Arquitectura de referencia para una historia clínica electrónica nacional y/o regional

Recomendaciones técnicas

RED AMERICANA DE COOPERACIÓN SOBRE SALUD ELECTRÓNICA

BID

RACSEL
RED AMERICANA DE COOPERACIÓN SOBRE SALUD ELECTRÓNICA

Fundación Julio Ricaldoni
INGENIERIA EN EL URUGUAY

AUTORIDADES

COLOMBIA

Ministerio de Tecnologías de la Información y las Comunicaciones
Dr. David Luna Sánchez, Ministro de Tecnologías de la Información y Telecomunicaciones
Dra. Juanita Rodríguez Kattah, Viceministra de Economía Digital
Dra. Martha Liliana Amaya Parra, Directora de Transformación Digital
Dra. Elizabeth Blandón Bermúdez, Directora de Gobierno Digital
Ing. Iván Darío Castaño Pérez, Subdirector de Digitalización Sectorial
Ing. Rafael Londoño Carantón, Subdirector de Estándares y Arquitectura de TI

Ministerio de Salud y Protección Social
Dr. Alejandro Gaviria Uribe, Ministro de Salud y Protección Social
Ing. Dolly Esperanza Ovalle Carranza. Jefe Oficina de Tecnología de la Información y la Comunicación -TIC[AP1]

COSTA RICA

Dra. Karen Mayorga Quirós, Ministra de Salud
Dr. Fernando Llorca Castro, Presidente Ejecutivo de la Caja Costarricense de Seguro Social

CHILE

Dr. Emilio Santelices Cuevas, Ministro de Salud
Marco Antonio Navarrete Mehech, Jefe División de TIC

PERU

Dr. Abel Salinas Rivas, Ministro de Salud
Karim Jacqueline Pardo Ruiz, Directora General de la Oficina General de Tecnologías de la Información – Ministerio de Salud
Pedro Julio Best Bandenay, Director Ejecutivo de la Oficina de Innovación y Desarrollo Tecnológico - Ministerio de Salud

URUGUAY

Dr. Jorge Basso, Ministro de Salud Pública
Ing. José Clastornik, Director Ejecutivo de Agesic.
Ing. Pablo José Orefice, Director Programa Salud.uy

COMITÉ TECNICO REGIONAL

Alejandra Lozano Schälchli, Ministerio de Salud Chile
Mario Ruiz Cubillo, Caja Costarricense de Seguro Social
Juan José Castillo, Ministerio de Salud de Perú
Martha Cajaleón Alcántara, Ministerio de Salud de Perú
Carlos Mauricio Parra Trillos, Ministerio TIC de Colombia
Pablo Orefice, AGESIC Salud.uy Uruguay
Fernando Portilla, AGESIC Salud.uy Uruguay
María Alejandra Piermarini, Coordinadora Comité Tecnico Regional Racsel
Marcelo Morante, Fundación Julio Ricaldoni

EQUIPOS TECNICOS DE TRABAJO

COLOMBIA

José Ricardo Aponte, Ministerio de Tecnologías de la Información Telecomunicaciones
Carlos Mauricio Parra Trillos, Ministerio de Tecnologías de la Información Telecomunicaciones
Esteban Armando Gaviria, Ministerio de Tecnologías de la Información Telecomunicaciones

Alexander Alfonso Pérez, Ministerio de Tecnologías de la Información Telecomunicaciones
Jennifer Andrée Uribe Montoya, Ministerio de Tecnologías de la Información Telecomunicaciones
Jorge Iván Rodríguez Rojas, Asesor Estudios Sectoriales, Ministerio de Tecnologías de la Información Telecomunicaciones

COSTA RICA
Ana Lorena Solís, Caja Costarricense de Seguro Social
Anton Zamora Ilarionov, Ministerio de Salud
Eduardo Rodriguez, Caja Costarricense de Seguro Social
Jeffry Elizondo Saldaña - Caja Costarricense de Seguro Social
José Manuel Zamora Moreira, Caja Costarricense de Seguro Social
José Willy Cortés Carrera, Caja Costarricense de Seguro Social
Manuel Oporto Mejía, Caja Costarricense de Seguro Social
Manuel Rodriguez Arce, Director Unidad ejecutora EDUS, Caja Costarricense de Seguro Social
María del Rocío Saenz, Caja Costarricense de Seguro Social
Mario Ruiz Cubillo, Caja Costarricense de Seguro Social
Priscila Balmaceda Chaves, Caja Costarricense de Seguro Social
Roger Lopez, Caja Costarricense de Seguro Social
Susana Lopez Delgado, Caja Costarricense de Salud
Xinia Cordero Sobalbarro, Caja Costarricense de Seguro Social

CHILE
Msc. Lorena Donoso Abarca, Ministerio Salud Chile
Ing. Jorge Herrera Reyes, Ministerio Salud Chile
Periodista Gonzalo León Erices, Ministerio Salud Chile
Msc. Alejandra Lozano Schälchli Ministerio Salud Chile
Sra. Hsiao - lan Lung Hsie, Ministerio Salud Chile
Dr. Alejandro Mauro Lalanne, Clínica Alemana Santiago
Ing. Nabelka Muñoz Muñoz, Ministerio Salud Chile
Msc. Dr. Juan José Ortega Callejas, Ministerio Salud Chile
Ing. José Villa Catalán, Ministerio Salud Chile
Msc. Gabriela Villavicencio Cárdenas, Ministerio Salud Chile
Dr. Soledad Zapata Villaseñor, Ministerio Salud Chile

PERU
Juan José Castillo Cueva, Ministerio de Salud
Claudia Córdova Yamauchi, Ministerio de Salud
Alicia Cedamanos Medina, Ministerio de Salud
Martha Cajaleón Alcántara, Ministerio de Salud
José Luis Huamán Villar, Ministerio de Salud
Isabel Falla Zevallos, Ministerio de Salud
Rocío Huamán Ramos, Ministerio de Salud
Boris Fazio Luna, Ministerio de Salud
Karol Bulnes García, Ministerio de Salud
Roxana Hilachoque Chumbe, Ministerio de Salud

URUGUAY
Cecilia Muxi, Articulación institucional - AGESIC
Juan Bertón, Coordinador de monitoreo en el área Agenda Digital - AGESIC
Maria Jimena Hernández, Grupo Jurídico - AGESIC
Betania Arispe, Centro Nacional de Recursos - AGESIC
Walter Callero, Medico Programa Salud.uy - AGESIC
Paulo Sande, Coordinador Historia Clinica Electrónica Nacional - AGESIC
Mauricio Bouza, Arquitecto Historia Clínica Electrónica Nacional - AGESIC
Ignacio Friedman, Arquitecto Plataforma de interoperabilidad - AGESIC
Fernando Portilla, Especialista Estándares de interoperabilidad - AGESIC

EQUIPO CONSULTOR

IN2 – TIC SALUT

Arquitectura
Bernat López

Desafíos regionales para la implementación de salud electrónica
Felix Vilar

Estándares
David Rodríguez Cocinero
Eli Marín

Normativa
Vanesa Alarcón

Terminología
Ariadna Rius

Índice

Introducción ... 11

1. Modelo de Referencia ... 13
1.1. Compartición de datos transfronterizos ... 14
1.1.1. SHIN-NY ... 14
1.1.1.1. Perfiles IHE utilizados ... 16
1.1.2 Trillium Bridge/Blue Button ... 16
1.1.2.1 Perfiles IHE utilizados ... 17
1.1.3. Blue Button ... 17
1.1.4. epSOS ... 17
1.1.4.1. Perfiles IHE utilizados ... 18
1.1.5. La Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS-España) ... 19
1.1.6. Historia clínica compartida de Cataluña (HC3) ... 20
1.1.6.1. Mensajería utilizada ... 21
1.1.7. Comparativa entre las experiencias evaluadas ... 21
1.2. Modelo de referencia a nivel nacional ... 22
1.2.1. IHE y perfiles de integración en un marco nacional: ... 22
1.2.1.1. Perfil XDS.b ... 23
1.2.1.1.1. Actores y transacciones ... 24
1.2.1.1.2. Envío y registro de documento- ITI-41 ... 25
1.3.1.1.3. Registro de documentos (Register Document set) - ITI-42 ... 26
1.2.1.1.4. Consulta de documentos (Query Document) - ITI-18 ... 27
1.2.1.1.5. Recuperación de conjunto de documentos (Retreive Document) - ITI-43 ... 28
1.2.1.1.6. Transacción PIX-QUERY - ITI-09 ... 28
1.2.1.2. Perfil XCA ... 28
1.2.1.2.1. Actores y transacciones ... 29
1.2.2. Identificación de paciente entre Dominios de Afinidad ... 29
1.2.2.1. Transacción Identificación de paciente ITI-08 ... 31
1.2.2.2.Transacción PIX-QUERY - ITI-09 ... 31
1.2.2.3. Transacción Notificación de actualización - ITI- 10 ... 31
1.2.3.Caso de uso ... 31
1.2.3.1. Caso de uso intercambio de informe de alta en un Dominio de Afinidad ... 33
1.2.3.2. Caso de uso entre dominios cruzados ... 33
1.3. Modelo de referencia para la región ... 34
1.3.1. Propuesta de arquitectura ... 35
1.4. Requisitos fundamentales y técnicos ... 36
1.4.1. Infraestructura de comunicaciones ... 36
1.4.1.1. Configuración IPSec ... 37
1.4.1.2. Configuración TLS ... 37
1.4.2. Seguridad ... 37
1.4.2.1. Políticas de Seguridad ... 38
1.4.3. Auditoria ... 38
1.4.3.1. Autenticación de usuario ... 39
1.4.3.2. Autenticación de conexión ... 39
1.4.3.3. Registros de auditoría ... 39
1.4.4. Índice Maestro de Pacientes ... 40
1.4.5.Conjunto de datos mínimos a compartir ... 40
1.4.6. Servicios soportados ... 41
1.4.6.1. Servicio de Identificación de Paciente ... 42
1.4.6.1.1. Contexto ... 42
1.4.6.1.2. Operación ... 42
1.4.6.1.3. Parámetro de entrada ... 42
1.4.6.1.4. Parámetro de salida (en caso de éxito) ... 42

1.4.6.1.5. Precondiciones para el caso de éxito ... 42
1.4.6.1.6. Escenario de éxito principal ... 43
1.4.6.1.7. Casos de fallos ... 43
1.4.6.2. Servicio de Recuperación Resumen de Paciente ... 43
1.4.6.2.1. Contexto ... 43
1.4.6.2.2. Operación ... 44
1.4.6.2.3. Parámetro de Entrada ... 44
1.4.6.2.4. Parámetro de Salida (en caso de éxito) ... 44
1.4.6.2.5. Precondiciones para el caso de éxito ... 44
1.4.6.2.6. Escenario de éxito principal ... 44
1.4.6.2.7. Casos de fallos ... 45
1.4.6.3. Actualización del Resumen de Paciente en el país de afiliación ... 45
1.4.6.3.1. Contexto ... 45
1.4.6.3.2. Operación ... 45
1.4.6.3.3. Parámetro de entrada ... 46
1.4.6.3.4. Parámetro de salida (en caso de éxito) ... 46
1.4.6.3.5. Precondiciones para el caso de éxito ... 46
1.4.6.3.6. Escenario de éxito principal ... 47
1.4.6.3.7. Casos de fallos ... 47
1.4.7. Consentimiento informado de paciente ... 47
1.4.7.1. Contexto ... 48
1.4.7.2. Operación ... 48
1.4.7.3. Parámetro de entrada ... 48
1.4.7.4. Parámetro de salida (en caso de éxito) ... 48
1.4.7.5. Precondiciones para el caso de éxito ... 48
1.4.7.6. Escenario de éxito principal ... 48
1.4.7.7. Casos de fallos ... 49
1.5. Componentes de la arquitectura ... 49
1.5.1. Componentes del Punto de Contacto Nacional ... 50
1.5.1.1. Punto de Terminación ... 51
1.5.1.1.1. Interfaz de Entrada ... 51
1.5.1.1.2. Interfaz de Salida ... 52
1.5.1.2. Gestor de Auditoría ... 52
1.5.1.3. Gestor de Flujo ... 52
1.5.1.4. Gestor de Enrutamiento ... 54
1.5.1.5. Gestor de Configuración ... 54
1.5.1.6. Gestor de Monitorización ... 55
1.5.1.7. Gestor de Seguridad ... 55
1.5.2. Componentes Nacionales ... 56
1.5.2.1. Componente Autoridad Proveedora de las Identidades de los Profesionales ... 56
1.5.2.2. Componente de Seguridad ... 57
1.5.2.3. Componente de Auditoria Nacional ... 57
1.5.2.4. Componente Servidor Terminológico ... 57
1.5.2.5. Componente de Transformación Sintáctica ... 57
1.5.2.6. Componente que implementa el Servicio de Identificación de Paciente ... 57
1.5.2.7. Componente que implementa el Servicio de Recuperación y Actualización de Resumen de Paciente ... 58
1.5.2.8. Comunicaciones ... 58
1.5.3. Interacción de los componentes nacionales ... 58
1.5.3.1. Vista de la infraestructura nacional que soporta IHE ... 59
1.5.3.1.1. Caso 1: Vista CN B → PCN-B con infraestructura nacional compatible ... 59
1.5.3.1.2. Caso 1: Vista PCN-A → CN A con infraestructura nacional compatible IHE ... 61
1.5.3.2. Vista de la infraestructura nacional que no soporta IHE ... 62
1.5.3.2.1. Caso 2: Vista CN B → PCN-B con infraestructura nacional no compatible IHE ... 63
1.5.3.2.2. Caso 2: Vista PCN-A → CN A con infraestructura nacional no compatible IHE ... 63
1.5.4. Red de confianza RACSEL ... 64

1.5.5. Autenticación del profesional y aserciones SAML ... 65
1.5.5.1. Centralización de HIS y de las autoridades proveedoras de las identidades profesionales ... 66
1.5.6. Servicio de Control de Acceso y XACML ... 68
1.5.6.1. Gestión de Urgencias ... 70
1.6. Casos de uso ... 70
1.6.1. Descripción de los procesos ... 71
1.6.1.1. Búsqueda de Paciente ... 72
1.6.1.1.1. El PCN-B firma la mensajería saliente ... 72
1.6.1.1.2. El PCN-A valida la firma del PCN-B ... 73
1.6.1.1.3. El PCN-A firma la respuesta ... 73
1.6.1.1.4. El PCN-B valida la firma del PCN-A ... 73
1.6.1.2. Recuperación del Resumen de Paciente desde el país de prestación de servicio ... 74
1.6.1.2.1. El PCN-A valida la firma del PCN-B ... 75
1.6.1.2.2. El PCN-B valida la firma del PCN-A con el componente de Gestión de Seguridad ... 75
1.6.1.3. Actualización del Resumen de Paciente en el país de afiliación ... 76
1.6.1.3.1. El Gestor de Flujo del PCN-A activa el Gestor de Seguridad para firma la respuesta como PCN-A ... 76
1.6.1.3.2. El PCN-B valida la firma del PCN-A con el componente de Gestión de Seguridad ... 76
1.6.1.4. Gestión del Consentimiento desde el país de prestación de servicio hacia el país de afiliación ... 76
1.6.2. Notas sobre la implementación con estándares internacionales ... 76
1.6.2.1. Servicio de Identificación de Paciente ... 78
1.6.2.2. Servicio de Recuperación del Resumen de Paciente ... 79
1.6.2.3. Servicio de Actualización del Resumen de Paciente ... 79
1.6.2.4. Servicio de Gestión del Consentimiento ... 80

2. Análisis de GAPS ... 83
2.1. Introducción ... 83
2.2. Elementos de evaluación ... 83
2.2.1. Infraestructura y comunicaciones ... 83
2.2.2. Estándares de comunicación ... 84
2.2.3. Seguridad y auditoría ... 85
2.2.4. Gobierno TIC ... 87
2.3. Descripción de las Brechas ... 87
2.3.1. Brechas de la Red RACSEL ... 87
2.3.1.1. Escenario ... 88
2.3.2. Brechas detectadas ... 89
2.3.2.1. Colombia ... 89
2.3.2.3. Costa Rica ... 92
2.3.2.4. Uruguay ... 94
2.3.2.5. Chile ... 95

3. Recomendaciones ... 99
3.1. Introducción ... 99
3.2. Necesidades previas ... 99
3.2.1. Gobernanza de la Red RACSEL ... 99
3.2.2. Integraciones nacionales: Digitalización y estructuración de la información de salud ... 103
3.2.2.1. Digitalización/ Estructuración de las historias clínicas en las Entidades Proveedoras de Salud (EPS´s) 104
3.2.2.1.1. Evaluación de HIMSS ... 104
3.2.3. Interoperabilidad entre Sistemas de Información a nivel nacional ... 105
3.2.3.1. Caso de uso de interoperabilidad entre EPS´s a nivel nacional ... 105
3.2.4. Acceso integral de la información clínica del paciente (acceso del paciente a su información de salud) ... 107
3.2.5. Identificación de paciente ... 108
3.2.6. Catálogos ... 109
3.2.7. Resumen de Paciente ... 110
3.2.7.1. Propuesta de Actualización de los datos de la prestación en país extranjero ... 112
3.2.8. Consentimiento informado de paciente ... 113

3.2.9. Recursos profesionales 113
3.2.9.1. Notas sobre la centralización de HIS y de las autoridades proveedoras de las identidades profesionales ... 114
3.2.10. Red de confianza RACSEL 115
3.2.11. Pruebas de interoperabilidad 116
3.2.12. Seguridad 117
3.2.13. Hoja de Ruta 118

4.Guía de Autoevaluación 121
4.1. Introducción 122
4.2. Elementos de la Guía de autoevaluación 122
4.2.1. Objetivo 122
4.2.2.Subobjetivos 122
4.3. Esquema de subconjuntos 124

Glosario 133

Referencias 137

Índice de ilustraciones

Ilustración 1-Arquitectura de SHIN-NY 14
Ilustración 2-Diagrama de flujo compartición de datos SHIN-NY 15
Ilustración 3-Trillium Bridge. 16
Ilustración 4-Esquema de la arquitectura de ePSOS 18
Ilustración 5-Esquema de la solución HCSNS 20
Ilustración 6-Esquema de la solución HC3 20
Ilustración 7-Flujo XDS.b 25
Ilustración 8-Flujo XCA 28
Ilustración 9-Flujo Identificación de paciente 30
Ilustración 10-Identificación de Paciente entre Dominios de Afinidad 30
Ilustración 11-Caso de uso entre Dominios de Afinidad 32
Ilustración 12-Caso de uso y transacciones XDS.b 32
Ilustración 13-Caso de uso recuperación de documento de alta de urgencias 33
Ilustración 14-Caso de uso recuperación de documentos entre dominios cruzados 33
Ilustración 15-Diagrama de flujo de recuperación de documentos entre dominios cruzados 34
Ilustración 16-Esquema de la Red RACSEL 36
Ilustración 17-Comunicación entre CN y PCN 41
Ilustración 18-Componentes de la Arquitectura de Referencia 50
Ilustración 19-Flujo de ejecución del Gestor de Flujo 53
Ilustración 20-Conector Nacional – vista genérica 56
Ilustración 21-Infraestructura nacional / CN del país prestador del servicio médico, compatible IHE 59
Ilustración 22-Componentes Infraestructura nacional / CN del país de afiliación del paciente, compatible IHE 61
Ilustración 23-Infraestructura nacional/CN del país prestador del servicio médico, no compatible IHE 63
Ilustración 24-Infraestructura nacional / CN del país de afiliación del paciente, no compatible IHE 63
Ilustración 25-Diagrama de secuencia – Gestión de aserciones SAML al país de prestación del servicio 66
Ilustración 26-Componente de gestión de las identidades – organización punto a punto 67
Ilustración 27-Componente de gestión de las identidades – organización federada por región sanitaria 67
Ilustración 28-Componente de gestión de las identidades – organización centralizada a nivel nacional 67
Ilustración 29-Diagrama de secuencia – Flujo del servicio de control de acceso basado en XACML 69
Ilustración 30-Caso de uso de actualización de paciente 70
Ilustración 31-Esquema de casos de uso Interoperabilidad transfronteriza 71
Ilustración 32-Proceso de Identificación de Paciente 72
Ilustración 33-Proceso de Recuperación de Resumen de Paciente 74
Ilustración 34-Proceso de Actualización de Resumen de Paciente 76
Ilustración 35-Comunicación entre PCN´s 78
Ilustración 36. Comisión de Interoperabilidad para la Región 100
Ilustración 37 Modelo de interoperabilidad 103
Ilustración 38 Modelo de adopción de HIMSS 105
Ilustración 39 Interoperabilidad Nacional 106
Ilustración 40. Interoperabilidad centrada en el ciudadano 107
(Informe IDIS) 107
Ilustración 41 Estructura del CDA óptimo para el traspaso transfronterizo 110
Ilustración 42 Progresión de la implementación de CDA 111
Ilustración 43 Actualización de Resumen de paciente 112
Ilustración 44 Componente de gestión de las identidades – organización punto a punto 114
Ilustración 45 Componente de gestión de las identidades – organización federada por región sanitaria 114
Ilustración 46 Componente de gestión de las identidades – organización centralizada a nivel nacional 115

Introducción

La historia clínica del paciente es uno de los elementos esenciales dentro del proceso asistencial de la relación médico-paciente, y se consolida como una herramienta base para las decisiones que el profesional de la salud toma. Se utiliza de forma complementaria con las diferentes fuentes de observación y diagnóstico que el médico explora y adquiere acerca de las condiciones de salud del usuario/paciente. La interacción del encuentro paciente-médico es guiada por un proceso sistémico, el cual se ajusta en la práctica por la experiencia propia que el galeno adquiere a través del conocimiento desde su propio ejercicio profesional y que se conjuga por condicionantes sociales como la organización, academia, zona geográfica, entre otros.

Durante la última década, la tecnología informática ha permeado los escenarios clínicos y asistenciales y ha permitido que el registro clínico se realice apoyándose de medios informáticos, en donde la historia clínica electrónica se consolida como una herramienta fundamental para el apoyo de los procesos de atención al paciente.

Los beneficios del registro electrónico apuntan hacia una mejora en la atención con mayor eficiencia, seguridad y calidad para el paciente. De igual manera, la digitalización de la información en salud trae consigo nuevos desafíos relacionados con la necesidad de la integración de esta información digital en los contextos de salud. La informática es soportada por tecnologías que deben ser ajustadas a las necesidades de los usuarios para que puedan representar un valor real para sus diferentes interesados.

Siendo conscientes de este advenimiento informático para la salud, es necesario crear un espacio para la reflexionar y para compartir acerca de las actuales experiencias en Historia Clínica Electrónica (HCE) en la región, el cual permita generar las primeras recomendaciones de gobierno para apoyar su desarrollo, como también para discutir acerca de los principios de una integración regional. La Red Americana de Cooperación sobre Salud Electrónica (RACSEL) ha logrado consolidar las experiencias de 5 países de América Latina y generar un trabajo reflexivo en torno a distintos elementos fundamentales para su evolución en nuestros países.

RACSEL nace como iniciativa de cooperación Sur-Sur cuyo propósito es facilitar el desarrollo de la salud electrónica en la región, con énfasis en la historia clínica electrónica. Tiene como países miembros a Colombia, Costa Rica, Chile, Perú y Uruguay, y se desarrolla en el contexto de un Bien Público Regional para el avance de la HCE en América Latina y el Caribe con apoyo del Banco Interamericano de Desarrollo (BID).

El propósito de las actividades de RACSEL ha sido el facilitar la colaboración, el diálogo y el intercambio de conocimiento y experiencias entre los países miembro para el desarrollo de la salud electrónica. Además del intercambio de experiencias, las actividades de la red también el desarrollo, la capacitación y el entrenamiento con consultores internacionales para la creación de una base de conocimiento en las agencias de gobierno.

Los principales temas en los que RACSEL ha trabajado, y que forman parte de los productos que como Bien Público Regional se colocan a disposición, son la recopilación técnica de aspectos relacionados con: marco institucional y normativo para la HCE, arquitectura de sistemas de información de HCE, estándares de interoperabilidad en salud, terminologías farmacéuticas, receta electrónica y lineamientos de medición TIC en salud. De igual manera, quedan disponibles cursos de aprendizaje en la red en una

plataforma web de uso libre para el aprovechamiento de los distintos interesados.

RACSEL ha realizado un esfuerzo inicial en el que ha logrado concretar los fundamentos para que los países y regiones que avanzan en los desarrollos de HCE cuenten con una referencia para sus propias iniciativas. Cada país, acorde a su modelo de salud y a su contexto, ahora puede analizar, ajustar, adaptar y adoptar o no las recomendaciones planteadas. Esperamos que el valor de las discusiones aquí consignadas, desde una visión de una red de gobiernos, logre inspirar para que la salud electrónica lleve mayor equidad, seguridad y calidad a nuestros ciudadanos.

1. **Modelo de Referencia**

Este capítulo tiene como objetivo mostrar una estructura de arquitectura de referencia sólida, escalable y replicable. Esta estructura pretende servir como referencia para los países de Latino América que se encuentren interesados en avanzar en proyectos de Historia Clínica Electrónica (HCE) a nivel nacional y, además, el documento presenta los siguientes pasos para una HCE regional de Latino América y el Caribe.

Mostraremos diferentes ejemplos y niveles de compartición de datos transfronterizos que en la actualidad están en uso en el mundo.

Marcaremos unos requisitos fundamentales a nivel técnico para poder alcanzar la propuesta de interoperabilidad transfronteriza, y posteriormente se realizará la especificación de los componentes de la arquitectura de referencia.

Finalizaremos con unos casos de uso, sobre los datos a compartir con los diagramas de iteración entre los componentes planteados de la arquitectura.

1.1. Compartición de datos transfronterizos

La compartición de datos transfronterizos forma parte de la hoja de ruta marcada por los gobiernos, siguiendo los apuntes de la Organización Mundial de la Salud (OMS).

La OMS promueve el uso de estándares y la interoperabilidad de los sistemas, para escalar las soluciones y promover la compartición de datos para el estudio y control de patologías. Asimismo, reconoce la importancia de estandarizar los datos sanitarios y su relevancia para los sistemas y servicios de eSalud.

La promoción de la atención de la salud requiere el uso apropiado de las Tecnologías de la Información y Comunicaciones (TIC) para proveer servicios de salud cualificados, reducir los costes y lograr la cobertura universal de estos servicios.

Las historias clínicas compartidas pueden ser la mayor fuente de conocimientos clínicos y ayudar a controlar pandemias o realizar estudios a alto nivel sobre la población mundial para promover sociedades sanas.

La compartición de datos clínicos, implica que se tengan que consolidar un mínimo de documentos para hacer viable la transferencia de conocimiento del paciente para su consulta.
A continuación, pasamos a describir una serie de casos de éxito a nivel territorial de compartición de datos entre países, regiones o provincias.

1.1.1. SHIN-NY

El SHIN-NY es la Red de Información de la Salud activa en todo el estado de Nueva York. La organización The New York eHealth Collaborative (NYeC) trabaja con el Departamento de Salud del Estado de Nueva York para coordinar el desarrollo técnico y la política de la red SHIN -NY, y también convoca una amplia gama de partes interesadas de la salud para asegurar que esta red ofrece acceso a los registros médicos electrónicos de un paciente.

El SHIN-NY es una red de redes que une a ocho de entidades habilitadas regionales de Nueva York en todo el estado. Cada entidad habilitada opera su propia red que recoge la historia clínica electrónica de los proveedores participantes.

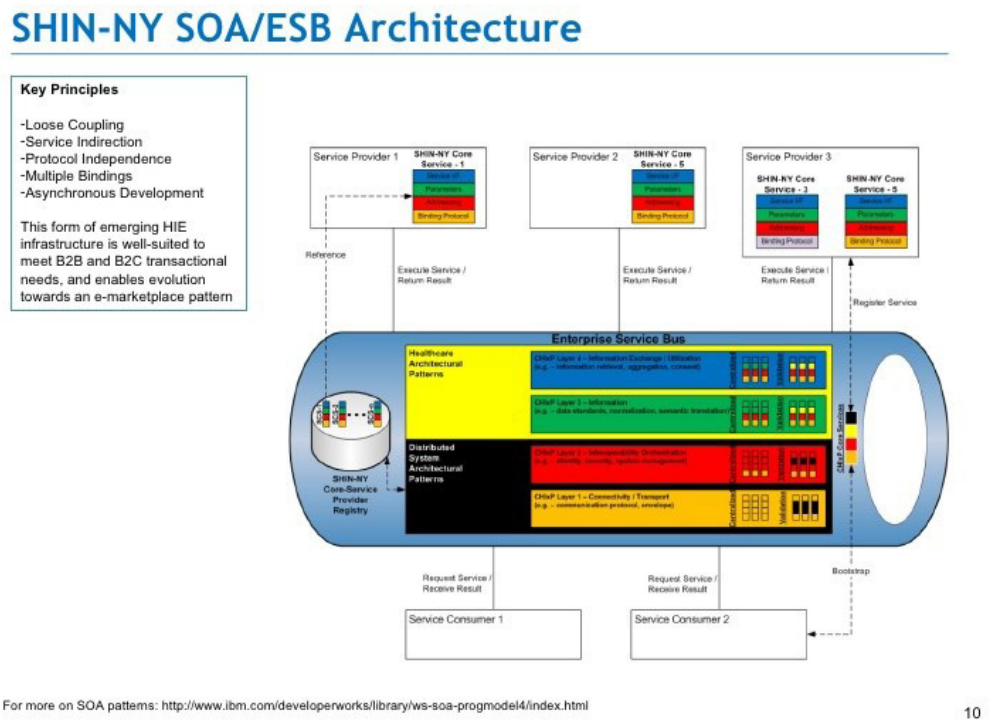


Ilustración 1-Arquitectura de SHIN-NY
(Fuente: ibm.com)

El SHIN-NY es un patrón de infraestructura que permite la interoperabilidad generalizada entre sistemas de salud heterogéneos.

Hay tres opciones principales para estructurar el intercambio de información de salud a través del SHIN-NY:

- Entre geografías
- Entre sistemas
- Entre grupos de afinidad

Se utilizan los perfiles IHE para el traspaso de información. A continuación mostramos un ejemplo de compartición de documentos.

Existen tres actores principales: Electronic Health Record, Patient Identifier Cross-Reference y Event Information Document.

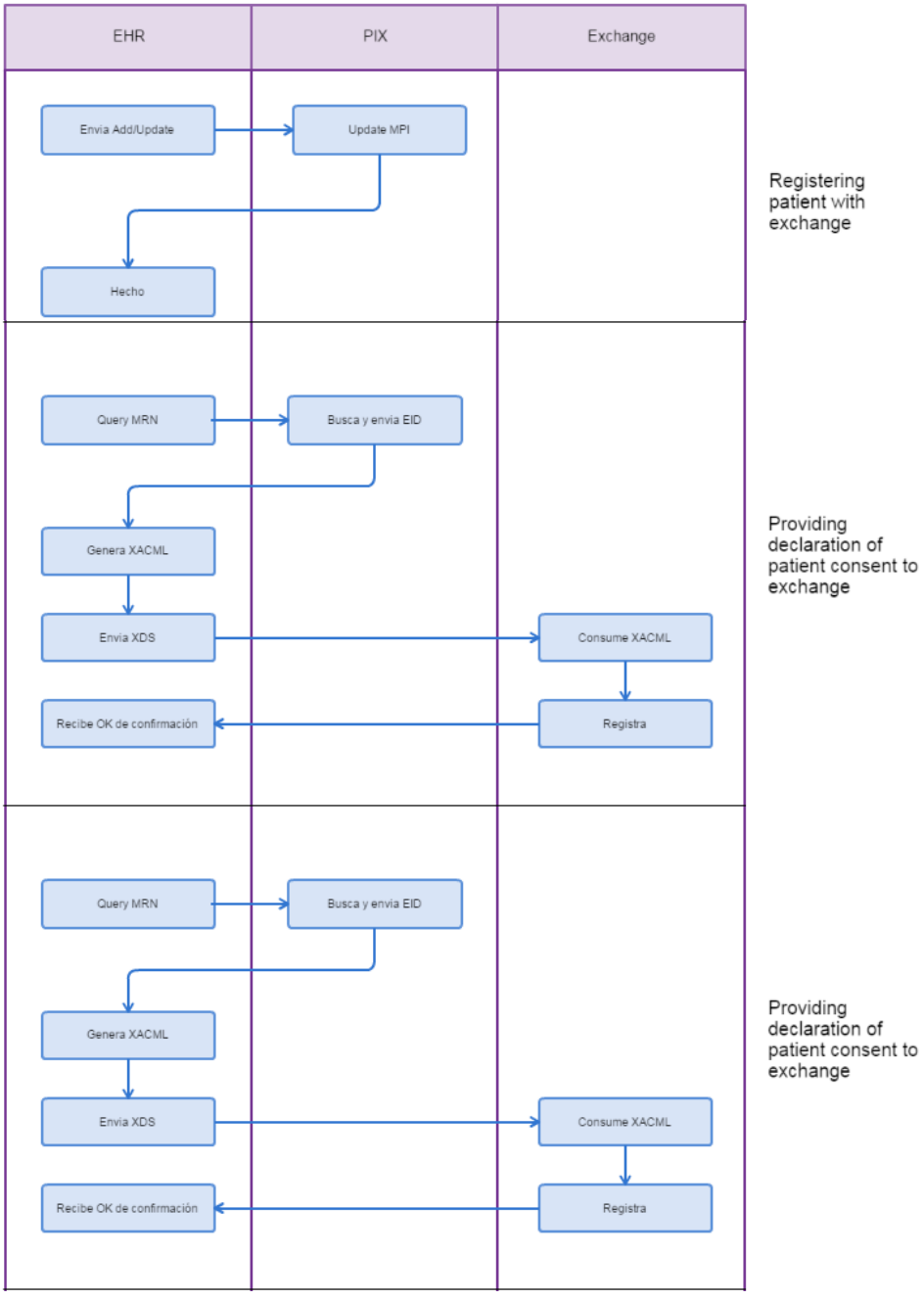


Ilustración 2-Diagrama de flujo compartición de datos SHIN-NY
(Fuente: omr.org)

1.1.1.1. Perfiles IHE utilizados

Perfiles	
XDS	Cross Enterprise Document Sharing
XUA	Cross-Enterprise User Assertion Profile
ATNA	Audit Trail and Node Authentication

1.1.2 Trillium Bridge/Blue Button

Trillium Bridge se crea para realizar la compartición de datos transfronterizos entre Estados Unidos (EEUU) y la Unión Europea (UE).

Aunando las tecnologías ya existentes en ambos continentes como es EPSOS y la extensión del Blue Button, se hace posible este intercambio.

Patrocinado por un consorcio compuesto por ministerios de los estados miembros de la UE, redes de proveedores, industria, asociaciones, SDOs, etc,. tiene la finalidad de realizar un estudio de factibilidad sobre el intercambio de resúmenes de pacientes a través del Atlántico mediante la comparación, análisis y cartografía de resúmenes de pacientes comenzando con uso significativo de CCDA CCD y los resúmenes de pacientes de la UE (ePsos).

La duración del proyecto fue de julio de 2013 hasta junio de 2015.

Ilustración 3-Trillium Bridge

Uno de los propósitos del Trillium Bridge es realizar un estudio de viabilidad con Informes de validación de la UE/EEUU sobre el intercambio de Resumen de Pacientes, los activos de interoperabilidad reutilizables y el trabajo de políticas para:

- Menores costes / barreras para la contratación comercial transatlántica
- Reducir los costes de implementación / configuración
- Disminuir los costes de desarrollo de estándares
- Acelerar la convergencia hacia los estándares mundiales

La arquitectura se basa en servicios SOA para realizar el intercambio de información e utiliza los perfiles de IHE (IHE XCPD, IHE XCA, IHE ATNA).

Ejemplos de problemas más importantes con la alineación de especificaciones:

- SAML: Diferencias significativas en los requisitos para la implementación de eHealth frente ePSOS
- Descubrimiento del paciente: Demografía versus búsqueda basada en identificadores
- Consulta de documento: Diferencia en el código de clase para el tipo de documento utilizado
- Recuperación de documentos: se utiliza el identificador específico del país para recuperar el documento en ePSOS.

1.1.2.1 Perfiles IHE utilizados

Perfiles	
XCA	Cross-comunity access
XCPD	Cross-comunity patient discovery
ATNA	User autentication

1.1.3. Blue Button

Nacido en un principio para compartir la información médica de los veteranos de guerra en EEUU de forma sencilla, Blue Button es una plataforma que permite compartir la información clínica de los pacientes, ya no solo a un sector, ahora en todo el país.

Blue Button tiene como objetivo permitir a los ciudadanos acceder, compartir o descargar su información clínica desde la página web de cada proveedor sanitario. Entre los servicios que ofrece la plataforma son:

- Medicación actual del paciente
- Datos relevantes de salud, tales como alergias
- Información sobre el tratamiento derivado de las consultas médicas o visitas hospitalarias
- Resultados de las pruebas de laboratorio
- Información sobre el seguro de salud (financiera, clínica, etc.).

1.1.4. epSOS

La Unión Europea promovió la creación de un marco de interoperabilidad sanitaria, con el proyecto epSOS, en el que participaron 23 países. Las entidades proveedoras de servicios sanitarios que participan en el proyecto cooperaron compartiendo sus datos.

ePSOS es el primer proyecto europeo de salud electrónica que aglutina tantos y tan variados países en un ejercicio práctico de cooperación.

Identifica varios medios de interoperabilidad que permitirán el uso de servicios transfronterizos tales como el resumen del paciente y la receta electrónica.

La arquitectura epSOS basa en perfiles IHE y los servicios se implementan como servicios web. La comunicación entre el servicio consumidor y el proveedor de servicio siempre es pasiva (iniciada por el consumidor). Cada Nación Participante (PN) ofrece estos servicios a través del Punto de Contacto Nacional (PCN) que actúa tanto cómo proveedor de servicios de cara a otra PN, como de puerta de entrada para los consumidores.

En epSOS el paciente es identificado y autenticado por su país de origen. Los profesionales a su vez, también siguen el mismo patrón de identificación/autenticación, propio de cada país.

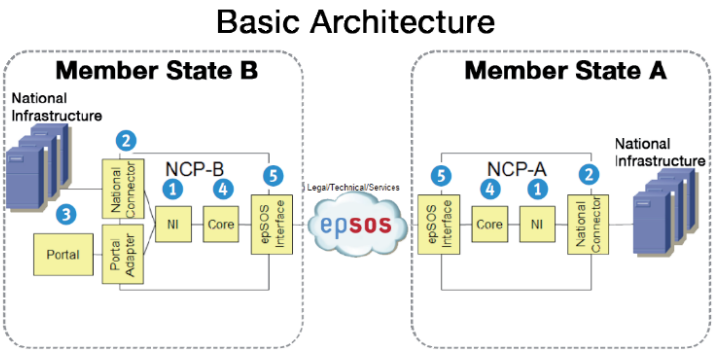


Ilustración 4-Esquema de la arquitectura de ePSOS
(Fuente:epsos.eu)

*1: Interface Nacional

*2: Conector Nacional

La Interfaz Nacional conecta los componentes comunes de epSOS con el Conector Nacional.
El Conector Nacional es el responsable de acceder a la infraestructura nacional y del cumplimiento de los requisitos nacionales.

*3: Core:

Son los elementos comunes que se han definido en el proyecto epSOS y que forman parte de la capa de negocio.

*5 Interfaz epSOS:

La interfaz epSOS es también una parte de los componentes comunes definidos en el proyecto y pertenece a la capa de comunicación con la arquitectura nacional del punto de contacto.

1.1.4.1. Perfiles IHE utilizados

Perfiles

XCA	Cross-Community Access
XDR	Cross Enterprise Document reliable Interface
XCPD	Cross-comunity patient discovery
ATNA	User autentication
BPPC	Basic Patient Privacy Consents

1.1.5. La Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS-España)

La historia clínica del Ministerio de Sanidad de España se basa en la compartición de datos entre todos los proveedores de salud de cada comunidad autónoma. Es una entidad territorial administrativa española dotada de cierta autonomía legislativa y de determinadas competencias ejecutivas y administrativas, y se basa en el envío de información estructurada.

El núcleo del Sistema Nacional de Salud (SNS) es un servidor centralizado, accesible actualmente a través de la Intranet Sanitaria, que permite el acceso al SNS a través de una red privada, exclusiva y dedicada. El acceso de los sistemas cliente al SNS a través de dicha red garantiza los niveles de servicio, respecto al ancho de banda, tiempo de respuesta, etc., y aumenta la seguridad del sistema.

El sistema de HCDSNS tiene como principal objetivo compartir información referente a la historia clínica del paciente fuera de su comunidad autónoma. Para ello, se recomienda intercomunicar los sistemas de historia clínica de las Comunidades Autónomas (CCAA) utilizando como nexo de unión el Nodo Central del Ministerio de Sanidad y Consumo. El sistema de HCDSNS, además, dotará al ciudadano de una herramienta donde podrá interactuar con su historia clínica. Así, se pondrá a su disposición los informes digitalizados de historia clínica que de ellos se tengan, pudiendo:

- Descargárselos para su posterior almacenamiento
- Solicitar la ocultación de alguno de ellos a profesionales de otras CCAA diferentes a donde se emitió el documento

También dispondrá de acceso al listado de accesos que se hayan hecho a sus informes y la procedencia de los mismos.

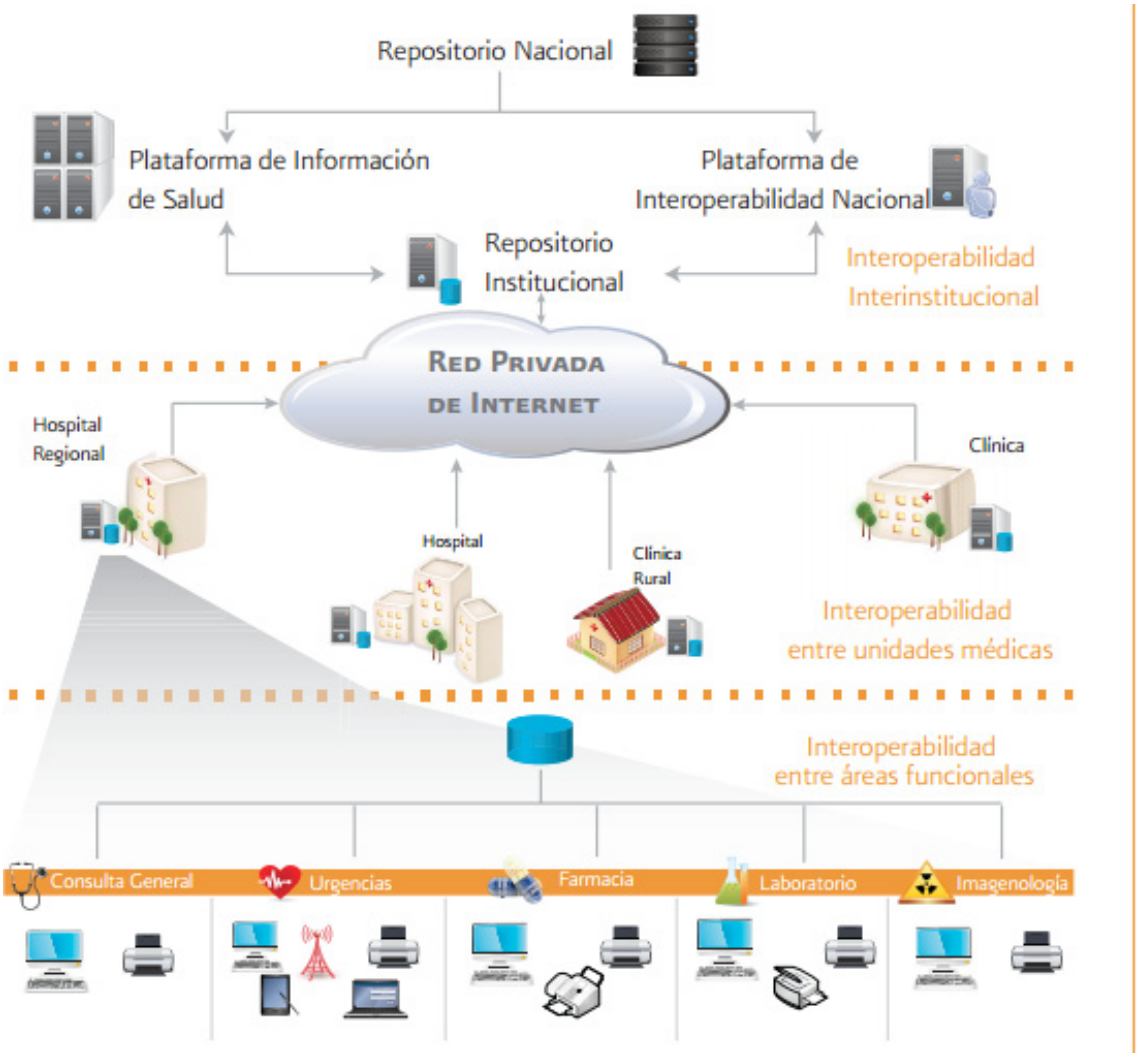


Ilustración 4-Esquema de la arquitectura de ePSOS
(Fuente:epsos.eu)

El núcleo del SNS se basa en un núcleo de intercambios común, capaz de procesar cualquier mensaje XML. La inclusión de nuevos servicios se realiza mediante la definición de nuevos mensajes XML, lo que permite la prestación de nuevas funcionalidades reutilizando la plataforma existente. El modo de operación no cambia.

La definición de nuevos servicios en el SNS implica el desarrollo de los módulos de tratamiento de la información en los sistemas cliente: la generación del XML a partir de la información contenida en los sistemas, y el tratamiento de los mensajes XML recibidos. No obstante, todo el núcleo de intercambio, la gestión de colas y mensajes y los procedimientos de localización y de seguridad forman parte del núcleo del SNS, no siendo necesario implementar nada en los nuevos servicios.

Comunicación
XML entre núcleo central y CCAA

1.1.6. Historia clínica compartida de Cataluña (HC3)

La Historia Clínica de Cataluña (HC3), es un proyecto que permite la compartición de datos sanitarios de los pacientes y centros sanitarios dentro de la comunidad autónoma de Cataluña.

HC3 dispone de un conjunto de servicios e integraciones que habilita a los centros sanitarios la publicación de información asistencial generada de los pacientes. Esta información queda registrada o referenciada a HC3.

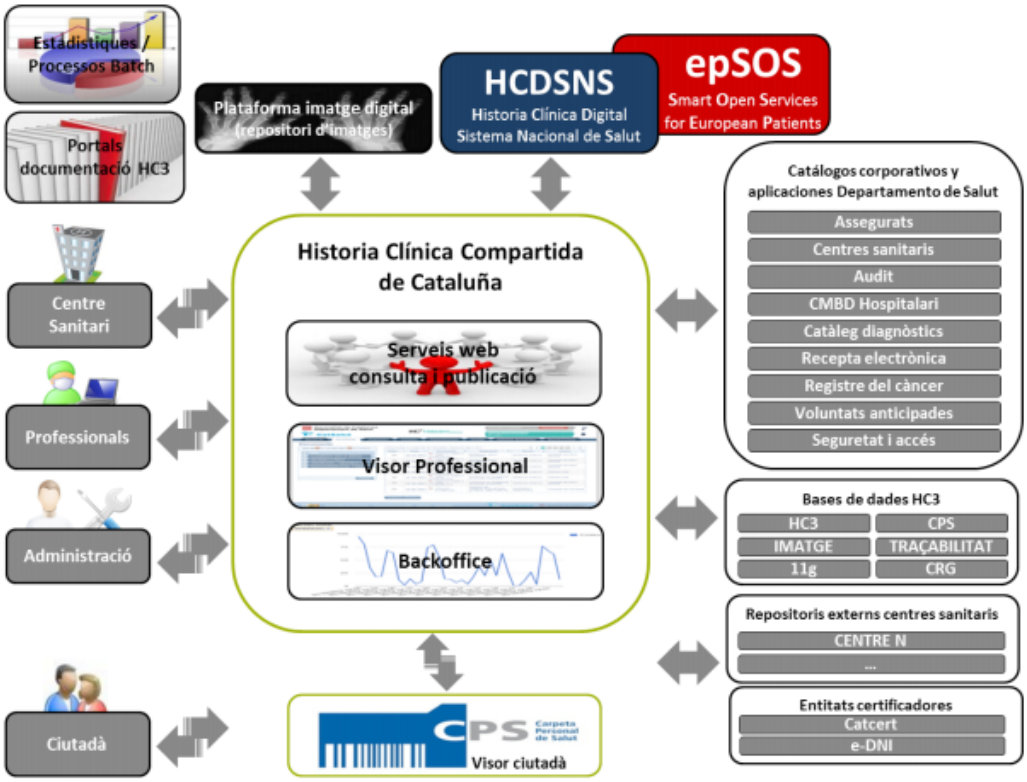


Ilustración 6-Esquema de la solución HC3

Se trata de un sistema híbrido que combina información centralizada con distribuida.

Desde un punto de vista cualitativo el profesional puede consultar diferentes tipologías de documentos y cada uno de ellos con sus respectivas versiones. Además, se puede acceder plataformas externas, tales como, un repositorio de imágenes digitales, que complementa la información disponible en HC3.

Los módulos que se incluyen en el aplicativo HC3 son los siguientes:

- **WS Mensajería**

  - Conjunto de servicios webs publicados por HC3 y por los centros. Los servicios web publicados por HC3 son consumidos desde los diferentes centros sanitarios, de este modo, los centros sanitarios pueden publicar y consultar información clínica.
  - HC3 también proporciona servicios webs de consulta de información clínica que se integran a las Estaciones de Trabajo Clínicas (ETC). Los centros también publican servicios web para facilitar a la HC3 el acceso a información que se mantiene en el propio centro. Dentro del ámbito de la mensajería se proporcionan servicios para que los profesionales puedan notificar ciertos contenidos por paciente a otros profesionales y suscribirse a algunos contenidos de todos sus pacientes asignados, o únicamente para algunos determinados.

- **Visor profesional**

  - Aplicativo web destinado al profesional para consultar por la información clínica de los pacientes, sin necesidad de que cada organización haya de implantar un visor.

- **Gestión centralizada y gobernanza**

  - Aplicativo web destinado a administradores que engloba acciones genéricas, para la gestión o consulta de datos maestros/parametrizables de HC3, y de seguimiento de actividades para las funciones de monitorización de HC3. Es útil tanto a nivel de comprobar que funcionen correctamente todas las capas de la aplicación como a nivel de visibilidad entre HC3 y repositorios de centros sanitarios externos. Dentro del ámbito de gestión y gobernanza se contempla la consulta y ejecución de los procesos por lotes que se utilicen.

1.1.6.1. Mensajería utilizada

Comunicación
XML entre núcleo central y Comunidades

1.1.7. Comparativa entre las experiencias evaluadas

Una vez evaluadas las experiencias, mostramos a continuación un cuadro en el que remarcamos las principales características de las mismas.

Características	Trillium Bridge	SHIN-NY	EPSOS	HCDSNS	HC3
Ámbito geográfico	EEUU-UE	EEUU	EU	ESPAÑA	CATALUÑA
Descripción breve proyecto	Compartición de datos transfronteriza entre EEUU-UE	Compartición de datos en el estado de NY	Compartición de datos transfronteriza en EU	Compartición de datos a nivel estatal Español	Compartición de datos a nivel regional entre todas las EPS´s de Cataluña
Consumidor final (organización/ paciente...)	Organización/ Paciente	Organización	Organización/ Paciente	Organización/ Paciente	Organización / Paciente
IHE SI/NO	SI	SI	SI	NO	NO
Perfiles IHE	XCPD XCA ATNA	XDS XCAML	XDR XCPD ATNA		
CDA	X		X	X	X
CCD	X	X			
Lógica Identificación paciente	Demografía frente búsqueda basada identificador	Demografía frente búsqueda basada identificador	Identificación Europea	Identificación Estatal	Identificación regional
MPI	No	Sí	No	Sí	No
Arquitectura (centralizada, distribuida/hibrida)	Distribuida	Distribuida	Distribuida	Centralizada	Distribuida
Dominio médico (laboratorio, radiología, Resumen Paciente, ...)	Resumen de Paciente + ePrecription	Toda información clínica	Resumen de Paciente + ePrecription	Toda información clínica	Toda la información clínica
Servidor Terminológico (existe, si/no)	Sí		Sí	No	No
Visor (paciente o profesional/ centralizado...)	Visor Profesional	Visor Profesional	Visor Profesional + Paciente	Visor Profesional + Paciente	Visor Profesional + Paciente

1.2. Modelo de referencia a nivel nacional

Para poder alcanzar el objetivo de realizar un traspaso transfronterizo de información clínica, será necesario poder contar inicialmente con una interoperabilidad nacional que haga posible la integración de la Historia Clínica Nacional, para la generación del Resumen de Paciente.

A continuación, introduciremos el concepto de Dominio de Afinidad para mostrar cómo IHE define el intercambio de documentos clínicos entre entidades/organizaciones de salud.

1.2.1. IHE y perfiles de integración en un marco nacional:

IHE es una iniciativa de profesionales de la salud y la industria para mejorar la forma en que los sistemas informáticos de salud comparten información. IHE promueve el uso coordinado de estándares establecidos tales como DICOM y HL7 para tratar las necesidades clínicas específicas en apoyo de la atención óptima del paciente. Los sistemas desarrollados de acuerdo con IHE se comunican entre sí mejor, son más fáciles de implementar y permiten a los proveedores de cuidado usar la información de manera más efectiva.

Siguiendo las propuestas de IHE para tal fin, podemos ver que se han desarrollado dos perfiles específicos para poder estandarizar el intercambio de información clínica entre entidades/organizaciones del

ámbito de salud.

IHE estructura su ecosistema de Marcos Técnicos en diferentes dominios. Los perfiles del dominio ITI están relacionados con tareas y necesidades comunes de los sistemas de información sanitaria.

Entre todos los perfiles existentes promoveremos el uso de aquellos que proveen la capacidad de obtener datos demográficos actualizados de una fuente confiable y la capacidad de participar en el flujo de trabajo de los documentos clínicos, la publicación, la consulta y la recuperación de los mismos.

El dominio de afinidad se rige por la compartición de un registro entre una serie de entidades/organizaciones. Dichas entidades/organizaciones han de trabajar bajo una de premisas de colaboración definidas como:

- Políticas comunes de seguridad
- Políticas comunes de confidencialidad
- Infraestructura común de comunicaciones

Podríamos poner como ejemplos de dominios de afinidad

- Una federación regional de varios hospitales locales y proveedores de salud
- Una Historia Clínica Nacional
- Varias organizaciones de salud asociadas a determinada patología

Entre lo que se debe definir y acordar al conformar un Dominio de Afinidad se encuentra la forma en que los pacientes son identificados, cómo obtener el consentimiento de los pacientes para usar sus documentos clínicos, cómo se realizará el control de acceso sobre los documentos, así como también su formato, contenido y estructura.

Mostraremos en el siguiente apartado la posibilidad de adoptar:

- Dominios de Afinidad a nivel nacional, en los países en los que sea posible, bien por las dimensiones reducidas en cuanto a territorio y población, así como de la capacidad de gestión política con respecto a la toma de decisiones. Dentro de un dominio de afinidad el perfil utilizado es el XDS.b
- En caso de países con una vasta extensión o bien con un alto índice poblacional, sería recomendable el uso de varios dominios de afinidad dentro de sus fronteras. Para tal escenario, se utilizaría el perfil Cross Community XCA, que se basa en la gestión del intercambio entre varios dominios de afinidad XDS.

1.2.1.1. Perfil XDS.b

El perfil XDS.b es un perfil de interoperabilidad que facilita el registro, la distribución y el acceso a las empresas de salud a los registros médicos electrónicos de los pacientes.

En el proceso asistencial es muy común que el profesional requiera consultar información asistencial y administrativa del paciente en diferentes sistemas y entre diferentes organizaciones sanitarias. Es en este escenario donde surge XDS, un modelo que permite integrar información sanitaria entre diferentes organizaciones y sistemas haciendo uso de los estándares.

El objetivo de XDS es desarrollar un modelo de intercambio de registro basado en normas que permita a los profesionales de la sanidad encontrar y acceder a todos los documentos pertinentes de información clínica con respecto a un paciente sin tener en cuenta la organización que los crea y custodia.

El perfil XDS permite:

- Distribución y compartición de datos entre diferentes entidades, disponiendo de las herramientas para la publicación de índices sobre los documentos disponibles.
- Garantiza la centralización de documentos, ofreciendo funciones de publicación organizadas en un registro único.
- Estructura neutral de los documentos, garantizando que estos pueden ser tratados por cualquier sistema.
- Aplicar medidas de control de acceso y autorización sobre los documentos mediante códigos de confidencialidad que se encuentran en los metadatos de los mismos.

El perfil XDS propone manejar repositorios de documentos federados o un único registro de documentos centralizado. De esta forma se crea un registro horizontal de documentos del paciente dentro de un Dominio de Afinidad.

1.2.1.1.1. Actores y transacciones

Actor	Transacción
Fuente documental	Provide & register document set -ITI-41
Consumidor	Query documents -ITI-18
Registro	Register document set - ITI-42
Repositorio	Retreive document- ITI-43
Fuente de Identidad (índice de pacientes)	Patient Identity Feed - ITI-08
Petición de id paciente	PIX- Query- ITI-9

Los actores principales en este perfil:

- Repositorio (Document Repository) responsable de almacenar documentos de forma transparente, confiable y segura y responder ante solicitudes de recuperación.
- Registro de Documentos (Document Registry) responsable de almacenar información (metadatos) sobre dichos documentos de forma que los documentos de interés para la atención del paciente puedan ser fácilmente encontrados, seleccionados y posteriormente recuperados independientemente del repositorio donde se encuentran. Entre los metadatos que se guardan en las entradas del registro se encuentran el identificador del documento y el identificador del repositorio donde se ubica el documento.
- El actor fuente de documentos (Document Source) envía documentos al registro (transacción Provide and Register Document Set) junto con la información necesaria para completar los metadatos al momento de registrar el documento en el Registro de Documentos. Cuando un repositorio recibe una transacción Provide and Register Document Set persiste el documento y además envía los metadatos al registro mediante la transacción Register Document Set.
- El Consumidor de Documentos (Document Consumer) consulta el registro de documentos con algún

criterio de búsqueda (transacción Registry Stored Query) para luego recuperar documentos de uno o más repositorios (transacción Retrieve Document Set).

- El actor Fuente de Identidad (Patient Identitiy Source) del perfil PIX se encuentra presente en el perfil XDS porque es quien debe dar de alta en el registro cada nuevo paciente para el cual se van a comenzar a intercambiar documentos en un Dominio de Afinidad. Se debería dar de alta el paciente en el registro con el identificador global al Dominio de Afinidad.

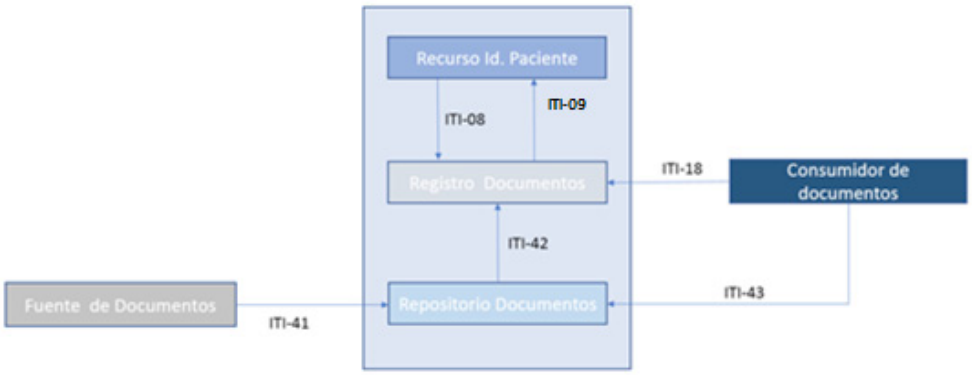


Ilustración 7-Flujo XDS.b
(Fuente: IHE.net)

A continuación, pasaremos a explicar cada una de las transacciones que plantea este perfil XDS.b.

1.2.1.1.2. Envío y registro de documentos (Provide & Register Document set) - ITI-41

Esta transacción es utilizada por el actor Fuente de Documentos para proporcionar un conjunto de documentos al repositorio, junto con los metadatos que describen el documento y que se almacenan en el registro de documentos.

En el Perfil XDS, la Fuente del Documento envía tanto los datos del documento como los metadatos al repositorio y éste los envía al registro de documentos que gestiona su persistencia. El perfil XDS utiliza el estándar de Servicios de Registro (ebRS) para el formato de datos de los metadatos y las transacciones del documento.

La transacción Envío y Registro de Documentos (Provider and Register Document set) admite los siguientes datos:

- Metadatos que describen cero o más documentos
- Dentro de los metadatos, un objeto XDSDocumentEntry por documento
- Definición de conjunto de sumisiones XDS junto con la vinculación a nuevos documentos y referencias a documentos existentes
- Cero o más definiciones de carpetas XDS junto con vinculación a documentos nuevos o existentes
- Cero o más documentos

Una Fuente de Documentos que envía un documento a través de esta transacción puede admitir una o

varias de las siguientes opciones:

- Opción de Reemplazo de Documento: En esta opción, el Origen del Documento ofrece la posibilidad de enviar un documento como reemplazo de otro documento que ya se encuentra en el registro/repositorio

- Opción de Adición de Documento: En esta opción, el Origen del Documento ofrecerá la posibilidad de presentar un documento como adición a otro documento ya en el registro/repositorio

- Opción de Transformación de Documento: En esta opción, el Origen del Documento ofrecerá la posibilidad de enviar un documento como una transformación de otro documento ya en el registro/repositorio

- Opción de administración de carpetas: En esta opción, el Origen del Documento ofrece la posibilidad de realizar la siguiente operación:

    - Crear una carpeta
    - Agregar uno o más documentos a una carpeta

Si se implementa la opción básica de privacidad del paciente:

- El actor Fuente de Documentos rellenará el código de confidencialidad en los metadatos del documento con la lista de valores que identifican las clasificaciones de sensibilidad que se aplican al documento asociado. Los códigos de confidencialidad para diferentes documentos en la misma presentación pueden ser diferentes.

- El actor Fuente de Documentos podrá configurarse con las políticas de privacidad del paciente, identificadores de políticas de privacidad del paciente y asociadas necesarias para comprender y hacer cumplir la política de dominio de afinidad XDS.

- El actor Fuente de Documentos, puede tener capacidades de interfaz de usuario o de regla de negocio para determinar los códigos de confidencialidad apropiados para cada documento.

- El Consumidor de Documentos deberá cumplir las Políticas de Dominio de Afinidad XDS representadas por el código de confidencialidad en los metadatos asociados con el documento. El agente receptor de documentos probablemente tendrá controles de acceso de usuario o capacidades de reglas de negocio para determinar los detalles de cómo se aplican los códigos de confidencialidad a los resultados de la consulta.

Cuando se haya completado el procesamiento de la solicitud, el repositorio de documentos enviará un mensaje de respuesta con el estado de la operación solicitada y un mensaje de error si la operación solicitada falla.

1.3.1.1.3. Registro de documentos (Register Document set) - ITI-42

El repositorio de documentos utiliza la transacción Registro de Documentos para pasar una solicitud de envío al registro de documentos.

La transacción incluye la siguiente información:

- Metadatos que describen cero o más documentos

- Definición de conjunto de sumisiones XDS junto con la vinculación a nuevos documentos y referencias a documentos existentes;

- Definiciones de carpetas XDS opcionales junto con vinculación a documentos nuevos o existentes.

Al recibir el mensaje de solicitud de Registro de Documentos, éste deberá realizar la siguiente acción:
- Aceptación de todos los SubmitObjectsRequests válido

- Validación de metadatos

El registro de documentos almacenará e incluirá posteriormente en las respuestas de consulta todos los atributos de metadatos del documento de registro.

Si el registro rechaza los metadatos se devolverá un error que incluya un mensaje descriptivo y la solicitud se debe revertir.

Cuando el registro finalice el procesamiento de un mensaje de solicitud de registro, responderá con un mensaje que incluirá el estado de la operación solicitada y/o un mensaje de error, si falló la operación solicitada. Las condiciones de fallo y los posibles mensajes de error se dan en el estándar ebRS.

1.2.1.1.4. Consulta de documentos (Query Document) - ITI-18

Se trata de una solicitud de consulta al Registro de Documentos de un consumidor.

La solicitud de consulta contiene:

- Una referencia a una consulta predefinida almacenada en el agente del registro de documentos

- Parámetros de la consulta

1.2.1.1.5. Recuperación de conjunto de documentos (Retreive Document) - ITI-43

El actor consumidor utiliza la transacción Recuperar Conjunto de Documentos (Retreive document), para recuperar un conjunto de documentos del repositorio. Se da por hecho que el Consumidor de Documento ya ha obtenido el XDSDocumentEntry.uniqueId y el Repository de documentos repositoryUniqueId del Registro de Documentos mediante la transacción de registro de consultas almacenadas.

El mensaje de transacción incluye la siguiente información:

- Un RepositoryUniqueId, requerido que identifica el repositorio desde el cual se va a recuperar el documento. El valor corresponde al objeto XDSDocumentEntry.repositoryUniqueId. El repositoryUniqueId asociado con cada documento solicitado puede ser diferente, por lo tanto, permitiendo una sola solicitud para identificar múltiples repositorios.

- DocumentUniqueId, requerido, que identifica el documento dentro del repositorio. Este valor corresponde al objeto XDSDocumentEntry.uniqueId.

En respuesta a un mensaje de solicitud de recuperación de conjunto de documentos, el repositorio de documentos generará una respuesta que contenga los documentos solicitados o los códigos de error si no se pudieran recuperar.

La respuesta al conjunto de documentos a recuperar llevará la siguiente información para cada uno de los documentos devueltos:

- Un RepositoryUniqueId, requerido que identifica el repositorio desde el cual se va a recuperar el documento. Este valor será el mismo que el valor de repositoryUniqueId en el mensaje original de la solicitud de recuperación de conjunto de documentos.

- DocumentUniqueId, requerido que identifica el documento dentro del repositorio. Este valor debe ser el mismo que documentUniqueId en el mensaje original de la solicitud de recuperación del conjunto de documentos.

El elemento respuesta de recuperación de documento se define como:

- Un RepositoryUniqueId, requerido que identifica el repositorio desde el cual se va a recuperar el documento. El valor de este elemento será el mismo que el valor del elemento RetrieveDocumentSetRequest/DocumentRequest/RepositoryUniqueId en el mensaje de solicitud original.

- Un DocumentUniqueId, requerido que identifica el documento dentro del repositorio. El valor de este elemento será el mismo que el valor del elemento RetrieveDocumentSetResponse/DocumentRequest/DocumentUniqueId en el mensaje de solicitud original.

1.2.1.1.6. Transacción PIX-QUERY - ITI-09

Esta transacción implica una solicitud por parte del consumidor de una lista de identificadores de pacientes que corresponden a un identificador de paciente conocido por el consumidor.

La solicitud es recibida por el administrador de referencias cruzadas del Identificador del Paciente.

El gestor de referencias cruzadas procesa inmediatamente la solicitud y devuelve una respuesta en el formulario de una lista de identificadores de pacientes correspondientes, si los hubiere.

1.2.1.2. Perfil XCA

Mostraremos como otra alternativa a nivel nacional, la utilización del perfil Cross Community Acces (XCA) utilizado para realizar consultas y recuperar datos médicos de pacientes que se encuentran almacenados en otras comunidades.
Una comunidad se define como un conjunto de las entidades prestadoras de salud, que se identifican por un identificador global único llamado homeCommunityId. La pertenencia en una comunidad no impide que sea miembro de otra comunidad. Dichas comunidades pueden ser dominios de afinidad XDS que definen el uso compartido de documentos con el perfil XDS o cualquier otra comunidad, sin importar su estructura de compartición interna.

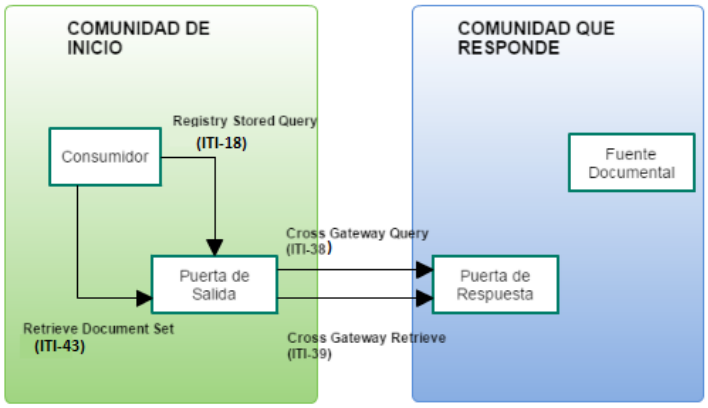


Ilustración 8-Flujo XCA
(Fuente: IHE.net)

1.2.1.2.1. Actores y transacciones

Las puertas de salida interactúan con los consumidores de documento dentro del Dominio de Afinidad XDS.

Flujo de acción entre las puertas:

- Las puertas recibirán las transacciones de la Consulta Almacenada en el Registro [ITI-18] del consumidor de documentos local y actuarán sobre esas solicitudes en nombre del consumidor de documentos. Al recibir una consulta almacenada en el registro, se requerirá el homeCommunityId como parámetro de entrada en las consultas pertinentes y que especifique el atributo homeCommunityId dentro de sus respuestas. Las puertas de salida que soportan esta opción deberán ajustar el identificador de paciente encontrado en la Consulta Almacenada en el Registro a un identificador de paciente apropiado conocido por la puerta de respuesta que recibe la Consulta de Puerta de enlace cruzada.

- Las puertas recibirán las transacciones de Recuperación de Documentos [ITI-43] de un consumidor local y actuarán sobre esas solicitudes en nombre del consumidor. Cuando reciban los documentos tras una petición a un HIS local, ésta deberá contener el HomeCommunityId como un parámetro de entrada.

Actor	Transacción	
Puerta de salida	Consulta Puerta de enlace cruzada Puerta de enlace cruzada Recuperación Consulta almacenada del registro Recuperación de conjunto de documentos	ITI-38 ITI- 39 ITI-18 ITI- 43
Puerta de respuesta	Consulta Puerta de enlace cruzada Recuperación Puerta de enlace cruzada	ITI-38 ITI- 39

1.2.2. Identificación de paciente entre Dominios de Afinidad

El perfil PIX permite identificar al mismo paciente en varios dominios manteniendo referencias cruzadas entre todos los identificadores que dicho paciente pueda tener.

Cuenta con las siguientes características:

- Transmitir información de identidad del paciente desde una fuente de identidad al administrador de referencia cruzada del identificador de paciente.

- Proporcionar la posibilidad de acceder a la lista de identificadores de pacientes con referencias cruzadas a través de una consulta o bien para notificar una actualización.

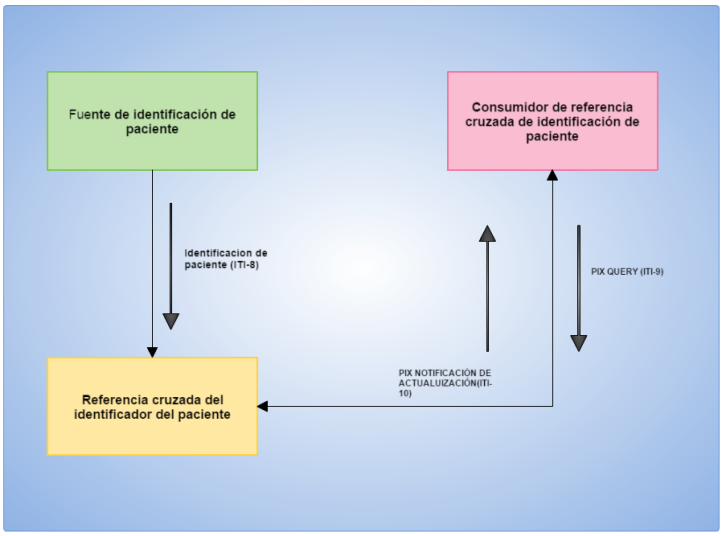


Ilustración 9-Flujo Identificación de paciente
(Fuente: IHE.net)

El actor Patient Identifier Cross-reference Manager (PIX Manager) es responsable de mantener el cruzamiento de la información de identificación de los pacientes. Cada nuevo paciente que se da de alta en el dominio de identificación debe ser dado de alta en el PIX Manager.
Esto último es realizado por el actor Patient Identity Source (PIS) mediante la transacción Patient Identity Feed junto con sus datos demográficos (fecha de nacimiento, lugar de nacimiento, sexo, etc.).

Dado el identificador de un paciente en un determinado domino un sistema actuando como actor Patient Identifier Cross-reference Consumer (PIX Consumer) puede consultar la lista de identificadores/dominio asociada a dicho paciente, así como los datos demográficos que lo identifican, mediante la transacción PIX Query. Además de realizar consultas un PIX Consumer puede registrarse para recibir notificaciones (transacción PIX Notification) ante cambios en la información de identificación de sus pacientes.

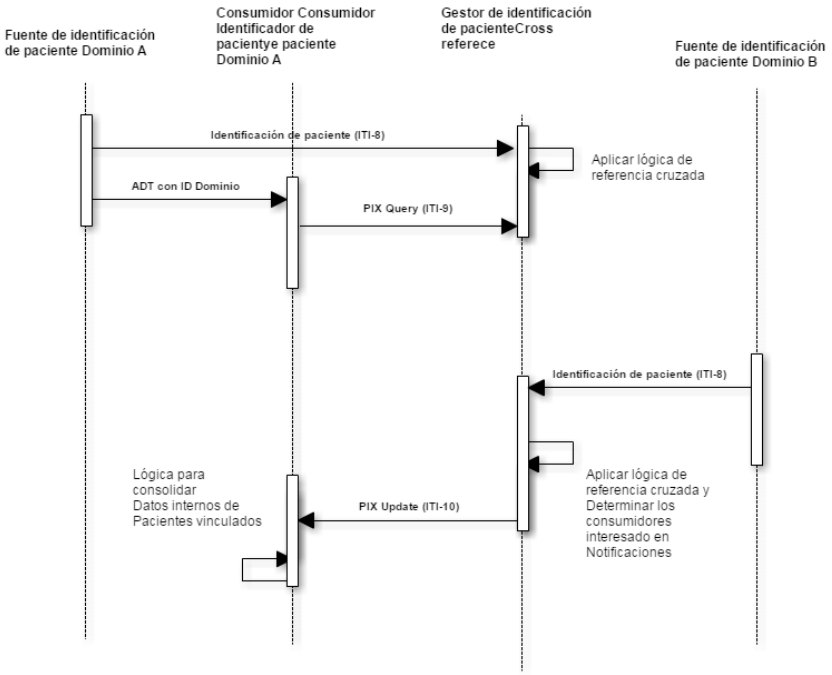


Ilustración 10-Identificación de Paciente entre Dominios de Afinidad
(Fuente: IHE.net)

Es fundamental dentro de un Dominio de Afinidad, que cada paciente se encuentre inequívocamente identificado, ya que cada documento pueda asociarse de forma fiable con el paciente al que se refieren los documentos. El registro de documentos XDS no pretende ser una autoridad para la identificación del paciente y la información demográfica, por lo tanto, la Fuente de Identidad del Paciente se utiliza como fuente autorizada de Identificadores de Pacientes.

Un determinado Dominio de Afinidad XDS utiliza un dominio de identificador de paciente administrado por una fuente de identidad y sirve para vincular los documentos a un paciente.
Las solicitudes de envío con documentos relacionados con pacientes con ID no conocidos por el registro de documentos XDS serán rechazadas por el servicio XDS.

1.2.2.1. Transacción Identificación de paciente ITI-08

Esta transacción comunica la información del paciente, incluyendo datos demográficos corroborantes, después de que se establezca, modifique o fusione la identidad de un paciente o después de que la clave certifique que los datos demográficos han sido modificados.

1.2.2.2.Transacción PIX-QUERY - ITI-09

Esta transacción implica una solicitud por parte del consumidor de una lista de identificadores de pacientes que corresponden a un identificador de paciente conocido por el consumidor.
La solicitud es recibida por el Administrador de Referencias Cruzadas del Identificador del Paciente.

El gestor de referencias cruzadas procesa inmediatamente la solicitud y devuelve una respuesta en el formulario de una lista de identificadores de pacientes correspondientes, si los hubiere.

1.2.2.3. Transacción Notificación de actualización - ITI- 10

Esta transacción usa el conjunto de parámetros propios del grupo de mensaje ADT (ADT-01, ADT-0, ADT-11, etc.) para notificar la actualización de la información del paciente.

1.2.3.Caso de uso

Como caso de uso clásico dentro de una nación mostraremos la compartición de un alta de urgencias entre entidades prestadoras de salud distintas, dentro de un mismo país.

La compartición de dicho informe de alta, deberá estar estructurado y siguiendo estándares sintácticos y semánticos para poder ser inteligible por cualquiera de las entidades que formen parte de la interoperabilidad nacional.

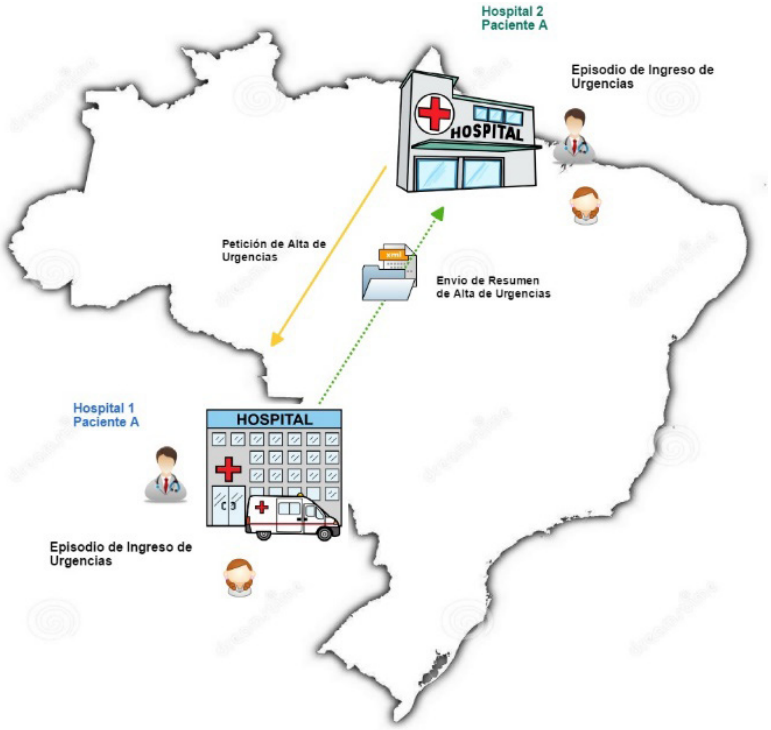


Ilustración 11-Caso de uso entre Dominios de Afinidad

Tal y como se ha explicado en el perfil XDS.b, los actores implicados serán:

- Registro
- Repositorio
- HIS Locales
- Identificación de paciente (MPI).

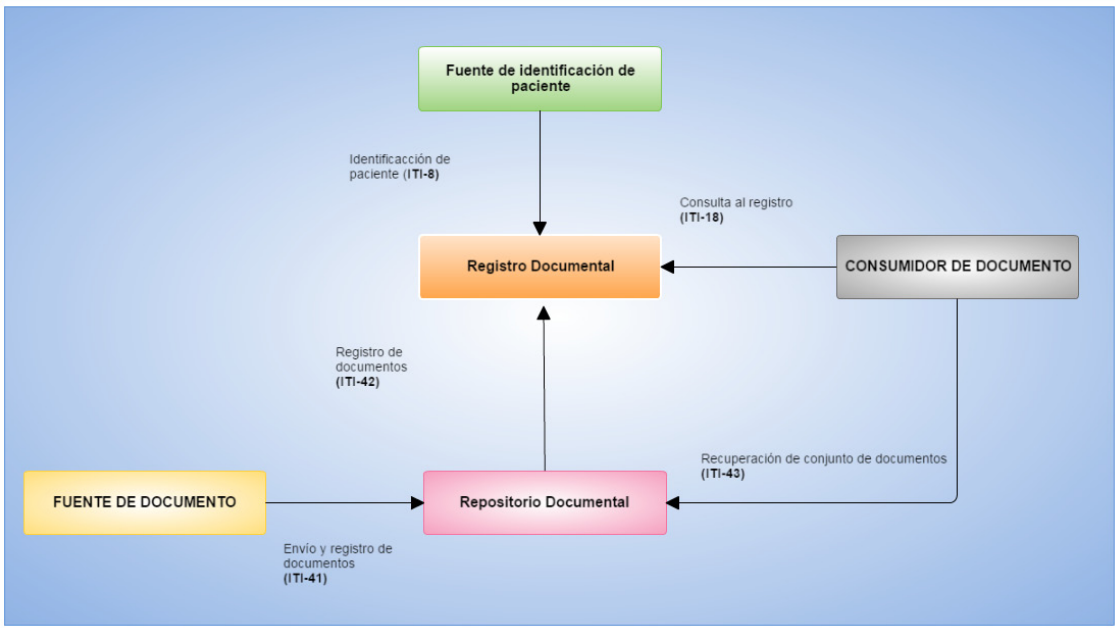


Ilustración 12-Caso de uso y transacciones XDS.b
(Fuente:IHE.net)

1.2.3.1. Caso de uso intercambio de informe de alta en un Dominio de Afinidad

Un paciente acude a un centro de salud (A) por una emergencia que es recurrente y que había sido tratada en otro centro del país.

La primera consulta que se realiza es hacia un MPI, que resuelve la identificación del paciente.
El profesional clínico, hace una consulta para poder visualizar el informe de alta realizado en otra entidad proveedora de salud.

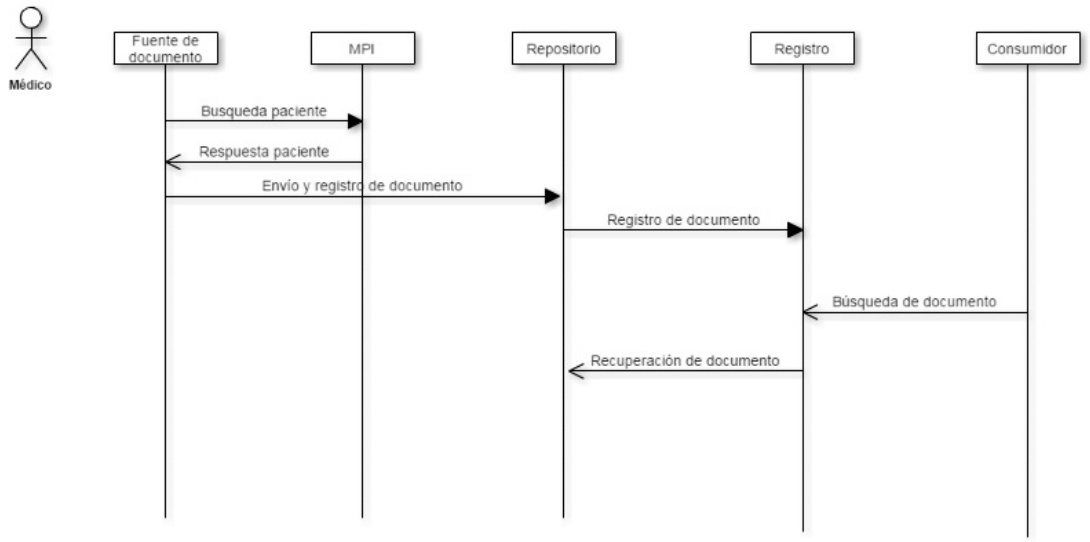


Ilustración 13-Caso de uso recuperación de documento de alta de urgencias

1.2.3.2. Caso de uso entre dominios cruzados

La petición de devolución del informe del paciente se realiza desde un Dominio de Afinidad diferente al que se encuentra la entidad proveedora de salud que custodia el documento.

Por lo tanto, se realizará un intercambio de información entre dos o más dominios de afinidad entre los que exista confianza.

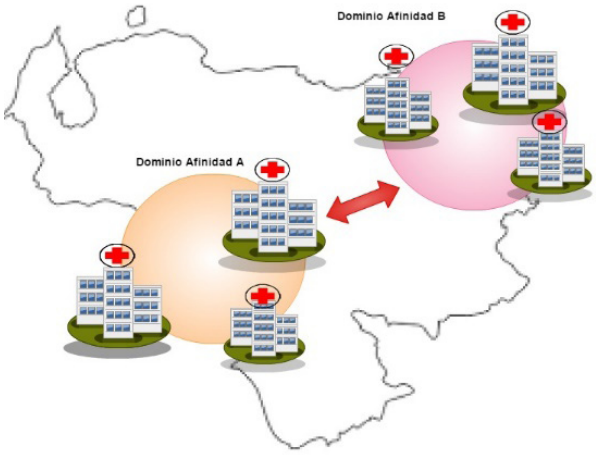


Ilustración 14-Caso de uso recuperación de documentos entre dominios cruzados

Paciente que se visita en un hospital que no pertenece al mismo Dominio de Afinidad dónde se ha realizado otra prestación, y del que el profesional clínico necesita realizar una consulta a su expediente clínico.

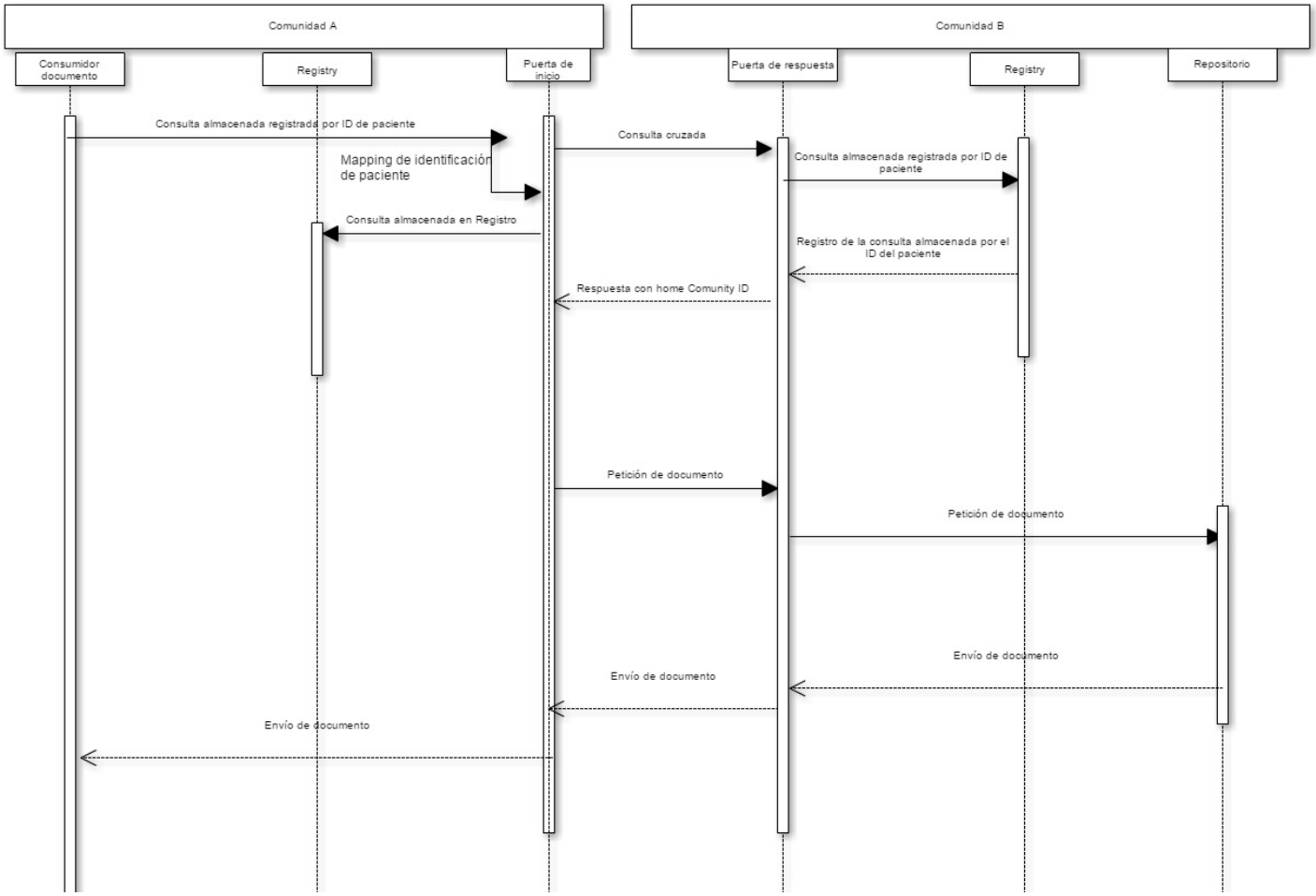
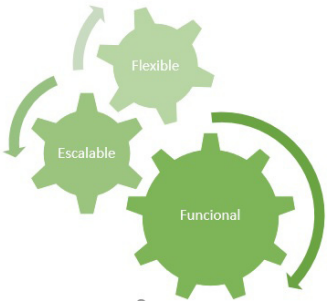


Ilustración 15-Diagrama de flujo de recuperación de documentos entre dominios cruzados

1.3. Modelo de referencia para la región



El objetivo de un modelo de arquitectura de referencia es convertir los requerimientos en funcionalidades orquestando en un conjunto de módulos que cubran las necesidades requeridas.

Dichos módulos, que conforman la arquitectura de referencia, serán convertidos en diversos productos, desarrollos, tecnologías, etc. que serán implantados para dar cobertura, como mínimo, a las necesidades detectadas inicialmente.

El principio básico de la solución propuesta es salvar las infraestructuras nacionales de salud electrónica existentes de los países miembros de RACSEL en lugar de crear una nueva red de servicios de salud centralizada a partir de cero.

Después de realizar un análisis de las experiencias existente sobre compartición de datos transfronterizos, hemos adaptado la propuesta referenciándonos en el modelo europeo, por las similitudes en los requisitos y premisas detectados.

Para estos enfoques son necesarios los trabajos de interoperabilidad técnica, semántica y legal entre

las infraestructuras de salud en línea del grupo perteneciente a la Red RACSEL que debe ser logrado. Esto incluye cuestiones de identidad, así como las cuestiones de seguridad y gestión de la información. Se recomienda a los estados miembros de la Red RACSEL facilitar la cooperación en la prestación de asistencia sanitaria transfronteriza a nivel regional y local, así como a través de las TIC y otras formas de cooperación transfronteriza.

1.3.1. Propuesta de arquitectura

El principio básico de esta propuesta es conectar las infraestructuras nacionales existentes de sanidad de cada uno de los países a una nueva red de Latino América y el Caribe, con la creación de servicios sanitarios comunes desde cero.

El desafío para el desarrollo de las especificaciones técnicas para la solución es:

- Solución que pueda evolucionar en los próximos años y sentar las bases para un intercambio de cualquier tipo de datos médicos en toda el área de influencia de RACSEL (los países adscritos en la actualidad y los futuros). Por lo tanto, una solución escalable.

- Que pueda conectarse fácilmente a las infraestructuras existentes sin imponer nuevos riesgos no razonables sobre la privacidad e integridad de los sistemas existentes de gestión de datos.

- Solución suficientemente flexible como para ser utilizada junto con diferentes medios de identificación, autenticación y autorización para permitir que cualquier ciudadano y país participe en base a los reglamentos legales y actualizaciones técnicas.

El modelo de plataforma se puede ver como federaciones de servicios conectados a través de contratos especificados que definen sus interfaces de servicio. El diseño del sistema resultante es una Arquitectura Orientada a Servicios (SOA).

El objetivo básico es un estilo arquitectónico que puede desacoplar la interfaz y la implementación, así como evitar la dependencia o la rigidez en un futuro.

Los países miembros pueden decidir ejecutar la lógica de negocio bajo diferentes entornos de operación con distinta arquitectura de la solución interna.

El diseño de la arquitectura general y el diseño de los servicios estarán basado en los siguientes supuestos básicos:

- El diseño utiliza el paradigma orientado a servicios

- Todos los servicios son pasivos, los consumidores de servicios y proveedores de servicios se comunican en modo síncrono

- Todos los datos médicos, así como todos los datos del paciente y la identidad de los proveedores de salud se administran en sistemas autónomos. Todo intercambio de estos datos estará mediado por las pasarelas nacionales

- La federación de los Puntos Nacionales de Contacto (PCN's) se implementará a través de un círculo de confianza de la Red de los miembros pertenecientes a la Red RACSEL.

La estrategia a seguir en la definición se basa en minimizar el intrusismo en los sistemas ya existentes mediante una capa de intermediación que se encargue de realizar las transformaciones y conexiones

oportunas entre los diferentes sistemas.

Esta capa de intermediación debe permitir establecer los mecanismos de virtualización, transformación, composición, seguridad y monitorización de las comunicaciones que se establezcan entre los diferentes sistemas.

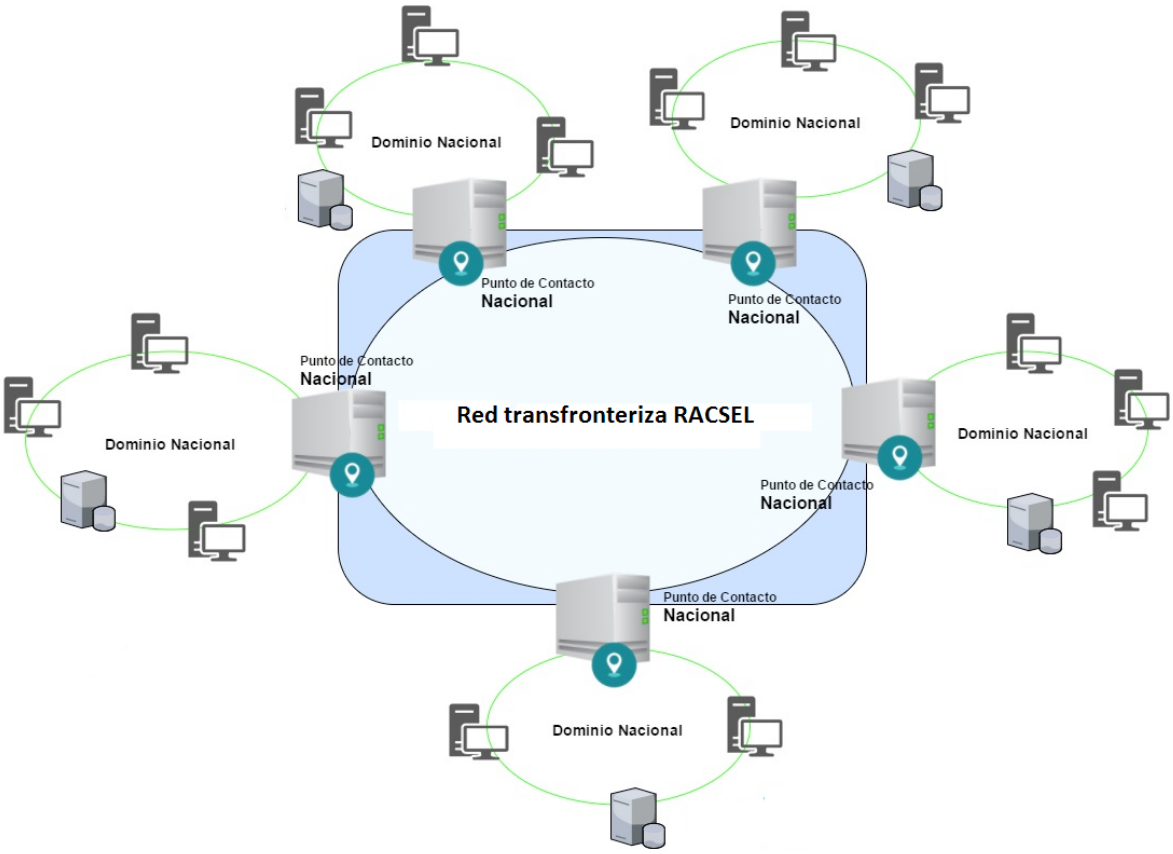


Ilustración 16-Esquema de la Red RACSEL

1.4. Requisitos fundamentales y técnicos

1.4.1. Infraestructura de comunicaciones

La infraestructura de nodo de confianza de la Red RACSEL debe implementar los principales servicios de seguridad para garantizar la confidencialidad y la autenticidad de la transmisión de datos médicos y la disponibilidad de los servicios de la red. Para ello se requiere:

- El establecimiento de una Red Privada Virtual (VPN) para la creación de un canal seguro a través de Internet
- La encriptación de las comunicaciones
- Una autenticación mutua de los Puntos de Contacto Nacionales

La infraestructura de mensajería de la Red proporciona mecanismos para la implementación de servicios de seguridad como, por ejemplo, no repudio y control de acceso, y para los datos y documentos:

- Transmisión de atributos de los profesionales autenticados

- Formato de mensaje común
- Firma sobre elementos del mensaje para la auditoría

El establecimiento de la confianza mutua entre nodos se realiza por:

- Internet Protocol Security (IPSec)
- Seguridad de la capa de transporte TLS v1.2
- IHE Audit Trail y Autenticación de los Nodos

1.4.1.1. Configuración IPSec

Debe establecerse una VPN entre todos los nodos pertenecientes a la Red. Los certificados de la puerta de enlace deben de cumplir con los perfiles de certificado definidos.

Las autoridades certificadoras emisoras y todos los componentes y servicios para la gestión del ciclo de vida de los certificados deben cumplir con las respectivas políticas de seguridad marcadas por la Red RACSEL

1.4.1.2. Configuración TLS

Todos los nodos de la Red que ejecutan los servicios consumidores o proveedores deben ser implementados como actores del perfil IHE ATNA. El establecimiento de la confianza mutua y la configuración del canal de capa de transporte seguro entre dos nodos de la Red RACSEL siempre se inician por un consumidor de servicios que se conecta a un proveedor de servicios.

Los mensajes para el establecimiento del canal seguro de la capa de transporte básico corresponden al protocolo TLS.

Con respecto a la especificación de transacciones ITI-19, se aplica la siguiente restricción:
Los certificados de autenticación de nodo deben cumplir con las respectivas políticas de seguridad marcadas por la Red RACSEL.

1.4.2. Seguridad

La seguridad en proyectos de esta envergadura es prioritaria, puesto que los datos que han de traspasar fronteras son de alta sensibilidad al tratarse de datos de salud.

Es necesario crear un entorno operativo seguro para desplegar lo servicios y por este motivo la política de seguridad debe ser suficientemente robusta para proteger los datos y procesos, que deben de ser implementados y acordados por los países que interactúen.

Es necesario por tanto que los países pertenecientes a la Red, creen una cadena de confianza mutua entre ellos.

La política de seguridad debe contemplar auditorias periódicas para garantizar la conformidad y cumplimiento de los acuerdos.

Para poder garantizar la seguridad de cada una de las transacciones de intercambio que se realizarán a través de los consumidores /proveedores de los servicios de la Red, éstas deberían ser registradas.

El Perfil de Integración (ATNA) contribuye al control de acceso limitando a la Red entre nodos, limitando el acceso a cada nodo a usuarios autorizados.

Los nodos seguros (por cada país) limitan el acceso a los usuarios autorizados según lo especificado por la autenticación local y la política de control de acceso.

Todos los flujos de datos deben estar adecuadamente protegidos, cubriendo tanto los marcados internamente por cada uno de los países, como las normas mínimas acordadas entre los países pertenecientes a la Red RACSEL, marcando el círculo de confianza.

A continuación, apuntaremos los puntos básicos con respecto a las normas mínimas:

- Los usuarios finales (personal que realiza las consultas) deben estar claramente identificados por el Punto de Contacto Nacional antes de poder entrar en el sistema

- Autenticación mutua entre proveedores nacionales y el punto de contacto cuando se inicia un flujo de información transfronteriza mediante certificados

- Que el sistema está usando procedimientos apropiados para asegurar que los datos sean auditados

- Debe prestarse especial atención al ente certificador, que está en el Conector Nacional para que éste pueda ser de confianza y pueda ser aceptado como ente certificador

1.4.2.1. Políticas de Seguridad

Todos los datos y procesos deben estar adecuadamente protegidos. La red constituyente entre los países que conforman la Red RACSEL, no debe generar ningún riesgo a cualquier país participante.

Para ello, se recomienda asegurar el uso de tecnologías y procedimientos apropiados para que los datos que son transmitidos por la Red, lo hagan de forma segura, y que sólo puedan tener acceso aquellos países que formen parte de la misma.

La seguridad de la información se caracteriza generalmente por la protección de:

- Confidencialidad: la información está protegida contra el acceso o divulgación a usuarios no autorizados

- Integridad: la información está protegida contra modificaciones no autorizadas.

- Disponibilidad: los recursos deben estar disponibles, sin demoras irrazonables para que los usuarios autorizados puedan tener acceso a la información y los medios relacionados cuando lo necesitan.

La política de seguridad de la Red RACSEL debe ayudar a asegurar y a hacer cumplir lo anterior. También debería proporcionar medios de prueba y controles esenciales que confieran a los usuarios dicha información.

1.4.3. Auditoria

Todos los consumidores de servicios y proveedores deben escribir entradas o registros de auditoría para todos los mensajes. El objetivo principal de la entrada de auditoría escrita en el país de la afiliación del paciente es para proteger la privacidad del paciente, y en el país que provee los servicios es proteger la reputación del profesional.

El transporte de los datos del registro de auditoría al repositorio de auditoria se realiza dentro de la competencia nacional y se rige por la seguridad del país. El intercambio de datos de la auditoría entre países es una cuestión que ha de estar regida por la gobernanza común.

Se pueden definir estas posibles acciones que están sujetas a ser auditadas:

- Identificación del evento - ¿Qué se hizo?
- Identificación del actor - ¿Quién lo hizo?
- Identificación del Punto de Acceso a la Red - ¿Iniciado desde dónde?
- Identificación de la Fuente de Auditoría: ¿con qué servidor?
- Identificación del Objeto del Participante - ¿Para qué paciente? ¿A qué registro?

El perfil de integración ATNA contribuye al control de acceso, limitando el acceso de red entre nodos y limitando el acceso a cada nodo a usuarios autorizados. Los nodos seguros limitan el acceso a los usuarios autorizados según lo especificado por la autenticación local y la política de control de acceso, cumpliendo así con la ley de protección de datos.

1.4.3.1. Autenticación de usuario

El rastro de auditoría y el perfil de integración de autenticación de nodo sólo requieren autenticación de usuario local. El perfil permite que cada nodo seguro utilice la tecnología de control de acceso de su elección para autenticar usuarios.

1.4.3.2. Autenticación de conexión

El rastro de auditoría y el perfil de integración de autenticación de nodo requieren el uso de autenticación bidireccional de nodos basada en certificados para las conexiones hacia y desde cada nodo. Adicionalmente, todos los protocolos DICOM, HL7 y HTML tienen mecanismos de autenticación basados en certificados definidos. Estos autentifican los nodos, en lugar del usuario. Las conexiones a estas máquinas que no estén bidireccionalmente autenticadas por nodo estarán prohibidas, serán diseñadas y verificadas para impedir el acceso.

1.4.3.3. Registros de auditoría

Es responsabilidad del cada uno de los países proporcionar a través de los registros de auditoría la posibilidad de permitir que una institución audite actividades, evalúe el cumplimiento de las políticas de un dominio seguro, detecte casos de conducta no conforme y facilite la detección de creación, acceso, información.

Principales características de la política de auditoría de seguridad
• Se basan y cubren tanto la política de seguridad de la Red como la norma ISO27002
• La política de auditoría de seguridad de la Red subraya principalmente las necesidades de confidencialidad e integridad más que las necesidades de disponibilidad.
• El procedimiento de auditoría de seguridad de la Red debe ser realizado por expertos en seguridad acreditados.

Disposiciones básicas para el procedimiento de auditoría de la seguridad:
• Se constituirá un grupo de auditoría de seguridad de los países pertenecientes a la Red RACSEL compuesto por expertos para procedimiento de auditoría y para decir la inclusión de los países según el cumplimiento de los requisitos de seguridad pactados.
• Los expertos en seguridad de la Red RACSEL deben definir una marca mínima aceptable para cada actuación en función de su importancia.
• Una actuación con una marca mínima se considera como un incumplimiento.
• El cumplimiento de medidas de seguridad críticas se requiere en cualquier circunstancia.
• Se aplicarán procedimientos de supervisión del cumplimiento en caso de fallo. Estos incluirán procedimientos de gestión adecuados o sanciones, requisitos para mejoras, etc.
• La validez de la auditoría es limitada en el tiempo. Después de un año, se recomienda realizar una nueva auditoría.
• La auditoría de seguridad debería haber sido completada por todos los socios antes de la puesta en marcha de los servicios en el piloto.

1.4.4. Índice Maestro de Pacientes

Para la identificación única e inequívoca del paciente, el país debería contar con una infraestructura para tal propósito.

Este índice deberá contener la información referida a la identificación del paciente, una tabla de centros sanitarios y una tabla de los sistemas de información de esos centros sanitarios.
La identificación de paciente será relacionada con la petición que se envíe desde un país perteneciente a la Red RACSEL con los datos mínimos para poder identificarlo.

1.4.5.Conjunto de datos mínimos a compartir

Se creará un conjunto de mínimo de datos a compartir, que se recomienda consensuar con todos los participantes del proyecto.

Internacionalmente llamado Patient Summary, nosotros utilizaremos su acrónimo castellano Resumen de Paciente (RP). Es la recolección de datos tanto administrativos como clínicos del paciente debe estar actualizado en el país de afiliación y listo para poder ser consumido por el resto de los países pertenecientes a la Red RACSEL.

Los datos proporcionados por el RP, deben ser los mínimos para poder garantizar una asistencia clínica de calidad.

La generación del Resumen de Paciente por parte de cada uno de los países conlleva varias posibilidades que habrán de adecuarse a la gestión de la información que esté establecida en cada uno de ellos:

- Contar con un Repositorio Centralizado a nivel país en donde se puedan localizar los Resúmenes de los Pacientes

- Posibilidad de redirigir la petición al centro de referencia del paciente, para poder enviar la información de manera transfronteriza

Así mismo debemos contar con que, una vez realizada la prestación en el país de tránsito, se cree oportuno la necesidad de actualizar de forma automática en el país de afiliación del paciente, la información generada de la prestación.

1.4.6. Servicios soportados

Los servicios que componen la solución propuesta dentro del modelo de referencia requerirán fundamentalmente de la definición, implementación y mantenimiento con una gobernanza común entre todos los participantes que interactúen.

Para tal fin, se propone la organización de un Grupo de Trabajo Coordinado para garantizar un conjunto de acuerdos, políticas y bases entre los países pertenecientes a la Red.

Se han identificado los siguientes servicios:

- Identificación del Paciente
- Recuperación del Resumen de Paciente
- Actualización del Resumen de Paciente
- Gestión del Consentimiento

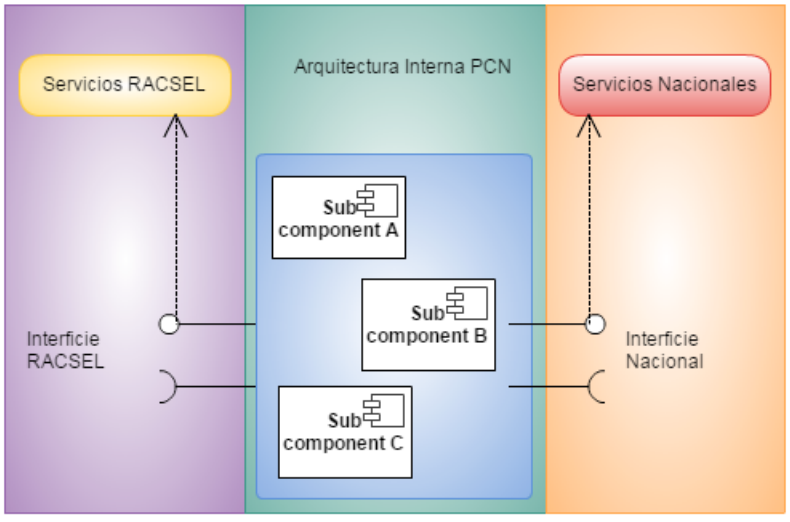


Ilustración 17-Comunicación entre CN y PCN

De aquí en adelante se aplicarán las siguientes convenciones:

- Se identificará al país de afiliación del paciente como: País A.

- El Punto de Contacto Nacional del país que actúa como país de afiliación del paciente será entonces: PCN-A.
- El Conector Nacional del país de afiliación se identificará como: CN-A;

- Se identificará al país prestador del servicio sanitario como: País B.

- El Punto de Contacto Nacional del país que actúa como prestador de servicio médico será entonces: PCN-B.
- El Conector Nacional del país prestador de servicio médico se identificará como: CN-B;

1.4.6.1. Servicio de Identificación de Paciente

1.4.6.1.1. Contexto

Un paciente afiliado en un país A se encuentra en la consulta de un centro de salud de un país B. El profesional que lo atiende, antes que nada, tiene que identificar el paciente en su país de afiliación de una forma univoca y para ello realiza una consulta a este servicio.

El identificador único recuperado se utilizará posteriormente para poder realizar el intercambio de los documentos del paciente entre los países.

1.4.6.1.2. Operación

La operación que describe este servicio es la siguiente: buscaldentidadPaciente() y sirve para obtener un identificador único del paciente en su país de afiliación a partir de una lista de parámetros identificativos proporcionados por el paciente.

1.4.6.1.3. Parámetro de entrada

Hay dos tipos de parámetros necesarios:

- Lista de generalidades identificativas como son: DNI, Pasaporte, Tarjeta Sanitaria, Código de Asegurado en la Seguridad Social, etc;

- Aserción SAML que asegura la identidad del profesional del país B.

1.4.6.1.4. Parámetro de salida (en caso de éxito)

Identificador único del paciente en el país de afiliación, que se usará para el intercambio de información médica entre los dos países.

1.4.6.1.5. Precondiciones para el caso de éxito

- El solicitante puede localizar al proveedor de servicios

- Existencia del canal seguro entre PCN-B y PCN-A

- Disponibilidad del certificado para establecer la comunicación segura con el PCN-B

- El profesional está correctamente identificado en la infraestructura nacional

- El profesional está autorizado para acceder a la Red RACSEL

- Disponibilidad de una aserción SAML del profesional firmada por una autoridad nacional que pueda ser validada por el PCN-B

- El paciente ha dado un consentimiento previo en su país A de afiliación para comunicar sus datos identificativos en su país A hacia el país B.

- El paciente es capaz de proporcionar suficientes datos al profesional para su identificación en el país A.

1.4.6.1.6. Escenario de éxito principal

Las siguientes acciones se refieren al país de afiliación del paciente:

- El PCN-A valida la firma del PCN-B

- Se verifica que el profesional sea habilitado para poder pedir el identificador del paciente del país A

- Se extraen las generalidades identificativas proporcionadas por el paciente y se realiza la búsqueda del mismo en la infraestructura nacional del país A (por ejemplo en el MPI). Dependiendo del resultado:

  - Si se encuentran múltiples resultados se pide al profesional más información o bien se le proporciona una lista de candidatos entre todos aquellos que tengan consentimiento para la tramitación transfronteriza de sus datos identificativos para que el profesional pueda seleccionar el paciente correcto
  - Si solo se encuentra un paciente, y éste tiene el consentimiento al traspaso de sus datos, se devuelve el identificador que posteriormente se usará para el acceso al Resumen de Paciente
  - Para cualquier otro caso se transmite el error correspondiente según se haya definido para este proceso
  - El PCN-A firma el mensaje de vuelta que se devolverá al peticionario

1.4.6.1.7. Casos de fallos

La siguiente casuística puede dar lugar a errores que se tendrán que gestionar en el servicio:

- No se dan las precondiciones del caso de éxito

- El profesional del país B no tiene suficientes permisos para acceder la identidad del paciente del país A

- No se ha encontrado ningún paciente en A que haya dado su consentimiento para el acceso a sus datos en RACSEL

- Las generalidades introducidas no son suficientes para identificar unívocamente el paciente en el país de afiliación

- El acceso a los datos infringiría alguna ley de privacidad que puede existir en el país A

1.4.6.2. Servicio de Recuperación Resumen de Paciente

1.4.6.2.1. Contexto

Un paciente afiliado en un país A se encuentra en la consulta de un centro de salud de un país B. El profesional B quiere obtener el Resumen de Paciente, custodiado en el país A.

1.4.6.2.2. Operación

La operación que describe este servicio es la siguiente: recuperaResumenPaciente() y sirve para que un profesional del país B pueda obtener el Resumen del Paciente del paciente A identificado por medio del servicio anterior.

1.4.6.2.3. Parámetro de Entrada

Hay dos tipos de parámetros necesarios:

- Identificador del paciente obtenido por la ejecución del servicio de Identificación de Paciente
- Aserción SAML[1] que asegura la identidad del profesional del país B
- Aserción SAML[2] que asegura la relación entre el profesional y el paciente para la obtención de su Resumen de Paciente

1.4.6.2.4. Parámetro de Salida (en caso de éxito)

Resumen de Paciente, definido para RACSEL, en formato CDA.

1.4.6.2.5. Precondiciones para el caso de éxito

- El solicitante puede localizar al proveedor de servicios
- Existencia del canal seguro entre PCN-B y PCN-A
- Disponibilidad del certificado para establecer la comunicación segura con el PCN-B
- El profesional está correctamente identificado en la infraestructura nacional
- Disponibilidad de una aserción SAML del profesional firmado por una autoridad nacional que pueda ser validada por el PCN-B
- Disponibilidad de una aserción SAML* que relacione el profesional con el paciente por lo que se pide el Resumen de Paciente firmado por una autoridad nacional que pueda ser validada por el PCN-B
- El paciente ha dado un consentimiento previo en su país A de afiliación para comunicar sus datos identificativos en su país A hacia el país B
- El profesional está autorizado para acceder a los datos del paciente
- Un Resumen de Paciente válido es disponible en la infraestructura nacional del país A.

1.4.6.2.6. Escenario de éxito principal

Las siguientes acciones se refieren al país de afiliación del paciente:

- El PCN-A valida la firma del PCN-B

1. Security Assertions Markup Language (SAML) es un entorno basado en XML para servicios web que permite el intercambio de información de autorización y autenticación entre diferentes sitios Web. Ofrece a los desarrolladores un estándar abierto que permitirá que los usuarios puedan visitar múltiples sitios web sin necesidad de identificarse nada más que una vez. Además, permite, a los visitantes, visitar dichos sitios alojados por distintas compañías, facilitando la adquisición de servicios en los mismos, al no requerir que estos usuarios tengan que registrarse y dar sus datos personales cada vez que entren en una Web.

- Se verifica que el consentimiento del paciente en del país A sea aplicable a este caso de uso
- Recuperación del Resumen de Paciente desde la infraestructura nacional del país A
- Verificar la integridad y la autenticidad del Resumen de Paciente
- Aplicar las políticas se seguridad nacional y las políticas de protección de datos del paciente (si aplicable)
- Transformar el Resumen de Paciente al formato establecido por RACSEL manteniendo el documento original. La transformación puede ser tanto sintáctica (formato de la mensajería) como semántica (que afecte a códigos y terminología)
- Firmar el Resumen de Paciente a nivel de PCN-A
- Realizar los apuntes de auditoria que apliquen

1.4.6.2.7. Casos de fallos

La siguiente casuística puede dar lugar a los siguientes errores que se tendrán que gestionar en el servicio:

- No se dan las precondiciones del caso de éxito
- El profesional del país B no tiene suficientes permisos para acceder Resumen de Paciente solicitado
- Ningún Resumen de Paciente está disponible para el paciente identificado
- Fallo temporal (por ejemplo de autenticación, debido a un problema de PKI)
- A parte, podrían darse algunas condiciones que no provoquen un error pero sí una alerta o una atención especial por parte del profesional que recibe el Resumen de Paciente:
- El país A permite ocultar algunos datos: en este caso un mensaje de aviso debería tramitarse al profesional con la respuesta ya que los datos podrían no ser completos
- El profesional debería considerar el documento original ya que podría contener más datos: se avisa al profesional
- El Resumen de Paciente no ha sido aprobado por ningún profesional en el país A, en este caso un aviso debería aparecer al profesional peticionario

1.4.6.3. Actualización del Resumen de Paciente en el país de afiliación

1.4.6.3.1. Contexto

Un paciente afiliado en un país A se encuentra en la consulta de un centro de salud de un país B. El profesional B añade un registro al Resumen de Paciente y envía los cambios al país de afiliación.

1.4.6.3.2. Operación

La operación que describe este servicio es la siguiente: actualizaResumenPaciente() y sirve para que un profesional del país B pueda añadir información al Resumen del Paciente del paciente identificado,, y que

este resumen pueda ser consolidado en el país A. Dicho con otras palabras, el profesional notifica al país de afiliación del paciente de una prestación de servicio en el país B.

1.4.6.3.3. Parámetro de entrada

Hay dos tipos de parámetros necesarios:

- Conjuntos de datos o registros a añadir al Resumen de Paciente según el formato establecido por RACSEL
- Aserción SAML que asegura la identidad del profesional del país B
- Aserción SAML que asegura la relación entre el profesional y el paciente para la actualización de su Resumen de Paciente

1.4.6.3.4. Parámetro de salida (en caso de éxito)

Indicador de suceso (éxito o fallo).

1.4.6.3.5. Precondiciones para el caso de éxito

- El solicitante puede localizar al proveedor de servicios
- Existencia del canal seguro entre PCN-B y PCN-A
- Disponibilidad del certificado para establecer la comunicación segura con el PCN-B
- El profesional está correctamente identificado en la infraestructura nacional
- Disponibilidad de una aserción SAML del profesional firmado por una autoridad nacional que pueda ser validada por el PCN-B
- Disponibilidad de una aserción SAML que relacione el profesional con el paciente para la actualización del Resumen de Paciente firmada por una autoridad nacional que pueda ser validada por el PCN-B
- El paciente ha sido correctamente con el servicio de identificación
- El profesional dispone del Resumen de Paciente que se quiere actualizar.

1.4.6.3.6. Escenario de éxito principal

Las siguientes acciones se refieren al país de afiliación del paciente:

- El PCN-A valida la firma del PCN-B
- Se verifica que el consentimiento del paciente en del país A sea aplicable a este caso de uso
- Extracción del documento a actualizar desde la petición de actualización
- Aplicar las políticas se seguridad nacional y las políticas de protección de datos del paciente (si aplicable)

- Firmar el éxito de la operación a nivel de PCN-A
- Realizar los apuntes de auditoria que apliquen

1.4.6.3.7. Casos de fallos

La siguiente casuística puede dar lugar a los siguientes errores que se tendrán que gestionar en el servicio:

- No se dan las precondiciones del caso de éxito
- El profesional del país B no tiene suficientes permisos para actualizar el Resumen de Paciente
- Fallo temporal (por ejemplo servicio interno temporalmente inaccesible)

1.4.7. Consentimiento informado de paciente

El consentimiento del paciente es la indicación específica e informada libremente dada por élque significa que está de acuerdo con los datos personales relacionados con su persona que se procesan y que pueden llegar a compartirse fuera de las fronteras del país de afiliación.

Cada paciente tiene derecho a restringir o permitir el acceso de sus datos de salud.

El consentimiento del paciente para la transferencia transfronteriza de datos de salud es una parte importante del proceso de autorización y su gestión es responsabilidad del país de afiliación del paciente.

El consentimiento del paciente es un requisito previo, no para la recopilación de datos si no con el fin de acceder a los datos ya existentes en el país de afiliación.

Se pueden distinguir los procesos para los que se necesita el consentimiento del paciente:

- Para recuperar los datos identificativos del paciente en el país de afiliación desde el país de prestación del servicio médico
- Para poder recuperar los datos del Resumen de Paciente
- Para actualizar los datos del Resumen de Paciente en el país de afiliación una vez realizada la consulta en el país proveedor de servicio.

Principios para el consentimiento del paciente:

- El consentimiento será específico para el traspaso de datos transfronterizos
- El consentimiento se dará libremente.
  - El paciente tiene la libertad de participar o no en este intercambio de datos transfronterizo, sin que exista posibilidad de denegación de prestación de servicio por parte del país prestador.
- El paciente puede retirar su consentimiento en cualquier momento
- Que su consentimiento es libre sin consecuencias si no se da el consentimiento
- Que la recopilación y el procesamiento de los datos de salud del paciente una vez realizada la prestación de servicios médicos es objeto de la legislación de un país proveedor de los cuidados

La gestión de este trámite para el país de prestación de servicio de un paciente afiliado en otro país podría ser informada mediante un Sí/No en la consulta de búsqueda de paciente, considerando un escenario de tramitación del consentimiento simplificado.
Alternativamente, podría implementarse el siguiente servicio:

1.4.7.1. Contexto

Un paciente afiliado en un país A se encuentra en la consulta de un centro de salud de un país B. Se notifica al país de afiliación del paciente A un nuevo consentimiento dado o revocado en el país de prestación del servicio B.

1.4.7.2. Operación

La operación que describe este servicio es la siguiente: nuevoConsentimiento(). La operación permite registrar un nuevo consentimiento en términos de consentido o revocado.

1.4.7.3. Parámetro de entrada

Hay dos tipos de parámetros necesarios:

- Información acerca del nuevo consentimiento dado o revocado
- Aserción SAML que confirma la identidad del profesional del país B
- Aserción SAML que confirma la relación entre el profesional, el paciente y el tratamiento.

1.4.7.4. Parámetro de salida (en caso de éxito)

Estado del consentimiento (dado o revocado).

1.4.7.5. Precondiciones para el caso de éxito

- El solicitante puede localizar al proveedor de servicios
- Existencia del canal seguro entre PCN-B y PCN-A
- Disponibilidad del certificado para establecer la comunicación segura con el PCN-B
- El profesional está correctamente identificado en la infraestructura nacional
- Disponibilidad de una aserción SAML del profesional firmada por una autoridad nacional que pueda ser validada por el PCN-B
- Disponibilidad de una aserción SAML que relacione el profesional con el paciente, mediante el relativo tratamiento firmado por una autoridad nacional que pueda ser validada por el PCN-B
- El paciente ha confirmado el estado del consentimiento a notificar

1.4.7.6. Escenario de éxito principal

Las siguientes acciones se refieren al país de afiliación del paciente:

- El PCN-A valida la firma del PCN-B
- Se extrae la información del consentimiento a actualizar desde la relativa petición
- Se verifica que el consentimiento tramitado es aplicable según las políticas de seguridad del país A
- Se aplica el cambio del estado del consentimiento limitadamente al país prestador del servicio
- Firmar el éxito de la operación a nivel de PCN-A
- Realizar los apuntes de auditoria que apliquen

1.4.7.7. Casos de fallos

La siguiente casuística puede dar lugar a los siguientes errores que se tendrán que gestionar en el servicio:

- No se dan las precondiciones del caso de éxito
- El profesional del país B no tiene suficientes permisos para tramitar un cambio de consentimiento
- Una autenticación del paciente es requerida (por ejemplo firma del documento del consentimiento)
- El país A requiere una copia escaneada del documento de consentimiento
- Los casos siguientes pueden dar lugar a advertencias:
- Los cambios de estado del consentimiento no son procesados por el país de afiliación
- Los cambios de estado del consentimiento no son procesados automáticamente por el país de afiliación, por lo que estos cambios no serán inmediatamente operativos

1.5. Componentes de la arquitectura

La arquitectura que se plantea para este proyecto diferencia dos estructuras. Por un lado, el Punto de Contacto Nacional, que contendrá todos los componentes arquitectónicos comunes, prácticamente podrá proporcionarse como caja negra a cada país que se incorpore a la Red RACSEL y configurar los elementos particulares (certificados y particularidades de conectividad como IPs, puertos, etc.). Toda comunicación en la Red RACSEL se realizará desde y hasta los PCNs de cada país.

Por otro lado, el Conector Nacional será la puerta de entrada y salida a la infraestructura de cada país, dejando libertad en la organización interna, en función de sus leyes, estructura geopolítica y sanitaria, o decisiones que ya estén tomadas o se vayan a tomar en un futuro de carácter interno al país.

1.5.1. Componentes del Punto de Contacto Nacional

La siguiente figura muestra los componentes de la arquitectura del PCN. En azul aquellos componentes que serán fijos para todos los PCN, en gris los que, a pesar de pertenecer al PCN deberán configurarse para cada país, y en naranja los componentes que dependerán completamente del país, que identifica-

mos como el Conector Nacional.

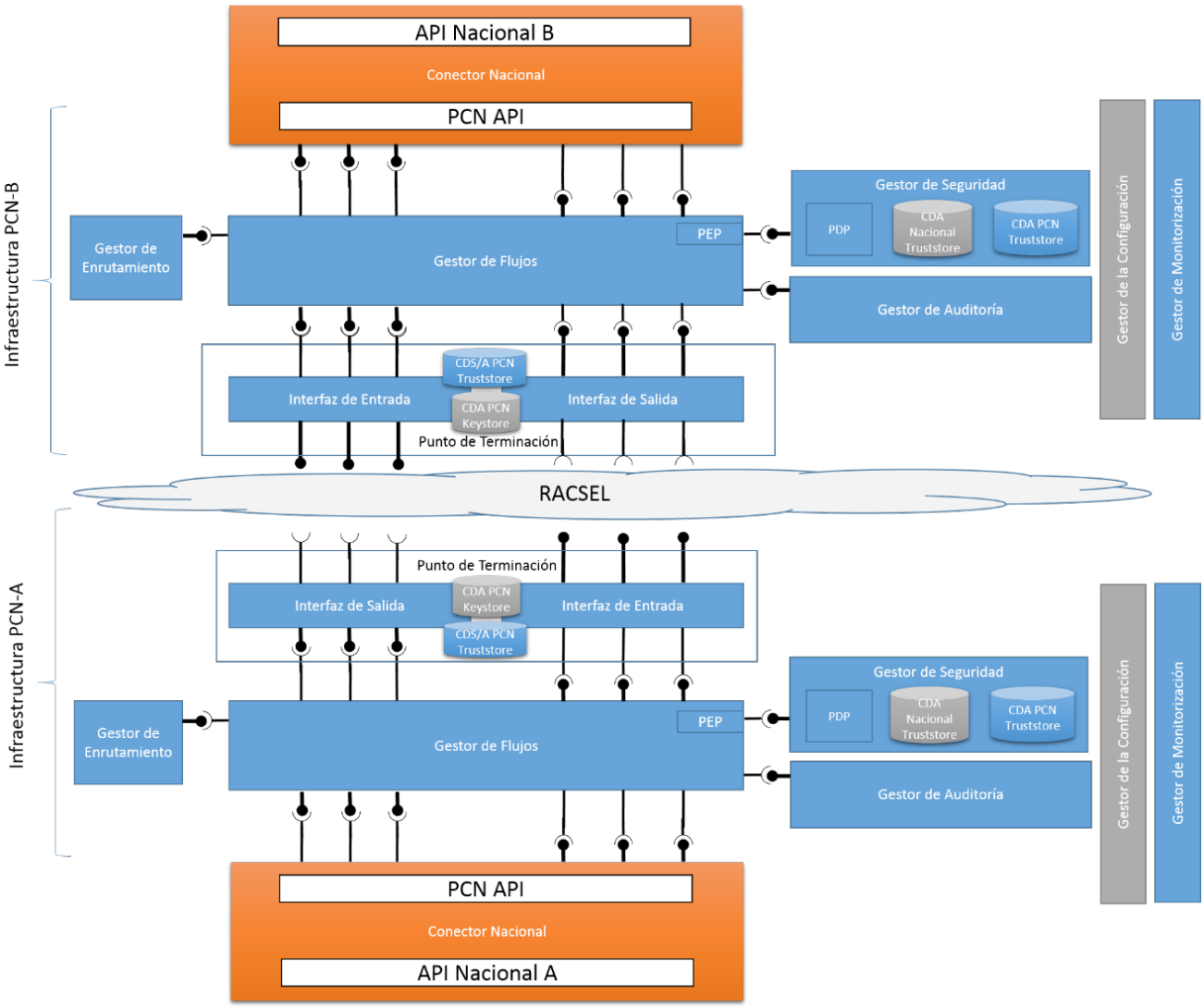


Ilustración 18-Componentes de la Arquitectura de Referencia

El PCN es el único punto de toda la infraestructura que tendrá acceso a la Red transfronteriza RACSEL.

Los siguientes puntos ofrecen una descripción de cada uno de los componentes que conforman el PCN, ofreciendo una serie de recomendaciones para la correcta interpretación de su propósito y, en caso necesario, de cómo integrarlo con diferentes configuraciones nacionales.

Esta interpretación de la arquitectura muestra los actores o roles principales que deben actuar en la construcción de la misma, pero será en la fase de implementación de ésta cuando se concreten los componentes a nivel de infraestructura. Puede haber componentes de infraestructura que cumplan más de un rol, o roles que requieran más de un componente de infraestructura.

1.5.1.1. Punto de Terminación

Conforma la capa de comunicación entre los distintos PCN de la Red. Toda comunicación transfronteriza debe pasar por esta capa, compuesta por un componente de entrada al PCN (Interfaz de Entrada) y por un componente de salida (Interfaz de Salida).

Debido a la sensibilidad de la información a transmitir, deben existir mecanismos de seguridad que garanticen la integridad y confidencialidad de la información. Es por ello, que entre todos los PCN se establece una red de confianza (ver punto 0). Esta red de confianza requiere que los distintos PCN deban conocerse y confiar entre ellos. Esta confianza se realiza mediante el uso de certificados digitales de servidor X509 (CDS).

Así, cada PCN, en su capa de comunicación (Punto de Terminación), requerirá de un par de claves PKI de tipo servidor. La clave privada identificará al PCN del propio país, mientras que la clave pública se distribuirá al resto de países para incorporarla en el almacén de claves de confianza (Truststore), creando de esta forma una red de confianza mutua entre todos los PCNs de la Red RACSEL. De esta forma, todos los mensajes que viajen por la Red RACSEL serán encriptados por el método de Autenticación Mutua (o Autenticación de dos vías), garantizando el nivel de confidencialidad requerido dentro de la propia Red RACSEL.

Además, se debe garantizar la integridad y no repudio de la información que se traspasa entre los diferentes países, por lo que será necesario que cada PCN disponga también de un par de claves PKI de tipo Aplicación (CDA). La clave privada permitirá firmar los mensajes salientes del PCN, mientras que la clave pública permitirá validar las firmas emitidas por otros PCNs en los mensajes entrantes. Estas firmas seguirán los estándares WS-Security para integridad de mensajes, recomendando la firma del Body del mensaje SOAP, así como de todos los elementos que viajen en el Header.

Se deberá garantizar que:

- El almacén de claves públicas debe estar protegido con contraseña
- El almacén de claves privadas debe estar protegido con contraseña
- Las claves privadas deben tener su propia contraseña
- El acceso a los almacenes debe estar restringido a los sistemas que lo utilicen
- El acceso a los almacenes debe estar restringido a los técnicos autorizados
- Los descriptores de los servicios (WSDLs) deben adjuntar la WS-Policy asociada.

1.5.1.1.1. Interfaz de Entrada

La Interfaz de Entrada (o Punto de Terminación de Entrada) representa el punto de entrada para un mensaje que llega a un PCN desde otro PCN.
Publica el conjunto de servicios SOAP sobre HTTPS que permiten a otros PCNs interaccionar con el país en cuestión. Estos servicios serán los mismos para todos los PCNs que conformen la Red RACSEL, dando acceso a la información alojada en cada país de forma unificada y homogénea. Los servicios identificados deben cubrir las necesidades de los procesos definidos:

- Identificación de Paciente
- Obtención del Resumen de Paciente
- Actualización del Resumen de Paciente
- Consentimiento de Paciente

La Interfaz de Entrada se encargará de establecer un canal seguro de comunicaciones con el PCN del

país peticionario, utilizando Autenticación Mutua SSL. Además, debe asegurar el cumplimiento de las políticas WS-Policy definidas para cada servicio, mediante la aplicación o validación de las cabeceras de seguridad WS-Security asociadas al mensaje. Es decir, debe validar la política de seguridad de los mensajes entrantes y firmar las respuestas a estos mensajes.

A nivel infraestructura, se recomienda que este componente:

- Utilice estándares de comunicación HTTP/S de forma nativa
- Utilice estándares SOAP, WS-Security, WS-Policy de forma nativa

1.5.1.1.2. Interfaz de Salida

La Interfaz de Salida (o Punto de Terminación de Salida) representa el punto de salida para un mensaje que debe enviarse al PCN de otro país. Es el encargado, por tanto, de establecer el canal seguro de comunicaciones (SSL Mutual Authentication) con el Inbound Terminator del PCN de destino, para que el mensaje SOAP pueda transmitirse de forma segura manteniendo la confidencialidad del mismo. Al igual que el Inbound Terminator, deberá garantizar el cumplimiento de la política de seguridad definida, firmando los mensajes salientes y validando la política de seguridad de los mensajes entrantes.

A nivel infraestructura, se recomienda que este componente:

- Utilice estándares HTTP/S de forma nativa
- Utilice estándares SOAP, WS-Security, WS-Policy de forma nativa

1.5.1.2. Gestor de Auditoría

La auditoría de las transacciones que pasarán por la Red RACSEL persigue dos objetivos. Por un lado, garantizar la privacidad del paciente con respecto a su información médica y las leyes propias de cada país. Por otro lado, registrar el mensaje firmado por el PCN para garantizar el no repudio del origen del mensaje.

Este componente implementa el actor Audit Record Repository dentro de la transacción ITI-20 de IHE IT Infrastructure Technical Framework. El Gestor de Flujo deberá registrar las peticiones entrantes y salientes y sus respectivas respuestas en el Gestor de Auditoría.

Se debe garantizar la persistencia de todas las peticiones, por lo que será necesario dotar a la infraestructura de algún mecanismo de entrega garantizada al repositorio de auditoría.

De acuerdo al perfil ATNA de IHE y a las características del proyecto, se deberá seguir los siguientes estándares para su implementación:

- RFC-3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
- RFC-5425: Transmisión de Mensajes Syslog sobre protocolo TLS

1.5.1.3. Gestor de Flujo

El Gestor de Flujo es el componente que permitirá orquestar toda la lógica interna del PCN mediante la invocación a los servicios proporcionados por el resto de componentes del PCN, o también los proporcio-

nados por la propia infraestructura nacional, que serán accesibles a través del CN.

El Gestor de Flujo actúa tanto en caso de peticiones entrantes al PCN desde la Interfaz de Entrada, como en las peticiones entrantes al PCN desde el CN, ejecutando para cada servicio un flujo, en el que se compondrá la secuencia de llamadas a los distintos servicios ofrecidos por el resto de componentes.

El Gestor de Flujo se encargará de extraer, del mensaje original, la información necesaria para invocar cada servicio. De esta forma se aísla a los componentes de la complejidad de los casos de uso definidos, enfocándose en un problema menor, lo que favorece la reutilización de los mismos.

Los flujos que se definan tendrán responsabilidades diferentes en función de si el origen de la petición viene del propio país (a través del CN) o de otro país (a través de otro PCN).

La siguiente imagen muestra un escenario en el que un país B realiza una petición al país A, quedando reflejadas las diferentes peticiones y respuestas que se realizan.

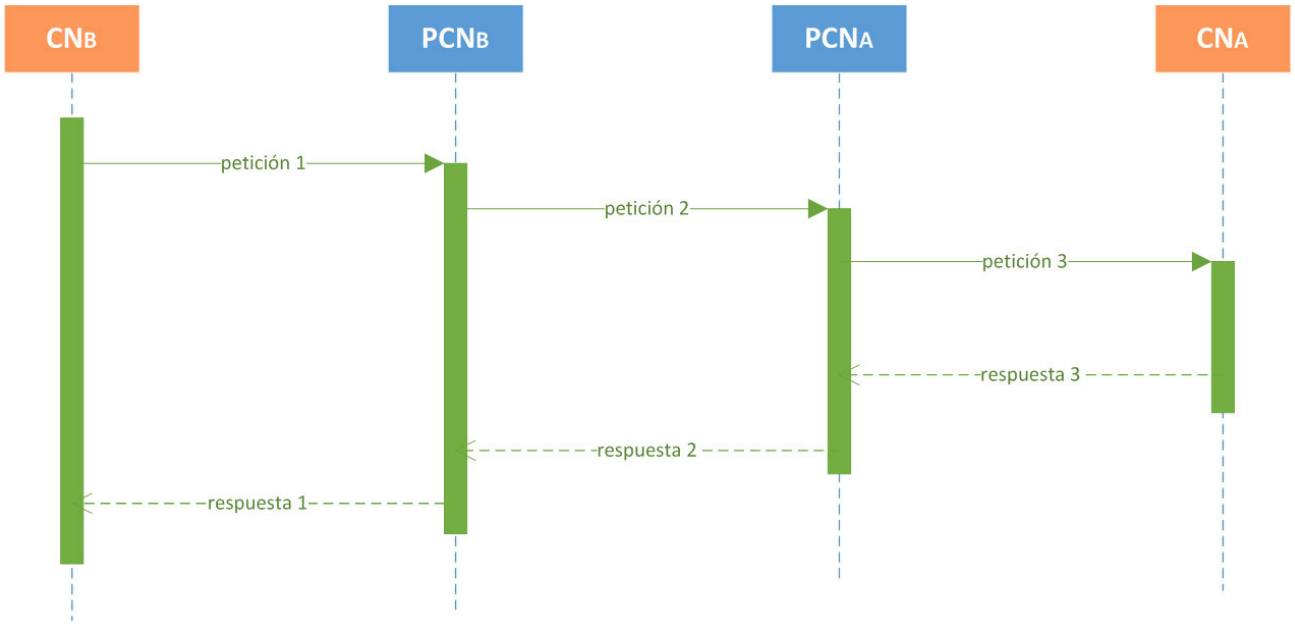


Ilustración 19-Flujo de ejecución del Gestor de Flujo

Esta imagen nos servirá para ilustrar el flujo de ejecución del Gestor de Flujo en función de dónde venga la petición.

Desde el CN del propio país: Las acciones básicas que debe realizar el Gestor de Flujo son:

- Solicitud (en la imagen, petición 1):
  - Una validación sintáctica para comprobar que el mensaje cumple con el XSD definido para el servicio. En caso contrario no permitirá continuar el proceso, devolviendo un error
  - Valida los tokens SAML mediante invocación al Gestor de Seguridad, garantizando que el autor de las peticiones ha sido correctamente autorizado
  - Determina la dirección del país de destino mediante una invocación al servicio del Gestor de Enrutamiento
  - Invoca al servicio de auditoría de forma que todas las peticiones salientes queden registradas para una posible auditoría legal
  - Pasar el flujo a la Interfaz de Salida, que se encargará de transmitir el mensaje al PCN B destino de forma segura

- Respuesta (en la imagen, respuesta 1):

  - Audita la respuesta obtenida, para tener constancia en caso de auditoría legal
  - Envía la respuesta al peticionario a través del CN nacional

Desde otro PCN: Las acciones básicas que debe realizar el gestor de flujo son:

- Solicitud (en la imagen, petición 2):

- Invocar al servicio de auditoría de forma que todas las peticiones entrantes queden registradas para una posible auditoría legal
- Una validación sintáctica para validar que el mensaje cumple con el XSD definido para el servicio. En caso contrario no permitirá continuar el proceso, devolviendo un error
- Invocar al servicio de control de acceso, que realizará las comprobaciones necesarias para garantizar que el peticionario tiene acceso a la información solicitada. Las reglas de acceso y consentimiento se encuentran en el CN
- Invoca al servicio correspondiente al tipo de petición en el CN

- Respuesta (en la imagen, respuesta 2):

- Valida la firma de la respuesta que ha realizado el CN del país, mediante invocación al servicio de validación de firma del Gestor de Seguridad
- Invoca al servicio de auditoría, para dejar registrada la respuesta que se va a enviar al PCN peticionario

Se deberá tener en cuenta la necesidad de:

- Identificación y catalogación de todos los casos de error, para garantizar que todos los países generan y entienden los mismos errores

- El flujo puede tener particularidades dependiendo del servicio que se esté invocando

1.5.1.4. Gestor de Enrutamiento

El Gestor de Enrutamiento consistirá en un registro de direccionamientos transfronterizos, en el que se almacenarán las direcciones de cada PCN de la Red RACSEL. Proporcionará un servicio que permita descubrir el endpoint (dirección) del PCN con el que se desea contactar. Se trata de un componente común, ya que en todos los países se tendrá la misma información.

Se deberá actualizar su contenido cada vez que un país modifique su dirección de integración a la Red RACSEL o cuando se incorpore un nuevo país a la red.

Dado que se trata de un registro de información y de bajo volumen y nivel de actualización, se recomienda utilizar mecanismos de caché que agilicen su consulta, reduciendo los tiempos de latencia debidos a su consulta.

1.5.1.5. Gestor de Configuración

La plataforma PCN requiere de la configuración de ciertos aspectos propios al país, por lo que este componente se encargará de establecer los parámetros necesarios para el correcto funcionamiento y acomodamiento de la plataforma en el país.

La centralización de la configuración en un único componente facilita su gestión y minimiza los riesgos

que pueden ocasionar una parametrización distribuida por componente.

Para facilitar las tareas de configuración se recomienda la utilización de algún mecanismo de notificación de cambio y actualización. Uno de los estándares que facilita la distribución de sitios de confianza es mediante la utilización del estándar TSL (Trust-service Status List) definido por ETSI-TS 102-231 para la distribución y actualización de sitios de confianza. En estas listas pueden distribuirse toda la información referente al conjunto de PCNs (URIs, certificados, CAs, etc.) que forman parte de la red de confianza RACSEL.

1.5.1.6. Gestor de Monitorización

El componente de monitorización es la garantía del correcto funcionamiento de la plataforma PCN. Esta monitorización debe realizarse tanto a nivel técnico, comprobando que todos los componentes y sistemas están funcionando correctamente, como a nivel funcional, realizando comprobaciones sobre los datos que se transmiten, alertando de algún mal funcionamiento.

Se deberán identificar todos los parámetros a monitorizar (disponibilidad de los servicios, recursos, rendimiento, estadísticas), así como la lógica de las reglas que provocarán que se disparen las alarmas.

Debido a la gran diversidad de alarmas y parámetros a monitorizar, este componente puede estar implementado por diferentes productos o sistemas especializados en monitorización y/o análisis de datos, mostrando diferentes cuadros de mando de monitorización en función de la información a mostrar, o lanzando alarmas o avisos en caso de situaciones críticas.

1.5.1.7. Gestor de Seguridad

El componente de seguridad se encargará de realizar las operaciones relacionadas con firma digital y control de acceso. Para ello dispondrá de los siguientes servicios:

- Servicio de validación de firma digital XML. Este servicio debe comprobar que el XML se ha firmado correctamente y se ha utilizado un certificado de confianza. Se deberá indicar el Truststore a utilizar, ya que puede realizar validaciones a nivel nacional o transfronterizo. Este servicio se utilizará para validar los tokens SAML generados por el propio país.

- Servicio de validación de acceso. Cuando el PCN actúa como país de afiliación del paciente (receptor de peticiones), comprobará que el peticionario dispone de la autorización necesaria para poder realizar la petición. Este servicio se basará en el estándar XACML para que, a partir de reglas definidas en el propio país (PIP), determinar (PDP) si el peticionario está autorizado o no.

Para llevar a cabo estas operaciones, será necesario disponer de diferentes Keystores independientes:

- CDA PCN Truststore: Almacén de claves de confianza, que contendrá todas las claves públicas de los certificados de aplicación (CDA) de todos los PCNs. Este almacén se deberá ir actualizando a medida que se vayan incorporando nuevos PCNs a la Red RACSEL, o se vayan renovando los certificados de los distintos PCNs

- CDA Nacional Truststore: Almacén de claves de confianza, que contendrá todas las claves públicas de los certificados de aplicación (CDA) de aquellos sistemas/aplicaciones que podrán realizar peticiones al PCN del propio país.

1.5.2. Componentes Nacionales

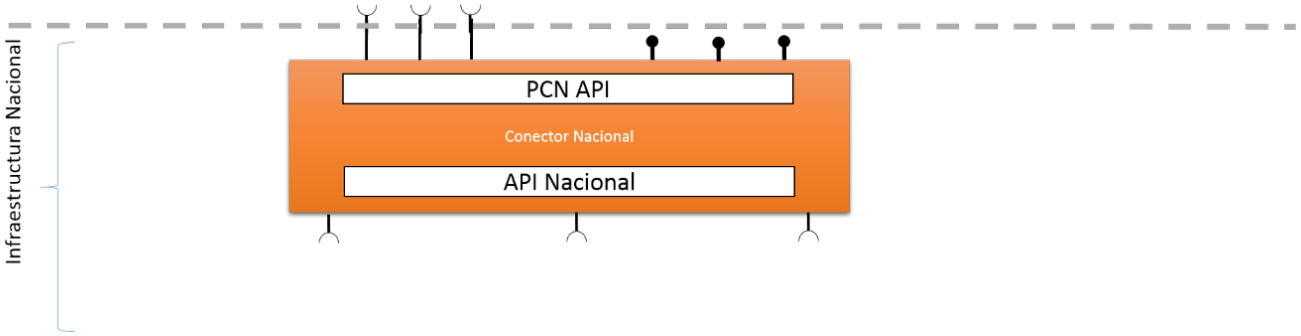


Ilustración 20-Conector Nacional – vista genérica

El Conector Nacional es la pieza lógica de la infraestructura de componentes de la arquitectura que constituye el punto de entrada y salida de la comunicación entre cada PCN y la implementación específica de la infraestructura nacional subyacente.

Por un lado, tendremos la interface del PCN de la Red RACSEL, la PCN API que proporciona:

- El punto de entrada para la realización de peticiones transfronterizas a partir de una entidad prestadora de salud del país que proporciona el servicio médico en el formato establecido por la Red RACSEL

- El punto de salida de peticiones transfronterizas de cara a una infraestructura nacional para la recuperación de datos médicos del país de afiliación del paciente en el formato establecido por la Red RACSEL

Y por otro tendremos la API Nacional que proporciona las interfaces de los mismos servicios en el formato nacional.

Más en detalle, los componentes de la infraestructura nacional que tienen que intervenir en las transacciones previstas son los detallados a continuación.

1.5.2.1. Componente Autoridad Proveedora de las Identidades de los Profesionales

La misma autoridad (o componente) que identifica al profesional en la infraestructura nacional cuando se conecta al sistema de salud local debería que ser capaz de emitir una aserción SAML2 (o Token SAML) firmada digitalmente para pasar la identidad del profesional correspondiente a la petición del servicio solicitado. Esta autoridad puede ser o bien un Servidor de Identidades (IDP), o bien un STS (Servicio de Token Seguro).

Más concretamente, en el caso del servicio de identificación de paciente, este componente debería emitir un Token SAML que formalice la identidad del profesional que pide la información. Además, para el servicio de recuperación del Resumen del Paciente, el mismo componente también debería poder emitir otro Token SAML firmado digitalmente que establezca la relación de tratamiento entre el profesional que pide la información y el paciente objeto de la consulta transfronteriza y propietario de los datos.

Veremos más adelante como estas aserciones SAML pueden estar relacionadas entre sí, y como este componente puede ser más o menos distribuido en la infraestructura nacional, dependiendo de la organización y del nivel de centralización de la misma.

1.5.2.2. Componente de Seguridad

El Componente de Seguridad proporciona los siguientes servicios:

- Administración y evaluación de políticas de seguridad con la finalidad del control de acceso y la autorización al uso de la Red RACSEL por parte del profesional, cuando un país actúa como prestador de servicio

- Administración y evaluación de políticas de seguridad para el control de acceso transfronterizo del uso de los datos clínicos del paciente solicitado por un profesional de otro país miembro de la Red RACSEL, cuando un país actúa como país de afiliación del paciente. Este servicio será publicado en el CN y consumido por el Gestor de Seguridad del PCN-A bajo la forma de un servicio XACML (ver sección 1.0

- Gestión del Consentimiento para la comunicación de datos transfronterizos y/o para tratamientos específicos desde otro país miembro. Este servicio será publicado en el CN y puede ser implementado con unas políticas XACML (ver sección 1.0).

Opcionalmente:

- Firma de la mensajería SOAP saliente para garantizar la no modificación del cuerpo del mensaje y su consecuente integridad o no repudio con la clave privada del Certificado Digital de Aplicación (CDA) del CN almacenado en el almacén de claves del mismo componente de seguridad. Se recomienda la adopción de WS-SecurityPolicy para la definición de las políticas de firma de todos los elementos del Header y del Body del mensaje SOAP.

Esta última funcionalidad puede ser obviada considerando que la comunicación saliente hacia el PCN-X solo puede establecerse a partir del CN-X e implementando todas aquellas medidas de seguridad perimetral que correspondan.

1.5.2.3. Componente de Auditoria Nacional

Para la trazabilidad de las peticiones hecha en el país prestador de servicio o bien para documentar la información recuperada y/o modificada en el país de afiliación del paciente.

1.5.2.4. Componente Servidor Terminológico

Es el componente que proporciona el servicio de transformación semántica de términos y códigos (por ejemplo OID's) adoptados a nivel nacional hacia los definidos en los catálogos RACSEL y viceversa.

1.5.2.5. Componente de Transformación Sintáctica

Este componente se ocupa de traducir el formato de la comunicación nacional al definido por la Red RACSEL (por ejemplo XML propios o JSON IHE) y viceversa. Este componente solo se aplica cuando la infraestructura nacional no soporta o no es compatible con IHE.

1.5.2.6. Componente que implementa el Servicio de Identificación de Paciente

La implementación de este servicio será más o menos complejo dependiente del nivel de centralización del repositorio de pacientes gestionado en la infraestructura nacional. La gestión de un MPI simplifica la

identificación única de un paciente.

1.5.2.7. Componente que implementa el Servicio de Recuperación y Actualización de Resumen de Paciente

Una vez identificado el paciente, la implementación de esos servicios permite obtener sus datos o actualizarlos y persistirlos en el repositorio nacional/local. Este servicio será más o menos complejo dependiendo del nivel de centralización de la información clínica del paciente.

1.5.2.8. Comunicaciones

En cuanto a la seguridad en las comunicaciones a nivel de transporte, se plantea la adopción del siguiente protocolo de encriptación:

- Infraestructura Nacional ←→ Conector Nacional: TLS v1.2 2 Way, Autenticación Mutua, en la que el sistema de información HCE del prestador de servicio de salud verifica la identidad del CN. Éste verifica la procedencia o la identidad del sistema de información HCE del prestador que lo invoca.

  Para establecer este tipo de comunicación ambas partes deben registrar la clave pública del certificado de servidor de la otra parte en un almacén de certificados de confianza. La privacidad del canal de comunicación y la integridad de los datos transmitidos serán así garantizadas por el algoritmo de encriptación del mismo.

- Conector Nacional → Punto de Contacto Nacional y viceversa: TLS v1.2 1 Way

  La adopción de autenticación 1 way para este caso es debido a que la procedencia (o la autenticación de la aplicación cliente) queda garantizada por la firma del envoltorio SOAP por parte de la aplicación que origina la comunicación. Para establecer este tipo de conexión el CN debe disponer de un almacén de certificado de confianza configurado con la clave pública del certificado de servidor (CDS) del PCN. Por el contrario, el PCN debe disponer de un almacén de certificado de confianza configurado con la clave pública del certificado de servidor (CDS) del CN.

1.5.3. Interacción de los componentes nacionales

Una vista más detallada de este componente según el ámbito de aplicación de los casos de uso correspondientes puede ayudar a concretar más sus funciones y responsabilidades. Puesto que los servicios soportados por la Red RACSEL son:

- Identificación de Paciente (paciente A en país B, paciente identificado en país B)
- Obtención de Resumen de Paciente (paciente A en país B, Resumen de Paciente recuperado del país A)
- Actualización de Resumen de Paciente (paciente A en país B, Resumen de Paciente A generado en el país B, se envía a país A)
- Servicio de Gestión de Consentimiento (paciente A en país B autoriza la comunicación transfronteriza de sus datos personales o para un tratamiento en concreto).

Mostraremos los siguientes esquemas:

- Vista de la infraestructura nacional que soporta IHE:
- Vista CN B → PCN-B, cuando la infraestructura nacional del país actúa como prestador del servicio sanitario
- Vista PCN-A → CN A, cuando la infraestructura nacional actúa como país de afiliación del paciente.
- Vista de la infraestructura nacional que no soporta IHE:
- Vista CN B → PCN-B, cuando la infraestructura nacional del país actúa como prestador del servicio de salud;
- Vista PCN-A → CN A, cuando la infraestructura nacional actúa como país de afiliación del paciente.

Esta distinción resulta necesaria para matizar de una forma exhaustiva el comportamiento del CN cuanto éste actúa como prestador de servicio o bien como país de afiliación del paciente, ya que cada CN tendrá que soportar las dos modalidades. A parte, se diferencia el caso que la infraestructura nacional sea capaz de ser compatible con IHE. Es el caso en que el CN expone una API Nacional compatible con IHE, lo cual comporta que los cuatro servicios definidos anteriormente pueden ser invocados desde la infraestructura nacional sin la necesidad de pasar por un paso intermedio de transformación sintáctica o cambio de formato (XML propio / JSON IHE no necesario).

1.5.3.1. Vista de la infraestructura nacional que soporta IHE

En este apartado se hace hincapié en la arquitectura de componentes del CN, por lo tanto, las referencias a los componentes internos al PCN serán mínimas, es decir que solo se indicarán aquellos componentes que tienen una implicación directa con el caso examinado.

1.5.3.1.1. Caso 1: Vista CN B → PCN-B con infraestructura nacional compatible

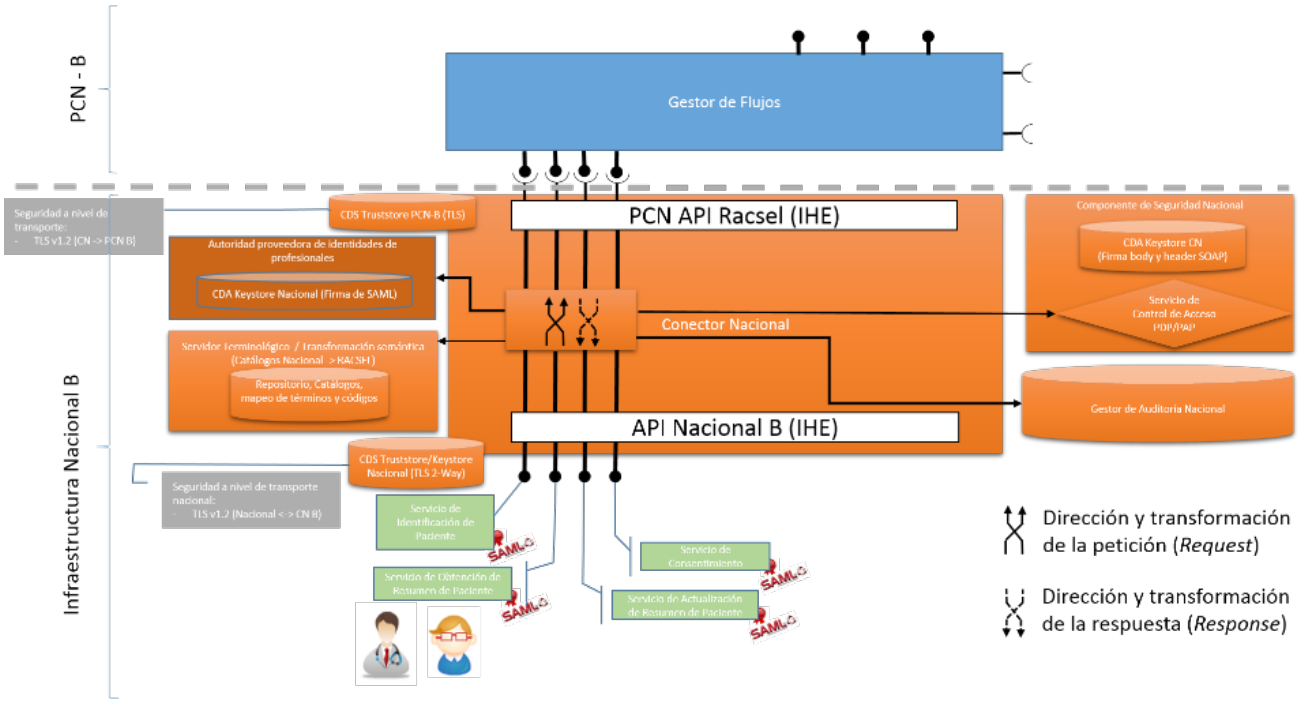


Ilustración 21-Infraestructura nacional / CN del país prestador del servicio médico, compatible IHE

En este contexto los actores que participan son:

- Las entidades proveedoras de salud del país B
- El profesional Prof B del país prestador del servicio B
- El paciente Pac A del país A que está atendido por el Prof B en un centro de salud del país B
- La infraestructura nacional del país B, que soporta IHE
- El CN del país B
- El PCN del país B (PCN-B)

Si observamos el CN, podemos comprobar que en la parte inferior de la interface nacional del mismo presenta una capa de API Nacional compatible con IHE lo que quiere decir que la infraestructura nacional puede prescindir de un paso intermedio de transformación sintáctica de formato. Aun así, los componentes de la infraestructura nacional que tienen que intervenir en la transacción son los detallados a continuación:

- El Componente Autoridad Proveedora de las Identidades de los Profesionales
- El Componente de Seguridad, por lo que se refiere al servicio de control de acceso del profesional y opcionalmente, al servicio de firma de los elementos Header y Body del SOAP
- El Componente de Auditoria Nacional
- El Componente Servidor Terminológico, ya que los términos y los códigos adoptados a nivel nacional y a nivel RACSEL pueden ser distintos

Cuanto a la seguridad en las comunicaciones a nivel de transporte vale lo comentado anteriormente.

1.5.3.1.2. Caso 1: Vista PCN-A → CN A con infraestructura nacional compatible IHE

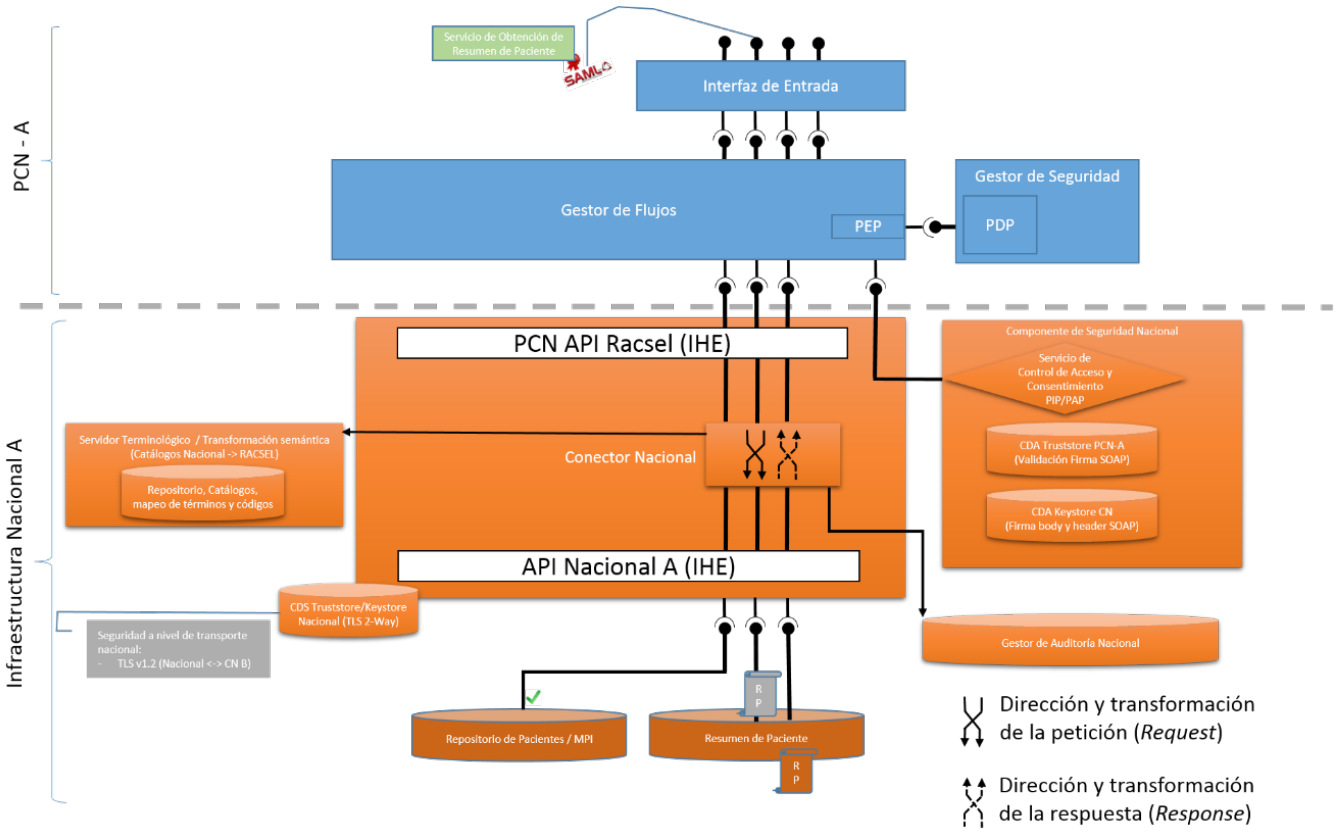


Ilustración 22-Componentes Infraestructura nacional / CN del país de afiliación del paciente, compatible IHE

En el contexto del país de destino nos centramos en una petición de ejemplo de Resumen de Paciente entrante al CN del país de afiliación, por la que los actores que participan en la transacción son:

- La infraestructura nacional del país de afiliación del paciente A, que soporta IHE
- El CN del país A
- El PCN del país A (PCN-A)
- Una petición de Resumen de Paciente entrante al CN A, solicitada por el Prof B para el Pac A desde el país B (ver el caso anterior)

El PCN-A establece la conexión TLS v1.2 con el CN A e invoca el servicio de Recuperación del Resumen de Paciente en el CN A en formato IHE RACSEL. El CN valida la firma del PCN-A aprovechando el certificado registrado en el almacén de certificado de confianza CDA del PCN-A ubicado en el Componente de Seguridad Nacional y se audita la petición. Nótese que a este nivel ya no se tiene que validar la firma del SAML, ya que la validación de la misma se realizó anteriormente en el PCN-B, que es un componente ubicado en la red segura. A continuación, se realizan las transformaciones semánticas pertenecientes aprovechando el servidor terminológico para que la implementación del servicio backend de recuperación de paciente pueda invocarse correctamente en el idioma y en la codificación nacional. La llamada se segurizará con TLS v1.2 2 Way. Una vez recuperado el documento, la respuesta se vuelve a pasar por el servicio terminológico para traducir los términos y códigos en conformidad al mapeo establecido para la comunicación con la Red RACSEL. Finalmente, la respuesta SOAP con el Resumen de Paciente obtenido se firmará por el CN a través del certificado CDA presente en su almacén de claves privadas, se auditará y se pasará al PCN-A para la transmisión transfronteriza.

Los componentes de la infraestructura nacional que tienen que intervenir en la transacción son los detallados a continuación:

- El Componente de Seguridad, por lo que se refiere al servicio de:
  - Control de acceso transfronterizo a los datos del paciente, por parte del país B de origen de la consulta
  - Gestión del consentimiento del paciente. En este proceso el servicio de gestión del consentimiento ya se habrá evaluado por medio de una invocación previa al servicio publicado en el CN A, desde el PCN-A
  - Validación de la firma del PCN-A
  - Firma del CN para asegurar la integridad de los datos recuperados
- El Componente de Auditoria Nacional
- El Componente Servidor Terminológico, ya que los términos y los códigos adoptados a nivel nacional y al nivel RACSEL pueden ser distintos
- El servicio de Identificación de Paciente (en cuanto paso previo a la recuperación del Resumen de Paciente)
- El servicio de Recuperación del Resumen de Paciente

En cuanto a la seguridad en las comunicaciones a nivel de transporte sirve lo comentado anteriormente.

1.5.3.2. Vista de la infraestructura nacional que no soporta IHE

A continuación, se puede evaluar la diferencia en el procesamiento de peticiones con una infraestructura que no soporta IHE. El ejemplo descrito será equivalente al anterior y por claridad separado según el rol asumido por el CN en cada casa de uso.

1.5.3.2.1. Caso 2: Vista CN B → PCN-B con infraestructura nacional no compatible IHE

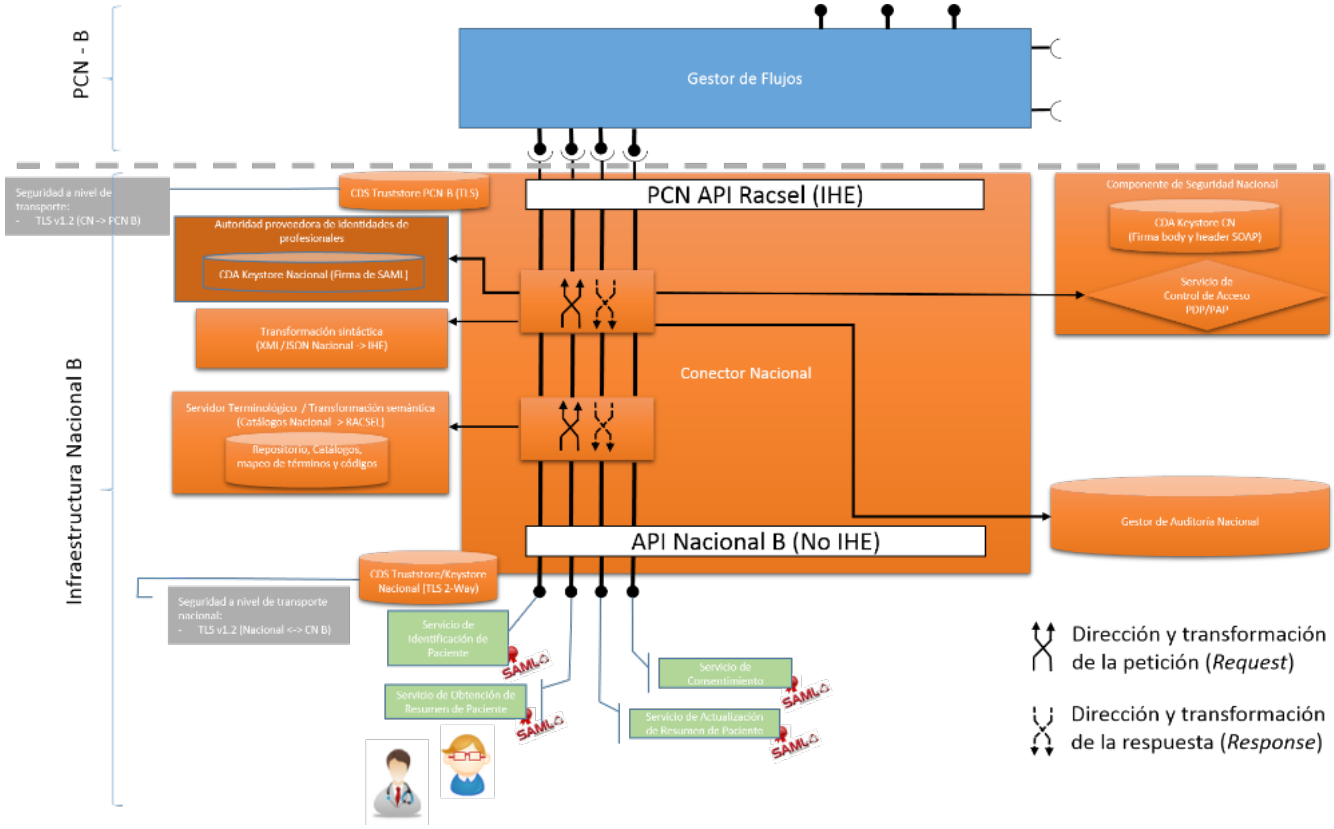


Ilustración 23-Infraestructura nacional/CN del país prestador del servicio médico, no compatible IHE

Observamos como los actores y los componentes que participan en este caso de uso son los mismos que los descritos en el apartado 1.0 – Caso 1: Vista CN B → PCN-B, con la única diferencia que para completar la comunicación hacia o desde la infraestructura nacional será necesario un paso más de transformación de formato de la mensajería de IHE al idioma nacional (XML propios / JSON) y viceversa.

1.5.3.2.2. Caso 2: Vista PCN-A → CN A con infraestructura nacional no compatible IHE

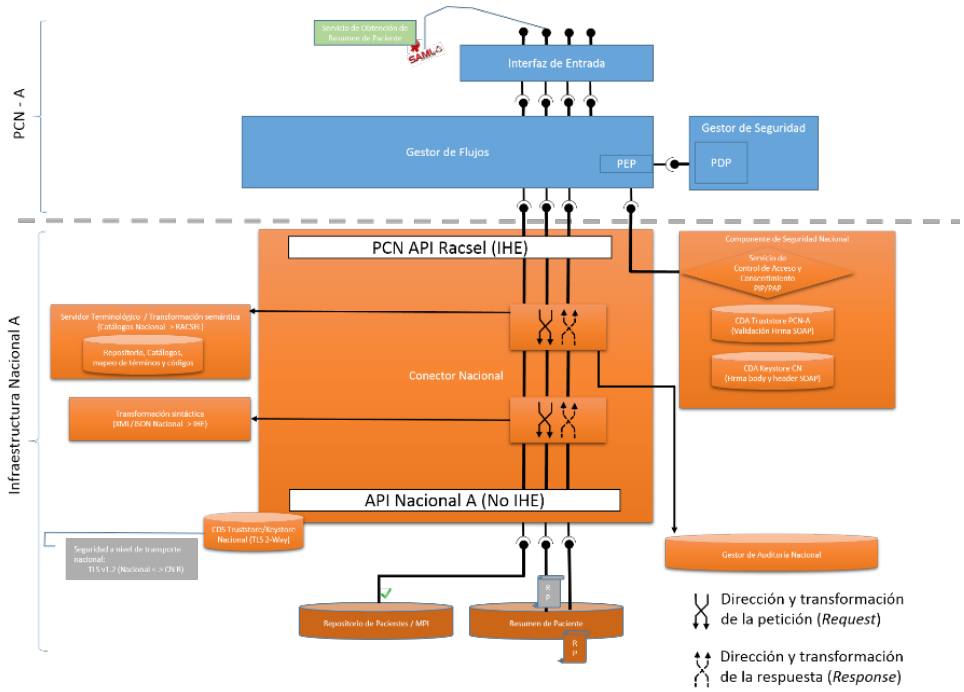


Ilustración 24-Infraestructura nacional / CN del país de afiliación del paciente, no compatible IHE

Observamos como los actores y los componentes que participan en este caso de uso son los mismos que los descritos en el apartado ¡Error! No se encuentra el origen de la referencia.–Caso 1: Vista PCN-A → CN A, con la única diferencia que para completar la comunicación hacia o desde la infraestructura nacional será necesario un paso más de transformación de formato de la mensajería de IHE al idioma nacional (XML propios / JSON) y viceversa.

1.5.4. Red de confianza RACSEL

Para poder establecer una red de confianza transfronteriza, se utilizarán diferentes herramientas que garanticen la confidencialidad y privacidad de la red y las comunicaciones. Todos los países dispondrán de un único punto de acceso a la Red RACSEL, denominado PCN el cual actuará de nexo de unión entre la Red RACSEL y el resto de la infraestructura de ámbito sanitario del país.

Dentro del PCN, es el Punto de Terminación (Interface de Entrada e Interface de Salida) quien realiza esta función de separador de fronteras, por lo que deberá disponer, al menos, de:

- Una interfaz de red disponible para conectar con la Red RACSEL;

- Una interfaz de red disponible para conectar con la red nacional.

La interfaz de red para RACSEL debe permitir conectar con una red virtual privada (VPN) que permitirá al PCN ver el resto de PCNs de la red. Las características de esta VPN se deberán determinar en el momento de implantación del proyecto (por ejemplo IPSec, según la especificación RFC 4301). Dentro de esta VPN sólo estarán visibles los Puntos de Terminación de cada país, quedando oculta el resto de los sistemas y componentes.

La interfaz de red para la red nacional dará acceso al resto de componentes del PCN, incluido el CN, lo que permitirá el flujo de comunicaciones entre la red nacional y la Red RACSEL.

La red de confianza se apoya también en el uso de tecnología X509 mediante:

- Certificado Digital de Servidor (Certificados CDS): Toda comunicación entre 2 PCNs se realizará mediante Autenticación Mutua TSL v1.2*, según la especificación RFC 5246. Esto garantizará:

  - Los PCNs deben conocerse y confiar entre sí, ya que previo al intercambio de información, cada PCN valida el certificado del otro PCN
  - El mensaje viaja encriptado por el canal de comunicación, de forma que solo los 2 PCNs que participan en la comunicación saben desencriptar el mensaje
  - Implementación del perfil ATNA, transacción ITI-19, tal y como se especifica en el documento [IHE ITI TF a].

- *: El protocolo TLS v1.2 mejora de forma sustancial las versiones anteriores, el algoritmo criptográfico y proporciona soporte para funciones hash de 256 bits (familia SHA-2).

- Certificado Digital de Aplicación (Certificados CDA): Estos certificados permitirán firmar el mensaje emitido por un PCN, y validar la firma por el PCN receptor. La firma del mensaje garantiza la integridad del mensaje (el mensaje no ha sido modificado) y el no repudio (el mensaje ha sido emitido por el propietario del certificado);

- La sincronización entre los nodos PCNs estará garantizada por la adopción del perfil de Integración IHE Consistent Time y Network Time Protocol (servicios NTP), según la especificación RFC 1305.

1.5.5. Autenticación del profesional y aserciones SAML

La autenticación del profesional es una tarea exclusiva del país prestador del servicio sanitario, por lo que el planteamiento de esta arquitectura no genera restricciones sobre las modalidades de autenticación del profesional en su entorno de trabajo institucional local. Lo que sí se requiere es una prueba que esta autenticación se haya producido, que esta marca esté disponible y pueda ser validada en la red de confianza RACSEL en un formato estándar para que se pueda compartir con el resto de los países miembros. De esta forma las distintas partes involucradas podrán ejecutar su lógica de negocio sin tener que identificar el peticionario ya que esta tarea se ha llevado a cabo por un servicio de autenticación tercero de confianza.

Una Aserción SAML (o un Token SAML 2.0) es un estándar basado en XML (OASIS SAML 2.0 Assertions) para el intercambio de datos de autenticación y autorización entre dominio seguros, es decir entre un proveedor de la identidad (o productor de aserciones) y un proveedor de un servicio (o consumidor de aserciones).

El contexto de la identidad está contenido en los atributos contenidos en la aserción que a su vez están respaldados por la firma digital del componente que la ha emitido.

En el contexto de la Red RACSEL el intercambio de datos transfronterizo se seguriza con hasta dos aserciones SAML que atestan por un lado la autenticidad del profesional (Aserción HCP) y por otro la existencia de una relación de tratamiento (Aserción TRC) entre el paciente y el profesional. Cuanto a los atributos contenidos por los dos tokens, la aserción SAML HCP contendrá los datos identificativos del profesional, su rol y del centro de la prestación de servicio mientras que la aserción SAML TRC contendrá el identificador único del paciente, podrá contener cualquier atributo que describa el contexto del tratamiento y estará enlazada a la anterior aserción del profesional (HCP) por medio de un elemente de enlace saml:Advise. Los dos Tokens SAML tendrán que ser emitidos por el mismo componente o la misma autoridad emisora.

Es importante observar como la presencia de un atributo PurposeOfUse en la aserción TRC cuyo valor sea Emergencia en lugar de Tratamiento (caso normal) activará las reglas del control de acceso especiales del riesgo vital de la Red RACSEL. Un ejemplo de dicha gestión puede ser el acceso a la información del paciente en el país de afiliación por parte de un país prestador de servicio médico sin consentimiento previo por parte del mismo paciente debido a su incapacidad.

Asimismo, la presencia de un atributo AuthorizationConsent podría contener el identificador de la política de privacidad del paciente relativamente a un consentimiento o bien la misma política de privacidad para que sea evaluada por el sistema de control de acceso del país de afiliación.

Por lo tanto, el uso de dichas aserciones también permite el control de acceso tanto a nivel de la Red RACSEL, como a nivel nacional. Por ejemplo, a nivel RACSEL podrían existir políticas de acceso que restrinjan el uso de la red a particulares roles (médicos, enfermeros/as, etc.) mientras que a nivel nacional puede facilitar la evaluación de control de acceso basadas en políticas de seguridad propias del país de afiliación del paciente.

Con el diagrama de secuencia que veremos a continuación se muestra la gestión de las aserciones SAML en el contexto del país prestador del servicio sanitario y la interacción de los varios componentes de la arquitectura de referencia involucrados, tanto para la parte nacional como para la parte común del PCN-B. Por motivos de simplicidad hemos obviado algunos detalles como por ejemplo el establecimiento de las conexiones seguras entre componentes, el Gestor de Enrutamiento y la validación de la firma de la mensajería SOAP.

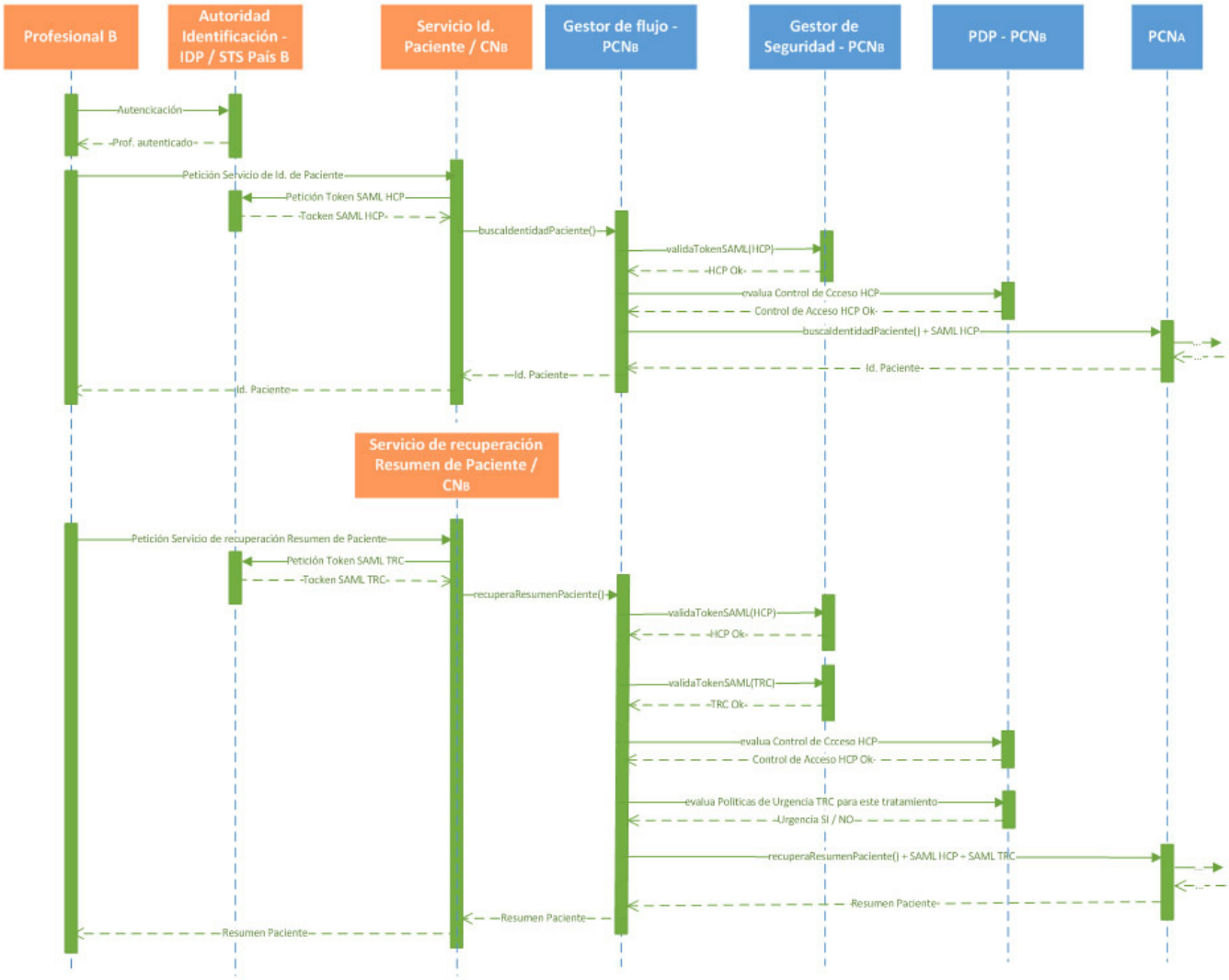


Ilustración 25-Diagrama de secuencia – Gestión de aserciones SAML al país de prestación del servicio

El perfil XUA (Cross-Enterprise User Assertion) regula el uso de estas aserciones en transacciones empresariales y es aceptado por IHE como un perfil de seguridad y control de acceso compatible con el intercambio de información médica transfronteriza. Todos los servicios soportados en la Red RACSEL tendrán que tener estas aserciones presentes en la mensajería de los respetivos servicio web e incluida en el elemento <wsse:Security> de la sección Header del envoltorio SOAP, según se indica en la siguiente tabla:

Servicio RACSEL	Aserción SAML HCP	Aserción SAML TRC
Identificación de Paciente	Sí	No
Recuperación de Resumen de Paciente	Sí	Sí
Actualización del Resumen de Paciente	Sí	Sí
Gestión del Consentimiento	Sí	Sí

1.5.5.1. Centralización de HIS y de las autoridades proveedoras de las identidades profesionales

En los apartados 1.0 y 1.0, se ha podido comprobar como una adecuada estructuración de los servicios de HIS y de las autoridades proveedoras de las identidades de la infraestructura nacional es un elemento muy importante a la hora de construir por encima de ellos un sistema de comunicación distribuido entre países.

Hay múltiples servicios que se requiere que estén disponibles y que afectan directamente a la organización de la información en la infraestructura nacional y cuya implementación pueden resultar mucho más sencilla y eficaz con un sistema centralizado.

A continuación, se ilustran unos ejemplos de posible organización de la gestión de las identidades de profesionales a nivel nacional.

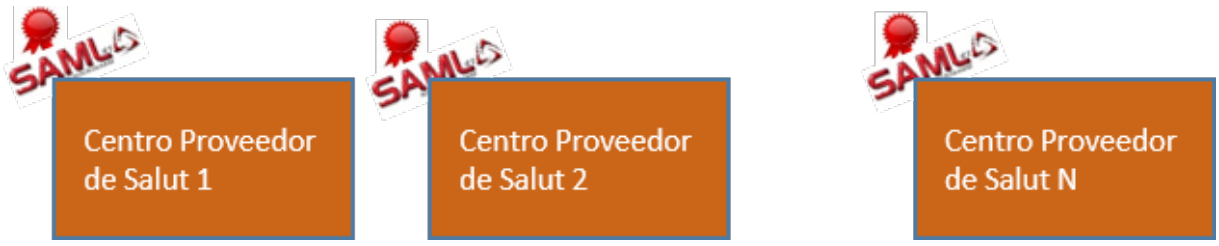


Ilustración 26-Componente de gestión de las identidades – organización punto a punto

En este caso los distintos centros prestadores de servicios de salud son los responsables de autenticar los profesionales de cada centro. Este tipo de gestión, aunque posible, dificulta la integración de cualquier servicio de nivel superior que se tendrá que ofrecer en todos los centros.

Ilustración 27-Componente de gestión de las identidades – organización federada por región sanitaria

En este caso la gestión es semicentralizada, es decir que la resolución de las identidades es mantenida por un repositorio común por región sanitaria. Con este planteamiento el despliegue de un nuevo servicio que involucre la identidad de los profesionales será inmediatamente eficaz a nivel regional.

Ilustración 28-Componente de gestión de las identidades – organización centralizada a nivel nacional

Con este tipo de centralización a nivel de país la integración con un servicio a nivel nacional estará disponible de inmediato para todos los profesionales de cualquier entidad proveedora de salud ubicados en cualquier área sanitaria.

A la hora de implementar un nuevo servicio común la gestión descentralizada de según qué componente de la infraestructura nacional implica más trabajo para el descubrimiento de los repositorios que mantienen la información que se solicite. Esto aplica directamente al servicio de identificación de paciente y al tipo de repositorio de usuario que se plantee, (por ejemplo MPI u otra organización más distribuida) o al mismo servicio de gestión del Resumen de Paciente. Otro campo de acción puede ser el mantenimiento de un repositorio de políticas de control de acceso a los datos y/o temas de privacidad. Dichas políticas pueden afectar a todo el país de igual manera o bien a regiones autonómicas, por lo que, una correcta estructuración de estos repositorios facilita el acceso a los datos de interés, su control de acceso y la interoperabilidad entre centros distintos.

A efectos prácticos, estas autoridades pueden ser vistas o bien como un Servidor de Identidades (IDP), o bien como un servicio Servicio de Token Seguro (STS) al que los componentes del CN pueden hacer referencia vía WS-Trust para pedir el Token.

1.5.6. Servicio de Control de Acceso y XACML

En el contexto de seguridad de la Red RACSEL existen tres tipos de políticas de control de accesos:

- Las políticas de privacidad del paciente
- Las políticas del consentimiento del paciente
- Las políticas de protección de datos específicas definidas por un estado miembro según la legislación vigente

Existen distintos paradigmas para asegurar el complimiento de estas políticas:

- Listas de Control de Acceso (ACL), donde se asigna a cada persona un recurso y una regla para poder acceder, de difícil mantenimiento dada la multitud de actores involucrados
- Control de Acceso Basado en Roles (RBAC), que es más efectivo de cara al mantenimiento, pero presenta el problema inverso de no tener una granularidad tal para poder diferenciar entre un actor en concreto;
- Control de Acceso Basado en Atributos (ABAC), que extiende el modelo RBAC con la posible evaluación de otros atributos
- Control de Acceso Basado en Políticas (PBAC), donde las políticas son un conjuntos de recursos y un conjunto de reglas. Este es el caso que refleja mejor los casos de uso del entorno RACSEL ya que cada país puede tener sus propias políticas, las cuales serán administradas autónomamente. Lo mismo aplica para el paciente acerca del consentimiento.

La tecnológica OASIS Extensible Access Control Markup Language (XACML) proporciona un modo para especificar una política en un formato entendible por la máquina y es un estándar que define un formato de intercambio de políticas de autorización entre sistemas.

Los actores que participan son los siguientes:

- Punto de Administración de Políticas (PAP), que permite la creación de las políticas a nivel nacional o internamente en el PCN

- Repositorio de las Políticas (PR), donde se almacenan dichas políticas

- Punto de Decisión de Políticas (PDP), es el componente que toma la decisión tras la evaluación de las políticas y retorna: Permitido, Denegado o Indeterminado/No aplicable. En el caso de RACSEL todo lo que no se pueda determinar será Denegado

- Punto de Aplicación de Políticas (PEP), es el componente que desde el PCN permite forzar la evaluación de políticas al CN, haciendo posible la implementación de políticas de seguridad diferentes en cada país

- Punto de Información de Políticas (PIP), con que el PDP puede recuperar más atributos, recursos o datos para la evaluación de sus políticas, en caso de necesitarlos.

Veremos a continuación un ejemplo de interacción de estos componentes para el caso de la recuperación del Resumen de Paciente:

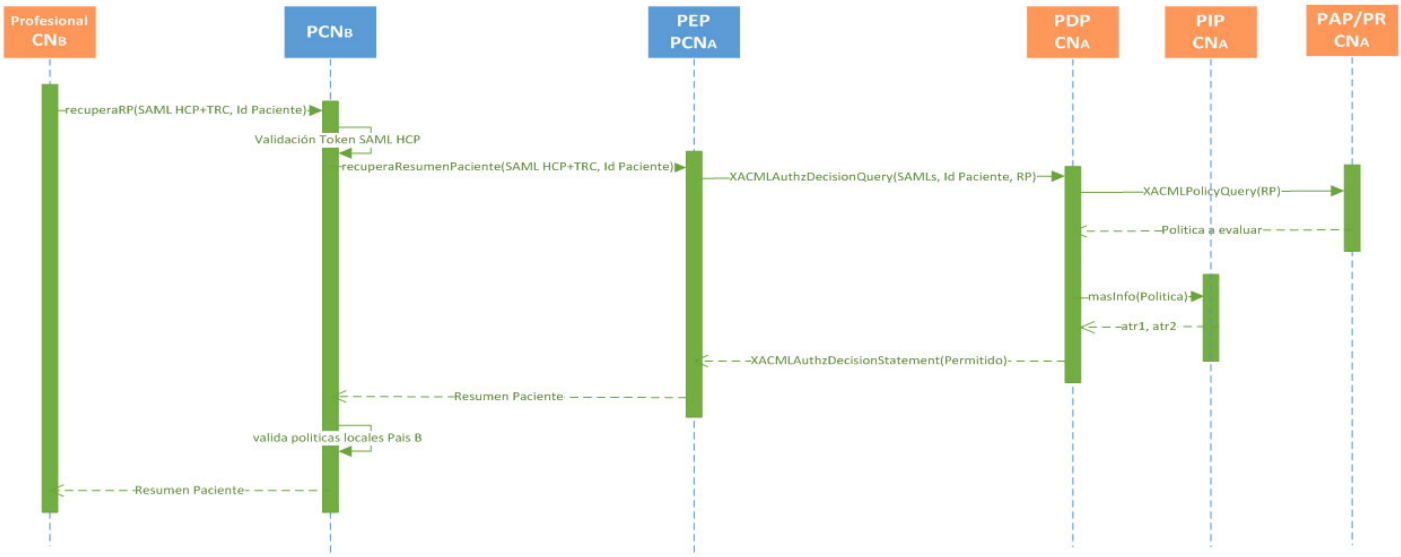


Ilustración 29-Diagrama de secuencia – Flujo del servicio de control de acceso basado en XACML

El profesional del país B realiza la consulta del Resumen de Paciente para el paciente que tiene en el dispensario médico. El PCN-B valida el Tocken SAML del profesional y envía la petición al PCN-A.

Dicha petición se interceptará por el PEP del PCN-A (ver. Fig. XX o Fig. YY) que se encargará de crear una petición XACMLAuthzDecisionQuery() pasando al PDP de la infraestructura nacional del país A el SAML, el identificador del paciente y el contexto de la petición (Resumen de Paciente). El PDP se encargará de recuperar las políticas que apliquen en el contexto de la petición por medio del PAP. A parte el PDP para la evaluación de las políticas a evaluar podría necesitar de más información, que puede recuperar con una invocación al componente PIP (recuperación de más datos locales a la infraestructura nacional). Una vez el PEP haya tomado una decisión, la notifica al mismo del país B con un XACMLAuthzDecisionStatement(Permitido). El PCN-B puede a su vez forzar la evaluación de sus políticas nacionales, esta vez a protección del profesional, aprovechando el PDP interno al PCN-B. Finalmente el PCN-B devuelve el Resumen de Paciente al peticionario.

1.5.6.1. Gestión de Urgencias

El proceso de Gestión de Urgencias prevé el salto de algunas contriciones importantes de seguridad. Según el esquema anterior, el PEP del PCN-B detecta el valor Emergencia del atributo PurposeOfUse del Token SAML y fuerza la evaluación de la relativa política a nivel nacional en el país de afiliación del paciente A.

Si un profesional declarara siempre un acceso de Emergencia para la consulta del Resumen de Paciente de sus pacientes, siempre se saltará totas las reglas de control de acceso definidas por RACSEL.

Una posible solución para prevenir estos casos de abuso podría ser la siguiente: el PEP del PCN-B persiste los accesos de cada profesional de modo que, si se detectan más de X accesos al proceso de urgencia en un periodo de tiempo prefijado, se le deniega el acceso con el siguiente mensaje: Demasiado intento de acceso al proceso de urgencia. Los parámetros de los intentos máximos se pueden definir por país y cada uno tendrá que implementar su política de gestión de ola urgencia.

1.6. Casos de uso

A continuación, se plantean los casos de uso que se realizarán a través de la Red RACSEL, en una primera fase del proyecto. Dichos casos de uso se mapearán contra los componentes de la arquitectura de referencias para evidenciar las responsabilidades de cada uno de ellos con respeto al proceso descrito en cada caso.

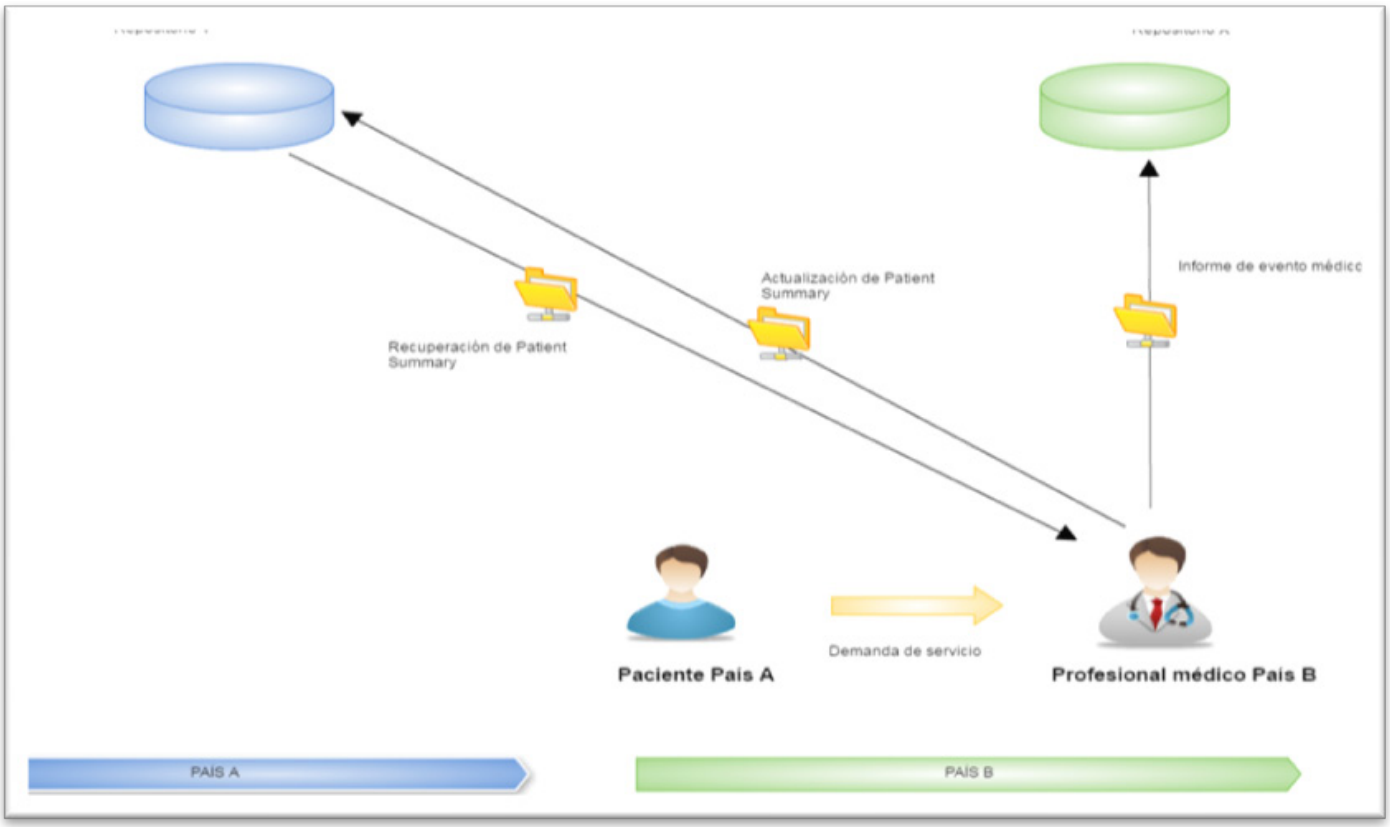


Ilustración 30-Caso de uso de actualización de paciente

Se han identificado los siguientes servicios:

- Identificación del Paciente

- Recuperación del Resumen de Paciente
- Actualización del resumen de paciente
- Gestión del Consentimiento

1.6.1. Descripción de los procesos

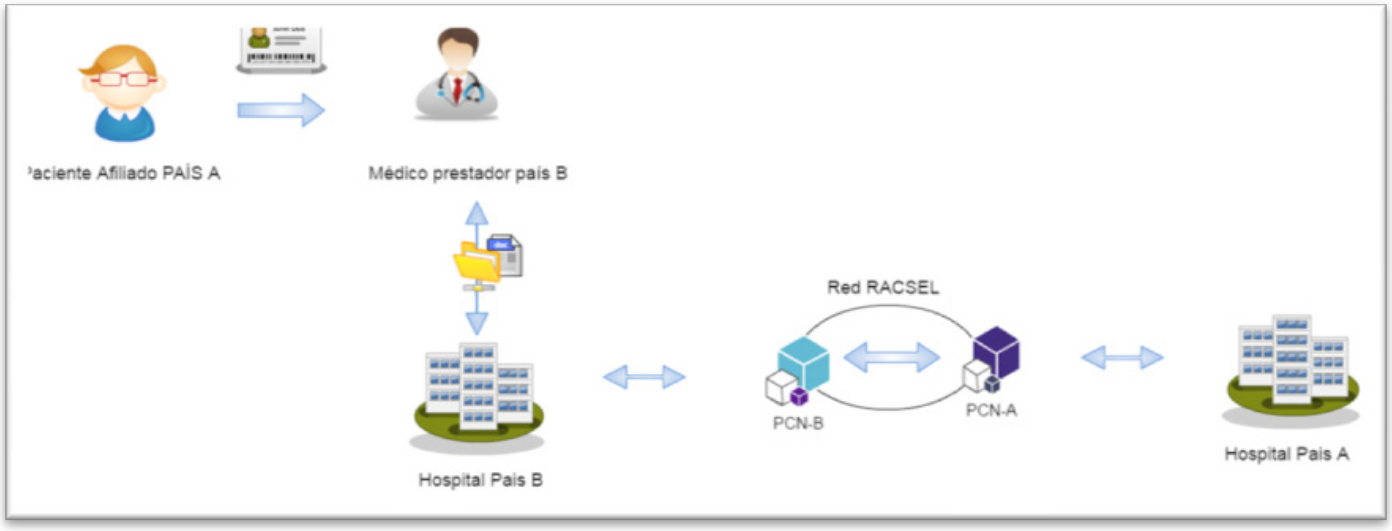


Ilustración 31-Esquema de casos de uso Interoperabilidad transfronteriza

1.6.1.1. Búsqueda de Paciente

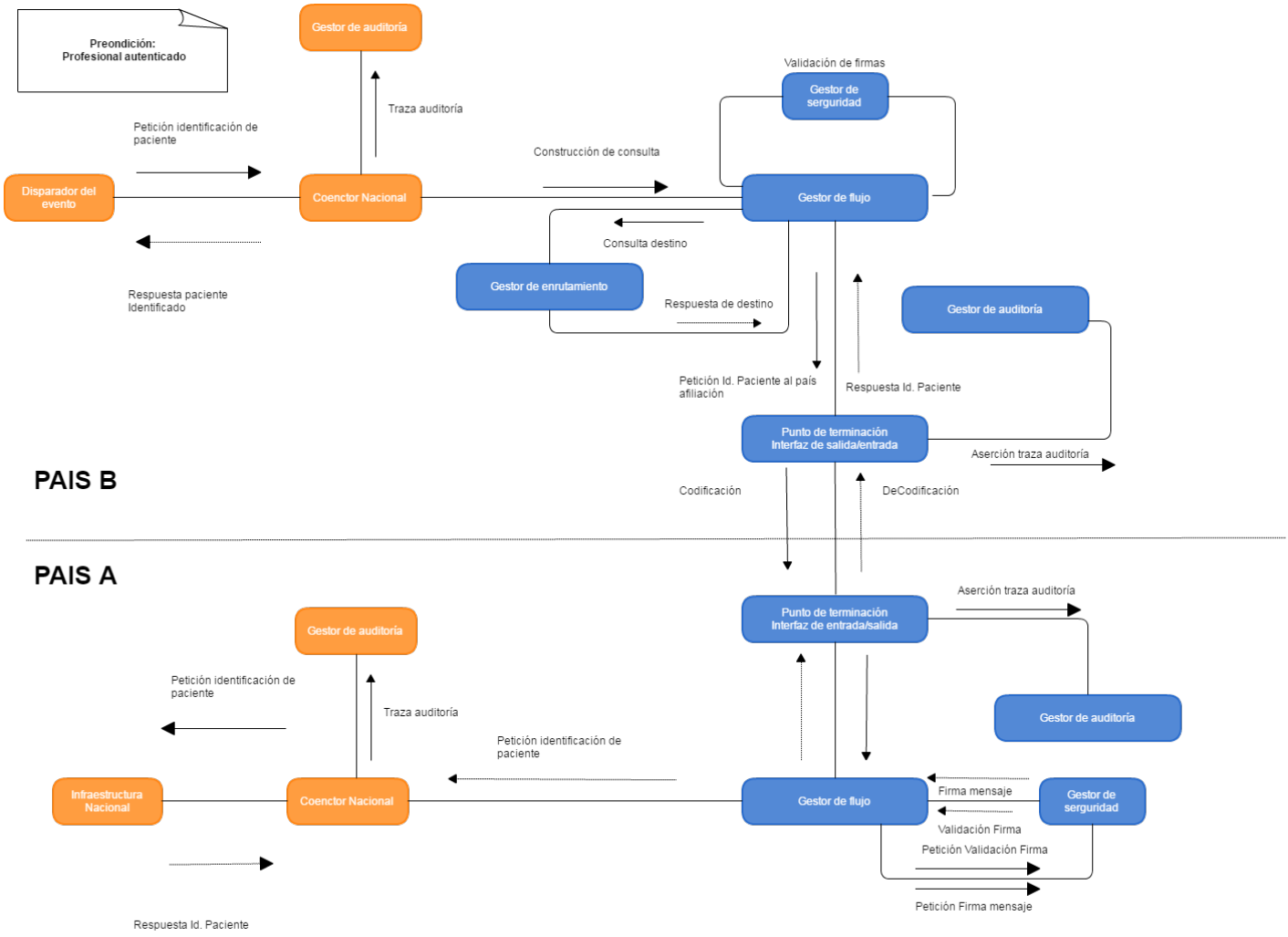


Ilustración 32-Proceso de Identificación de Paciente

Como paso previo a cualquier intercambio de datos transfronterizo, es necesario que se identifique correctamente al paciente entre ambos países, sin que pueda existir ningún tipo de error en este proceso.

Para ello, será necesario un proceso de identificación en el que habrá de seguir una serie de acciones que pasamos a describir a continuación.

El proceso empieza suponiendo que el profesional ya haya sido autenticado en la infraestructura nacional del *país B* y que el profesional haya activado la relativa función de identificación de paciente hacia el *CN-B* desde su portal de aplicación o su interfaz de usuario, informando todas las generalidades proporcionadas por el paciente en la consulta.

La llegada de la petición en el *CN-B* comporta la traducción de la misma al formato definido por *RACSEL* para ser tramitada a través de la Red *RACSEL*. Antes del envío al *PCN-B*, el *CN-B* genera una traza de autoría del **Gestor de Auditoría Nacional** según el formato establecido para esta transacción.

La petición pasa al componente *Gestor de Flujos* del *PCN-B* que a su vez activa al *Gestor de* Enrutamiento para extraer el endpoint del *PCN-A* de destino de la transmisión.

1.6.1.1.1. El PCN-B firma la mensajería saliente

El *Gestor de Flujo* transmite entonces la petición a la *Interfaz de Entrada* del *PCN-A* y lo hace a través de la *Interfaz de Salida* del *PCN-B*. Ambas interfaces realizan como primera acción una traza de auditoria correspondiente al servicio en uso para así mantener la información del mensaje que sale del *PCN-B* y que acaba de llegar al *PCN-A*, respectivamente.

1.6.1.1.2. El PCN-A valida la firma del PCN-B

En el *PCN-A*, la *Interfaz de Entrada* pasa la petición al *Gestor de Flujo* que invoca al *CN-A* para que se ejecute en la infraestructura nacional el servicio local de identificación del paciente.

El *CN-A* recupera el identificador único del paciente, audita y retorna la respuesta al *Gestor de Flujo* del *PCN-A*.

1.6.1.1.3. El PCN-A firma la respuesta

La respuesta fluye de vuelta hacia el *Gestor de Flujo* del PCN-B a través la *Interfaz de Salida* del *PCN*-A y la *Interfaz de Entrada* del *PCN-B* de sus respetivos *Puntos de Terminaciones*. Ambas interfaces generan sus correspondientes trazas de auditoría, según el formato establecido para este proceso.

1.6.1.1.4. El PCN-B valida la firma del PCN-A

El *Gestor de Flujo* del *PCN-B* transmite la respuesta al *CN-B* que adaptará la respuesta al formato nacional para retornarla al profesional que hizo la petición.

Al finalizar el proceso, en caso de éxito, el profesional dispone de los datos de identificación única del paciente en su país de afiliación, para poder posteriormente solicitar la recuperación o la actualización de su *Resumen de Paciente*.

1.6.1.2. Recuperación del Resumen de Paciente desde el país de prestación de servicio

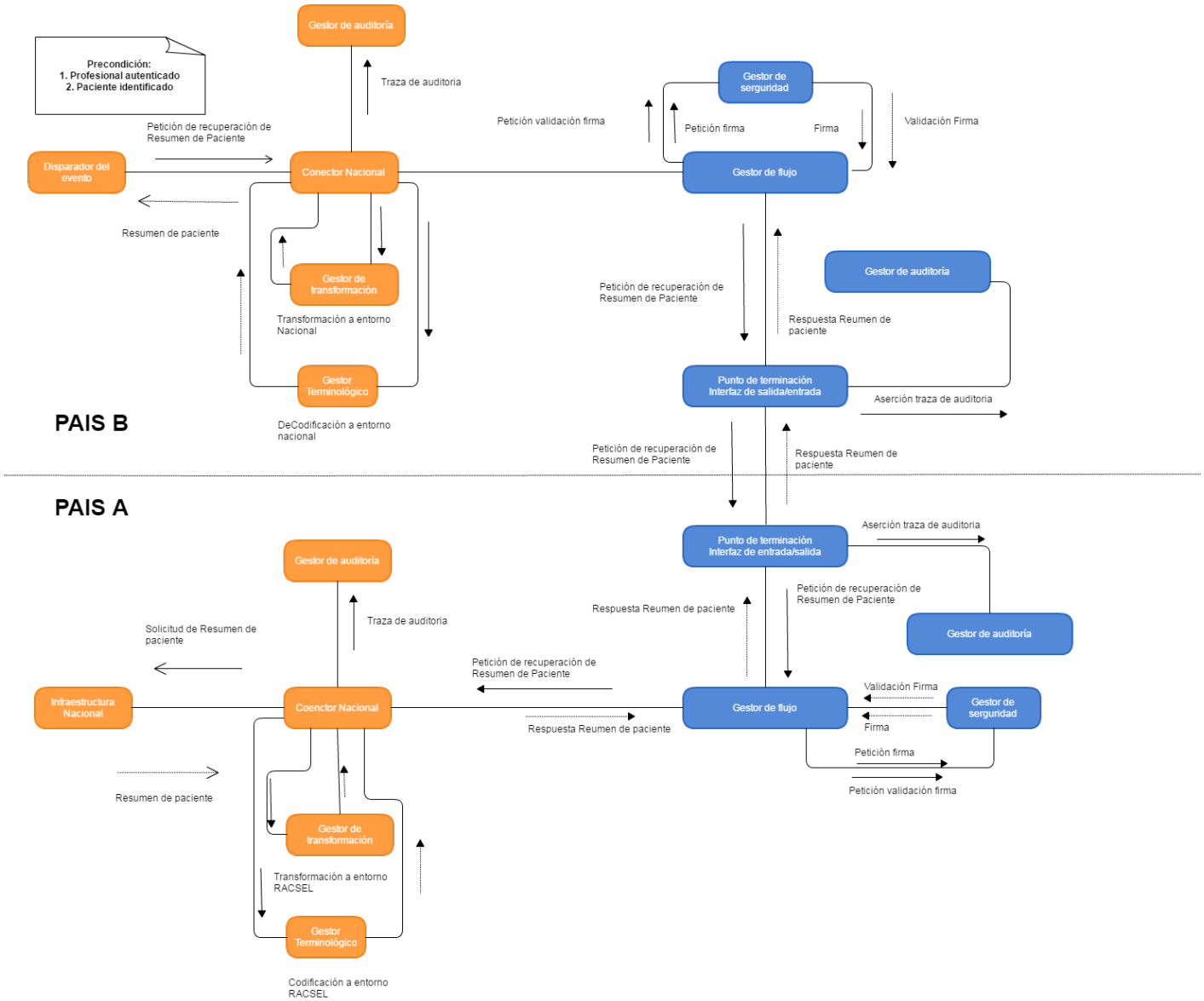


Ilustración 33-Proceso de Recuperación de Resumen de Paciente

El proceso empieza suponiendo que el profesional ya haya sido autenticado en la infraestructura nacional del país B y el paciente ha sido identificado con el servicio de identificación descrito en el apartado anterior. También se supone que el profesional ha activado la relativa función de **Recuperación del Resumen de Paciente** del *CN-B* desde su portal de aplicación o su interfaz de usuario.

La llegada de la petición en el *CN-B* comporta la traducción de la misma al formato definido por *RACSEL* para ser tramitada a través de esta red. Antes del envío al *PCN-B*, el *CN-B* genera una traza de autoría del *Gestor de Auditoría Nacional* según el formato establecido para esta transacción.

La petición pasa al componente *Gestor de Flujos* del *PCN-B* que a su vez activa al *Gestor de* Seguridad para que firme la mensajería saliente como *PCN-B*.

El *Gestor de Flujo* transmite entonces la petición a la *Interfaz de Entrada* del *PCN-A* y lo hace a través de la *Interfaz de Salida* del *PCN-B*. Ambas interfaces realizan como primera acción una traza de auditoria

correspondiente al servicio en uso para así mantener la información del mensaje que sale del *PCN-B* y que acaba de llegar al *PCN-A*, respectivamente.

1.6.1.2.1. El PCN-A valida la firma del PCN-B

En el *PCN-A*, la *Interfaz de Entrada* pasa la petición al *Gestor de Flujo* que invoca al *CN-A* para que se ejecutara en la infraestructura nacional el servicio local de *Recuperación del Resumen de Paciente*.

El *CN-A* realiza las trasformaciones para poder invocar al servicio de recuperación del *Resumen de Paciente* disponible en la infraestructura nacional. Una vez recuperado el documento, el *CN-A* realiza las conversiones semánticas y sintácticas para adaptar la respuesta al formato establecido por *RACSEL*. Tras realizar una traza de auditoría, retorna la respuesta al *Gestor de Flujo* del *PCN-A*.

El *Gestor de Flujo* del *PCN-A* activa el *Gestor de Seguridad* para firma la respuesta como *PCN-A*.
La respuesta pasa de vuelta hacia el *Gestor de Flujo* del *PCN-B* a través la *Interfaz de Salida* del *PCN-A* y la *Interfaz de Entrada* del *PCN-B* de sus respetivos *Puntos de Terminaciones*. Ambas interfaces generan sus correspondientes trazas de auditoría, según el formato establecido para este proceso.

1.6.1.2.2. El PCN-B valida la firma del PCN-A con el componente de Gestión de Seguridad

Finalmente, el *Gestor de Flujo* del *PCN-B* transmite la respuesta al *CN-B* que adaptará la respuesta al formato nacional para retornarla al profesional que hizo la petición.

Al finalizar el proceso, en caso de éxito, el profesional dispondrá del *Resumen de Paciente* del paciente obtenido en su en su país de afiliación, según el formato y el contenido definido por *RACSEL*.

NOTA: Para este trámite, a parte de la autenticación del profesional se necesita una confirmación de relación de tratamiento entre el profesional y el paciente. Veremos más adelante como se formalizan estas relaciones de una forma estándar en el contexto de servicios web *SOAP*.

1.6.1.3. Actualización del Resumen de Paciente en el país de afiliación

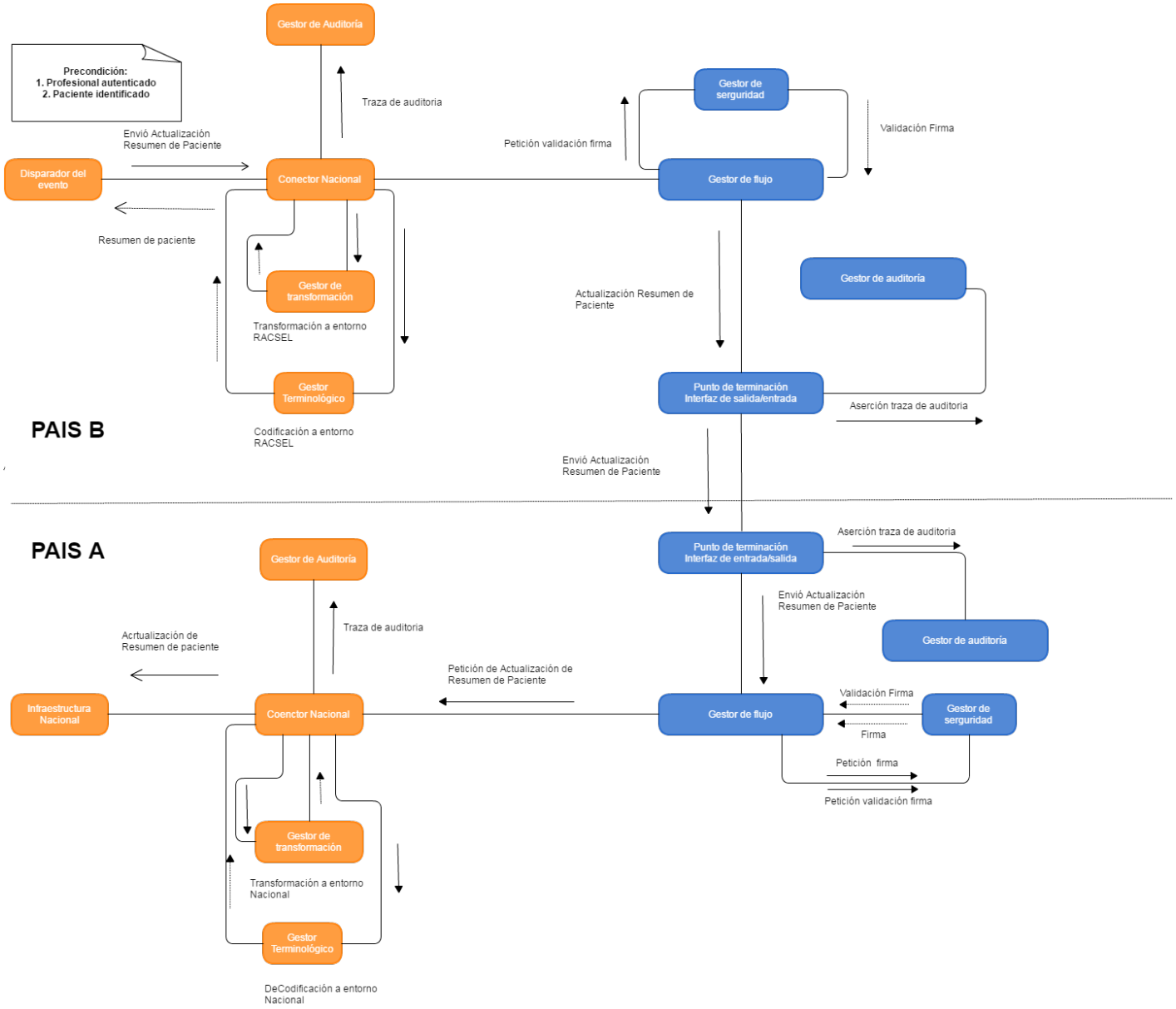


Ilustración 34-Proceso de Actualización de Resumen de Paciente

El proceso empieza suponiendo que el profesional ya haya sido autenticado en la infraestructura nacional del *país B*, el paciente ha sido identificado con el servicio de identificación descrito en el apartado anterior y el profesional ya dispone de un *Resumen de Paciente* actualizado. El profesional, además, ha activado la relativa función de *Actualización del Resumen de Paciente* del *CN-B* desde su portal de aplicación o su interfaz de usuario completando el relatico formulario con el detalle del nuevo tratamiento a notificar.

La llegada de la petición en el *CN-B* comporta la traducción de la misma al formato definido por *RACSEL* para ser tramitada a través de la Red *RACSEL*. Antes del envío al *PCN-B*, el *CN-B* genera una traza de autoría del *Gestor de Auditoría Nacional* según el formato establecido para esta transacción.

La petición pasa al componente *Gestor de Flujos* del *PCN-B* que a su vez activa al *Gestor de Seguridad* para que firme la mensajería saliente como *PCN-B*.

El *Gestor de Flujo* transmite entonces la petición a la *Interfaz de Entrada* del *PCN-A* y lo hace a través de

la *Interfaz de Salida* del *PCN-B*. Ambas interfaces realizan como primera acción una traza de auditoria correspondiente al servicio en uso para así mantener la información del mensaje que sale del *PCN-B* y que acaba de llegar al *PCN-A*, respectivamente.

- En el *PCN-A* el *Gestor de Flujo* del *PCN-A* activa al *Gestor de Seguridad* para que valide la firma del *PCN-B*.

- En el *PCN-A*, la *Interfaz de Entrada* pasa la petición al *Gestor de Flujo* que invoca al *CN-A* para que se ejecutara en la infraestructura nacional el servicio local de *Actualización del Resumen de Paciente.*

El *CN-A* realiza las trasformaciones para poder invocar al servicio de *Actualización del Resumen de Paciente* disponible en la infraestructura nacional. Una vez actualizado el documento, el *CN-A* realiza las conversiones semánticas y sintácticas para adaptar la respuesta al formato establecido por *RACSEL*. El *CN-A* entonces, tras realizar una traza de auditoría, retorna la respuesta al *Gestor de Flujo* del *PCN-A*.

1.6.1.3.1. El Gestor de Flujo del PCN-A activa el Gestor de Seguridad para firma la respuesta como PCN-A

La respuesta pasa el *Gestor de Flujo* del *PCN-B* a través la *Interfaz de Salida* del *PCN-A* y la *Interfaz de Entrada* del *PCN-B* de sus respetivos *Puntos de Terminaciones*. Ambas interfaces generan sus correspondientes trazas de auditoría, según el formato establecido para este proceso.

1.6.1.3.2. El PCN-B valida la firma del PCN-A con el componente de Gestión de Seguridad

Finalmente, el *Gestor de Flujo* del *PCN-B* transmite la respuesta al *CN-B* que adaptará la respuesta al formato nacional para dar el respaldo del éxito de la operación al profesional que hizo la petición de actualización.

Al finalizar el proceso, en caso de éxito, el profesional habrá actualizado el *Resumen de Paciente* en su en su país de afiliación del paciente.

NOTA: Para este trámite, a parte de la autenticación del profesional se necesita una confirmación de relación de tratamiento entre el profesional y el paciente. Veremos más adelante como se formalizan estas relaciones de una forma estándar en el contexto de servicios web *SOAP*, mediante las aserciones *SAML*.

1.6.1.4. Gestión del Consentimiento desde el país de prestación de servicio hacia el país de afiliación

Los pasos y la interacción entre los componentes de la Arquitectura para este proceso son los mismos que lo explicado en el punto anterior, aplicado al contexto de la *Notificación de un Cambio de Consentimiento* del *país B* al *país A*.

1.6.2. Notas sobre la implementación con estándares internacionales

La propuesta se basa en la adopción de un subconjunto de perfiles de integración *IHE X** para las transacciones realizadas entre los puntos de contacto nacionales.

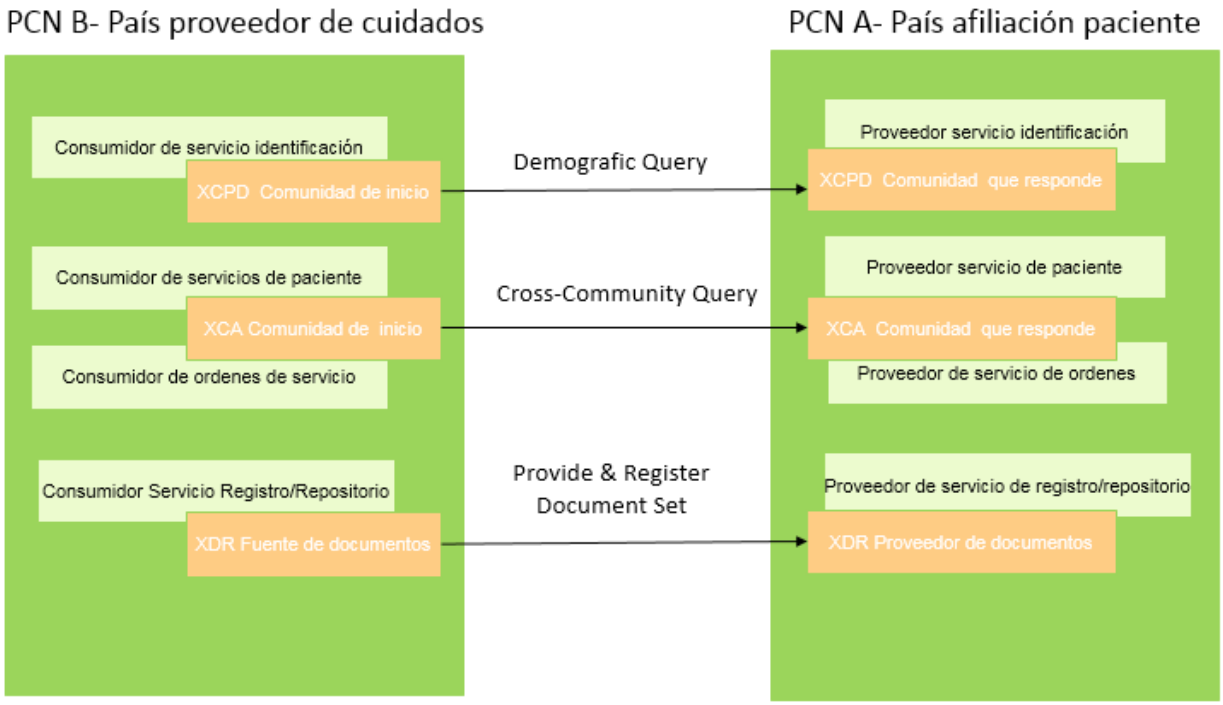


Ilustración 35-Comunicación entre PCN´s

La adopción de dichos estándares frente a otros emergentes (por ejemplo **Fast Healthcare Interoperability Resources**) es debida a la necesidad de usar un conjunto de tecnologías maduras que sean reconocidas a nivel internacional, y que garanticen los más altos niveles de seguridad, confidencialidad y estabilidad en el intercambio de información clínica transfronterizas.

A continuación, comentaremos los perfiles y las transacciones propuestas de cara a la implementación de cada uno de los servicios soportado por la arquitectura de referencia.

1.6.2.1. Servicio de Identificación de Paciente

El perfil *IHE* que se utilizará será *el XCPD Cross-Community Patient Discovery*, con la transacción *ITI-55 del IHE ITI* Technical Framework.
El mensaje de la petición iniciado en el país de prestación del servicio médico quedará envuelto en una estructura de datos que conforma el tipo **Patient Registry Find Candidates Query** *(HL7 PRPA_IN201305UV02)*. En ella se pasará la lista de las generalidades identificativas disponibles del paciente para intentar obtener su identificación única en el sistema de afiliación del *país A*.

El mensaje de la respuesta conformará a la estructura *HL7 Patient Registry Find Candidates Query Response (PRPA_IN201306UV02)*.

Cuanto a los *acknowledgement*, como previsto por *IHE XCPD*, en caso positivo el campo *Acknowledgement.typeCode* de la respuesta valdrá *AA* y el campo *QueryAck.queryResponseCode* del elemento *ControlActProcess* valdrá *OK*. Por el contrario, en caso de error, el elemento *QueryAck.queryResponseCode* valdrá *AE* y en el apartado *ControlActProcess* aparecerá en tag *reasonOf* con la indicación de la causa del error.

En cuanto a la cabecera del mensaje, éste deberá incluir una aserción *HCP* del profesional como explicado al apartado anterior y la referencia a las *WS-SecurityPolicy* para la identificación de las partes firmadas digitalmente.

Para más información acerca de esta mensajería se deriva al relativo componente de estándares *RACSEL* y a la documentación técnica de los estándares mencionados.

NOTA: Es importante observar que todos los catálogos terminológicos, códigos, espacios de nombres de la mensajería (***namespaces***), *OID's* o cualquier lista de valores propios de *RACSEL* tendrá que ser definido como el estándar de comunicación *RACSEL* y mapeados por los varios países miembros a través de los componentes nacionales **Gestor Terminológico** (o de Transformación Semántica) y **Gestor de Transformación Sintáctica** (si aplica).

1.6.2.2. Servicio de Recuperación del Resumen de Paciente

El perfil *IHE* que se propone es una extensión del perfil *XCA*: *Cross-Gateway Query With Documents (Query and Retrieve)* para poder realizar la búsqueda y la obtención del *Resumen de Paciente* en una única transacción. Alternativamente, será posible usar la combinación de las transacciones ITI-38 y ITI-39 en secuencia: *Cross-Gateway Query* y *Cross-Gateway Retrieve,* duplicando así el coste de procesamiento ya que la primera transacción solo recupera una referencia al *RP* y la segunda recupera el documento.

La sintaxis de la extensión de la mensajería *XML* para una petición *XCA Cross-Gateway Query With Documents,* es la misma que la establecida por una petición *XCA Cross-Gateway Query* con las siguientes extensiones:

- El elemento *<ws:Action>* es *urn:ihe:iti:2010:CrossGatewayQueryRetrieve*;

- En el elemento *@AdhocQueryRequest/ResponseOption* se deberá usar el literal *LeafClassWithRepositoryItem* ya que, como especificado en el estándar *ebRS v3.0*, esto indica que será devuelta la totalidad de los metadatos y el documento a la vez.

Por lo que se refiere a la respuesta, el formato de la misma es una combinación de los mensajes *Cross Community Query Response* y de *Cross Community Retrieve Response* ya que contempla la presencia eventual de un nuevo elemento *<Document/>* cuyo namespace es *urn:ihe:iti:xds-ebrim:extensions:2010*
Por lo que respecta a los errores, éstos son los contemplados en la documentación *XCA ITI TF-2b,* más los eventuales que se definirán para *RACSEL* con su codificación.

En cuanto a la cabecera del mensaje, éste deberá incluir una aserción *HCP* del profesional y una aserción *TRC* de relación de tratamiento, como lo explicado al apartado anterior, y la referencia a las *WS-SecurityPolicy* para la identificación de las partes firmadas digitalmente.

Para más información acerca de esta mensajería se deriva al relativo componente de estándares *RACSEL* y a la documentación técnica de los estándares mencionados.

NOTA: Es importante observar que todos los catálogos terminológicos, códigos, espacios de nombres de la mensajería (***namespaces***), *OID's* o cualquier lista de valores propios de *RACSEL* tendrá que ser definido como el estándar de comunicación *RACSEL* y mapeados por los varios países miembros a través de los componentes nacionales *Gestor Terminológico* (o de Transformación Semántica) y *Gestor de Transformación Sintáctica* (si aplica).

1.6.2.3. Servicio de Actualización del Resumen de Paciente

El perfil *IHE* que se utilizará será el *XDR Cross-Enterprise Reliable Exchange*, relativamente a la transacción ITI-41 del *IHE* **ITI Technical Framework** (*IHE* Provide And Register Document Set-b).

La petición es conforme al elemento *ProvideAndRegisterDocumentSetRequest* relativamente al documento *RP* que se defina puede ser actualizado con este servicio.

La respuesta conforma un elemento *ebXML RegistryResponse* con un atributo *status* que vale:

- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success, en caso de éxito
- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure, en caso de fallo

El mensaje de vuelta puede contener una lista de errores como parte de la lista *RegistryErrorList* con distintos calificadores:

- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Warning, para pasar información adicional
- urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Error, para retornar los errores que se hayan codificados para esta transacción en caso de Failure

Cuanto a la cabecera del mensaje, éste deberá incluir una aserción *HCP* del profesional y una aserción *TRC* de relación de tratamiento, como explicado al apartado anterior, y la referencia a las *WS-SecurityPolicy* para la identificación de las partes firmadas digitalmente.

Para más información acerca de esta mensajería se deriva al relativo componente de estándares *RACSEL* y a la documentación técnica de los estándares mencionados.

NOTA: Es importante observar que todos los catálogos terminológicos, códigos, espacios de nombres de la mensajería (***namespaces***), *OID's* o cualquier lista de valores propios de *RACSEL* tendrá que ser definido como el estándar de comunicación *RACSEL* y mapeados por los varios países miembros a través de los componentes nacionales *Gestor Terminológico* (o de Transformación Semántica) y *Gestor de Transformación Sintáctica* (si aplica).

1.6.2.4. Servicio de Gestión del Consentimiento

El servicio *RACSEL* cumple con los estándares definidos por el *perfil* **IHE XDR Cross-Enterprise Reliable Exchange** (*ITI-41*) e **IHE BPPC Basic Patient Privacy Consent** (*ITI TF-3*).

La operación del servicio de *Gestión del Consentimiento* (*Nuevo Consentimiento)* se activa por el profesional en el país de prestación de servicio para tramitar el cambio de estado de un consentimiento por parte del paciente hacia el país de afiliación. Para ello y de cara al servicio web, una notificación de cambio de estado se formalizará con un *Patient Privacy Consent Acknowledgment Document* .

La mensajería con que se envía este documento (petición) corresponde a la que vimos en detalle anteriormente: *IHE XDR ITI-41: Provide And Register Document Set-b***.** Por cada documento enviado se tendrán que informar los correspondientes conjuntos de metadatos tal y como definido en *IHE BPPC ITI TF-3*. En particular es de extrema importancia que se codifiquen bien los conceptos por lo que será posible dar o revocar un consentimiento, por ejemplo:

Id. de Política de Privacidad (OID)	Valor	Descripción
1.3.6.1.4.1.12559.11.10.1.3.2.4.1.1	Opción In	El paciente dio el consentimiento para permitir a los profesionales de este país B de acceder sus datos médicos en el contexto de RACSEL.
1.3.6.1.4.1.12559.11.10.1.3.2.4.1.2	Opción Out	El paciente revocó el consentimiento para permitir a los profesionales de este país B de acceder sus datos médicos en el contexto de RACSEL.

El servicio implementado, en cada caso tiene que comprobar que el usuario peticionario esté autorizado para tramitar esta información. Además de*bRIMs* cualquier error relacionado con la tramitación del

Token SAML que identifica al profesional tendrá que resolverse como un *Fault* de trasmisión.

La mensajería de la respuesta seria la misma que la anterior y conforma con el estándar *ebXML*: un elemento *RegistryResponse* con un *status* definido como:

- *urn:oasis:names:tc:ebxmlregrep:ResponseStatusType:Success* indica un éxito de la tramitación.
- *urn:oasis:names:tc:ebxmlregrep:ResponseStatusType:Failure*o
- *urn:oasis:names:tc:ebxmlregrep:ResponseStatusType*:*Warning* indicará un caso de fallo o alerta, respectivamente.

Cuanto a la cabecera del mensaje, éste deberá incluir una aserción *HCP* del profesional y una aserción *TRC* de relación de tratamiento, como explicado al apartado anterior, y la referencia a las *WS-SecurityPolicy* para la identificación de las partes firmadas digitalmente.

Para más información acerca de esta mensajería se deriva al relativo componente de estándares *RACSEL* y a la documentación técnica de los estándares mencionados.

2. Análisis de *GAPS*

2.1. Introducción

Mediante el presente apartado se analizan las brechas detectadas a nivel nacional con respecto al modelo de referencia de arquitectura para la Red de desarrollo de la *Historia Clínica Electrónica de América Latina y el Caribe*.

El principio básico de la solución propuesta en el modelo de referencia de arquitectura es salvar las infraestructuras nacionales de salud electrónica existentes en lugar de establecer una nueva red de servicios de salud, pero para alcanzar tal propósito es necesario que cada uno de los países desarrolle una serie de módulos para interoperar con el resto de la red, así como la utilización de determinadas tecnologías y recursos.

El objetivo de este apartado es analizar la situación nacional de cada uno de los países y detectar las brechas con respecto al modelo presentado.

2.2. Elementos de evaluación

Se ha desglosado el informe en cuatro puntos en el que hemos dividido el componente, para atacar los grandes rasgos que conforman la arquitectura técnica:

- Infraestructura y comunicaciones
- Estándares
- Seguridad y auditoría.
- Gobierno *TIC*

Se ha realizado la evaluación de los diferentes aspectos tratados mediante el envío de una serie de cuestionarios de manera individualizada a cada uno de los grupos de trabajo de los países pertenecientes a la Red *RACSEL*, que se consensuaron mediante reuniones virtuales para tratar los puntos referidos.

En los puntos tratados durante la evaluación, y después de mantener reuniones y misivas aclaratorias, algunos de los puntos tratados en la documentación se encuentran parcialmente disponibles. Se entiende como parcialmente disponible aquellos aspectos en los que existe algún/os componente/s previos o están proyectados para un futuro inmediato.

2.2.1. Infraestructura y comunicaciones

Es necesario considerar la necesidad de una infraestructura de comunicaciones a nivel nacional que pueda permitir el intercambio de información en el entorno de salud.

Dentro de la infraestructura de comunicaciones se han atacado:

- Estado de las infraestructuras de comunicaciones nacional

- Interoperabilidad de la red sanitaria a nivel nacional
- Necesidades para interoperar con la Red *RACSEL*

Será necesario contar con una infraestructura de comunicaciones que permita, el traspaso de información con garantías entre los diferentes sistemas de información y el punto de contacto nacional.

La interoperabilidad entre los sistemas se realizará mediante tecnología *SOAP* sobre *HTTP*, utilizando servicios sincronizados, ya que el profesional se encuentra delante del paciente durante la solicitud.

Dado que la información a transmitir consistirá en mensajes de un tamaño elevado y potencialmente afecte a un elevado número de usuarios, se deberá dimensionar la infraestructura para garantizar unos tiempos de respuesta óptimos de la mensajería.

Además, será necesario contar con una infraestructura robusta que asegure que ningún agente externo pueda ingresar a la red. Para ello se creará una red de confianza en la que una puerta de enlace de cada nación tendrá acceso y confiará en las del resto de países participantes de la Red *RACSEL*. Esta red estará formada por una *VPN* que garantizará la seguridad de las comunicaciones.

La relación de confianza entre las dos puertas de enlace se establecerá mediante el uso de certificados *X509* de servidor *SSL*. Para garantizar la seguridad en las comunicaciones dentro de la red, emisor y receptor encriptarán el canal de comunicación utilizando mutual *SSL* (*SSL 2-way*).

La incorporación de un nuevo miembro a la Red *RACSEL* se realizará mediante la inclusión de su puerta de enlace a la red de confianza *VPN* y la publicación de su clave pública al resto de las de la red.

Los servicios deben estar accesibles a nuevos miembros de la Red, cumpliendo siempre los parámetros de seguridad establecidos por la solución.

Aunque el propósito de la plataforma *RACSEL* debe ser independiente de la infraestructura nacional, ésta se basa en el estándar *IHE*, por lo que toda aproximación que las diferentes naciones adopten hacía este estándar facilitarán la integración y la interoperabilidad dentro de la Red *RACSEL*. No obstante, no entra dentro de las competencias del proyecto la imposición del uso de éste o ningún otro estándar en la infraestructura nacional,siendo responsabilidad de cada nación implementar los servicios definidos para interactuar con la Red *RACSEL*.

2.2.2. Estándares de comunicación

Es necesario unificar las estructuras de los mensajes mediante estándares internacionales que hagan posible la interoperabilidad entre los diferentes países a través de los puntos de contacto nacionales.

Para ello, se analizará la realidad actual, con la necesidad marcada en las especificaciones del modelo de arquitectura de referencia.

En cuanto a mensajería, en *RACSEL* se ha propuesto la utilización de *IHE* como marco técnico para conseguir la interoperabilidad entre los *Puntos de Contacto Nacional*, puesto que permite que haya coherencia e integridad en los distintos procesos, además de que trabaja mediante los estándares internacionales más utilizados, *HL7*, *DICOM*, etc.

En cuanto a catálogos, a nivel regional, para que la información que se traspasa tenga la coherencia establecida, tal y como se plantea en el modelo de referencia de terminología, se adoptará el estándar semantico **Systematized Nomenclature of Medicine – Clinical Terms** (*SNOMED CT*), que es la terminología clínica integral, multilingüe y codificada de mayor amplitud, precisión e importancia desarrollada en el mundo, para la codificación de los medicamentos.

Será necesario definir *OIDs* o codificaciones propias a *RACSEL* para todos aquellos conjuntos de valores que queden establecidos en cada dominio por la mensajería (perfiles, roles...).

La realidad de cada nación no tiene por qué acomodarse a los requisitos de *RACSEL*, por lo que, en caso de no utilizar los mismos estándares, se deberá realizar una transformación entre aquéllos definidos por la gobernanza *TIC* de *RACSEL* y los propios de cada nación. Es por ello necesario que todos los países dispongan de catálogos que permitan identificar de forma única todos los conceptos que así lo requieran en la mensajería.

Dado que los distintos países pueden utilizar diferentes catálogos y lenguaje, es necesario realizar una tarea de transformación semántica en la comunicación. Esta transformación se llevará a cabo a través del **Conector Nacional**, ya que será responsabilidad de cada país decidir cómo resolver la implementación de dicho servicio. La transformación que debe acometerse afecta a tantos niveles como diferencias tenga el país con respecto a la propuesta de interoperabilidad de la Red *RACSEL*, es decir, puede afectar tanto a mensajería (*IHE*) como terminología (catálogos médicos), como identificación única de objetos (*OID*).

2.2.3. Seguridad y auditoría

La información que trata la plataforma *RACSEL* requiere de unas políticas de seguridad que garanticen la confidencialidad e integridad de la misma.

Será necesario crear un marco general de seguridad adaptado a las necesidades del sistema de información, que abarque tanto la infraestructura como los procedimientos de intercambio de la información.

Los principales objetivos de la seguridad informática que siguen las indicaciones *ISO / IEC 27002*, son:

- **Autenticidad**: la identidad de un actor ha sido probada como verdadera. Esta autenticidad puede realizarse de varias formas, por ejemplo, mediante la utilización de usuario y contraseña o el uso de un certificado *X.509* expedido por una *Autoridad Certificadora de Confianza*.
- **Confidencialidad**: la información sólo es accesible a usuarios autorizados.
- **Integridad**: La información no puede ser modificada por un tercero.
- **Disponibilidad**: los usuarios autorizados tienen acceso a la información y los activos asociados cuando sea necesario bajo ciertos criterios de calidad de la solución.
- **No Repudio**: En toda comunicación existe un emisor y receptor reconocidos, debe quedar constancia de la autoría de todos los mensajes de forma irrevocable.

A continuación, analizaremos las medidas de seguridad y protocolos aplicados a nivel nacional, y las posibles brechas detectadas con respecto al modelo de arquitectura de referencia.

Hay dos niveles de flujo de datos que se distinguen en el sistema:

- El nivel de flujo de datos nacional (flujo de datos de dominio nacional):
    - Entre el usuario final y el *PCN*.
- El nivel de flujo de datos transfronterizo:
    - Entre el *PCN* del país que provee la asistencia y el *PCN* del país de afiliación del paciente.

Para la comunicación a nivel nacional:

- Aplicar las medidas de seguridad perimetral necesarias que garanticen el acceso al *PNC* a aquellos agentes autorizados, mediante el uso de sistemas de seguridad y la aplicación de reglas de acceso.

- Se debe garantizar la identidad del profesional mediante la incorporación de un *token SAML* firmado con certificado *X509* por el gestor de identidades encargado de autenticar al profesional. Este token viajará en toda la mensajería.

- Debe quedar constancia de la relación entre el paciente y el profesional que solicita su información médica mediante la incorporación en la mensajería de otro token *SAML* que establezca dicha relación. Este token debe estar firmado con un certificado *X509* propiedad del centro de salud desde donde se realiza la petición.

- Control de acceso: El país que realiza la consulta debe aplicar las reglas necesarias que autoricen la consulta que realiza el profesional.

- Control de acceso: El país que custodia la información del paciente debe aplicar las reglas necesarias que autoricen la consulta de la información solicitada.

- El *PCN* debe tener la capacidad de validar las firmas emitidas por todos los centros de su país. Para ello debe disponer de un almacén con todas las claves públicas de los centros de su país.

- Todas las comunicaciones han de ser cifradas utilizando, al menos, protocolo de seguridad TLS 1.2 y SSL 2-way.

Para la comunicación transfronteriza:

- Los medios de identificación y autenticación del usuario final deben haber sido auditados y certificados por una organización independiente certificada por las autoridades nacionales.

- Los procedimientos de **Protección de Datos y Privacidad** del *PCN* deben ser auditados y certificados por la autoridad nacional responsable de protección de datos.

- Cada *PCN* debe pasar por una auditoría de seguridad de acuerdo a estándares nacionales e internacionales. La auditoría de seguridad debe repetirse anualmente.

- Las auditorías de seguridad deben realizarse anualmente para auditar los sistemas según *ISO / IEC27001,ISO / IEC 17799 / ISO / IEC 27002*, o normas de nivel equivalente.

- Autenticación mutua entre los *PNCs* que intercambien información. Para conseguirla se debe establecer un canal seguro *SSL 2-way*.

- La traza de los mensajes intercambiados se consigue mediante incorporación del perfil *ATNA*, generando unos mensajes de log o auditoría secuencial, que son transmitidos mediante *TLS* a un repositorio de auditoria del *PNC*.

- La protección del canal mediante el uso de tecnología *IPSec / VPN* que restrinjan el acceso a la red privada.

- Todos los mensajes deben ser firmados con certificado *X509* por los *PNC*s que generan el mensaje y validadas por el que lo recibe.

- Reglas robustas para evitar ataques a los diferentes *Puntos finales* publicados por cada uno de los

países y así evitar cualquier actividad irregular e inmediatamente aplicar acciones acordes a cada ataque.

2.2.4. Gobierno TIC

La *OMS*, la *OCDE* y otros organismos internacionales han señalado la importancia de un planteamiento mundial coordinado para abordar las cuestiones específicas relacionadas con la salud electrónica.

Hemos querido hacer un apunte en la necesidad de contar con una gobernanza común para poder gestionar y abordar las necesidades que serán requeridas para poder generar los *PCNs*, y que deberán ser consensuadas por los miembros pertenecientes a la Red *RACSEL*.

La gobernanza la marcamos como de necesidad incluso antes de la puesta en marcha del proyecto puesto que deberá tomar decisiones que podrían implicar en las características de alguno de los componentes que conforman la arquitectura como:

- Workflow Manager
- Security Manager
- Consentimiento informado de paciente
- Confidencialidad de la información que se envía de forma transfronteriza

Los componentes que se encuentran en el *PCN*, son los encargados de aplicar la lógica del proyecto, marcar las políticas de seguridad, etc.

2.3. Descripción de las Brechas

Para realizar la descripción de las brechas, se ha tenido en cuenta:

- La información facilitada en el taller presencial que se realizó en **Lima** 20-21/11
- El análisis de las respuestas proporcionadas en las diversas encuestas que hemos articulado hasta la fecha
- Información socavada de las reuniones virtuales realizadas con los miembros de los grupos de trabajo
- Se han consultado los portales web de los diferentes ministerios de salud y *TIC* de los países miembros de la Red *RACSEL*
- A nivel mundial, se recabó información de la *PAHO/OMS*

Para ello hemos realizado un primer desglose de los ítems, mostrando el escenario actual y el deseado (*AS IS/TO BE*) tanto a nivel de la Red *RACSEL* como a nivel nacional de cada uno de los países miembros de la red y posteriormente hemos realizado la descripción de cada uno de los ítems enumerados.

2.3.1. Brechas de la Red RACSEL

Este apartado documenta las brechas de implementación de los componentes comunes de la Red *RACSEL*, a todos los niveles. Se han marcado como brechas, por tratarse de elementos que se han de construir exprofeso para el proyecto.

2.3.1.1. Escenario

Mediante este cuadro se muestra el *AS IS*, siendo éste el estado actual de la implementación de cada componente, para llegar a un *TO-BE* que alcance el modelo de la infraestructura planteado en la arquitectura de referencia.

ÍTEM	AS IS	TO BE
Almacén de certificados de confianza	• No existe	• Cada PCN tendrá que tener su almacén de certificados de confianza, con que valida las firmas de las aserciones SAML's emitidas por las instituciones nacionales con las identidades de los profesionales y/o las relaciones profesionales/paciente.
Certificados para traspaso transfronterizo	• No existe	• Su implementación dentro de la Red RACSEL tendrá que ser definida y consensuada por el equipo de Gobernanza.
Estándares de mensajería	• Pendiente de definición	• Utilización de perfiles IHE, según la documentación del componente de Estándares.
Gestor de Auditoría	• No existe	• Gestor de auditorías para garantizar el correcto seguimiento del traspaso trasfronterizo de información basado en el perfil ATNA.
WS-Security Policy y SAML	• No existe	• Necesario para la garantía de identidad del emisor de los mensajes
TLS	• No existe	• Requisito obligatorio: TLS 1.2
Gobernanza conjunta	• No existe	• Necesaria la definición de los procesos y competencias a asumir por parte de los miembros de la Red RACSEL
Workflow Manager	• No existe	• Componente que gestiona el ciclo de vida de las interacciones de los procesos definidos imponiendo el cumplimiento de las reglas de negocio interna a la Red RACSEL: • Identificación de Paciente; • Obtención de Resumen de Paciente • Actualización de Resumen de Paciente • Transmisión del consentimiento
Transformation Manager	• No existe	• Componente interno del PCN activado por el Workflow Manager. Realiza las invocaciones al servicio de traducción de términos clínicos y códigos a través del CN.
Routing Manager	• No existe	• Para realizar el enrutamiento de los mensajes hacia los puntos finales de otros países (PCN's) miembros de la Red RACSEL.
Gestión de Configuración y Monitoring	• No existe	• Componente que monitoriza el correcto funcionamiento de la plataforma y su configuración.
Security Manager	• No existe	• Contiene los servicios de firma digital y comprobación de firma de la información médica transfronteriza. • Contiene los servicios de encriptación y desencriptado. • Puede contener llamadas a los servicios nacionales de Control de Acceso.
Catálogos nacionales de codificación semántica y códigos (OID´s)	• No existe	• Necesario para el mapeo en el PCN para la transmisión de información transfronteriza

2.3.2. Brechas detectadas

En los siguientes puntos haremos mención a las brechas detectadas a nivel nacional, por cada una de las naciones pertenecientes a la Red *RACSEL*.

2.3.2.1. Colombia

Pasamos a la descripción de las brechas detecta das a nivel nacional con respecto al modelo de referencia de arquitectura planteado.

En la actualidad se está implementando a nivel nacional la red de comunicación para salud, mediante el proyecto *IO/AAS* para la implementación del **Marco de Referencia de Arquitectura Empresarial** para la *Gestión de TI*.

A continuación, se describen las carencias detectadas:

Necesidad de mejorar la red de telecomunicaciones en el país, puesto que no en todos los centros de la nación cuentan con una buena infraestructura, para poder cumplir con los requisitos de interoperabilidad entre los proveedores de salud.

Despliegue de servicios para que las entidades de salud puedan interoperar y comunicar eventos acaecidos por los pacientes a nivel nacional.

Creación de los maestros necesarios para la identificación única a nivel nacional de los conceptos relevantes de cara a la interoperabilidad nacional con la Red *RACSEL*:

- Posibilidad de utilización de *OID´*s nacionales o internacionales

Necesidad de articular a nivel nacional un *Resumen de Paciente* para poder realizar el traspaso de información transfronterizo, mediante documento *CDA*:

- Dicho resumen de paciente podrá ser custodiado en el hospital de referencia del paciente y quedar marcado en el registro de datos de pacientes nacional (por ejemplo *MPI*).

Adecuación del repositorio/registro de pacientes nacional para identificar de forma inequívoca a los pacientes:

- Centro de referencia del paciente
- Marcaje de consentimiento informado por parte del paciente para aceptación de traspaso de información transfronterizo.

Creación del *Conector Nacional*, para proporcionar la implementación de los servicios necesarios al *PCN* y así poder interoperar con la Red *RACSEL*

- Adecuación de la mensajería nacional propia a la mensajería requerida por el *PCN* según los perfiles *IHE* que se utilizarán en la Red *RACSEL*.
- Servicio de traducción:

  Para cualquiera de las codificaciones utilizadas a nivel nacional y que difieran de lo planteado en el modelo de referencia:

  - Codificación médica

- *OID´*s nacionales – *OID´*s de la red

Estándares de comunicación

- **Perfiles *IHE***

Colombia en la actualidad para el intercambio de información entre las entidades utiliza mensajería *XML/JSON* con formato propio, sin seguir los perfiles de *IHE*. Para poder interoperar con el resto de los países a través de la Red *RACSEL*, teniendo en cuenta que se han marcado los perfiles *IHE*, será necesario que en el *Conector Nacional*, antesala al *Punto de Contacto Nacional*, se realice una adecuación de los mismos.

- **Gestor terminológico**

En la mensajería existe un conjunto de conceptos que pertenecen a dominios delimitados (por ejemplo: **h**-hombre, **m**-mujer) que deben compartir emisor y receptor para su correcta interpretación. Estos conceptos deben estar, por tanto, identificados y codificados en un catálogo unificado a nivel nacional.

Uno de estos dominios es el catálogo de medicamentos, para el que se ha escogido *SNOMED CT* a nivel de la Red *RACSEL*. **Colombia**, en la actualidad, no está utilizando *SNOMED CT*, por lo que se deberá proceder a la creación de un servicio de mapeo y traducción entre *SNOMED CT* y el catálogo de medicamentos nacional, previo al envío de la información a través de la Red *RACSEL*.

Este mismo servicio de mapeo y transformación deberá implementarse para el resto de catálogos y dominios en los que el país difiera con respecto a la Red *RACSEL*.

Seguridad y auditoría

- Gestor de auditoria

Para el intercambio de información trasfronteriza será necesario a nivel nacional, y dentro del **Conector Nacional,** contar con un gestor de auditoría que trace tanto entradas como salidas de las peticiones.

- Seguridad

Dentro de las capacidades técnicas del modelo *IO/AAS*, se tiene que hacer énfasis en las necesidades de seguridad que ha de tener la red:

- Certificados *X509*, con los que realizar
    - **Certificado de Aplicación** para la realización de firma digital y encriptación de la mensajería
    - **Certificado de Servidor** para la encriptación de las comunicaciones
- Ticket *SAML*
- Incorporación de las piezas de infraestructura necesarias que garanticen la seguridad perimetral (firewalls, DMZ, ...)

2.3.2.2. Perú

Pasamos a la descripción de las brechas detectadas a nivel nacional con respecto al *Modelo de Referencia de Arquitectura* planteado.

Infraestructura de comunicaciones

En la actualidad se está implementando a nivel nacional la red de comunicación para salud mediante los proyectos *BID-HCE-RENHICE*, para el despliegue del **Registro Nacional de Historias Clínicas.**

A continuación se describen las carencias detectadas:

- Necesidad de mejorar la red de telecomunicaciones en el país, puesto que no en todos los centros de la nación cuentan con una buena infraestructura, para poder cumplir con los requisitos de interoperabilidad transfronteriza.

    - Primera actuación en **Junin** y **Puno**.

- El proyecto *RENHICE* contempla la infraestructura necesaria a nivel nacional para que las entidades de salud puedan interoperar y comunicar eventos acaecidos a los pacientes, para poder confeccionar el *Resumen de Paciente* en el hospital de referencia, y la posibilidad de almacenar información clínica en el *RENHICE* con la autorización del paciente. Esta infraestructura todavía no está implantada.

- Adecuación del *MPI* con el que contará la infraestructura nacional para identificar de forma inequívoca a los pacientes:

    - Marcaje de consentimiento informado por parte del paciente para aceptación de traspaso de información transfronterizo.

- Creación de los maestros necesarios para la identificación única a nivel nacional de los conceptos relevantes de cara a la interoperabilidad nacional con la Red *RACSEL*:

    - Posibilidad de utilización de *OID´*s nacionales o internacionales

    - Articular a nivel nacional un *Resumen de Paciente* para poder realizar el traspaso de información transfronterizo, mediante documento *CDA*:

    - Se podrá generar y mantener un *Resumen de Paciente* centralizado con la autorización de éste.

    - En caso de no contar con la autorización para centralizar el *Resumen de Paciente*, cada centro de salud también generará y mantendrá un resumen local y quedará marcado en el registro de datos de pacientes nacional.

- Creación del **Conector Nacional**, para proporcionar la implementación de los servicios necesarios al *PCN* y así poder interoperar con la Red *RACSEL*

    - Adecuación de la mensajería nacional propia a la mensajería requerida por el *PCN* según los perfiles *IHE* que se utilizarán en la Red *RACSEL*.

    - Servicio de traducción:

        Para cualquiera de las codificaciones utilizadas a nivel nacional y que difieran de lo planteado en el **Modelo de Referencia**:

        - Codificación médica

        - *OID´*s nacionales – *OID´*s de la Red.

    Estándares de comunicación

    - **Perfiles *IHE***

Perú en la actualidad para el intercambio de información entre las entidades utiliza mensajería *XML* con formato propio, y en un futuro tiene previsto utilizar *FHIR* o *CDA*. No obstante, la mensajería definida para la Red *RACSEL* sigue los perfiles *IHE*. Para poder interoperar con el resto de los países a través de la Red *RACSEL* será necesario que en el **Conector Nacional,** antesala al **Punto de Contacto Nacional**, se realice una adecuación de los mismos.

- **Gestor terminológico**

En la mensajería existe un conjunto de conceptos que pertenecen a dominios delimitados (por ejemplo **h**-hombre, **m**-mujer) que deben compartir emisor y receptor para su correcta interpretación. Estos conceptos deben estar, por tanto, identificados y codificados en un catálogo unificado a nivel nacional.

Uno de estos dominios es el catálogo de medicamentos, para el que se ha escogido *SNOMED CT* a nivel de la Red *RACSEL*. **Perú**, en la actualidad, no está utilizando *SNOMED CT*, por lo que se deberá proceder a la creación de un servicio de mapeo y traducción entre *SNOMED CT* y el catálogo de medicamentos nacional, previo al envío de la información a través de la Red *RACSEL*.

Este mismo servicio de mapeo y transformación deberá implementarse para el resto de catálogos y dominios en los que el país difiera con respecto a la Red *RACSEL*.

Seguridad y auditoría

- Gestor de auditoria

Para el intercambio de información trasfronteriza será necesario a nivel nacional, y dentro del *Conector Nacional*, contar con un gestor de auditoría que trace tanto entradas como salidas de las peticiones.

- Seguridad

En la puesta en marcha del proyecto *RENHICE*, **Perú** debería hacer énfasis en las necesidades de seguridad que ha de tener la red:

- Certificados *X509*, con los que realizar
    - *Certificado de Aplicación* para la realización de firma digital y encriptación de la mensajería
    - *Certificado de Servidor* para la encriptación de las comunicaciones
- Ticket *SAML*
- Incorporación de las piezas de infraestructura necesarias que garanticen la seguridad perimetral (firewalls, *DMZ*, ...)

2.3.2.3. Costa Rica

Pasamos a la descripción de las brechas detectadas a nivel nacional con respecto al modelo de referencia de arquitectura planteado.

Infraestructura de comunicaciones

Costa Rica cuenta con el sistema centralizado de sistemas de información *EDUS*, por lo que en gran medida algunos de los grandes problemas de interoperabilidad entre los diversos centros de salud de atención a priori están resueltos.

A continuación, se describen las carencias detectadas:

- Creación de los maestros necesarios para la identificación única a nivel nacional de los conceptos relevantes de cara a la interoperabilidad nacional con la Red *RACSEL*:

    - Posibilidad de utilización de *OID´s* nacionales o internacionales

- Necesidad de articular a nivel nacional un *Resumen de Paciente* para poder realizar el traspaso de información transfronterizo, mediante documento *CDA*:

    - Dicho *Resumen de Paciente* podrá ser custodiado en el hospital de referencia del paciente y quedar marcado en el registro de datos de pacientes nacional.

- Creación del **Conector Nacional**, para proporcionar la implementación de los servicios necesarios al *PCN* y así poder interoperar con la Red *RACSEL*

    - Adecuación de la mensajería nacional propia a la mensajería requerida por el *PCN* según los perfiles *IHE* que se utilizarán en la Red *RACSEL*.

    - Servicio de traducción:

        Para cualquiera de las codificaciones utilizadas a nivel nacional y que difieran de lo planteado en el modelo de referencia:

        - Codificación médica

        - OID´s nacionales – OID´s de la Red

        Estándares de comunicación

- **Perfiles *IHE***

Costa Rica en la actualidad para el intercambio de información entre las entidades utiliza mensajería *XML* con formato propio, pero la mensajería definida para la Red *RACSEL* sigue los perfiles *IHE*. Para poder interoperar con el resto de los países a través de la Red *RACSEL* será necesario que en el *Conector Nacional,* antesala al *Punto de Contacto Nacional*, se realice una adecuación de los mismos.

- **Gestor terminológico**

En la mensajería existe un conjunto de conceptos que pertenecen a dominios delimitados (por ejemplo **h**-hombre, **m**-mujer) que deben compartir emisor y receptor para su correcta interpretación. Estos conceptos deben estar, por tanto, identificados y codificados en un catálogo unificado a nivel nacional.

Uno de estos dominios es el catálogo de medicamentos, para el que se ha escogido *SNOMED CT* a nivel de la Red *RACSEL*. **Costa Rica**, en la actualidad, no está utilizando *SNOMED CT*, por lo que se deberá proceder a la creación de un servicio de mapeo y traducción entre *SNOMED CT* y el catálogo de medicamentos nacional, previo al envío de la información a través de la Red *RACSEL*.

Este mismo servicio de mapeo y transformación deberá implementarse para el resto de catálogos y dominios en los que el país difiera con respecto a la Red *RACSEL*.

Seguridad y auditoría

- Gestor de auditoria

Para el intercambio de información trasfronteriza será necesario a nivel nacional, y dentro del **Conector Nacional,** contar con un gestor de auditoria que trace tanto entradas como salidas de las peticiones.

Seguridad

Costa Rica debe adaptar su red de salud nacional para acoger las necesidades de seguridad que ha de tener la Red *RACSEL*:

- Certificados *X509*, con los que realizar:
    - Certificado de Servidor para la encriptación de las comunicaciones
- Ticket *SAML*
- Incorporación de las piezas de infraestructura necesarias que garanticen la seguridad perimetral (firewalls, *DMZ*, ...)

2.3.2.4. Uruguay

Pasamos a la descripción de las brechas detectadas a nivel nacional con respecto al modelo de referencia de arquitectura planteado.

Infraestructura de comunicaciones

Uruguay cuenta con una arquitectura distribuida y la plataforma de salud está en proceso de despliegue de servicios, y también abarca la implantación del *HCEN* en todos los proveedores de salud.

A continuación, se describen las carencias detectadas:

- Adecuación del índice de pacientes con el que cuenta la infraestructura nacional para identificar de forma inequívoca a los pacientes con la inclusión de los parámetros de:
    - Marcaje de consentimiento Informado por parte del paciente para aceptación de traspaso de información transfronterizo.
- Revisión de los maestros necesarios para la identificación única a nivel nacional de los conceptos relevantes de cara a la interoperabilidad nacional con la Red *RACSEL*
- Necesidad de articular a nivel nacional un *Resumen de Paciente* para poder realizar el traspaso de información transfronterizo, mediante documento *CDA*:
    - Dicho *Resumen de Paciente* podrá ser custodiado en el hospital de referencia del paciente y quedar marcado en el registro de datos de pacientes nacional.
- Creación del *Conector Nacional*, para proporcionar la implementación de los servicios necesarios al *PCN* y así poder interoperar con la Red *RACSEL*
    - Adecuación de los perfiles *IHE* utilizados en **Uruguay** a los que se utilizarán en la Red *RACSEL*
    - Servicio de traducción:

        Para cualquiera de las codificaciones utilizadas a nivel nacional y que difieran

de lo planteado en el modelo de referencia:

- Codificación médica
- *OID´s* nacionales – *OID´s* de la Red

Estándares de comunicación

- **Perfiles *IHE***

Uruguay, ya utiliza los perfiles *IHE*, como marco técnico, así pues, solo será necesario la adaptación de los perfiles utilizados en la actualidad a los propuestos en el *Modelo de Arquitectura* de referencia para el traspaso transfronterizo.

- **Gestor terminológico**

Con respecto al servidor terminológico, **Uruguay** cuenta con un servidor terminológico que utiliza *SNOMED CT*, y cuentan con una extensión nacional de medicamentos de *SNOMED CT*. Por lo que la codificación de medicamentos estará resuelta.

El resto de catálogos se deberá analizar las diferencias entre los catálogos de **Uruguay** y los utilizados en la Red *RACSEL*. En caso de encontrar diferencias se deberá implementar el servicio de mapeo y transformación entre catálogos y códigos.

Seguridad y auditoría

- Gestor de auditoria

Para el intercambio de información trasfronteriza será necesario a nivel nacional, y dentro del *Conector Nacional*, contar con un gestor de auditoría que trace tanto entradas como salidas de las peticiones.

- Seguridad

Uruguay debe adaptar su red de salud nacional para acoger las necesidades de seguridad que ha de tener la Red *RACSEL*:

- Certificados *X509*, con los que realizar
    - *Certificado de Aplicación* para la realización de firma digital y encriptación de la mensajería
    - *Certificado de Servidor* para la encriptación de las comunicaciones
- Ticket *SAML*
- Incorporación de las piezas de infraestructura necesarias que garanticen la seguridad perimetral (firewalls, *DMZ*, ...)

2.3.2.5. Chile

Pasamos a la descripción de las brechas detectadas a nivel nacional con respecto al modelo de referencia de arquitectura planteado.

Descripción de las brechas detectadas a nivel nacional con respecto al modelo de referencia de arquitectura planteado.

Infraestructura de comunicaciones

Chile cuenta con un sistema distribuido en nodos. En la actualidad la integración a nivel nacional de los sistemas se realiza punto a punto, puesto que no se cuenta con una plataforma tecnológica unificada a nivel nacional .

Chile está realizando un fortalecimiento de la red de comunicaciones, para poder dar soporte de calidad a la red de salud nacional.

A continuación, se describen las carencias detectadas:

- Necesidad de identificar de forma inequívoca a los pacientes a nivel nacional y también para el traspaso de información transfronteriza. Se cuenta como iniciativa de la carpeta personal de paciente. Creación de un índice de pacientes para identificar de forma inequívoca a los pacientes con la inclusión de los parámetros de:
    - Centro de referencia del paciente
    - Marcaje de consentimiento informado por parte del paciente para aceptación de traspaso de información transfronterizo.
- Revisión de los maestros necesarios para la identificación única a nivel nacional de los conceptos relevantes de cara a la interoperabilidad nacional con la Red *RACSEL*:
    - Posibilidad de utilización de *OID´s* nacionales o internacionales
- Necesidad de articular a nivel nacional un *Resumen de Paciente* para poder realizar el traspaso de información transfronterizo, mediante documento *CDA*:
    - Dicho resumen de paciente podrá ser custodiado en el hospital de referencia del paciente y quedar marcado en el registro de datos de pacientes nacional.
- Creación del *Conector Nacional*, para proporcionar la implementación de los servicios
- necesarios al *PCN* y así poder interoperar con la Red *RACSEL*
    - Adecuación de los *XML´s* propios utilizados a los perfiles *IHE* que se utilizarán en la Red *RACSEL*.
    - En un futuro se plantea la utilización de *FHIR* como estándar de mensajería, en ese caso se deberá realizar la readaptación en el *Conector Nacional* , para adecuación a los perfiles *IHE*.
    - Servicio de traducción:

        Para cualquiera de las codificaciones utilizadas a nivel nacional y que difieran de lo planteado en el *Modelo de Referencia*:

        - Codificación médica
        - *OID´s* nacionales – *OID´s* de la Red
- La interoperabilidad basada en comunicación punto a punto dificulta el uso de estándares y la localización de la información

Estándares de comunicación

- **Perfiles *IHE***

Chile en la actualidad para el intercambio de información entre las entidades utiliza mensajería *XML* con formato propio, pero la mensajería definida para la Red *RACSEL* sigue los perfiles *IHE*. Para poder interoperar con el resto de los países a través de la Red *RACSEL* será necesario que en el *Conector Nacional*, antesala al *Punto de Contacto Nacional*, se realice una adecuación de los mismos.

- **Gestor terminológico**

Con respecto al servidor terminológico, **Chile** cuenta con un servidor terminológico que utiliza *SNOMED CT*, y cuentan con una extensión nacional de medicamentos de *SNOMED CT*. Por lo que la codificación de medicamentos estará resuelta.

El resto de catálogos se deberá analizar las diferencias entre los catálogos de **Chile** y los utilizados en la Red *RACSEL*. En caso de encontrar diferencias se deberá implementar el servicio de mapeo y transformación entre catálogos y códigos.

Seguridad y auditoría

- Gestor de auditoria

Para el intercambio de información trasfronteriza será necesario a nivel nacional, y dentro del *Conector Nacional*, contar con un gestor de auditoría que trace tanto entradas como salidas de las peticiones.

- **Seguridad**

Chile debe adaptar su red de salud nacional para acoger las necesidades de seguridad que ha de tener la Red *RACSEL*:

- Certificados *X509*, con los que realizar
    - *Certificado de Aplicación* para la realización de firma digital y encriptación de la mensajería
    - *Certificado de Servidor* para la encriptación de las comunicaciones
- Ticket *SAML*
- Incorporación de las piezas de infraestructura necesarias que garanticen la seguridad perimetral (firewalls, *DMZ*, ...)

3. Recomendaciones

3.1. Introducción

En este apartado , se plantea una propuesta de las recomendaciones con respecto a la implementación del *Modelo de Arquitectura* de referencia que se propone, para poder alcanzar la meta del traspaso transfronterizo de información clínica entre los países pertenecientes a la Red *RACSEL*.

3.2. Necesidades previas

3.2.1. Gobernanza de la Red RACSEL

La *Commission Global Governance* creada en 1992 por iniciativa de **Willy Brandt** definió la gobernanza como *la suma de diferentes modos en que los individuos y las instituciones, públicos y privados, gestionan los asuntos comunes. Es un proceso continuo de cooperación y acomodación entre intereses diversos y conflictivos. Incluye a las instituciones oficiales y a las dotadas con poderes ejecutivos, así como los acuerdos informales sobre los que los pueblos y las instituciones se ponen de acuerdo o que prevén serán de su interés*. En 1995 el informe de las **Naciones Unidas** sobre la gobernanza la definió como *el conjunto de diferentes procesos y métodos a través de los cuales los individuos y las instituciones, públicas y privadas, gestionan los asuntos comunes.*

Los países pertenecientes a la Red *RACSEL*, cuentan a nivel nacional de comités *TIC*, para poder abordar el proyecto transfronterizo, apostamos por la creación de una gobernanza conjunta para el proyecto, para tratar de unificar las posturas entre los diferentes gobiernos o entidades participantes y poder abordar la toma de decisiones.

Se podría plantear la creación de una **Comisión de Interoperabilidad,** formado por miembros de cada uno de los comités *TIC* nacionales, para poder marcar las bases y necesidades para alcanzar la finalidad del proyecto de realizar un traspaso transfronterizo de información clínica entre los países miembros de la Red *RACSEL*.

Dicho comité se marca como un objetivo estratégico, basado en un conjunto de principios para cuya operatividad se han de aplicar a determinados medios. Los objetivos principales deberían ser:

- Ejercer de puente entre expertos y los tomadores de decisiones.
- Mejorar y alinear entorno a las políticas de salud a nivel de la Red *RACSEL* y nacional
- Fortalecer la gobernanza política de la e-salud
- Coordinar y consolidar las actividades en curso
- Reforzar y apoyar a las naciones pertenecientes a la Red *RACSEL* para garantizar el despliegue y el uso de los modelos de referencia que se plantean en esta consultoría
- Proporcionar orientaciones esenciales y apoyo a las iniciativas en materia de **eSalud**, que puedan surgir en los países pertenecientes a la Red *RACSEL*
- Explotar todo el potencial del conocimiento existente

- Garantizar un uso rentable de los recursos sanitarios

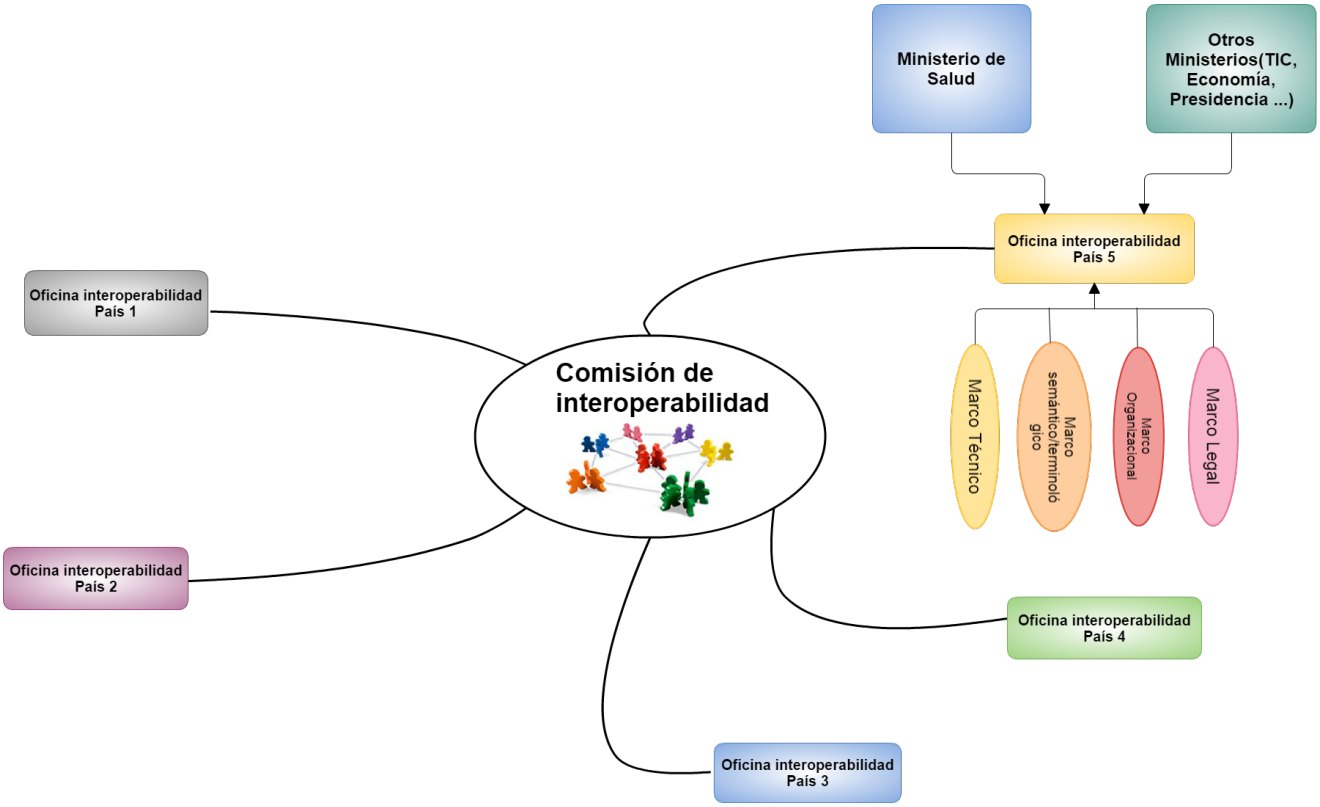


Ilustración 36. Comisión de Interoperabilidad para la Región

Así pues, se estaría hablando de la generación de una esta **Comisión de Interoperabilidad** para que velase por el buen cumplimiento de las bases marcadas del proyecto, basándose en los siguientes preceptos:

- **Marco técnico**
  - Permitir la transferencia segura de datos sanitarios entre prestadores de atención en diferentes regiones y naciones pertenecientes a la Red *RACSEL*
  - Permitir la continuidad de la atención a través de los sistemas internos mediante la interoperabilidad de los sistemas electrónicos de registro de salud
- **Identificación y autenticación**
  - Asegurarse de que sólo los profesionales de la salud autorizados con una relación de tratamiento hacia el paciente tengan acceso a los datos de salud
  - Asegurarse de que el paciente es identificado de una manera segura e inequívoca
  - Permitir el registro de acceso seguro a los datos de salud, mediante auditorías
- **Semántica y terminología**
  - Asegurar que los datos médicos sean entendidos e interpretados y de manera unificada
  - Garantizar datos comparables de alta calidad para el seguimiento, la investigación y la gobernanza de los sistemas de salud

- **Aspectos jurídicos y organizativos**

  - Velar por que se mantenga una protección adecuada de la vida privada al intercambiar datos médicos a través de las fronteras

  - Garantizar que el consentimiento libremente consentido, específico e informado del paciente esté garantizado en situaciones de atención transfronteriza

  - Mejorar la seguridad jurídica de los profesionales de la salud cuando utilicen datos médicos como contribución al tratamiento de pacientes de otros estados miembros

  - Aclarar las responsabilidades si se han superado los derechos a la protección de datos

  - Promover un uso sostenible y bien integrado de los servicios de **eSalud**

Para tal fin podrían valerse de estos procesos y acciones de los mismos:

Proceso	Acciones
Planificación e iniciación	• Definir y comunicar los programas e hitos de la evaluación regional a nivel proyecto. • Elaborar y comunicar los marcos, herramientas y plantillas para la supervisión y evaluación regional. • Ofrecer asesoramiento y apoyo a los equipos a nivel de actividad para definir los indicadores y objetivos adecuados en apoyo de los indicadores y objetivos a nivel regional.
Análisis y elaboración de informes de progreso	• Cotejar los informes a nivel de actividad sobre el desempeño real comparado con el objetivo para los indicadores • Coordinar con los equipos a nivel de actividad para investigar el desempeño e intentar comprender las causas de las divergencias. • Elaborar informes en los que se describa el desempeño real comparado con el objetivo para los indicadores a nivel regional. • Identificar las causas de las divergencias en los desempeños real y objetivo a nivel regional
Planificación de las medidas correctivas	• Coordinarse con los equipos a nivel de actividad para estudiar las medidas correctivas que puedan adoptarse para resolver las divergencias a nivel de actividad y a nivel regional • Identificar y evaluar las medidas correctivas a nivel de regional para resolver las divergencias en el desempeño real y el objetivo a nivel nacional • Evaluar la repercusión, los costes y los riesgos de implementar las medidas correctivas a nivel regional. • Examinar y conseguir la aprobación de las medidas correctivas a nivel regional por parte del comité de dirección del proyecto. • Gestionar los cambios del alcance del programa nacional (en su caso) para implementar las medidas correctivas para alcanzar los hitos del proyecto.
Perfeccionamiento	• Identificar las medidas objetivo para los indicadores que puedan resultar poco realistas o inalcanzables en el plazo necesario • Coordinarse con los equipos a nivel de actividad para estudiar los cambios de los objetivos a nivel de actividad • Estudiar las repercusiones sobre las medidas objetivo a nivel nacional para los indicadores • Elaborar la revisión de las medidas objetivo nacionales para los indicadores • Examinar y conseguir la aprobación por parte del comité de dirección del programa de la revisión de las medidas objetivo nacionales

Las funciones fundamentales de tal marco técnico podrían englobarse en:

- Asesorar en la formulación del plan estratégico de *TIC*
- Propiciar la modernización la utilización de las tecnologías más actuales en las *TIC* en el entorno *RACSEL*
- Proponer las políticas generales sobre *TIC*
- Revisar periódicamente el marco para la gestión de *TIC*
- Proponer los niveles de tolerancia al riesgo.
- Presentar al menos semestralmente o cuando las circunstancias así lo ameriten, un reporte sobre el impacto de los riesgos asociados a *TIC*
- Monitorear que el **Comité de Interoperabilidad** tome medidas para gestionar el riesgo de *TI* en forma consistente con las estrategias y políticas y que cuenta con los recursos necesarios para esos efectos
- Recomendar las prioridades para las inversiones en *TIC*
- Asegurar que *TIC* contribuya a los objetivos estratégicos, así como también los costos y los riesgos relacionados
- Proponer el *Plan Correctivo-Preventivo* derivado de la auditoría y supervisión externa de la gestión de *TIC*
- Dar seguimiento a las acciones contenidas en el *Plan Correctivo-Preventivo*.

Rol	Perfil
Tecnólogo	• Administradores de sistemas • IT. Soporte • Arquitectos Informáticos
Gestión	• Coordinadores de proyectos • Gestores del sector TIC aplicada a la salud
Salud	• Profesionales del ámbito de la salud con gestión TIC • Biomédicos
Administraciones Públicas	• Profesionales TIC que gestionen a nivel de la administración pública las necesidades del proyecto

Proponemos que estos sean los pasos principales a dar para el establecimiento de la estrategia, a alto nivel.

 Adopción efectiva de la estrategia por el **Comité de Interoperabilidad.** Asunción de la dirección de las necesidades, tiempos y objetivos. Definición de los indicadores de evaluación del éxito de la estrategia y definición del alcance del modelo.

 Definir modelo y gobierno de la relación del negocio con sistemas de información. Cómo se van a definir los grupos funcionales, cómo se van a adjudicar las responsabilidades, qué criterios de priorización se van a seguir, etc.

 Definir modelo y gobierno tecnológico, de forma independiente, de manera que la respuesta tecnoló-

gica mantenga su evolución y capacidad de adaptación a las necesidades funcionales, aunque el modelo de traspaso no progrese al mismo tiempo.

Modelar el negocio, todos sus flujos, procesos de intercambio de información con actores, casos de uso, utilización de datos maestros, etc. Requiere un gran nivel de participación por parte de los expertos en el proyecto y tiempo.

 Establecer marco de normas y estándares, políticas de uso y difusión y procedimientos.

 Definir datos maestros para el proyecto y las responsabilidades sobre los mismos.

 Convergencia de los sistemas al nuevo modelo, proyecto a proyecto, en el marco de un macroproyecto global, asegurando la coexistencia con lo existente.

3.2.2. Integraciones nacionales: Digitalización y estructuración de la información de salud

Mediante la digitalización de todos los sistemas de información de los proveedores de salud, el sistema es lo suficiente maduro para poder hacer posible la interoperabilidad con otros sistemas que se encuentren en el mismo estado, pudiendo hacer intercambios integrales de cualquier apunte clínico de los pacientes.

Es importante que se plantee la necesidad que la información almacenada en los sistemas de información dentro de cada una en los sistemas de los proveedores, debe realizarse de forma estructurada.

Ilustración 37 Modelo de interoperabilidad

Para que la interoperabilidad sea posible es condición primordial que se establezcan criterios de normalización y equivalencia entre los datos de manera que estos datos queden identificados y puedan ser tratados de manera automática por los diferentes sistemas. La interoperabilidad no consiste en que se envíen informes y documentos entre los sistemas entre sí, sino que los datos generados en un sistema puedan ser tratados por los otros y manejados de manera fiable por los profesionales que operan con los diferentes sistemas.
La interoperabilidad permitirá que cada servicio de salud pueda tener su propio sistema de información, no siendo necesario que todos tengan el mismo para que sean interoperables.
Cada **Entidad Proveedora de Salud** (*EPS*) puede tener sus propias iniciativas, sus propios sistemas que pueden marcar su aspecto diferencial de calidad frente a otros, sin que la imposición de un sistema igua-

litario cercene su capacidad de innovación y desarrollo.

Se debería contemplar esta digitalización completa de los servicios de salud de cada una de las naciones, como la antesala de la posibilidad de intercambiar la información con los miembros de la Red de *RACSEL*. Ello se da por el hecho que sólo en el caso de que los países cuenten con una red sanitaria digital, las peticiones que se puedan llegar a realizar entre los países contendrán la información actualizada y con la seguridad que es necesaria para poder realizar una consulta con la calidad esperada.

3.2.2.1. Digitalización/ Estructuración de las historias clínicas en las Entidades Proveedoras de Salud (EPS´s)

Contar con la información clínica de manera estructurada y digitalizada (en el componente histórico) debería considerarse la prioridad para poder realizar un traspaso transfronterizo de información.

Se ha de tener en cuenta que la digitalización completa de las historias clínicas, debería realizarse siguiendo los estándares, para conseguir la posible interoperabilidad y el posible intercambio de información, con otros sistemas y con la Red *RACSEL*.

Tanto para la interoperabilidad sintáctica, referida a la estructura de la comunicación, como para la interoperabilidad semántica que hace referencia al significado de la comunicación, el sector salud ha desarrollado y apropiado estándares para varios propósitos relacionados con mensajería, terminología, documentos, esquemas conceptuales, aplicación y arquitecturas.

3.2.2.1.1. Evaluación de HIMSS

Para poder evaluar los niveles de digitalización de la información clínica de las *EPS´s*, nosotros en este apartado hacemos mención a la guía *EMRAM* de HIMSS Analytics.

Como se ha venido desarrollando a lo largo del documento de recomendaciones, uno de los puntos previos a poder realizar un envío de información clínica transfronteriza, pasa por tener el sistema de salud que permita la interoperabilidad entre todas las entidades, con el intercambio de información clínica entre las mismas.

Para alcanzar ese objetivo, es necesario que, las entidades proveedoras de salud digitalicen y estandaricen la información.

El **Modelo de Adopción EMR** (*EMRAM*), está orientado a los hospitales**,** y sirve para realizar un seguimiento de su propio progreso hacia un entorno completamente digital (sin papel). *EMRAM* determina la capacidad de los hospitales utilizando un registro médico electrónico (*EMR*), que va desde sistemas auxiliares básicos, hasta llegar a un entorno *EMR* completamente digital.

Uno de los grandes aportes de esta evaluación es que, junto con identificar el nivel en que se encuentra cada establecimiento, entrega un análisis de las brechas que dificultan su avance hacia niveles más altos y recomienda un mapa de ruta para alcanzarlos.

Hoy, en **Latino América**, existen ocho hospitales certificados en *Etapa 6*, siete de los cuales están en **Brasil** y uno en **Chile**.

EMR ADOPTION MODEL

EMR Adoption Model SM	
Nivel	**Capacidades Requeridas**
Stage 7	Registro Médico Eléctronico (EMR) esta completamente integrado con todas las áreas clínicas (ej. Cuidados Intensivos, Emergencia, Consultas) sustituyendo a todos los registros (clínicos) en papel. Se utilizan standards tales como CCD/CCR para compartir datos; Data Warehouse para analizar datos clínicos y generar informes
Stage 6	La documentación clínica interacciona con el sistema de apoyo a la toma de decisiones (CDSS) basado en elementos de datos discretos. Y Circuito Cerrado de Administración de Medicamentos.
Stage 5	La solución de Gestión de Imagenes esta integrada con el registro médico eléctronico y reemplaza, en su totalidad, a todas las imagenes basadas en pelicula
Stage 4	La Prescripción Eléctronica provee apoyo a la decisión clínica (basada en reglas definidas) en al menos un servicio clínico y para medicación
Stage 3	La documentación clínica, peticiones eléctronicas para cuidados médicos o de enfermería. incluye el seguimiento de la administración de medicamentos (eMAR)
Stage 2	El Repositorio de Datos Clínicos / Registro Eléctronico del Patiente permite recolectar y normalizar datos provenientes de diferentes servicios médicos de todo el hospital
Stage 1	Los sistemas de información de los principales servicios de apoyo (Laboratorio, Radiología, Farmacia) estan instalados o los resultados enviados por un proveedor de servicio externo son procesados eléctronicamente
Stage 0	No se tiene implementados sistemas de información en los principales servicios de apoyo (Laboratorio, Radiología, Farmacia) o no se puede procesar y enviar eléctronicamente resultados de un proveedor de servicio externo

Ilustración 38 Modelo de adopción de HIMSS

3.2.3. Interoperabilidad entre Sistemas de Información a nivel nacional

Es necesario que, para poder alcanzar la interoperabilidad a nivel transfronterizo, cada uno de los países cuente con sistemas de información de salud interoperables entre sus diferentes *Entidades Proveedoras de Salud*.

El intercambio de información entre diferentes centros puede realizarse mediante la utilización de servicios web, que puede permitir que la entidad que tiene asignado un asegurado disponga de la información clínica generada fuera de su entidad de referencia.

3.2.3.1. Caso de uso de interoperabilidad entre EPS´s a nivel nacional

Cuando un paciente acude a un servicio de salud que pertenece a una entidad diferente a la que tiene asignada, se ha de generar de manera estructurada un informe por parte de la entidad proveedora de salud.

Los informes pueden acotarse a ingresos de urgencias e intervenciones quirúrgicas, en caso de realizar fases de cara a la incorporación de información.

Ilustración 39 Interoperabilidad Nacional

La *Entidad Proveedora de Salud* deberá enviar a la entidad de referencia del paciente una petición para poder enviar el informe.

Posteriormente a la recepción de la conformidad, se haría el envío del archivo

Con esta información se podría actualizar el informe de *Resumen de Paciente* para la compartición transfronteriza de información.

Para poder llevar a cabo la adopción de la estrategia necesitamos establecer una serie de objetivos estratégicos que deben establecerse como reglas:

- Adoptar un modelo escalable, sostenible y coherente
- Convertir en expertos al personal de las organizaciones
- Establecer marco de normas y estándares, difundirlos y hacerlos cumplir
- El modelo tecnológico debe permitir una gobernanza tecnológica eficaz, la integración de la información de los distintos ámbitos, la modelización adecuada de los procesos para poder automatizarlos en base a la tecnología y la reutilización de todo lo desarrollado de forma eficaz

País	Recomendación
Colombia	• Necesidad de contar con servicios de comunicación en todas las EPS´s para poder interoperar a nivel nacional
Perú	• Necesidad de contar con servicios de comunicación en todas las EPS´s para poder interoperar a nivel nacional
Costa Rica	• Estado muy favorable para poder interoperar a nivel transfronterizo, puesto que, al tratarse de un país con un sistema centralizado, ya se cuenta con la información disponible para poder armar un CDA
Chile	• Debería existir interoperabilidad entre todos los niveles de atención para poder interoperar primero a nivel nacional y posteriormente a nivel trasfronterizo
Uruguay	• Estado muy favorable para poder interoperar a nivel transfronterizo, puesto que ya existe comunicación entre los diferentes niveles de atención a nivel nacional, a través de la red de salud.

3.2.4. Acceso integral de la información clínica del paciente (acceso del paciente a su información de salud)

Entendemos que los proveedores de salud deben asumir, como servicio al público que es, el derecho que asiste a los pacientes de ofrecerles las ventajas y las posibilidades que la sociedad de la información tiene, poniendo a su disposición las tecnologías que faciliten su asistencia.

Además, tal el uso de las tecnologías de la información y las comunicaciones hacen posible acercar la asistencia sanitaria al hogar de los ciudadanos.

Para tal fin sería interesante aplicar las mejoras necesarias en el ámbito sanitario para que la *Salud Digital* sea un derecho de los ciudadanos. Instamos a las distintas administraciones sanitarias a hacer una apuesta decidida por un modelo de *Salud Digital* para que se consagre la relación con las administraciones sanitarias por medios digitales como un derecho de los ciudadanos y pacientes y como una obligación correlativa para aquellas entidades sanitarias, públicas o privadas, que presten servicios públicos. Siendo el reconocimiento del derecho de los ciudadanos y pacientes y su correspondiente obligación el eje a la hora de incorporar las *TIC* en sanidad.

Ilustración 40. Interoperabilidad centrada en el ciudadano
(Informe IDIS)

Mejorar el acceso de los ciudadanos, profesionales, entidades sanitarias y empresas a los servicios de la *Salud Digital* para ello es necesario que:

• Definir de forma clara el catálogo de servicios administrativos, asistenciales y clínicos de la *Salud Digital*, así como las reglas para utilización contando con los profesionales sanitarios

• Identificar las demandas de los pacientes y las dificultades para hacer uso de estos servicios

• Aprovechar la *Salud Digital* para reducir la carga administrativa en la relación con la administración sanitaria.

Es necesario la creación de las condiciones adecuadas para que las redes de *Salud Digital* y los servicios innovadores puedan florecer.

Se pondrá el foco en:

• Analizar las plataformas existentes de *Salud Digital* en el mercado

• Reforzar la confianza y la seguridad de los pacientes en los servicios de la *Salud Digital*, especialmente en relación con los datos personales

• Establecer una colaboración con la industria en materia de ciberseguridad para la seguridad en línea

3.2.5. Identificación de paciente

Para poder realizar un intercambio de información transfronterizo, una de las condiciones que deben cumplirse es la identificación de forma inequívoca de los pacientes a nivel nacional.

A modo de recomendación, y para estandarizar dicho requerimiento, hacemos la propuesta de contar con un **Indice de Pacientes** a nivel nacional (*MPI*), que haga posible la consulta a través de la red cuando se inicia el proceso de intercambio de información clínica entre los países.

Un índice maestro de pacientes resuelve referencias cruzadas del mismo paciente, y es posible realizar una verificación de datos conjuntos incompletos de datos demográficos.

Un *MPI* guarda copias de registros de información demográfica de los pacientes y los identificadores para cada organización. Y asigna un denominador propio a cada uno de los pacientes, para la gestión interna.

Con los datos introducidos en este maestro, la consulta y devolución de datos en las peticiones realizadas desde cualquier país perteneciente a la Red *RACSEL*, cuenta con la seguridad de equivocidad.

A continuación, se presenta una tabla en la que se muestra a modo de ejemplo una serie de datos mínimos a informar.

Datos	**Posibles Valores**
Nombre	Mejorar la consistencia de los datos y normalizar los datos
Nombre II	
Apellido1	Mejorar la coherencia de los datos y normalizar los datos
Apellido2	Mejorar la coherencia de los datos y normalizar los datos
Sexo/ Genero	Value Set Género Administrativo (HL7 V3): M, F, UN
Fecha de nacimiento	Año, mes y día son necesarios

Documento de identidad nacional	
Pasaporte /Identificación de persona/Tarjeta Sanitaria	
Cédula de extrranjería	
Dirección	
Ciudad*	
Estado	
Código Postal	
País	
Teléfono	Utilizar un formato ISO que permita la captura de código de país.
Hospital de referencia	Codificado según maestro

En cada uno de los países pertenecientes a la Red y dependiendo de la mensajería con la que se realice la interoperabilidad, se hace énfasis en la necesidad de este *Maestro de Pacientes* centralizado.

País	Recomendación
Colombia	• No se cuenta con un índice maestro de pacientes a nivel nacional, debería resolverse para poder conseguir la identificación unívoca a través de la Red RACSEL
Perú	• Se encuentra dentro de la previsión de la puesta en marcha del proyecto RENHICE, se aconseja que se preparen todos los sistemas de las EPS´s a adecuar sus sistemas para nutrir al MPI nacional
Costa Rica	• Estado óptimo
Chile	• Necesidad de contar con el repositorio, y la capacidad de las entidades de poder nutrir el índice maestro a nivel nacional
Uruguay	• Estado óptimo puesto que ya cuenta a nivel nacional con un MPI

3.2.6. Catálogos

Al igual que es un requisito indispensable la estandarización e identificación de los pacientes a nivel nacional, otro de los requisitos necesarios para interoperar a nivel nacional y poder hacerlo posteriormente a nivel internacional es la necesidad de contar con catálogos tanto de terminología clínica (*DICOM*, *SNOMED*, *LOINC* ...) como de centros (*EPS´s*), profesionales (diferenciación por roles) y demás ítems que intervengan a la hora de interoperar entre entidades proveedoras de salud y posteriormente entre los países actuales y futuros de la Red *RACSEL*, y que contengan de manera estructurada y unificada la información.

Se recomienda la utilización de *OID´s* para catalogar e identificar este conjunto de ítems. Un *OID* consiste en una estructura en árbol de códigos y descripciones, en la que las ramas representan los dominios de valores y las hojas los diferentes valores que pueden formar parte de ese dominio.

La utilización de los *OID´s* facilita la interoperabilidad semántica entre organizaciones. Un ejemplo de su uso en información clínica podría ser en las comunicaciones entre varios agentes por medio de mensajería electrónica. En esos mensajes suele hallarse información clínica codificada y no saber con exactitud qué catálogo, clasificación o terminología representan esos códigos. Los *OID* nos ayudan a identificar la fuente de información a la que pertenecen esos códigos de forma inequívoca.

3.2.7. Resumen de Paciente

Se ha marcado un conjunto de datos mínimos para poder hacer el intercambio de información transfronterizo.

El contenido del *Resumen del Paciente* no es el expediente médico completo, pero sí contiene la información esencial del paciente para proporcionarle la asistencia necesaria, es decir, aquella información que contiene un conjunto de datos, definidos desde el punto de vista médico, de información de salud esencial y comprensible en el punto de atención para brindar atención segura al paciente.

A nivel nacional será necesario que los estados miembros tengan la posibilidad de exponer a la Red *RACSEL*, de dicho documento con los estándares de calidad de información que son requeridos para tal efecto.

Para tal propósito es necesario contar con la *Interoperabilidad* que se ha mencionado en este documento.

A parte de la estructura que tendrá que realizarse de forma consensuada entre todos los países, tal y como se explicó en el modelo de referencia partimos de que el *Resumen de Paciente* se encontrará actualizado en el país de afiliación del paciente, siendo éste donde el resto de los países realicen la consulta.

La generación del documento en formato *CDA* estructurado hará posible realizar la transcodificación de la información, puesto que, si contamos con un *CDA* no estructurado (con *PDF* incrustado), la transcodificación adquiere un nivel de complejidad en la Arquitectura que creemos que no es el óptimo por el tema de los recursos con los que debe contar la misma.

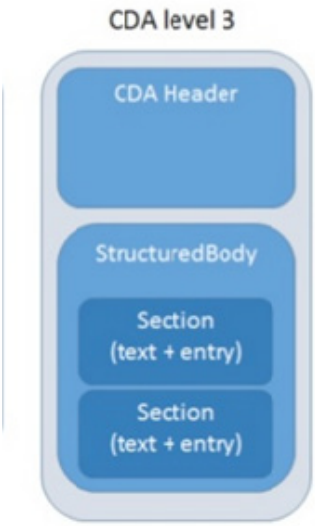


Ilustración 41 Estructura del CDA óptimo para el traspaso transfronterizo

Contando que ésta es la opción más óptima para el traspaso de información, hemos de tener en cuenta las posibilidades reales con las que cuentan los países para alcanzar este propósito.

En la actualidad, no todos los miembros de la Red *RACSEL*, se encuentran en disposición de poder generar un *CDA* estructurado de nivel 3, por lo que como recomendación se propone la adaptación paulatina de los niveles de *CDA*, pasando por los niveles establecidos hasta alcanzar el nivel óptimo, completamente estructurado.

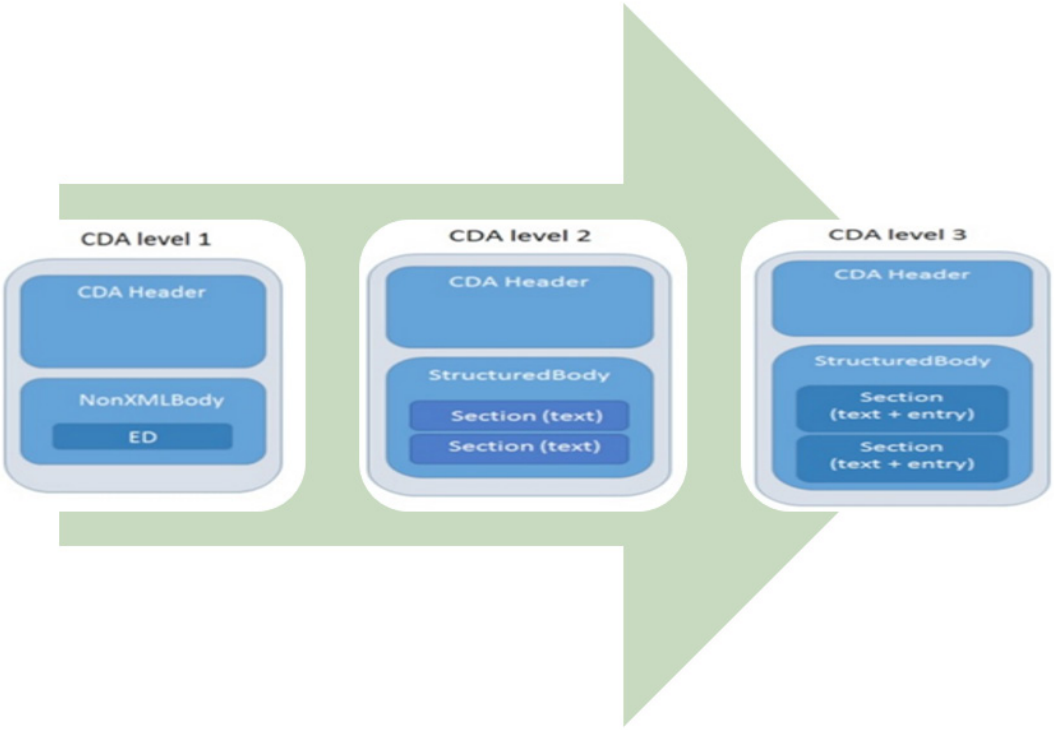


Ilustración 42 Progresión de la implementación de CDA

Creemos que es importante remarcar que el contenido del resumen del paciente debería ser desarrollado por profesionales que tengan un perfil clínico.

Se debe tener en consideración que:

- La actualización del *Resumen de Paciente* en el país de afiliación del paciente evita la complejidad de los flujos a la hora de realizar las consultas transfronterizas.

- El documento estará siempre actualizado, tanto con las prestaciones realizadas en el propio país de afiliación del paciente como en los servicios prestados de forma transfronteriza.

    - Implica que cualquier servicio prestado dentro de las fronteras del país de afiliación y en cualquiera de las entidades prestadoras de salud. Y para ello es imprescindible que exista interoperabilidad entre las instituciones a nivel nacional.

Se evitará la duplicidad del *Resumen de paciente* del mismo ciudadano en diferentes repositorios, puesto que será únicamente reconocido el que se encuentre dentro del país de afiliación del paciente, en el centro de referencia marcado del paciente, en caso de no contar con repositorio nacional centralizado.

País	Recomendación
Colombia	• Necesidad de que las EDP´s tengan la capacidad de poder generar informes estructurados con la utilización de estándares para poder interoperar a nivel nacional
Perú	• Necesidad de que las EDP´s tengan la capacidad de poder generar informes estructurados con la utilización de estándares para poder interoperar a nivel nacional
Costa Rica	• Necesidad de utilización de catálogos estandarizados y la utilización de OID´s • Comenzar a trabajar en la generación de CDA´s
Chile	• Necesidad de que las EDP´s tengan la capacidad de poder generar informes estructurados con la utilización de estándares para poder interoperar a nivel nacional • Necesidad de utilización de catálogos estandarizados y la utilización de OID´s
Uruguay	• Comenzar a trabajar en la generación de CDA´s

3.2.7.1. Propuesta de Actualización de los datos de la prestación en país extranjero

Se hace la propuesta de poder hacer el envío únicamente de los datos que hayan sido modificados del original *Resumen de Paciente*, con lo que, a pesar de tener la misma estructura, los campos insertados serán únicamente aquellos que hayan sufrido modificación en el transcurso de la prestación.

Un ejemplo de este caso de uso sería:

Si el paciente del *país A*, al recibir una prestación de servicio en el *país B*, es diagnosticado con una nueva alergia. De los datos del *Resumen de Paciente* sólo se tendría que actualizar los datos que han sufrido alguna modificación.

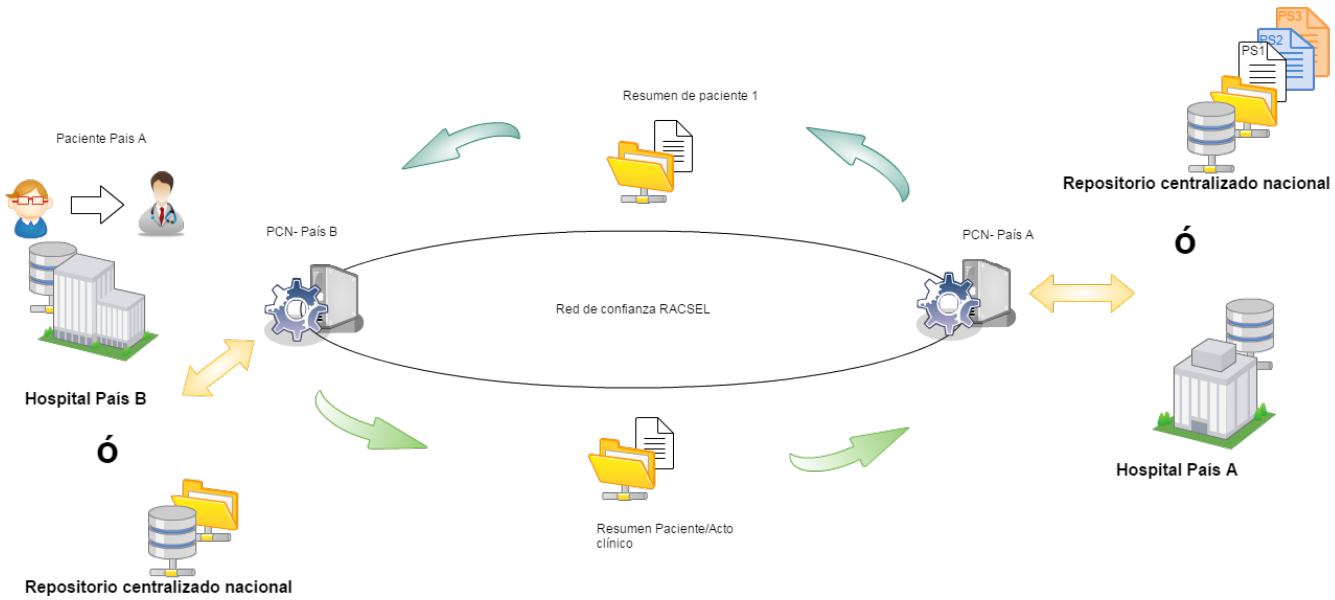


Ilustración 43 Actualización de Resumen de paciente

- El país de afiliación del paciente recibirá desde el país prestador de servicio, los datos a actualizar dentro del *Resumen de Paciente* en la entidad proveedora de salud marcada como de referencia para el paciente, o directamente en el repositorio nacional, dependiendo del caso.

- Los datos se enviarán una vez finalizada la prestación de servicio en el país prestador.

3.2.8. Consentimiento informado de paciente

El consentimiento del paciente es la condición previa legal para cualquier transacción que pueda realizarse a través de la red de confianza de *RACSEL*, antes de que cualquier función pueda ser activada, debe existir un consentimiento válido del paciente.

El paciente debe proporcionar el consentimiento para crear su *Resumen del Paciente* en el país de afiliación y que este pueda ser trasladado a otros países pertenecientes a la *Red.*

Se tomará una disposición para asegurar que, si un paciente no ha dado su consentimiento para acceder a *sus datos* desde otro país perteneciente a la *Red*, no se pueda proceder al intercambio de información, únicamente excluido en el supuesto de *riesgo vital,* en que, en tal caso, se realizaría el traspaso a pesar de no contar con el consentimiento, generando una excepción al respecto en el circuito.

El paciente tiene la opción libre de participar sin restricciones posteriores o influencia negativa para recibir todos los tratamientos médicos necesarios o cualquier otro servicio médico si rechaza la participación.
El paciente puede retirar su consentimiento en cualquier momento.

Este consentimiento debe confirmarse antes de solicitar el acceso a los datos desde el país prestador de servicio al país de afiliación del paciente.

El suministro de datos médicos para los casos de uso médico transfronterizo debe requerir un acto voluntario y documentable de acuerdo por parte del paciente:

- Este acto deliberado debe cumplir con todos los requisitos de un consentimiento informado, libre y documentado de acuerdo con al menos la legislación del país de afiliación del paciente.

- La documentación de este acto deliberado debe ser salvaguardado por medios criptográficos apropiados.

Un país debe asegurar que los datos del paciente sólo son accesibles si existe un consentimiento válido del paciente para el aprovisionamiento de datos, así como de asegurarse que los datos ya no son accesibles después de que el consentimiento respectivo haya sido revocado o expirado.

Cualquier modificación en el consentimiento del paciente debe ser auditada.

3.2.9. Recursos profesionales

Debemos hacer una incisión en la necesidad de contar con el personal cualificado para poder llevar a cabo las acciones necesarias para el desarrollo de este proyecto, con lo que debemos entender que el profesional de **eSalud** debe poseer algunas características importantes que lo diferencian de otros profesionales, entre las que se destacan:

- Fomentar e incorporar las mejores prácticas y los más altos estándares de nomenclatura, terminología, codificación y representación de la información de salud

- Promover y utilizar la información para facilitar la toma de decisiones

- Difundir sus ideas de manera sencilla, directa y libre de jerga, lo que permitirá que el equipo multidisciplinario pueda entenderlo

- Entender y traducir conceptos al lenguaje formal, las informaciones advenidas del paciente, de

los legos en la materia y también del especialista (profesional de la salud, gerente u otro miembro del equipo multidisciplinario)

• Tener iniciativa y buscar la innovación responsable en todos los aspectos de su trabajo, desde los conocimientos técnicos hasta los principios éticos y legales

• Poseer una educación que combine el aprendizaje formal con la experiencia laboral

También se debe incorpora la noción de que el profesional ideal de **eSalud** es el que se mueve de manera fluida entre médicos, enfermeros y administradores de *TIC*, que entiende su lenguaje y que actúa como puente entre ellos en todas las cuestiones relativas a la *eSalud*, tanto organizativas como funcionales o tecnológicas.

3.2.9.1. Notas sobre la centralización de *HIS* y de las autoridades proveedoras de las identidades profesionales

En los dos apartados anteriores se ha podido comprobar como una adecuada estructuración de los servicios de *HIS* y de las autoridades proveedoras de las identidades de la infraestructura nacional sea un elemento muy importante a la hora de construir por encima de ellos un sistema de comunicación distribuido entre países.

Hay múltiples servicios que se requiere que estén disponibles y que afectan directamente a la organización de la información en la infraestructura nacional y cuya implementación pueden resultar mucho más sencilla y eficaz con un sistema centralizado.

A continuación, se ilustra un ejemplo de posible organización de la gestión de las identidades de profesionales a nivel nacional.

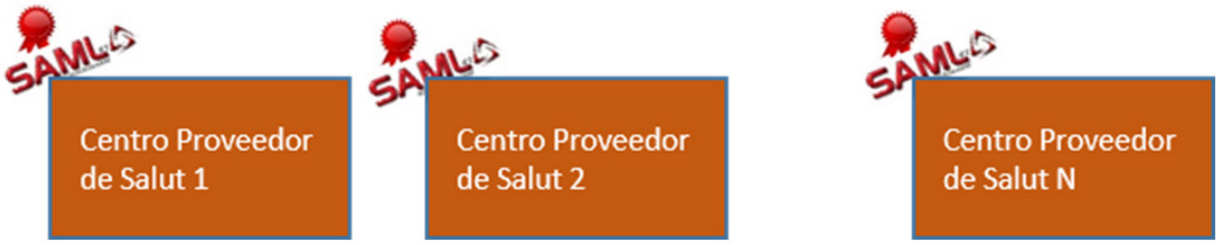


Ilustración 44 Componente de gestión de las identidades – organización punto a punto

En este caso los distintos centros prestadores de servicios de salud son los responsables de autenticar los profesionales de cada centro. Este tipo de gestión, aunque posible, dificulta la integración de cualquier servicio de nivel superior que se tendrá que ofrecer en todos los centros.

Ilustración 45 Componente de gestión de las identidades – organización federada por región sanitaria

En este caso la gestión es semicentralizada, es decir que la resolución de las identidades es mantenida por un repositorio común por región sanitaria. Con este planteamiento el despliegue de un nuevo servicio que involucre la identidad de los profesionales será inmediatamente eficaz a nivel regional.

Ilustración 46 Componente de gestión de las identidades – organización centralizada a nivel nacional

Con este tipo de centralización a nivel de país la integración con un servicio a nivel nacional estará disponible de inmediato para todos los profesionales de cualquier entidad proveedora de salud ubicados en cualquier área sanitaria.

A la hora de implementar un nuevo servicio común la gestión descentralizada de según qué componente de la infraestructura nacional implica más trabajo para el descubrimiento de los repositorios que mantienen la información que se solicite. Esto aplica directamente al servicio de identificación de paciente y al tipo de repositorio de usuario que se plantee, (por ejemplo *MPI* u otra organización más distribuida) o al mismo servicio de gestión del *Resumen de Paciente*. Otro campo de acción puede ser el mantenimiento de un repositorio de políticas de control de acceso a los datos y/o temas de privacidad. Dichas políticas pueden afectar a todo el país de igual manera o bien a regiones autonómicas, por lo que, una correcta estructuración de estos repositorios facilita el acceso a los datos de interés, su control de acceso y la interoperabilidad entre centros distintos.

Una mención particular se tiene que hacer para el repositorio de catálogos clínicos y no clínicos. Se recomienda que estos repositorios y el relativo servidor terminológico sean gestionados a nivel central.

Por último, y de cara al traspaso de información clínica transfronteriza, hemos visto que, si la infraestructura nacional soporta *IHE*, la integración con la Red *RACSEL* a nivel de *CN* resultará más sencilla, no requiriendo la traducción sintáctica de la mensajería.

3.2.10. Red de confianza *RACSEL*

Para poder establecer una red de confianza transfronteriza, se utilizarán diferentes herramientas que garanticen la confidencialidad y privacidad de la red y las comunicaciones. Todos los países dispondrán de un único punto de acceso a la Red *RACSEL*, denominado *PCN* el cual actuará de nexo de unión entre la Red *RACSEL* y el resto de la infraestructura de ámbito sanitario del país.

Dentro del *PCN*, es el **Bound Terminator** quien realiza esta función de separador de fronteras, por lo que deberá disponer, al menos, de:

- Una interfaz de red disponible para conectar con la red *RACSEL*

- Una interfaz de red disponible para conectar con la red nacional

La interfaz de red para *RACSEL* debe permitir conectar con una red virtual privada (*VPN*) que permitirá al *PCN* ver el resto de *PCN*'s de la red. Las características de esta *VPN* se deberán determinar en el momento de implantación del proyecto. Dentro de esta VPN sólo estarán visibles los *Bound Terminator* de cada país, quedando oculta el resto de los sistemas y componentes.

La interfaz de red para la red nacional dará acceso al resto de componentes del *PCN*, incluido el *CN*, lo que permitirá el flujo de comunicaciones entre la red nacional y la Red *RACSEL*.

La red de confianza se apoya también en el uso de tecnología *X509* mediante:

- **Certificado Digital de Servidor** (*Certificados CDS*): Toda comunicación entre 2 *PCN*'s se realizará mediante *SSL Mutual Authentication*. Esto garantizará:
  - Los *PCN*'s deben conocerse y confiar entre sí, ya que previo al intercambio de información, cada *PCN* valida el certificado del otro *PCN*.
  - El mensaje viaja encriptado por el canal de comunicación, de forma que solo los dos *PCN*'s que participan en la comunicación saben desencriptar el mensaje.
- **Certificado Digital de Aplicación** (*Certificados CDA*): Estos certificados permitirán firmar el mensaje emitido por un *PCN*, y validar la firma por el *PCN* receptor. La firma del mensaje garantiza la integridad del mensaje (el mensaje no ha sido modificado) y el no repudio (el mensaje ha sido emitido por el propietario del certificado).

3.2.11. Pruebas de interoperabilidad

Será necesario que los miembros técnicos (ingenieros informáticos, arquitectos informáticos, etc.) que formen parte de los equipos nacionales de los países pertenecientes a la Red *RACSEL* realicen pruebas de interoperabilidad. Para ello será necesario que se apliquen programas informáticos para apoyar el intercambio transfronterizo a través de la red de confianza.

Se plantea como necesario:

- Realizar pruebas unitarias de los distintos componentes que intervienen en la Arquitectura
- Realizar pruebas integradas de todos los componentes de la Arquitectura
- Contar con personal dentro de la oficina de interoperabilidad, que tenga conocimiento sobre *IHE* para poder adaptar la mensajería para el traspaso de información a los *PCN´*s
- Contar con personal dentro de la oficina de interoperabilidad, con conocimientos de generación de *CDA*'s
- Contar con personal dentro de la oficina de interoperabilidad, con conocimientos de desarrollo de *Web Services* y aplicación de *WS-Security*
- Definir el conjunto de casos de prueba necesarios para garantizar el correcto funcionamiento de la plataforma
- Elaborar el informe de calidad de las pruebas, que será validado por el equipo de gobernanza, para garantizar el correcto funcionamiento de la plataforma

3.2.12. Seguridad

La aplicación de las normas de **Seguridad** se realizará por un lado en el entorno nacional, y por otro en la comunicación con la Red *RACSEL*.

Para la comunicación a nivel nacional:

- Las comunicaciones han de ser encriptadas utilizando *TLS* v1.2 con el protocolo de encriptación simétrico *AES*-128
- Utilización de autenticación mutua entre el sistema origen y el **Conector Nacional,** es decir, el reconocimiento mutuo de que cada sistema es quién dice ser
- La comunicación entre el sistema origen y el **Conector Nacional** se debe realizar sobre una red dedicada/Intranet

Para la comunicación a nivel internacional:

- Utilización de una **Red Virtual Privada** (*VPN*)
- Las comunicaciones han de ser encriptadas utilizando *TLS* v1.2 con el protocolo de encriptación simétrico *AES*-128
- Utilización de autenticación mutua en la comunicación entre 2 *PCN*'s

Además, se deberá tener en cuenta que:

- Se utilizará tecnología *SAML2* para la federación de las identidades:
    - Se debe identificar al profesional que está realizando la petición, mediante una aserción *SAML2*
    - Se debe identificar la relación de tratamiento entre el profesional y el paciente mediante una aserción *SAML2*
    - Las aserciones *SAML2* deben venir firmadas por el **Proveedor de Identidades** (*IdP*) que ha autenticado al profesional
    - Las aserciones *SAML* las validará el *PCN* del país que genera el *token SAML*, por lo que deberá disponer de los certificados de los *IdP* que generan el token
- Cada país debe crear las reglas de negocio que determinarán la lógica del control de acceso para:
    - El país prestador del servicio médico debe validar que el profesional está autorizado a acceder a la información que solicita del paciente
    - El país de afiliación del paciente debe validar que el profesional del país prestador está autorizado a acceder a la información del paciente
    - Una de las reglas de negocio consistirá en la evaluación del consentimiento del paciente para la información solicitada.
- Los mensajes que viajen entre dos *PCN*'s estarán firmados para:
    - Garantizar la integridad del mensaje, evitando su modificación

- Garantizar el no repudio por parte del emisor del mensaje, al estar firmado con su propio certificado

La firma debe cubrir tanto el mensaje (*Body*) como los parámetros de cabecera (*Header*)

Recomendaciones técnicas con respecto a la política de seguridad.
• El servidor de Punto de Contacto Nacional debe encontrarse en un entorno seguro, donde el acceso físico sea controlado, monitoreado y permitido sólo al personal autorizado, basado en declaraciones escritas y aceptadas, siguiendo el diseño general y estándares internacionales.
• El acceso lógico al Punto de Contacto Nacional esté protegido por certificados digitales, que sean expedidos por una Autoridad de Certificación que se encuentre debidamente acreditada por las autoridades nacionales.
• Los profesionales deben ser conscientes de la seguridad de la información y estar autenticados en el lugar de acceso. También deberían aceptar la responsabilidad de proteger las contraseñas, las tarjetas inteligentes, las claves privadas, etc., mediante la declaración de una firma.
• El sistema debe usar procedimientos de registro apropiados para asegurar los datos para la pista de auditoría.
• Debe prestarse especial atención a la Autoridad de Certificación, que está en los certificados del Punto de Contacto Nacional, con el fin de garantizar que dicha Autoridad de Certificación puede ser confiable y puede ser aceptada como Autoridad Raíz.
• El software en el que se ejecute el sistema debe estar actualizado e incluir todas las actualizaciones de seguridad necesarias y soportadas.
• Los países pertenecientes a la Red RACSEL deberán cooperar en la investigación de incidentes de seguridad.
• Las auditorías de seguridad deben aprobar el cumplimiento de la instalación marcadas en las directrices previas pactadas.
• Las recomendaciones técnicas de seguridad anteriores deberán ser revisadas cada año por el órgano de gobernanza de la Red RACSEL y las actualizaciones se harán de acuerdo con las necesidades.

3.2.13. Hoja de Ruta

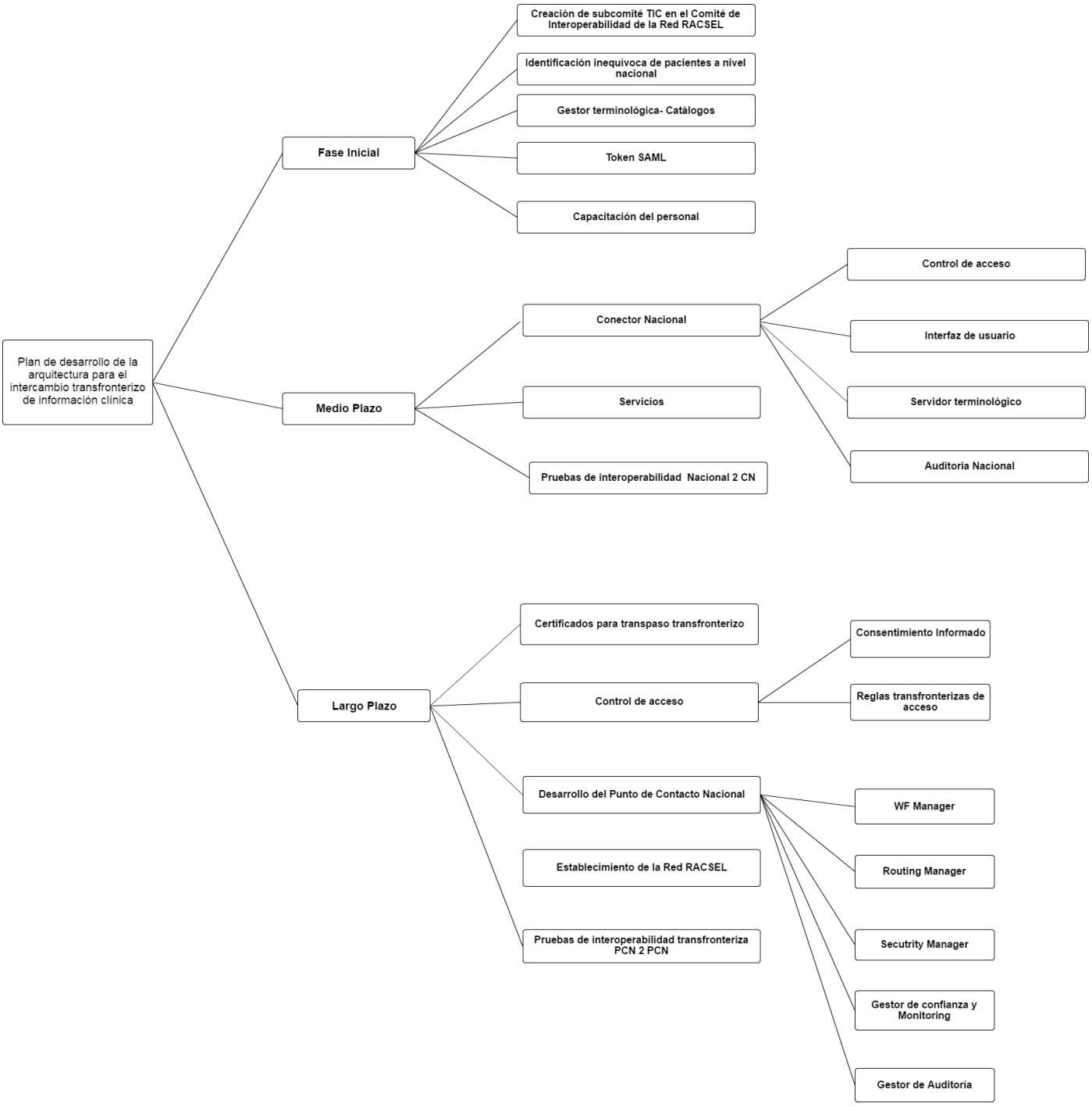
Proponemos asimismo un plan de puesta en marcha que quiere ser el reflejo de un plan ejecutivo de arranque que facilite el enfoque y la definición concreta de tareas al iniciar un proyecto de este tipo.

- Una vez planteada la arquitectura de referencia para la región se debe Iniciar el proceso de modelado a nivel nacional de los conectores:
    - Es necesario que el personal seleccionado adquiera conocimiento práctico de las herramientas e inmersión rápida en el proyecto.
- Implementación de los modelos lógicos y físicos:
    - Adquisición de infraestructuras y aplicaciones, despliegue, formación del personal, etc.
- Difusión de las tareas a desarrollar para la consecución del **Conector Nacional** y posterior difusión de las necesidades a todas las entidades y sus proveedores, que deben también ser conscientes del cambio.
    - Servicios a desarrollar

    - Priorización del desarrollo
    - Reutilización
    - Quién desarrolla y mantiene el servicio
    - Definir las responsabilidades sobre el servicio. o difusión del gobierno del negocio y tecnológico

- Generalización del uso de estándares y normas
- Estandarización de procedimientos de desarrollo
- Difusión de los datos maestros utilizados en el proyecto y de sus formas de actualización, adecuándolas al uso que se haga de los mismos
- Contemplación de la necesidad de nuevas funcionalidades en caso de no contar con ellas, y de su posible evolución

4. Guía de Autoevaluación



4.1. Introducción

La **Guía de Autoevaluación** se concibe como una herramienta que permite establecer la calidad y efectividad de los controles establecidos para cada proceso, para poder determinar la contribución para el logro de los objetivos del proyecto.

Esta **Guía de Autoevaluación** debe ser un análisis crítico y debe identificar y separar los aspectos que afectan los resultados del proyecto, hasta llegar a conocer cada uno de sus elementos constitutivos y sus características. Su propósito es juzgar y valorar sus niveles de resultados, con relación al marco de referencia establecido.

El proceso debe identificar hallazgos en términos de fortalezas y debilidades, entendiendo las fortalezas como aspectos que acercan a los países a la consecución a los requisitos del proyecto, y debilidades aquellos que pueden significar un escollo para alcanzar los umbrales de éxito de este.

Mediante esta **Guía de Autoevaluación** se pretende marcar el camino de aspectos imprescindibles para poder interoperar con la red *RACSEL*, de los actuales países que la componen y de posibles futuras incorporaciones, facilitando así la hoja de ruta.

4.2. Elementos de la Guía de autoevaluación

A continuación, haremos una descripción de los elementos que componen la *Guía de Autoevaluación*, que habrán de ser completados en parte por la consultora y en parte por cada uno de los países.

4.2.1. Objetivo

Marcamos como objetivo principal, el asunto de la consultoría para el componente, que es la creación del *Modelo de Referencia de Arquitectura* para el desarrollo de la **Historia clínica Electrónica de América Latina y el Caribe.**

4.2.2.Subobjetivos

La *Guía de Autoevaluación* estará compuesta por una serie de subconjuntos de requisitos anidados en tres fases (inicial, medio plazo, largo plazo) que se han marcado como necesarias para alcanzar la consecución de los hitos de forma progresiva, para la finalidad del proyecto.

Dentro de los subobjetivos se hará un desglose de las acciones a realizar para alcanzar el objetivo final de la consultoría.

Cada uno de los cuatro componentes comprenderá los ítems detectados como necesarios para tal consecución.

Los subobjetivos estarán divididos en una serie de componentes:

- **Descripción**

Descripción del subobjetivo en la que se hará mención a la característica principal del mismo.

- **Grado de complejidad**

El grado de complejidad marcado entre Bajo - Medio - Elevado para poder alcanzar la consecución del mismo.

- **Dependencias**

Se identificarán las dependencias que pudiera tener el ítem con otro/otros de los componentes : **Normativa, Estándares, Terminología** y **Arquitectura**. O bien del propio componente.

- **Recursos necesarios**

Los recursos necesarios que deben ser creados/tomados en cuenta para la realización del mismo.

- **Disponibilidad de los recursos**

Marcar si los recursos existen en la actualidad o bien si se han de generar.

- **Faseado**

Posibilidad de fasear el objetivo para su consecución, fase inicial - medio plazo - largo plazo.

- **Período de tiempo previsto (en meses)**

Duración estimada para la consecución del subobjetivo, en caso de estar faseado, cada una de las fases incluiría su margen de tiempo previsto.

- **Impacto**

Impacto que este subobjetivo plantea para la actual situación del componente en el país.

- **Beneficios obtenidos**

Descripción de los beneficios que este subobjetivo puede llegar a añadir a nivel nacional.

- **Grado de consecución alcanzado**

Valoración del 1 al 5 del estado de consecución del subconjunto, siendo 1 la fase más inicial y 5 la consecución completa del mismo.

4.3. Esquema de subconjuntos

Plantilla Autoevaluación Componente Arquitectura		
Objetivo		
Plan de desarrollo de la arquitectura para el intercambio transfronterizo de información clínica		
Notas/Acciones: El modelo de referencia se base en una arquitectura para posibilitar el traspaso de información clínica entre los miembros pertenecientes a la Red RACSEL, sin la compartición de elementos comunes.		
Fase Inicial	Medio Plazo	Largo Plazo
• Creación del Subcomité TIC del comité de interoperabilidad de la Red RACSEL • Identificación de paciente a nivel nacional • Gestor terminológico- catálogos • Token SAML • Capacitación de los profesionales técnicos	• Desarrollo del conector nacional • Auditoria • Seguridad:firma y control de acceso • Transformador sintáctic • Transformador semántico • Generación de servicios • Pruebas de interoperabilidad a nivel nacional.	• Certificados traspaso transfronterizo • Control de Acceso • Consentimiento • Reglas transfronterizas de acceso • Desarrollo del PCN: • WF Manager • Routing Manager • Security Manager • Gestor de conf. y Monitoring • Gestor de auditoría • Establecimiento de la Red RACSEL • Pruebas de interoperabilidad a nivel de la Red RACSEL.
Notas/Acciones: Previo a poder realizar la Guía de Autoevaluación, se deberá contar con la interoperabilidad integral de la mayoría de los centros de cada uno de los países, para poder contar con la información a traspasar entre los países.		

Subobjetivo 1: Creación del Subcomité TIC en el Comité de Interoperabilidad de la Red RACSEL	
Descripción	• Necesidad de creación del subcomité para marcar las bases y necesidades del traspaso transfronterizo de información entre los miembros pertenecientes a la Red.
Grado de complejidad	• Medio
Dependencias	• Consenso entre los países para determinar los participantes
Recursos necesarios	• Disponer de un comité TIC a nivel nacional, para gestionar las decisiones a tomar en el desarrollo del proyecto.

Tareas requeridas	• Consensuar:
	  • Estándares a utilizar
	  • Definición de políticas de seguridad y auditoría
	  • Definición de estándares sintácticos.
	  • Resumen de paciente
	  • Consentimiento informado
	  • Seguimiento y mejoras de la plataforma

Faseado	• Fase inicial
Período de tiempo previsto (meses)	• 6 meses
Impacto	• Disponer del personal cualificado para formar parte del subcomité
Beneficios esperados	• Unificación de criterios entre los miembros de la Red RACSEL
	• Posibilidad de poder interoperar intra-nacional entre todos los centros y posibilitar uno de los requisitos indispensables para la interoperabilidad transfronteriza
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 2: Identificación inequívoca de paciente	
Descripción	• Creación del Master Patient Index a nivel nacional, para la identificación de pacientes y correlación con los centros de referencia.
Grado de complejidad	• Medio - Elevado
Dependencias	
Recursos necesarios	• Registro de pacientes
Tareas requeridas	• Identificación de todos los pacientes a nivel nacional con todos los datos mínimos
Faseado	• Fase inicial
Período de tiempo previsto (meses)	• 9 meses
Impacto	• Identificación a nivel nacional estandarizada de los pacientes
Beneficios esperados	• Posibilidad de poder interoperar intra-nacional entre todos los centros y posibilitar uno de los requisitos indispensables para la interoperabilidad transfronteriza
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 3: Gestor terminológico – Catálogos	
Descripción	• Tener catálogos para todos los dominios identificados en la mensajería que deban explotarse (profesionales, centros, medicamentos, alergias, ...). Es necesario identificar todos los dominios identificando con código y descripción todos los conceptos, y que estos dominios sean compartidos, utilizados y entendidos por todos los participantes a nivel nacional
Grado de complejidad	• Alto
Dependencias	• Estandares - Definición de catálogos nacionales
Recursos necesarios	• Directorio de los centros • Directorio de los profesionales • Catálogos semánticos
Tareas requeridas	• Definición e implementación
Faseado	• Fase inicial
Período de tiempo previsto (meses)	• 6 meses
Impacto	• Todas las entidades proveedoras deben utilizar el catálogo unificado para inter-operar satisfactoriamente.
Beneficios esperados	• Identificación estandarizada de todos los profesionales ,centros del país, y catálogos clínicos
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 4: Token SAML	
Descripción	• Utilización de estándares para la federación de identidades entre sistemas independientes. El uso de token SAML permite que el usuario (profesional) solo deba identificarse una única vez, pero pueda utilizar su identidad en otros sistemas, al establecerse un vínculo de confianza entre ambos sistemas
Grado de complejidad	• Alto
Dependencias	• Identificación inequívoca de pacientes y profesionales
Recursos necesarios	• Profesionales con conocimientos sobre la materia
Tareas requeridas	• Implantación de un gestor de identidades con capacidad de generar token SAML
Faseado	• Fase inicial
Período de tiempo previsto (meses)	
Impacto	• Posibilidad de que los sistemas que identifiquen a profesionales tengan la capacidad de generar tokens SAML
Beneficios esperados	• Federación de identidad entre sistemas remotos de forma segura.
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 5: Capacitación de los profesionales	
Descripción	• Necesidad de capacitación en los estándares a utilizar y en la seguridad a aplicar en la Red, tanto a nivel nacional como transfronterizo
Grado de complejidad	• Medio
Dependencias	
Recursos necesarios	• Profesionales para capacitar a los técnicos TIC, sobre la materia necesaria a nivel regional/nacional • IHE • WS-* • Protocolos de seguridad • Costo de los cursos
Tareas requeridas	• Liberación de los profesionales que hayan de realizar las formaciones.
Faseado	• Fase inicial
Período de tiempo previsto (meses)	• 3 meses
Impacto	• Contar con profesionales con los conocimientos necesarios para la consecución de los ítems esperados • Posible incentivación a las entidades que cumplan los objetivos formativos de su personal.
Beneficios esperados	• Capacidad de interoperar a nivel nacional entre EPS´s • Capacidad de poder interoperar con el Conector Nacional
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 6: Desarrollo del conector nacional	
Descripción	• Adaptador para poder interoperar con el resto de los países de la Red RACSEL
Grado de complejidad	• Alto
Dependencias	• Gobernanza Red RACSEL • Catálogos • Identificación de paciente
Recursos necesarios	• Técnicos especializados

Tareas requeridas	• Gestor de auditoria
	• Seguridad:
	  • Firma
	  • Control de acceso
	• Transformador sintáctico
	• Transformador semántico

Faseado	• Medio Plazo
Período de tiempo previsto (meses)	• 9 meses
Impacto	• Tener un conector que haga posible la adaptación de los estándares y los catálogos a nivel nacional y los prepare para la posibilidad de interactuar con el Punto de Contacto Nacional
Beneficios esperados	• Capacidad de poder enviar/recibir información según los estándares de la Red RACSEL
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 6: Desarrollo del conector nacional	
Descripción	• Definición y generación de los servicios para la interoperabilidad con el Conector Nacional
Grado de complejidad	• Medio
Dependencias	• Estándares de mensajería
Recursos necesarios	• Técnicos especializados

Tareas requeridas	• Identificación de Paciente • Obtención de Resumen de Paciente • Actualización de Resumen de Paciente • Consentimiento informado
Faseado	• Medio Plazo
Período de tiempo previsto (meses)	• 9 meses
Impacto	• Posibilitar el intercambio de datos para facilitar la interoperabilidad entre los sistemas
Beneficios esperados	• Posibilidad de preparar el intercambio transfronterizo de información de paciente
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 7: Generación de los servicios	
Descripción	• Definición y generación de los servicios para la interoperabilidad con el Conector Nacional
Grado de complejidad	• Medio
Dependencias	• Estándares de mensajería
Recursos necesarios	• Técnicos especializados
Tareas requeridas	• Identificación de Paciente • Obtención de Resumen de Paciente • Actualización de Resumen de Paciente • Consentimiento informado
Faseado	• Medio Plazo
Período de tiempo previsto (meses)	• 9 meses
Impacto	• Posibilitar el intercambio de datos para facilitar la interoperabilidad entre los sistemas
Beneficios esperados	• Posibilidad de preparar el intercambio transfronterizo de información de paciente
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 8: Pruebas de interoperabilidad a nivel nacional	
Descripción	• Realizar las pruebas de conexión de las EPS´s con el Conector nacional, para el envío de información siguiendo los estándares
Grado de complejidad	• Medio
Dependencias	• Identificación de paciente • Token SAML • Catálogos nacionales • Gestor terminológico • Conector Nacional • Servicios • Certificados
Recursos necesarios	• Capacidades de las EPS's para interoperar
Tareas requeridas	• Definir el conjunto de casos de prueba a realizar
Faseado	• Medio Plazo
Período de tiempo previsto (meses)	• 3 meses
Impacto	• Interoperabilidad nacional
Beneficios esperados	• Certificación de la plataforma para interoperar a nivel transfronterizo
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 9: Certificados transfronterizos	
Descripción	• Disponer de los certificados necesarios para permitir la interoperabilidad entre PCNs de forma segura, completando la red de confianza
Grado de complejidad	• Bajo
Dependencias	•
Recursos necesarios	• Contar con Autoridades Certificadoras
Tareas requeridas	•
Faseado	• Largo Plazo
Período de tiempo previsto (meses)	• 2 meses
Impacto	•
Beneficios esperados	• Seguridad en las comunicaciones
Grado de consecución alcanzado (1 a 5)	•

Subobjetivo 10: Control de acceso	
Descripción	• Reglas de negocio que determinarán si una petición de servicio está autorizada.
Grado de complejidad	• Medio
Dependencias	• Articulación del consentimiento informado
Recursos necesarios	• Técnicos especializados
Tareas requeridas	• Definición de las reglas de negocio que determinarán la autorización o no de acceder a la información
Faseado	• Largo Plazo
Período de tiempo previsto (meses)	• 9 meses
Impacto	• Seguridad
Beneficios esperados	• Limitar el acceso a la información al personal autorizado
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 11: Desarrollo del Punto de Contacto Nacional	
Descripción	• El PCN es el componente que permite a un país conectar a la Red RACSEL para el intercambio de información transfronterizo.
Grado de complejidad	• Alto
Dependencias	• Conectores Nacionales • Creación de los perfiles IHE • Generación de los servicios • Certificados
Recursos necesarios	• Anilla Sanitaria (VPN)
Tareas requeridas	• WebServices • WF Manager • Routing Manager • Security Manager • Gestor de Configuración • Gestor de Monitoring • Gestor de Auditoria
Faseado	• Largo Plazo
Time frame previsto (meses)	• 24 meses
Impacto	• Creación del gateway de acceso a la Red RACSEL
Beneficios esperados	• Posibilidad de interoperar con otros países pertenecientes a la Red RACSEL
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 12: Establecimiento de la Red de Confianza RACSEL	
Descripción	• Posibilitar la conexión segura entre los PCN´s de los países pertenecientes a la Red mediante VPN
Grado de complejidad	• Medio
Dependencias	
Recursos necesarios	• Tecnicos especialistas en comunicaciones
Tareas requeridas	• Identificar las características de la VPN a configurar
Faseado	• Largo Plazo
Time frame previsto (meses)	• 6 meses
Impacto	• Establecer una red de confianza segura
Beneficios esperados	• Comunicación segura entre los PCN´s
Grado de consecución alcanzado (1 a 5)	

Subobjetivo 13: Pruebas de Conexión transfronteriza	
Descripción	• Pruebas de conexión con el resto de los países para interoperar a través de la Red
Grado de complejidad	• Medio
Dependencias	• Conector Nacional • Punto de Contacto Nacional • VPN RACSEL
Recursos necesarios	• Personal técnico cualificado
Tareas requeridas	• Definicion de los casos de prueba • Pruebas de conectividad • Informe de resultados
Faseado	• Largo Plazo
Time frame previsto (meses)	• 3 meses
Impacto	• Interoperabilidad transfronteriza
Beneficios esperados	• Certificación de la plataforma para interoperar a nivel transfronterizo
Grado de consecución alcanzado (1 a 5)	

Glosario

A

AES: *Advanced Encryption Standard*

C

CA: *Certificate Authority*
CDA: *Clinical Document Architecture* (CDA), arquitectura clínica de documentos, de HL7, es un estándar basado en XML para el marcaje de documentos que especifica la estructura y semántica de documentos clínicos para el propósito de facilitar su intercambio en un entorno de interoperabilidad.
CDS: *Certificado Digital de Servidor*
CIE-10: Clasificación internacional de enfermedades correspondiente a la versión en español de las inglesas ICD, siglas de International *Statistical Classification of Diseases and Related Health Problems*) y que determina la clasificación y codificación de las enfermedades y una amplia variedad de signos, síntomas, hallazgos anormales, denuncias, circunstancias sociales y causas externas de daños y/o enfermedad...
CN: Conector Nacional

D

DICOM: *Digital Imaging and Communications in Medicine*. Protocolo estándar de comunicación entre sistemas de información y a la vez un formato de almacenamiento de imágenes médicas que aparece como solución a los problemas de interoperabilidad entre tipos de dispositivos.

E

ebXML: *Electronic Business using eXtensible Markup Language*. Aunque la última versión es la 4.0, el más implementado es el 3.0.
ebRIM: *Electronic Business - Registry Information Model*. Especifica tipos de metadatos y contenido que puede ser almacenado en un RegRep ebXML
ebRS: *Electronic* Business - Registry Service and Protocols. Especifica servicios y protocolos para RegRep ebXML
EMRAM: *European Medical Report Adoption Model***.**
EPS : Entidad Proveedora de Salud

F

FHIR: *Fast Healthcare Interoperability Resources*

I

IdP: *Identity Provider.*
ISO: La *Organización Internacional de Normalización* (del nombre original en inglés, *International Organization for Standardization*, conocida por las siglas ISO) es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

L

LOINC: Significa *Identificadores Nombres y Códigos Lógicos de Observación* por sus siglas en inglés.

LOINC proporciona una clasificación completa de observaciones clínicas en medicina. Se utiliza especialmente para codificar resultados de laboratorio

O

OASIS: *Organization for the Advancement of Structured Information Standards* (Organización para el Avance de Estándares de Información Estructurada, en idioma castellano), es un consorcio internacional sin fines de lucro que se orienta al desarrollo, la convergencia y la adopción de los estándares de comercio electrónico y servicios web. Los miembros del consorcio deciden cómo y qué trabajó se realiza mediante un proceso abierto y democrático. El trabajo técnico se lleva a cabo en categorías tales como: Energía, Servicios Web, Comercio electrónico, Internet de las cosas, Seguridad, Leyes y Gobierno, Cadena de Suministro, Administración de Computación, Focos de Aplicación, Document-Centric, Procesamiento XML, Conformance/Interop y Dominios Industriales, entre otras áreas.

P

PAP: *Policy Administration Point,* en el ámbito de uso de tecnología XACML.
PCN : Punto de Contacto Nacional
PDP: *Policy Decision Point,* en el ámbito de uso de tecnología XACML.
PEP: *Policy Enforcement Point,* en el ámbito de uso de tecnología XACML.
PIP: *Policy Information Point,* en el ámbito de uso de tecnología XACML.
PKI: *Public Key Infraestructure*

S

SAML2: *Security Assertion Markup Language v2.*
SNOMED CT: Significa *Nomenclatura Sistematizada de Medicina – Términos Clínicos* por sus siglas en inglés. Tiene como propósito ambicioso proporcionarnos todos los conceptos que alguna vez se hayan expresado en el dominio de la medicina en forma no ambigua, es decir, sin riesgo de confusión.
SOAP: *Simple Object Access Protocol*
SSL: *Secure Socket Layer*
SP: *Service Provider*
STS: *Secure Token Service*

T

TLS: *Transport Layer Security*
TSL: *Trust-service Status List*

U

URI: *Uniform Resource Identifier*

V

VPN: *Virtual Private Network*

X

XACML: **OASIS** standard for *E**X**tended **A**ccess **C**ontrol **M**arkup **L**anguage* que implementa el control de acceso a través de la gestión distribuida de políticas de seguridad basadas en atributos en conformidad con la especificación que se encuentra aquí. La última versión consolidada es la 3.0.
XML: *eXtensible Markup Language*

W

WSDL: *Web Service Definition Language*
WS-Policy: *Web Service Policy Framework*
WS: *Webservice*, Servicio Web
WS-Policy: *Web Service Policy Framework*
WS-Security: *Web Service Security*
WS-SecurityPolicy: *Web Service Security Policy Framework*
WS-Trust: *OASIS standard que proporciona extensiones para WS-Security y la gestión de Tokens seguros en el ámbito de servicios Web*

Referencias

A continuación, mostramos un listado de las fuentes utilizadas para la elaboración de este documento:

- *Conjunto de herramientas para una estrategia de eSalud nacional*. Biblioteca de la OMS – **http://www.who.int/library/es/**
- *European Interoperability Architecture (EIA) action of ISA*
- *IHE International, IHE IT Infrastructure Technical Framework*: **https://www.ihe.net/**
- *Historia clínica nacional, informe de situación* – Ministerio de salud-**http://www.msssi.gob.es/**
- *Experiencia de implementación de historia clínica única en el estado de Nueva York* - **www.readycomputing.com**
- *Perfiles IHE para la interoperabilidad en Europa*: EPSOS
- *Historia clínica compartida de Catalunya* – Generalitat de Catalunya_ Departament de Salut
- **http://www.valuehealth.eu/**
- **https://usecase-repository.ihe-europe.net**
- **https://www.hl7.org**
- **https://www.himss.org**
- **http://www.ihe.net/**
- **https://www.health.ny.gov**
- **www.healthlinkny.com**
- La información sobre la transacción IHE XCPD y la mensajería para el servicio de identificación de paciente se puede encontrar en el documento: **http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCPD.pdf**
- **http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf**
- **http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCA_Rev2-1_TI_2010-08-10.pdf**
- **http://docs.oasis-open.org/regrep/regrep-core/v4.0/regrep-core-rs-v4.0.html**
- **http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf**
- **http://www.mintic.gov.co/arquitecturati/630/w3-article-9434.html**

- **https://www.intersystems.com/assets/sites/8/IntroductiontoIHE.pdf**
- **http://docs.oasis-open.org/regrep/regrep-core/v4.0/regrep-core-overview-v4.0.html**
- *Conjunto de herramientas para una estrategia de eSalud nacional*. Biblioteca de la OMS – **http://www.who.int/library/es/**
- European Interoperability Architecture (EIA) action of ISA
- *IHE International, IHE IT Infrastructure Technical Framework* . https://www.**ihe**.net/
- *Historia clínica nacional, informe de situación* – Ministerio de salud-**http://www.msssi.gob.es/**
- *Experiencia de implementación de historia clínica única en el estado de Nueva York* - **www.readycomputing.com**
- *Perfiles IHE para la interoperabilidad en Europa*: EPSOS- Fundació TicSalut
- *Historia clínica compartida de Catalunya* – Generalitat de Catalunya_ Departament de Salut
- **http://www.valuehealth.eu/**
- **https://usecase-repository.ihe-europe.net**
- **https://www.hl7.org**
- **https://www.himss.org**
- **http://www.ihe.net/**
- **https://www.health.ny.gov**
- **www.healthlinkny.com**


BID


RACSEL
RED AMERICANA DE COOPERACIÓN
SOBRE SALUD ELECTRÓNICA


Fundación
Julio Ricaldoni
INGENIERIA EN EL URUGUAY