectura sigue un modelo de múltiples capas que separa la presentación, la lógica de negocio y la persistencia de datos.

Justificación basada en Requerimientos No Funcionales

Escalabilidad (AC006, AC007): El componente central se despliega en múltiples instancias de servidores de aplicación sin estado local, permitiendo escalado horizontal mediante balanceadores de carga. Esta arquitectura permite agregar o quitar instancias dinámicamente según la demanda del sistema.

Disponibilidad (AC019): El uso de Elastic Cloud de ANTEL proporciona alta disponibilidad mediante redundancia de servidores y mecanismos de failover automáticos, garantizando la continuidad del servicio incluso ante fallos de hardware.

Seguridad (AC002, AC003, AC004): Todas las comunicaciones entrantes y salientes utilizan HTTPS. El componente central actúa como punto único de integración, aplicando políticas de seguridad centralizadas para las interacciones con nodos periféricos, componentes móviles y la PDI.

Performance (AC008, AC009): La separación en capas y el uso de caché distribuido permiten optimizar los tiempos de respuesta. El balanceador de carga distribuye las peticiones entre múltiples instancias del servidor de aplicaciones.

Descripción de Nodos

Balanceador de Carga «device»:

- Función: Distribuir peticiones HTTP/HTTPS entre instancias del servidor de aplicaciones
- Protocolo: HTTPS (puerto 443)
- Características: Health checks, session affinity basada en cookies

Servidor de Aplicaciones (múltiples instancias):

- Software: Servidor de aplicaciones JEE (WildFly)
- Componentes desplegados: Portal Admin HCEN, Portal Usuarios de Salud, APIs REST y SOAP
- Requisitos mínimos: 2 vCPU, 4GB RAM
- Sistema Operativo: Linux (Ubuntu/CentOS)
- Características: Sin estado local de sesión para facilitar escalabilidad

Servidor de Base de Datos «device»:

- Software: Sistema de gestión de base de datos relacional (ej. PostgreSQL, MySQL)
- Almacena: INUS, RNDC, políticas de acceso, auditoría
- Características: Backups automáticos, replicación para alta disponibilidad

Servidor de Caché:

- Software: Redis o Memcached
- Función: Caché distribuido para sesiones y datos frecuentemente accedidos

Conexiones

- **Cliente Web ↔ Balanceador:** HTTPS, ancho de banda variable según usuarios concurrentes
- **Balanceador ↔ Servidores App:** HTTP interno, red privada de alta velocidad
- **Servidores App ↔ Base de Datos:** Protocolo nativo DB (ej. PostgreSQL protocol), conexión persistente, red privada
- **Servidores App ↔ Caché:** Utilizando Redis, red privada de baja latencia

7.2. Escenario 2: Despliegue de Componentes Periféricos

Este escenario describe la distribución de los componentes periféricos que alojan las aplicaciones de las clínicas en un modelo multi-tenant. Estos componentes se despliegan en plataformas PaaS o IaaS externas con cuentas gratuitas.

Justificación basada en Requerimientos No Funcionales

Multi-tenancy (AC024, AC025): La arquitectura del componente periférico permite que múltiples clínicas operen sobre la misma infraestructura manteniendo aislamiento logico completo de datos. Cada clínica tiene su propio espacio lógico con acceso exclusivo a sus usuarios y profesionales.

Escalabilidad (AC006, AC007): Similar al componente central, los servidores de aplicación no mantienen estado local, permitiendo escalar horizontalmente agregando instancias según la cantidad de clínicas y el volumen de uso.

Disponibilidad (AC020): El despliegue en plataformas PaaS/IaaS con tier gratuito (ej. Heroku, Railway, Render) proporciona un nivel básico de disponibilidad adecuado para el contexto del laboratorio, con posibilidad de migrar a tiers pagos para producción.

Seguridad (AC002): Las comunicaciones con el componente central y con los nodos periféricos externos utilizan HTTPS. El aislamiento multi-tenant en la base de datos previene acceso cruzado entre clínicas.

Usabilidad (AC023): Cada clínica puede personalizar su interfaz (look & feel, logos) almacenando configuraciones específicas en la base de datos multi-tenant.

Descripción de Nodos

Servidor de Aplicaciones PaaS:

- Plataforma: Heroku, Railway, Render u otra con tier gratuito
- Componentes: Portal Admin Clínica, Portal Profesionales de Salud, APIs de integración
- Configuración: Auto-escalado según disponibilidad del PaaS
- Runtime: Node.js, Java, Python según tecnología elegida

Base de Datos Multi-tenant:

- Software: PostgreSQL
- Modelo: Schema por tenant o discriminador de tenant en tablas
- Almacena: Usuarios de salud, profesionales, documentos clínicos, configuraciones por clínica
- Respaldos: Según capacidades del proveedor PaaS

Almacenamiento de Documentos:

- Servicio: Object storage (ej. AWS S3, Azure Storage Account) o local filesystem según disponibilidad
- Contenido: Documentos clínicos (PDFs, imágenes, etc.)
- Organización: Por tenant y por usuario de salud

Conexiones

- **Navegadores ↔ Servidor App PaaS:** HTTPS
- **Servidor App ↔ Componente Central:** HTTPS, REST/SOAP según operación (registro INUS/RNDC, recepción de alta de clínica)
- **Servidor App ↔ Base de Datos:** Conexión cifrada, protocolo nativo
- **Servidor App ↔ Almacenamiento:** HTTPS (para object storage) o local

7.3. Escenario 3: Integración con Sistemas Externos y Componente Móvil

Este escenario muestra la distribución e integración del componente central con sistemas externos (PDI, Usuario gub.uy) y el componente móvil.

Justificación basada en Requerimientos No Funcionales

Interoperabilidad (AC011, AC012, AC013-AC016): Se utilizan protocolos estándar para garantizar la comunicación entre sistemas heterogéneos. SOAP para la PDI (según especificación gubernamental), REST para el componente móvil (más adecuado para aplicaciones móviles), e interfaces bien definidas para nodos periféricos.

Seguridad (AC002, AC004, AC021, AC022): Todas las comunicaciones externas utilizan HTTPS. La autenticación mediante Usuario gub.uy delega la gestión de identidades a una plataforma gubernamental confiable, reduciendo riesgos de seguridad.

Notificaciones (AC028, AC029): La arquitectura permite enviar notificaciones push al componente móvil sobre eventos relevantes (nuevos accesos, pedidos de acceso) utilizando servicios de notificaciones (Firebase, APNs, SignalR, WebSockets).

Privacidad (AC026, AC027): La integración con la PDI se realiza bajo estrictas políticas de privacidad, solicitando únicamente datos necesarios (fecha de nacimiento) y respetando las políticas de acceso configuradas por usuarios.

Descripción de Nodos

Componente Móvil «device»:

- Plataforma: Android
- Tecnología: Flutter
- Funciones: Autenticación, visualización de resumen del paciente, gestión de notificaciones
- Conectividad: Requiere conexión a Internet (WiFi/datos móviles)

Servicio de Notificaciones:

- Plataforma: Firebase Cloud Messaging (FCM) o similar (a definir)
- Función: Gestión y envío de notificaciones push
- Integración: API REST desde componente central

PDI Mock/Simulador:

- Función: Simular servicios de la Plataforma de Interoperabilidad
- Interfaz: SOAP (Servicio Básico de Información de DNIC)
- Despliegue: Puede estar en el mismo servidor que el componente central o separado (a definir)
- Datos: Retorna información simulada de usuarios (fecha de nacimiento)

Usuario gub.uy (Sistema Externo):

- Función: Autenticación de usuarios mediante OAuth 2.0 / OpenID Connect
- Protocolo: HTTPS, REST
- Nota: Sistema real del gobierno

Conexiones

- **App Móvil ↔ Componente Central:** HTTPS, REST API, autenticación mediante tokens
- **Componente Central ↔ PDI Mock:** HTTPS, SOAP, WS-Security
- **Componente Central ↔ Usuario gub.uy:** HTTPS, OAuth 2.0/OpenID Connect
- **Componente Central ↔ Servicio Notificaciones:** HTTPS, REST API
- **Servicio Notificaciones ↔ App Móvil:** Push notification protocols (FCM)

7.4. Consideraciones de Despliegue

Estrategia de Despliegue

Se utilizará una estrategia de despliegue continuo utilizando pipelines CI/CD (GitLab CI) que automaticen:

- Ejecución de pruebas automatizadas (AC017, AC018)
- Build de artefactos desplegables
- Depliegue utilizando contenedores
- Despliegue en ambientes de desarrollo, staging y producción
- Rollback automático en caso de fallos

Monitoreo y Observabilidad

Para cumplir con los requerimientos de performance (AC008, AC009, AC010) es necesario implementar:

- Monitoreo de métricas del sistema (CPU, memoria, tiempos de respuesta)
- Logging centralizado para análisis de errores
- Alertas automáticas ante degradación del servicio
- Dashboards para visualización de métricas en tiempo real

8. Vista de Implementación

La Vista de Implementación describe cómo los componentes lógicos definidos en la arquitectura se materializan en artefactos concretos de software en tiempo de ejecución. Esta vista establece el puente entre el diseño conceptual y la realidad física del sistema, especificando los elementos ejecutables, bibliotecas, frameworks y archivos de configuración que conforman la plataforma hcen.uy. El objetivo principal de esta vista es identificar las dependencias entre los artefactos implementados, facilitar la comprensión de la estructura de deployment y proporcionar una guía para el proceso de construcción y empaquetado del sistema. Se detallan los componentes ejecutables para cada uno de los tres componentes principales del sistema: el Componente Central, el Componente Móvil y los Componentes Periféricos. Para el Componente Central, se especifican los archivos WAR que encapsulan los subsistemas de Frontoffice y Backoffice, el simulador de PDI para entornos de desarrollo, y las bases de datos necesarias. Para el Componente Móvil, se identifica el paquete de aplicación (APK/IPA) que se distribuye a los dispositivos. Para los Componentes Periféricos, se detallan los artefactos WAR correspondientes a los portales de administración y profesionales de salud, junto con sus sistemas de almacenamiento y bases de datos multi-tenant. Esta vista utiliza el Diagrama de Deployment UML para representar tanto los artefactos de software como su distribución en los nodos de infraestructura, mostrando cómo los componentes implementados se despliegan en los diferentes ambientes (cloud, PaaS/IaaS, dispositivos móviles).

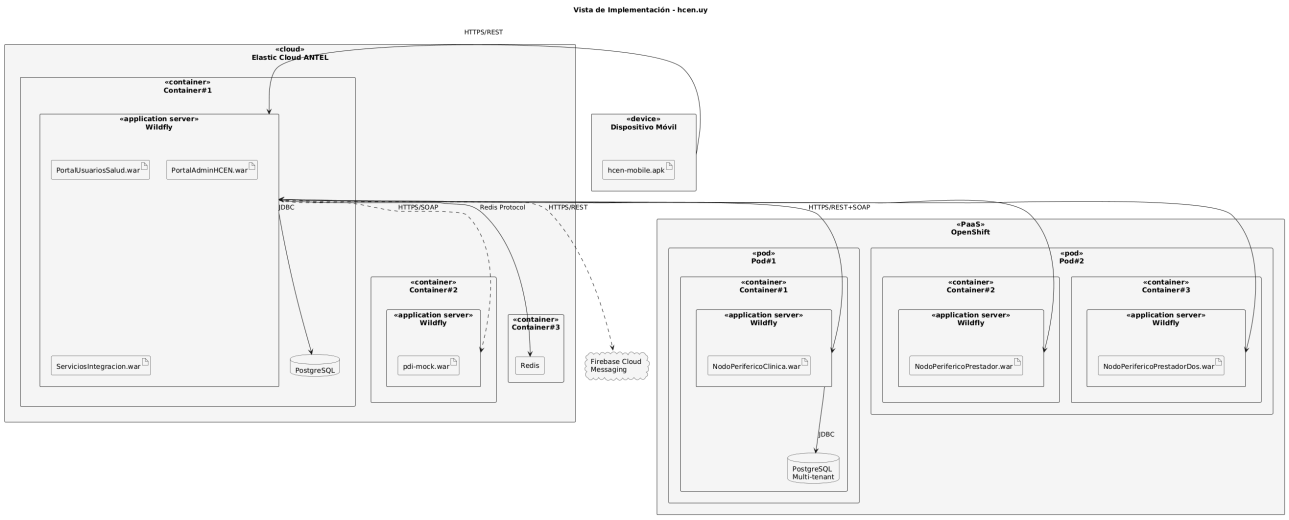


Figura 15: Diagrama de vista de implementaciones

9. Vista de Decisiones de Arquitectura

La Vista de Decisiones de Arquitectura presenta y describe las principales decisiones de arquitectura tomadas.

Tabla 5: Decisión de Arquitectura 1

Identificador	DA-01.
Nombre	Elección de la arquitectura del sistema apk.
Categorías	Componente: interfaz de usuario. Atributo de calidad: mantenibilidad. Restricción: el desarrollo debe realizarse con tecnologías open source y un único código base para Android e iOS.
Problema	Se necesita definir una arquitectura base para la aplicacón movil(Apk) que permita desarrollar e implementar en android a partir de una base de codigo.
Alternativas	*(React Native o Flutter).
Decisión	Se adopta React Native como framework de desarrollo multiplataforma, utilizando una arquitectura basada en componentes funcionales y patrón Flux/Redux para la gestión de estado. Se usará Axios para la comunicación con el backend mediante API REST y Firebase Cloud Messaging (FCM) para el manejo de notificaciones PUSH.
Justificación	- Permite compartir la mayor parte del código entre Android e iOS, reduciendo costes y tiempo de desarrollo. - Basado en JavaScript y React, tecnologías ampliamente conocidas por el equipo. - Facilita la integración con librerías nativas y servicios externos. - Soporta una arquitectura modular, escalable y fácil de probar. - Buen equilibrio entre rendimiento y productividad.
Decisiones Relacionadas	DA-02: Selección del motor de base de datos para notificaciones PUSH.

Tabla 6: Decisión de Arquitectura 2

Identificador	DA-002
Nombre	Selección del motor de base de datos para la gestión de notificaciones PUSH.
Categorías	Componente de persistencia de datos, mensajería y comunicación en tiempo real, atributo de calidad (rendimiento, escalabilidad y disponibilidad), restricción: la solución debe operar completamente en la nube, integrarse con React Native y minimizar la gestión de infraestructura.
Problema	Se requiere definir el motor de base de datos y los servicios asociados para soportar el sistema de notificaciones PUSH. El sistema debe manejar eventos en tiempo real, sincronizar el estado de las notificaciones entre dispositivos y usuarios, y permitir la integración directa con la aplicación móvil desarrollada en React Native
Alternativas	Firebase (Firestore + Cloud Messaging + Cloud Functions).
Decisión	Se adopta Firebase como plataforma integral para el almacenamiento y gestión de notificaciones, utilizando los siguientes servicios: - Cloud Firestore como base de datos NoSQL principal, con sincronización en tiempo real. - Firebase Cloud Messaging (FCM) para el envío y recepción de notificaciones PUSH. - Cloud Functions para ejecutar lógica backend sin necesidad de servidor (serverless).
Justificación	- Firebase ofrece integración nativa con React Native, reduciendo la complejidad de configuración y el tiempo de desarrollo. - Cloud Firestore proporciona sincronización en tiempo real entre dispositivos y almacenamiento flexible orientado a documentos. - FCM facilita el envío de notificaciones segmentadas o personalizadas a usuarios o grupos. - Arquitectura serverless, sin necesidad de administrar infraestructura. - Alta escalabilidad automática y disponibilidad garantizada por Google Cloud. - Simplifica la gestión de autenticación, métricas y analíticas (Firebase Authentication y Analytics). - Ideal para aplicaciones móviles que requieren baja latencia y sincronización instantánea.
Decisiones Relacionadas	DA-001: Elección de la arquitectura móvil con React Native.

Tabla 7: Decisión de Arquitectura 3

Identificador	DA-03
Nombre	Despliegue de la aplicación web en Elastic Cloud (ANTEL)
Categorías	Componente de infraestructura y despliegue, atributo de calidad (disponibilidad, rendimiento, seguridad, escalabilidad), restricción: el entorno de despliegue debe residir en infraestructura nacional (ANTEL) por políticas de soberanía de datos y cumplimiento normativo
Problema	Se requiere definir la infraestructura de despliegue para la aplicación web institucional hcen.uy, garantizando alta disponibilidad, bajo tiempo de respuesta y cumplimiento de las políticas de seguridad y privacidad de datos del sector público uruguayo. Además, se busca una solución que simplifique la gestión operativa y permita escalar según la demanda.
Alternativas	* Servicios cloud internacionales (AWS, Google Cloud, Azure). * Elastic Cloud de ANTEL (servicios cloud nacionales con soporte y cumplimiento local).
Decisión	Se elige Elastic Cloud de ANTEL como plataforma de despliegue para la aplicación hcen.uy, utilizando contenedores y balanceadores gestionados, almacenamiento persistente y red privada nacional. Se configurará un pipeline CI/CD que automatice el despliegue desde el repositorio Git hacia el entorno cloud.
Justificación	- Elastic Cloud de ANTEL garantiza infraestructura nacional, cumpliendo con normativas de protección de datos uruguayas. - Permite despliegues escalables basados en contenedores con administración simplificada. - Integración con servicios de red y DNS gestionados por ANTEL. - Menor latencia para usuarios locales. - Soporte técnico local y disponibilidad 24/7. - Compatibilidad con herramientas de automatización (GitLab CI/CD, Jenkins, GitHub Actions). - Costos predecibles en moneda local y sin dependencia de proveedores extranjeros
Decisiones Relacionadas	DA-001: Arquitectura del sistema móvil con React Native. DA-002: Selección de base de datos (Firebase). DA-004: Estrategia de seguridad y autenticación.