

AIMS Orientación

Intercambios de Datos de Salud Pública Centralizados

Herramientas para Diseñadores de Plataformas,
Expertos en Tecnología y Responsables de la
Salud Pública

The AIMS logo is a circular emblem. It features a stylized representation of a DNA double helix or a series of vertical bars of varying heights, colored in shades of blue and green. Below this graphic, the word "AIMS" is written in a bold, blue, sans-serif font.

Resumen Ejecutivo

Aprovechar el poder de los datos de salud pública

Para la salud pública es fundamental el intercambio confiable y seguro de los datos de salud, ya que permite a los profesionales de la salud pública, funcionarios gubernamentales y otros responsables, monitorear enfermedades infecciosas, detectar amenazas emergentes y planificar respuestas ante brotes epidémicos. El intercambio a tiempo de los resultados de pruebas de laboratorio, datos de vacunación, registros médicos y otros datos entre proveedores de atención médica, laboratorios, organismos de salud pública y gobiernos ayuda a tomar conciencia de la situación y a colaborar entre las entidades involucradas en las respuestas de salud pública. El intercambio centralizado de datos es fundamental para la gestión de la salud pública en cualquier país o región.

La experiencia AIMS

En Estados Unidos, la plataforma de Servicios de Mensajería Informática de la Asociación de Laboratorios de Salud Pública (APHL Informatics Messaging Services, AIMS) funciona como eje principal para el intercambio de datos de salud pública. La plataforma AIMS conecta organismos federales, estatales y territoriales de salud pública, laboratorios, proveedores de atención médica, Intercambio de Información de Salud (Health Information Exchanges, HIE) y más, en un modelo “hub and spoke” que intercambia más de un millón de mensajes al día. AIMS promueve un intercambio nacional de datos rápido, confiable y escalable mediante la prestación de servicios compartidos a los socios del intercambio de datos para garantizar interoperabilidad, seguridad, alojamiento y visualización de datos electrónicos y aplicaciones.

Compartir el modelo AIMS

En los últimos 15 años, AIMS ha crecido para facilitar el intercambio de miles de millones de mensajes que contienen datos de laboratorio, vacunación, informes de casos y registros vitales para las decisiones de los líderes de la salud pública. APHL junto a Ruvos, su socio técnico, crearon este recurso para documentar y sintetizar las lecciones aprendidas a través de la creación, expansión y operación continua de la plataforma AIMS. Este documento sirve de modelo para los países y las organizaciones que deseen implementar el intercambio de datos a escala nacional y regional. Ofrece sugerencias y prácticas recomendadas que cualquier jurisdicción puede utilizar para diseñar y construir una plataforma de intercambio de datos que cumpla con sus requisitos específicos. Los temas que se van a desarrollar son los siguientes:

- Estructura e infraestructura;
- Estándares, seguridad y cumplimiento;
- Gobernanza y política de datos;
- Mantenimiento y operaciones;
- Asistencia técnica e integración;
- Implicación de las partes interesadas;
- Estrategia y liderazgo.

Beneficios extraordinarios del intercambio centralizado de datos

El procesamiento centralizado de mensajes, la transformación y el enrutamiento permiten reducir los recursos necesarios para que cualquier socio del intercambio de datos (incluidas las capacidades técnicas, hardware y software) pueda intercambiar datos de salud y vigilancia. Una plataforma con un buen diseño es segura, confiable y permite escalar rápidamente. Se puede desarrollar de manera progresiva para dar soporte a sistemas de monitoreo y auditoría, paneles de visualización de datos, e incluso para alojar aplicaciones de terceros que beneficien las iniciativas de salud pública.

Permitir el intercambio de datos de manera oportuna

Una plataforma centralizada permite el intercambio oportuno de muchos tipos de datos vitales para la salud pública, como los siguientes:

- Resultados de pruebas de patógenos, incluidos la gripe y SARS-CoV-2;
- Informes de enfermedades que se pueden prevenir con vacunas;
- Datos sobre amenazas biológicas;
- Vacunaciones;
- Secuenciación del genoma;
- Registros de nacimientos y defunciones (hechos vitales);
- Órdenes de pruebas electrónicas;
- Informes electrónicos de laboratorio;
- Informes electrónicos de casos.

Crear eficiencias

La capacidad de los usuarios para gestionar el intercambio de datos de rutas y de socios se ve mejorada al enrutar mensajes a través de una plataforma centralizada. Cuando un socio de intercambio de datos se conecta a la plataforma, puede enviar y recibir datos para hacer intercambios con cualquier otro socio comercial que ya esté en el servicio. Es muy sencillo, el socio de intercambio de datos, en lugar de establecer y mantener múltiples conexiones entre cada remitente y solicitante, solo necesita mantener una conexión con la plataforma centralizada y enviar datos a través de su protocolo de transporte preferido.

Estandarizar, traducir y transformar los datos

Una plataforma centralizada de intercambio de datos puede establecer y hacer cumplir la estandarización de los datos, creando canales de datos de alta calidad que se puedan incorporar fácilmente por sistemas de datos diversos. Este tipo de plataformas brindan interoperabilidad entre varios protocolos de transporte, lo que permite que un remitente que utiliza un protocolo pueda enviar datos de manera segura a un receptor que utiliza otro protocolo diferente.

Análisis

Una plataforma centralizada de intercambio de datos funciona como base para el análisis avanzado mediante la creación de canales de datos sólidos de datos estandarizados. Con los paneles de control y las integraciones de las herramientas analíticas, una plataforma centralizada de datos puede aprovechar técnicas avanzadas de ciencia de datos para capacitar a los líderes casi en tiempo real a fin de monitorear tendencias y detectar brotes.

Un recurso integral

Los departamentos de informática, los ministerios de salud y los responsables de la salud pública pueden consultar la información de este documento para diseñar una guía que les permita establecer una plataforma de intercambio de datos que se ajuste a sus circunstancias y necesidades, ya sea alojada localmente o en la nube, y que respete las normas aplicables que rigen la ubicación, el uso y la preferencia de proveedores de datos.

Contenidos

Resumen Ejecutivo	2
Objetivo y Uso Del Documento.....	6
La Historia de AIMS	7
Orígenes, evolución y casos de usos esenciales	7
Introducción a AIMS	7
Orígenes.....	8
Beneficios principales	8
Funciones en constante expansión	9
<i>Transporte de datos.....</i>	<i>9</i>
<i>Mejora de datos.....</i>	<i>10</i>
<i>Alojamiento de datos.....</i>	<i>10</i>
<i>Servicios de intercambio de datos para socios.....</i>	<i>10</i>
Evolución de la estructura de AIMS.....	11
Ampliación de la plataforma mediante aplicaciones de terceros.....	14
Casos de uso esenciales de AIMS.....	15
<i>Informe electrónico de laboratorio (Electronic Laboratory Reporting, ELR).....</i>	<i>15</i>
<i>Informes electrónicos de casos (eCR).....</i>	<i>16</i>
<i>Lago de datos para el informe electrónico de laboratorio de COVID-19 (COVID-19 Electronic Laboratory Reporting, CELR).....</i>	<i>17</i>
<i>Órdenes y resultados de pruebas electrónicas (ETOR).....</i>	<i>17</i>
<i>COVIDSTATEDX.....</i>	<i>19</i>
<i>Sara Alert.....</i>	<i>19</i>
<i>Red de Laboratorios de Resistencia a los Antimicrobianos (Antimicrobial Resistance Laboratory Network, ARLN)</i>	<i>20</i>
El Modelo de AIMS.....	21
Tecnología.....	21
<i>Seguridad y cumplimiento</i>	<i>22</i>
<i>Infraestructura.....</i>	<i>22</i>
<i>Portal de datos.....</i>	<i>24</i>
<i>Archivo de datos.....</i>	<i>24</i>
<i>Procesamiento de datos</i>	<i>25</i>
<i>Análisis de datos.....</i>	<i>25</i>
Gobernanza de datos	26
<i>Gestión de la calidad de los datos.....</i>	<i>26</i>
<i>Seguridad de los datos y privacidad</i>	<i>26</i>
<i>Administración de datos</i>	<i>26</i>
<i>Interoperabilidad y estandarización.....</i>	<i>27</i>
<i>Gestión de riesgos y respuesta a incidentes.....</i>	<i>27</i>
<i>Cumplimiento y auditoría</i>	<i>27</i>
<i>Uso ético de los datos.....</i>	<i>27</i>
Partes interesadas y operaciones	27
<i>Marco de gestión de la prestación de servicios</i>	<i>28</i>
<i>Servicios principales.....</i>	<i>29</i>

Contenidos, continúa

Implementación de un Sistema de Intercambio de Datos Centralizado: Consideraciones de Diseño y Prácticas Recomendadas.....	32
Tecnología.....	32
<i>Seguridad y cumplimiento</i>	<i>33</i>
<i>Infraestructura.....</i>	<i>34</i>
<i>Puerta de enlace de datos</i>	<i>38</i>
<i>Almacenamiento de datos</i>	<i>39</i>
<i>Procesamiento de datos</i>	<i>40</i>
<i>Análisis de datos.....</i>	<i>42</i>
Gobernanza de datos	43
<i>Objetivos y consideraciones</i>	<i>43</i>
Partes interesadas y operaciones	44
<i>Componentes fundamentales para respaldar cualquier nueva plataforma de intercambio de datos.....</i>	<i>44</i>
<i>Promoción y persuasión.....</i>	<i>45</i>
<i>Fomento de la aceptación de las partes interesadas.....</i>	<i>45</i>
<i>Fomentar la confianza con los socios de intercambio de datos.....</i>	<i>46</i>
<i>Participación crítica: equipos de seguridad de IT</i>	<i>46</i>
Apéndices	47
Cronología del desarrollo de AIMS.....	47
Mirth en la plataforma AIMS	49
Políticas y procedimientos ilustrativos	50
<i>Estructura e infraestructura</i>	<i>50</i>
<i>Estándares, seguridad y cumplimiento</i>	<i>50</i>
<i>Gobernanza y política de datos</i>	<i>52</i>
<i>Mantenimiento y operaciones.....</i>	<i>53</i>
<i>Gestión de la prestación de servicios.....</i>	<i>54</i>
<i>Asistencia técnica (TA) e incorporación</i>	<i>54</i>
<i>Implicación de las partes interesadas</i>	<i>55</i>
<i>Estrategia y liderazgo</i>	<i>55</i>
<i>Comunicaciones y marketing.....</i>	<i>55</i>
Consideraciones sobre el alojamiento en la nube.....	56
<i>Atracciones de la nube.....</i>	<i>56</i>
<i>Desafíos de mantenimiento de recursos locales</i>	<i>56</i>
<i>Impulso para la migración.....</i>	<i>56</i>
<i>Beneficios de estar registrado en la nube.....</i>	<i>56</i>
<i>Selección de un proveedor de servicios en la nube</i>	<i>57</i>
Terminología	59

Objetivo y Uso Del Documento

El objetivo de este documento es ofrecer una descripción exhaustiva y detallada de la plataforma AIMS, su historia y casos de uso, los fundamentos conceptuales y técnicos en los que se basa su modelo y, por último, diseños a tener en cuenta y que puedan servir de referencia a otros países a la hora de conceptualizar, planificar e implementar un sistema de intercambio centralizado de datos de salud pública.

Al detallar la funcionalidad y la estructura de la plataforma AIMS y compartir las prácticas recomendadas y las lecciones aprendidas en su crecimiento y desarrollo durante los últimos 15 años, este documento ofrece un punto de partida que puede acelerar la implementación de plataformas centralizadas de intercambio de datos que fortalecerán la salud pública a nivel global.

Este documento es un recurso y una guía para los interesados en el diseño, la planificación, la implementación y la operación de un sistema centralizado de intercambio de datos en sus contextos locales. Está dividido en tres partes que se complementan entre sí y pueden consultarse por separado a medida que el lector pasa por las distintas fases de conceptualización de una plataforma centralizada de intercambio de datos, la justificación de la inversión en un sistema de este tipo, la toma de decisiones técnicas y estructurales y la planificación del funcionamiento continuo del sistema. Las tres partes son las siguientes:

- **La historia de AIMS:** la primera parte detalla la función principal y utiliza casos de la plataforma AIMS; también describe la evolución de la estructura de AIMS en los últimos 15 años. Al detallar el AIMS como ejemplo, esta parte pretende aportar una visión del intercambio centralizado de datos de salud pública, así como demostrar cómo un sistema de este tipo puede empezar con una función limitada y, a medida que se demuestra su utilidad y valor, ampliarse de manera progresiva.
- **El modelo de AIMS:** la segunda parte detalla los componentes fundamentales de la plataforma AIMS, su tecnología, gestión de datos, partes interesadas y operaciones, ofreciendo a los lectores una visión del marco técnico sobre el que se asienta.
- **Implementación de un sistema de intercambio de datos centralizado:** la parte final ofrece sugerencias y prácticas recomendadas para diseñar los elementos básicos de una plataforma de intercambio de datos. Esta sección proporciona herramientas detalladas de toma de decisiones para ayudar a determinar el diseño más adecuado según el contexto y las necesidades específicas del lector.

La Historia de AIMS

Orígenes, evolución y casos de usos esenciales

Esta primera parte detalla la función principal, utiliza casos y muestra los beneficios principales de la plataforma AIMS, así como la evolución de su estructura durante los últimos 15 años. Esta sección muestra los beneficios de un sistema centralizado de intercambio de datos; también demuestra cómo dicho sistema puede comenzar de manera simple con funcionalidades limitadas y expandirse de manera iterativa con el tiempo, a medida que los socios de intercambio de datos y las partes interesadas perciben el valor de sus servicios.

Introducción a AIMS

AIMS es una plataforma de intercambio seguro de datos alojada en la nube que cumple la normativa de privacidad y seguridad sanitaria de Estados Unidos para facilitar el intercambio de datos relacionados con la salud y la sanidad pública entre socios de intercambio de datos verificados. Perteneciente a la Asociación de Laboratorios de Salud Pública, una organización sin ánimo de lucro que representa los intereses de los laboratorios de salud pública estatales, territoriales y locales de todo Estados Unidos, y gestionada por ella, la plataforma AIMS es el mayor intermediario de intercambio de datos de los CDC de Estados Unidos. Entre los socios de intercambio de datos que envían y reciben datos a través de la plataforma AIMS se incluyen los siguientes:

- Laboratorios (públicos y privados);
- Organismos federales;
- Departamentos de salud estatales, locales y territoriales;
- Organismos de salud pública;
- Proveedores y sistemas de atención médica (hospitales, clínicas);
- Servicios uniformados militares y civiles (incluida la Marina de Estados Unidos).

En un principio, la plataforma AIMS se creó para facilitar el intercambio de resultados de las pruebas de la gripe y se ha ampliado para facilitar el intercambio de datos en muchos y variados casos de uso. Por ejemplo:

- Resultados de las pruebas de la gripe;
- Datos de vacunación;
- Informes electrónicos de laboratorio (electronic laboratory reports, elr);
- Órdenes y resultados de pruebas electrónicas (electronic test orders and results, etor);
- Registro electrónico de casos (electronic case reporting, ecr) entre los sistemas de historias clínicas electrónicas (health providers' electronic health records systems ehrrs) de los proveedores y los organismos de salud pública;
- Datos de secuenciación del genoma;
- Datos sobre amenazas biológicas;
- Informes de enfermedades que se pueden prevenir con vacunas;
- Pruebas de resistencia a los antimicrobianos;
- Registros de nacimientos y defunciones (hechos vitales).

Orígenes

En la primera década del siglo XXI, muchas de las comunicaciones esenciales entre los sistemas de laboratorios de salud pública de Estados Unidos seguían transmitiéndose en papel a través de fax o servicios de mensajería.

La plataforma de intercambio de datos AIMS se creó para permitir una comunicación rápida y segura de información sanitaria crítica entre los laboratorios de salud pública y las agencias federales de Estados Unidos, con el objetivo de reforzar en gran medida la capacidad de los organismos de salud pública para identificar y coordinar su respuesta a las amenazas emergentes.

El primer caso de uso de la nueva plataforma consistió en hacer posible que los diversos sistemas sanitarios de todo el país intercambiaran los resultados de las pruebas de la gripe, empezando por la necesidad de persuadir a las autoridades estatales para que participaran en ello.

El reto era importante. Estados Unidos tiene un sistema de salud pública muy fragmentado, en el que las decisiones sobre el diseño y la aplicación del sistema se producen a nivel estatal y no federal. Debido a esta fragmentación aparecen sistemas muy diferentes que requieren un aporte técnico considerable para habilitar el intercambio de datos, la coordinación y la interoperabilidad.

El primer mensaje de seguimiento de la gripe que envió AIMS al CDC fue en 2008; desde entonces la plataforma ha crecido para manejar una amplia gama de casos de uso en la salud pública, desempeñando un papel clave en informar la respuesta a la pandemia de COVID-19. Hoy en día, la historia y evolución de AIMS proporcionan un tesoro de información para las iniciativas emergentes de intercambio de datos.

Beneficios principales

Al centralizar el procesamiento, la transformación y el enrutamiento de los mensajes, la plataforma AIMS reduce los recursos que necesita cualquier socio comercial (capacidades técnicas, hardware y software) para poder intercambiar datos. Además del procesamiento de mensajes, AIMS ofrece una infraestructura segura, confiable y de máxima disponibilidad que se puede ampliar rápidamente para hacer frente a las fluctuaciones del volumen de mensajes, así como sistemas de supervisión y auditoría, paneles de visualización de datos y alojamiento de aplicaciones de terceros que benefician a las iniciativas de salud pública.

La plataforma AIMS le brinda a Estados Unidos una infraestructura fundamental para el intercambio diario de mensajes de salud pública. Gracias a las constantes inversiones en la plataforma y su desarrollo desde 2008, se pudo escalar rápidamente para manejar el aumento repentino de los resultados de laboratorio y los informes electrónicos de casos de COVID-19 una vez que comenzó la pandemia, les brindó a los líderes de la salud y del gobierno información vital para orientar la respuesta de salud pública. Hasta la fecha, la plataforma AIMS ha procesado más de 2.25 mil millones de mensajes relacionados con el COVID.

Para dar una idea de la escala de las operaciones de AIMS, en 2024 la plataforma:

- Procesa 1,200 millones de mensajes de interfaz al mes.
- Gestiona 23 millones de mensajes al mes entre más de 8,000 socios de intercambio de datos.
- Brinda servicios a más de 7,800 proveedores de informes electrónicos de casos (eCR).
- Procesa los informes electrónicos de laboratorio que presentan los socios de intercambio de datos en representación de cientos a miles de instalaciones de pruebas agregadas.

Para visualizar la estructura que permite que AIMS funcione eficazmente a gran escala, consulte [“Evolución de la estructura de AIMS” \(pág. 11\)](#) más abajo.

Funciones en constante expansión

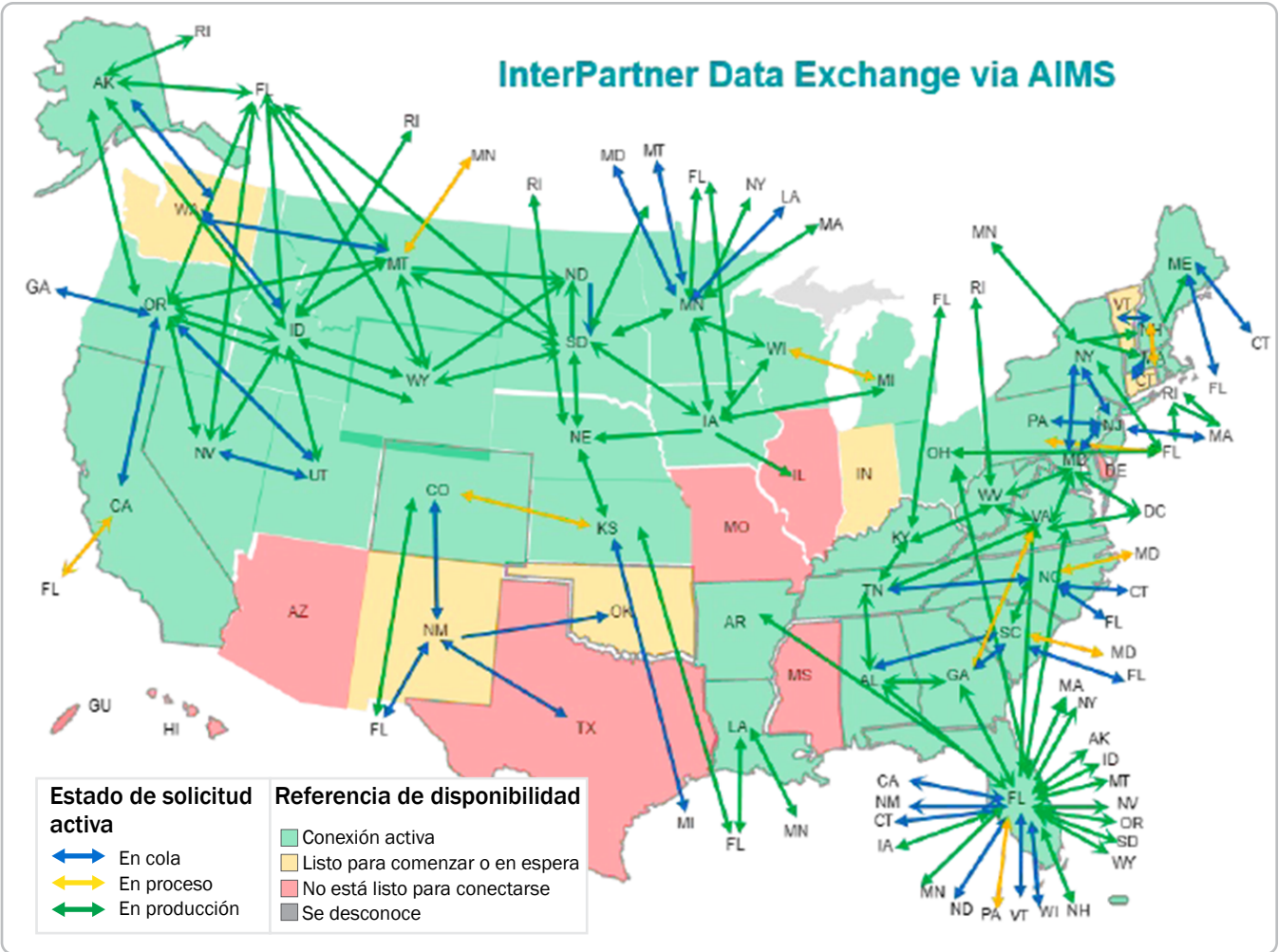
La plataforma AIMS ha desarrollado y ofrecido nuevas capacidades en respuesta a las necesidades cambiantes de las partes interesadas, basándose en un conjunto central de funcionalidades de alojamiento, transporte y mejora de datos, complementadas por servicios proporcionados a socios de intercambio de datos por parte de APHL.

Transporte de datos

AIMS facilita una transmisión de datos segura, confiable y escalable entre todos los socios de intercambio de datos mediante el uso de estándares de mensajería como HL7, Fast Healthcare Interoperability Resources (FHIR), Clinical Document Architecture (CDA), Continuity of Care Document (CCD), ASC X12 e Integrating the Health Enterprise (IHE).

Intercambio de datos InterPartner de AIMS, que se presentó en 2019, ofreció una estructura de mensajería fácil de implementar que simplificó en gran medida el intercambio de datos entre proveedores, organismos de salud pública, HIE y remitentes no tradicionales. Se basa en una estricta convención de nomenclatura de archivos que permite el enrutamiento inteligente de datos sin inspeccionar el contenido. Una vez integrados, los socios pudieron establecer interconexiones con un soporte mínimo por parte de AIMS y añadir casos de uso acordados mutuamente según fuera necesario. La adopción de InterPartner provocó una explosión en los intercambios de datos entre estados.

Figura 1. Intercambio de datos InterPartner



Mejora de datos

AIMS ofrece servicios centralizados de traducción y transformación de datos para analizar y mapear datos a estándares y terminologías de vocabulario de salud pública como LOINC, SNOMED e ICD-10, así como para traducir mensajes de un tipo a otro. Los servicios de validación de AIMS garantizan que los mensajes y las cargas útiles se ajusten a los estándares de estructura y contenido de los mensajes. [AIMS Validador](#) ofrece una herramienta de validación en línea de autoservicio para que los remitentes de datos comprueben la estructura y el contenido de los mensajes con varios protocolos, incluidos eCR y ELR, antes de enviarlos a través de AIMS. AIMS también realiza la validación en línea de los mensajes transportados a través de la plataforma para garantizar que los destinatarios reciban cargas útiles de calidad.

Alojamiento de datos

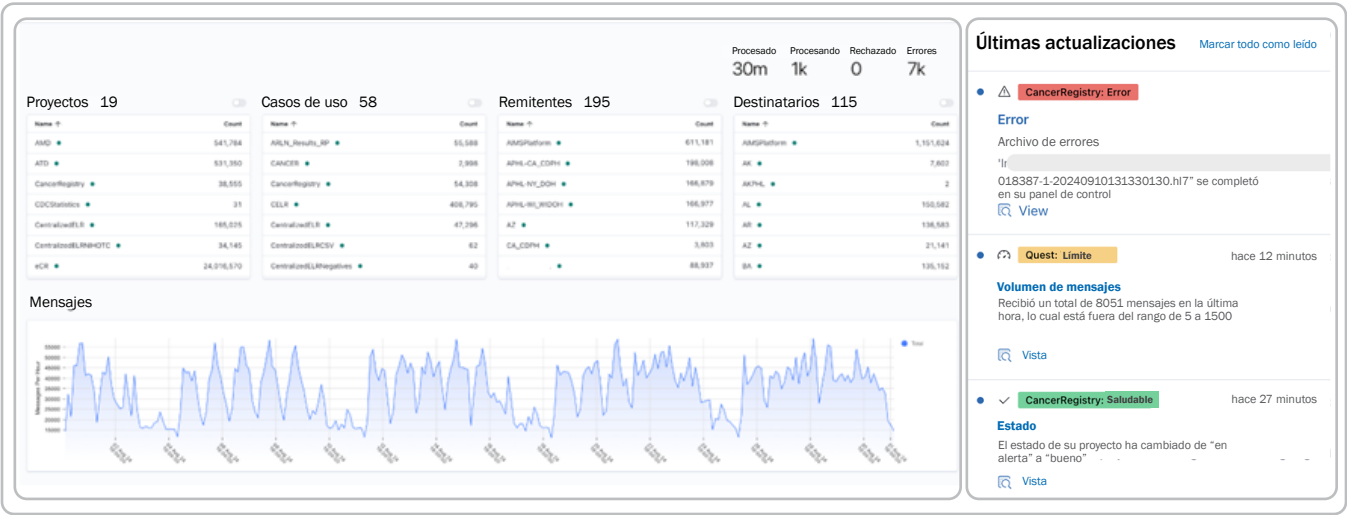
AIMS también ofrece servicios de alojamiento y almacenamiento seguros y compatibles para aplicaciones de terceros. Esto incluye servicios de almacenamiento de datos a pedido, para hacer copias de seguridad y archivar, descargar y exportar datos, así como entornos seguros de desarrollo, pruebas y producción accesibles mediante escritorios virtuales. Mediante los servicios en la nube, AIMS ofrece Computación de Alto Rendimiento (High Performance Computing, HPC) para permitir a los usuarios construir y gestionar rápidamente clústeres HPC para casos de uso con gran cantidad de datos. Todos los datos del AIMS se gestionan según las prácticas recomendadas de alojamiento, acceso y destrucción de datos, de conformidad con la normativa sobre datos de salud.

Servicios de intercambio de datos para socios

A través del panel de control interactivo de la plataforma AIMS, los socios de intercambio de datos pueden supervisar el flujo de mensajes en tiempo real y el volumen de mensajes que se pueden buscar y filtrar por tipo de proyecto, fecha y hora, remitente y destinatario en todos los entornos (prueba, preparación y producción). Los usuarios pueden programar notificaciones (a través de correo electrónico, mensajes e Internet) según eventos específicos, disparadores o umbrales de volumen de mensajes, y también pueden recibir alertas cuando el estado de interfaces específicas o rutas de mensajes se ralentizan o se vuelven “no saludable”. Esto permite a los usuarios controlar las tendencias de sus flujos de datos y detectar y solucionar los problemas a medida que surgen.

APHL también ofrece asistencia técnica de expertos en validación, vocabulario y servicios de datos a todos los socios de intercambio de datos para garantizar que todos los remitentes y destinatarios tengan acceso a la variedad de servicios de AIMS.

Figura 2. Panel de control de AIMS



Evolución de la estructura de AIMS

Para verlo en orden cronológico consulte el Apéndice *“Cronología del desarrollo de AIMS”* (pág. 47).

Antes de que se creara la plataforma AIMS, todo el intercambio de datos de laboratorios de salud pública entre jurisdicciones y organismos federales se producía mediante **conexiones punto a punto** a través del Sistema de Mensajería de Redes de Información de Salud Pública (Public Health Information Networking Messaging System, PHINMS). Este modelo de conexión punto a punto requería establecer y mantener un servidor y un cliente para cada nodo que se conectara, lo cual implicaba un mantenimiento considerable y continuo para garantizar configuraciones actualizadas con certificados válidos para cada servidor y cliente. Cada nodo que intercambiaba datos tenía que mantener cientos de conexiones, lo que exigía una inversión considerable en el mantenimiento continuo y cotidiano. Un mensaje dirigido a varios destinatarios debía enviarse a cada uno por separado, de modo que un mensaje dirigido a cinco destinatarios se enviaba cinco veces distintas.

Este modelo exigía una inversión significativa de todas las partes implicadas en el intercambio de datos, y la calidad y fiabilidad del intercambio de datos era muy variable entre los socios de intercambio de datos debido a su dependencia de los recursos y el mantenimiento a nivel de cada nodo. En este modelo, debido a que el número de conexiones que se deben mantener entre todos los nodos (n) es $n^2 + 1$, cada nuevo socio comercial aumenta la complejidad del sistema, haciendo que el modelo punto a punto sea difícil y requiera muchos recursos para escalarse.

La complejidad y el costo de este tipo de modelo hicieron necesaria la transición a un **modelo de centro de intercambio**, en el que todos los nodos se conectan a un socio central para intercambiar datos con las demás partes. Gracias a la posición de confianza ante los laboratorios de salud pública, los CDC confiaron en APLH para desarrollar dos **plataformas de tipo hub-and-spoke** a fin de facilitar el intercambio centralizado de datos y utilizaron los datos de la gripe como el primer caso de uso. Estas plataformas (que luego se unificaron para convertirse en la plataforma AIMS) reemplazaron la presentación de informes en papel de los resultados de la gripe de los laboratorios de salud pública al CDC y redujeron el número de conexiones punto a punto que el CDC tenía que mantener de 50 a 2. La implementación de un mensaje estándar HL7 para vigilar la gripe mejoró la calidad de los datos y la capacidad del CDC para procesar los resultados. El modelo *hub-and-spoke* reduce en gran medida el número de conexiones que se debe mantener en todo el sistema y reduce las conexiones $n^2 + 1$ del modelo punto a punto a $n + 1$, lo que aumenta drásticamente la eficiencia del sistema.

Al inicio, la plataforma AIMS se implementó como un eje de **no lectura (route-not-read, RnR)**, con cifrado de extremo a extremo para que un mensaje solo lo lea el destinatario. Este modelo sirve en ambientes de “desconfianza” ya que el intermediario no puede leer los mensajes enviados a través de ese eje. En este diseño de AIMS, los “puntos finales” (socios de intercambio de datos) solo necesitan mantener un cliente (en lugar de un cliente y un servidor) para enviar datos al eje. Un socio comercial envía un mensaje al eje y recibe un mensaje en respuesta para confirmar la recepción. En este mensaje se incluyen todos los mensajes pendientes enviados al socio comercial a través del eje. Los socios de intercambio de datos pueden conectarse al AIMS a través de su protocolo preferido (PHINMS, SFTP, AWS S3), lo que les permite intercambiar datos con socios que utilicen protocolos diferentes a los suyos.

Al iniciar el intercambio de datos mediante un modelo RnR, AIMS tuvo que establecer un umbral de confianza más bajo con cada socio comercial, lo que aceleró la incorporación de los emisores de datos. Con el tiempo, a medida que AIMS incorporaba más socios de intercambio de datos y proporcionaba un servicio coherente y asistencia técnica práctica, la confianza de los socios de intercambio de datos aumentó y pudieron ofrecer servicios de datos centralizados que requieren la capacidad de leer el contenido de los mensajes. AIMS empezó a ofrecer servicios de datos como traducción, transformación y validación, lo que disminuyó la necesidad de que cada socio comercial invirtiera en personal costoso para la integración y transformación, y aumentó así el valor de ser parte de AIMS. En este modelo de **servicios**

centralizados, los socios de intercambio de datos cifran sus mensajes en AIMS, que los descifra, realiza la función de servicio, los vuelve a cifrar y envía el mensaje al destinatario. Cuando el intermediario está habilitado para descifrar y leer el contenido del mensaje, puede enviar un único mensaje a varios destinatarios, en lugar de que un remitente envíe el mismo mensaje varias veces a varias partes. Esto reduce la carga de los emisores de datos y aumenta la eficacia global del sistema.

Con los informes electrónicos de casos (eCR), AIMS añadió un patrón de intercambio de datos de **publicación y suscripción**. En este modelo, los emisores de datos “publican” mensajes en AIMS y los destinatarios crean reglas de “suscripción” para los tipos de mensajes que desean recibir. La publicación y suscripción le da el control a los destinatarios de los datos para que determinen los tipos de datos que quieren recibir, en lugar de limitarse a recibir todo lo que se les envíe.

En la actualidad, AIMS utiliza todos los patrones de intercambio de datos mencionados (no lectura, servicio centralizado, hub-and-spoke y publicación y suscripción) en los distintos casos de uso de la plataforma. Cada modelo tiene ventajas y motivos para su uso. Los lectores que consideren construir sistemas de intercambio de datos a nivel nacional o regional deberán tener en cuenta los niveles de confianza de la parte centralizada, los recursos, las capacidades de los socios de intercambio de datos y los volúmenes de mensajes anticipados al seleccionar sus modelos de intercambio de datos. Consulte [Figura 5 \(pág. 13\)](#), modelos de intercambio de datos, más abajo para comparar las ventajas y desventajas de cada modelo.

En todos los patrones de intercambio de datos, es fundamental diseñar la estructura de un sistema que sea escalable. La migración de AIMS a la nube permitió un procesamiento de mensajes **basado en eventos** que aprovecha las listas de prioridades para evitar fallas del sistema cuando los volúmenes aumentan muy rápido. El diseño basado en eventos de AIMS aprovecha los almacenes de objetos y las listas de prioridades para lograr su estabilidad. Un objeto de mensaje enviado a AIMS se guarda en un almacén de objetos y genera un “evento”, que luego se envía al destinatario correspondiente, quien a su vez recupera una copia del objeto del almacén. Esto reduce drásticamente el tamaño de los mensajes procesados a través del sistema. Cada evento tiene unos pocos KB, en comparación con un archivo de mensaje completo, que puede ser bastante grande (varios gigabytes, en el caso de los informes electrónicos de casos). Con un diseño basado en

Figura 3. El modelo punto a punto requiere una conexión directa entre cada socio de intercambio.

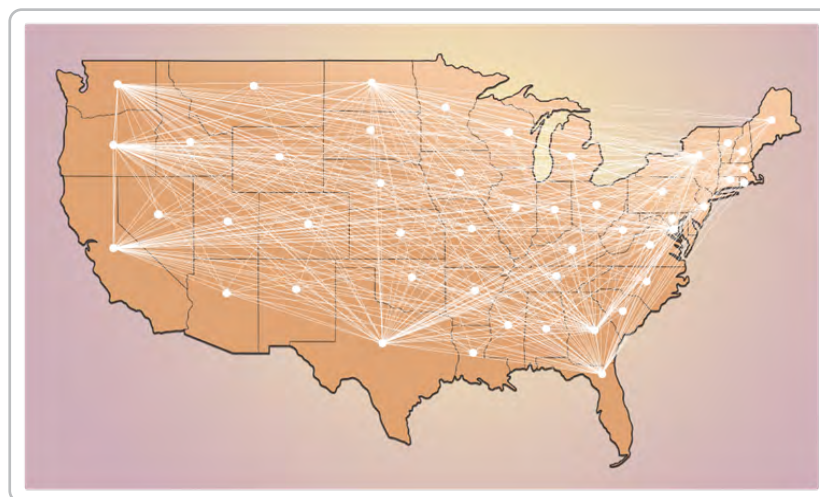
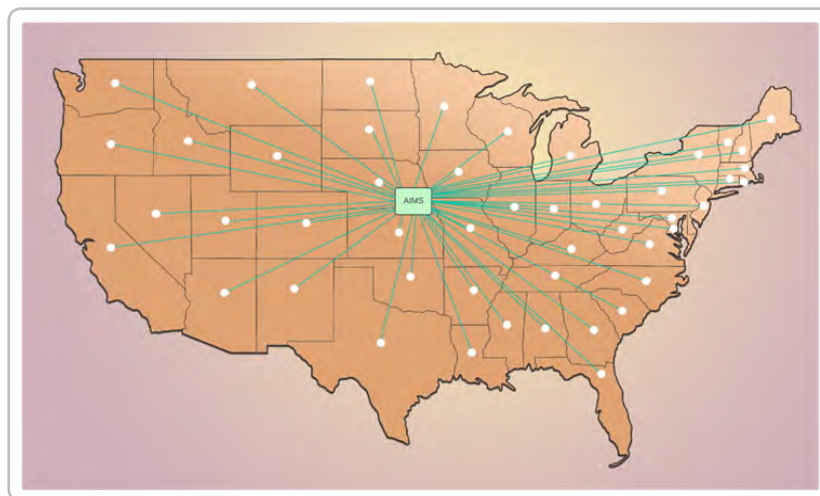


Figura 4. El modelo “hub-and-spoke” simplifica las conexiones entre todos los socios a través de un eje central.



eventos, un mensaje dirigido a varios destinatarios se enviará una sola vez a un almacén de objetos, desde donde cada destinatario lo recuperará, en función de los eventos que reciba cada uno.

El procesamiento basado en eventos de AIMS aprovecha las listas de prioridades para garantizar que los mensajes se sigan procesando incluso cuando aumenta el volumen, de modo que nunca se pierdan datos. AIMS aprovecha el procesamiento en paralelo dentro de canales individuales de su motor de interfaz, así como entre múltiples canales, escalando horizontalmente a medida que los volúmenes crecen. AIMS también puede escalar horizontalmente al operar a través de múltiples instancias del motor de interfaz. Consulte el Apéndice [Mirth en la plataforma AIMS \(pág. 49\)](#) para obtener una mayor ilustración.

Figura 5. Modelos de intercambio de datos

Modelo	Estructura de conexión	Características
Punto a punto <i>p. ej., PHINMS</i>	- Requiere establecer un servidor (para recibir) y un cliente (para enviar) en cada nodo. - Cada nuevo nodo que se agregue a la red requiere nuevas conexiones bidireccionales en todos los nodos (n^2+1).	- La fiabilidad del intercambio de datos varía según el nivel de recursos y mantenimiento en cada nodo. - Mantenimiento complejo y costoso. - Se necesitan muchos recursos para escalar. - La gestión de certificados se complica a medida que aumenta el número de socios de intercambio de datos. - El tamaño de la carga suele ser un inconveniente. - Cualquier mensaje que se deba enviar a varios receptores se debe enviar varias veces.
Hub-and-spoke También conocido como modelo de centro de intercambio. <i>p. ej., vigilancia de la gripe de AIMS</i>	- Todos los nodos se conectan con otros nodos a través de un socio central. - Se requiere una sola conexión para añadir un nuevo nodo ($n+1$).	Es mucho más fácil de mantener y escalar que el modelo de punto a punto.
No lectura (route-not-read, RnR) Es una variante del modelo hub-and-spoke.	Los mensajes se cifran de extremo a extremo, es decir, el contenido no es legible en el eje central.	- Es útil en entornos no fiables o cuando el contenido es muy sensible. - Puede ser un buen punto de partida para una nueva plataforma de intercambio.
Servicios centralizados Es una variante del modelo hub-and-spoke.	Los mensajes se cifran y se envían al socio central, que los descifra, presta servicios, los vuelve a cifrar y los entrega a los destinatarios.	- Un socio central de confianza puede transformar, traducir, validar y dirigir los mensajes a múltiples destinatarios según lo desee el remitente. - Permite una gran eficacia en la interoperabilidad y la distribución de mensajes.
Publicación y suscripción Es una variante del modelo hub-and-spoke. <i>p. ej., eCR</i>	Los remitentes publican mensajes en el eje central, los destinatarios se suscriben a los mensajes (autorizados) que desean recibir.	- Permite a los destinatarios gestionar qué datos reciben. - Permite una gran eficacia en la interoperabilidad y la distribución de mensajes.

En un principio, AIMS se alojaba en los servidores de dos departamentos de salud jurisdiccionales y luego se consolidó en un centro de datos de terceros que ya cuenta con protección para uso federal. Sin embargo, la dependencia de la

provisión física de hardware se convirtió en un obstáculo cuando se presentó el segundo caso de uso de AIMS, que requería considerablemente más escalabilidad y seguridad. Con el fin de facilitar el informe electrónico de laboratorio de Quest Diagnostics, uno de los laboratorios comerciales más grandes de Estados Unidos, AIMS necesitaba procesar mensajes que contenían información de salud muy protegida, lo que requería una infraestructura escalable que cumpliera con los estándares federales de privacidad y seguridad de la información de salud. El alojamiento en la nube ofreció considerables eficiencias para lograr esto, tanto en costos como en operaciones. AIMS primero desarrolló un prototipo utilizando los servicios en la nube de Amazon Web Services (AWS) para probar y medir su eficacia, y para 2014, ya funcionaba por completo en la nube.

Además del alojamiento seguro y redundante, AIMS aprovecha servicios y herramientas especializadas en la nube para transporte, almacenamiento y extracción de datos, análisis y visualización, lo que permite una funcionalidad sólida sin necesidad de instalar y gestionar otro software.

Consulte [Implementación de un Sistema de Intercambio de Datos Centralizado \(pág. 32\)](#) para obtener un análisis detallado sobre la infraestructura.

Ampliación de la plataforma mediante aplicaciones de terceros

Los servicios en la nube también permiten la seguridad, el cumplimiento y la redundancia del sistema necesarios para alojar y dar soporte a aplicaciones de terceros en AIMS. En 2017, AIMS comenzó a alojar el software State and Territorial Exchange of Vital Events (STEVE), lo que facilitó el intercambio a escala nacional de datos de registros de nacimientos y defunciones. Con las zonas de disponibilidad múltiple y los servicios administrados de AWS, AIMS podría ofrecer un alto nivel de fiabilidad y disponibilidad del sistema, lo que es necesario para ejecutar canales de datos críticos. En la actualidad, además de STEVE, AIMS contiene muchas aplicaciones de terceros que son esenciales para la infraestructura sanitaria de Estados Unidos, como las siguientes:

- [Sistema de gestión de conocimientos sobre enfermedades de declaración obligatoria \(Reportable Conditions Knowledge Management System, RCKMS\)](#)
- [Portal de vacunación](#)
- [Red de Acción Mundial en el Ámbito Sanitario: módulo de infecciones relacionadas con la asistencia sanitaria \(Global Action in Healthcare Network – Healthcare-Associated Infections, GAIN-HAI\)](#)
- [Datos para la acción sobre las amenazas de resistencia a los antimicrobianos](#)
- [Portal web del laboratorio](#)
- [Validadores del Instituto Nacional de Estándares y Tecnología \(National Institute of Standards and Technology, NIST\)](#)

Casos de uso esenciales de AIMS

Listos, preparados... el caso del COVID-19

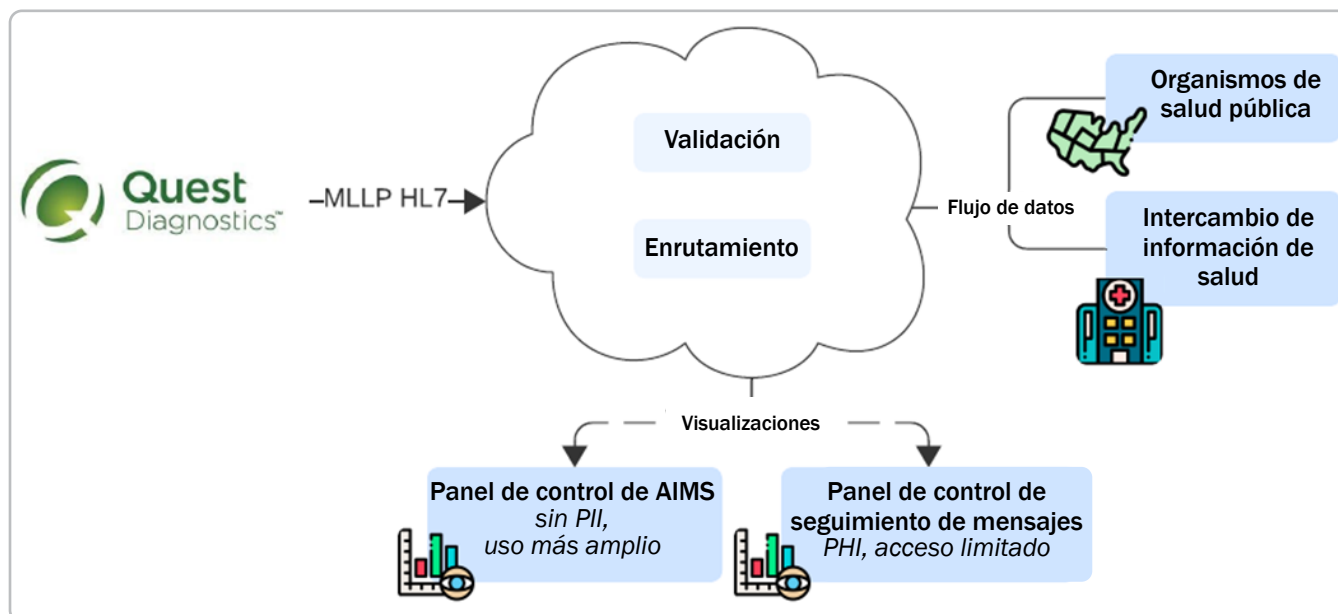
Las decisiones de estructura y de alojamiento mencionadas anteriormente colocaron a AIMS en una posición para escalar con rapidez. Mientras el brote de COVID-19 en 2020 ejercía excesiva presión en la respuesta de salud pública, la plataforma nacional de mensajería de datos que conecta a las entidades de salud pública ya estaba firmemente establecida y tenía capacidad para manejar el súbito y vasto aumento en la cantidad de datos que se necesitaban procesar y transmitir. La ruta que se creó en 2008 para transmitir datos de la gripe al CDC se modificó para aceptar nuevos datos, y en el transcurso de un mes, laboratorios y agencias de cada estado estaban informando datos de COVID-19 al CDC y a la Casa Blanca. Esto contribuyó a comprender la incidencia de la enfermedad y el estado de los esfuerzos de respuesta, la cobertura de las pruebas y los problemas existentes en la cadena de suministro de laboratorios.

Los casos de uso esenciales desarrollados en la plataforma AIMS desempeñaron un papel clave en la respuesta a COVID-19 y están muy presentes en la actualidad. Debajo, se describen por separado.

Informe electrónico de laboratorio (Electronic Laboratory Reporting, ELR)

AIMS facilita la transmisión de informes de laboratorio digitales desde los laboratorios a los departamentos de salud pública estatales y locales, los sistemas de atención médica y los CDC. Como ejemplo notable, APHL se asoció con Quest Diagnostics, uno de los mayores laboratorios comerciales de Estados Unidos, para facilitar el enrutamiento seguro de informes electrónicos de laboratorio desde todas las instalaciones de Quest Diagnostics a los organismos de salud pública de todo el país. AIMS permitió a Quest enviar todos los resultados al organismo de salud pública de la jurisdicción correspondiente a través de una única conexión, en lugar de crear y mantener conexiones con cada jurisdicción de manera individual. AIMS también ofrece a Quest servicios de control, validación y seguimiento que permiten supervisar el flujo de mensajes e investigar los problemas de contenido que puedan surgir.

Figura 6. Informe electrónico de laboratorio de QUEST



Informes electrónicos de casos (eCR)

Los organismos de la salud pública dependen de que la notificación de casos específicos sea a tiempo para así tomar las acciones necesarias y proteger la salud pública. La mayoría de las jurisdicciones requieren que los proveedores de atención médica informen sobre las condiciones de interés, las cuales pueden variar de una agencia a otra.

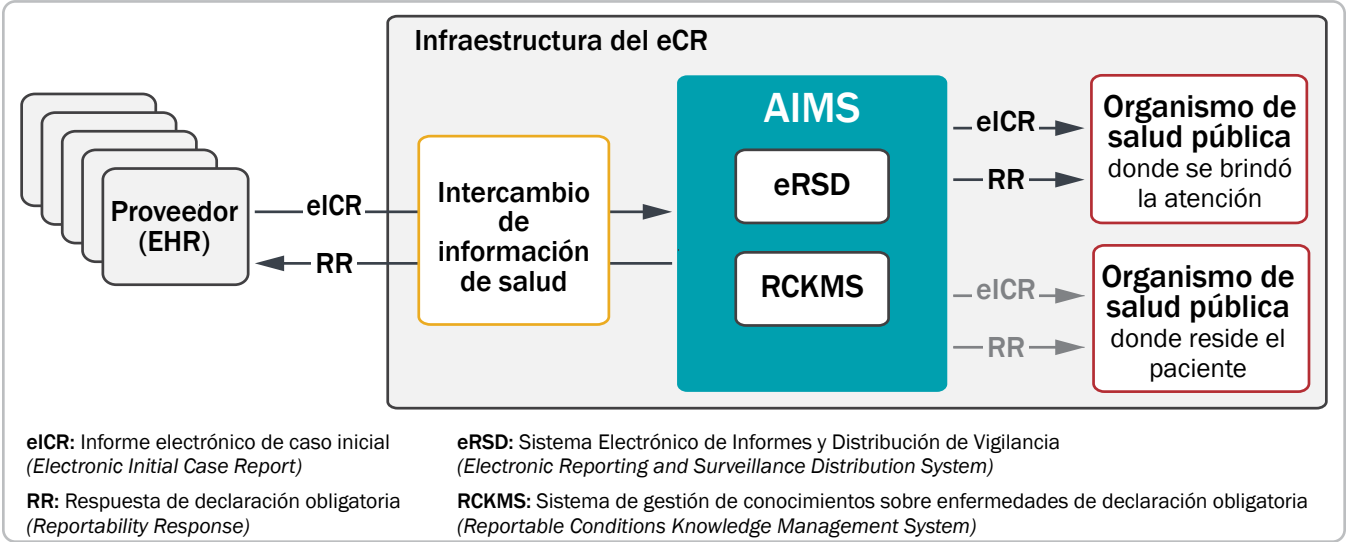
La automatización en la generación y el envío de informes iniciales y de seguimiento desde los registros electrónicos de salud hacia los organismos de salud pública, para su revisión y acción, alivia a los proveedores de atención médica de la carga de cumplir con sus obligaciones legales de presentación de informes, y mejora la puntualidad y exhaustividad de los informes de casos a nivel local, estatal y nacional. Esta eficiencia en la recopilación de datos mejora en gran medida la capacidad de los organismos de salud pública para gestionar las investigaciones de casos y responder a los brotes emergentes.

Durante el brote de COVID-19, se implementó rápidamente una versión piloto de eCR que ya estaba funcionando en la plataforma AIMS, lo que permitió disponer de esta funcionalidad en todo el país. Al día de hoy, más de 7,800 hospitales y proveedores de atención médica envían informes electrónicos de casos a través de AIMS.

Figura 7. Cómo funcionan los informes electrónicos de casos (eCR)



Figura 8. Estructura de los informes electrónicos de casos (simplificado)

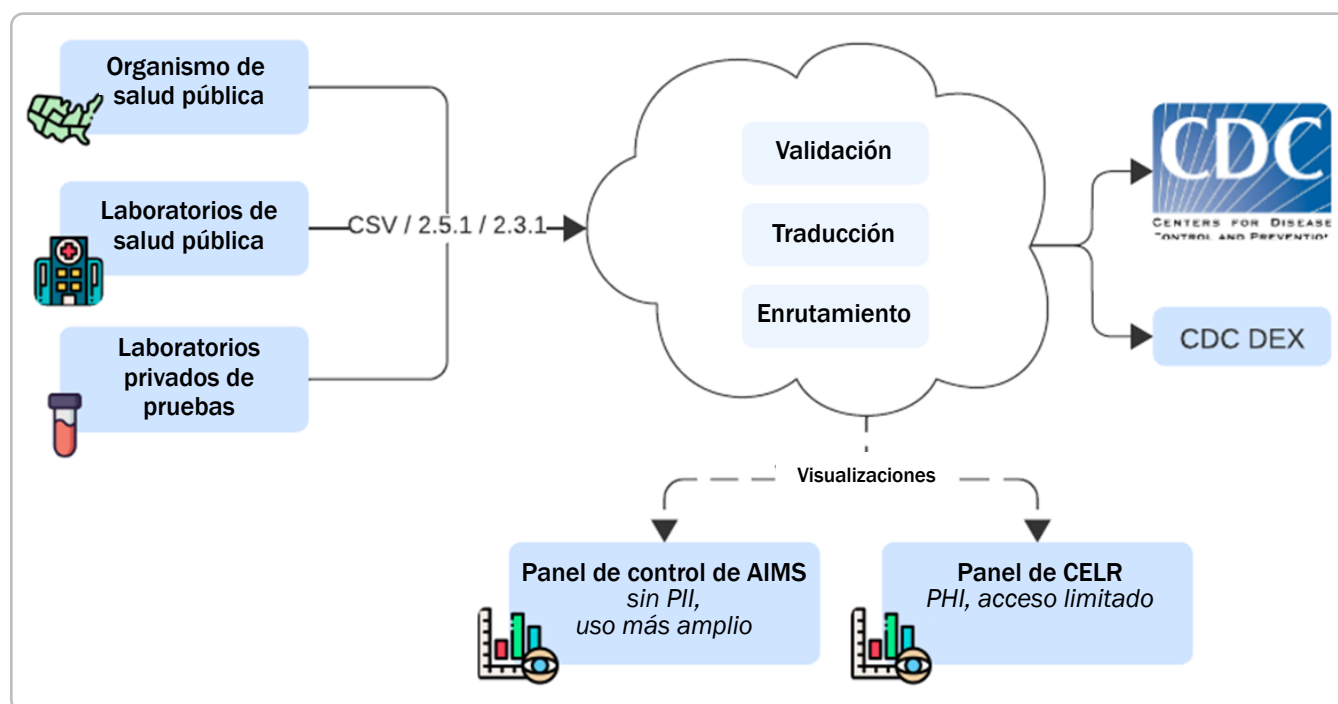


Lago de datos para el informe electrónico de laboratorio de COVID-19 (COVID-19 Electronic Laboratory Reporting, CELR)

La respuesta de salud pública ante el COVID-19 se basó en datos exhaustivos de pruebas de laboratorio. Estos datos ayudaron a comprender el impacto del COVID-19 y la cobertura de pruebas, y a identificar problemas en la cadena de suministro de reactivos y otros materiales.

Se autorizó al CDC a obtener datos de laboratorio sobre el COVID-19 de todos los laboratorios de salud pública, organismos de salud pública y algunos laboratorios privados para entender el número de pruebas solicitadas y realizadas, los resultados de cada prueba y el porcentaje de resultados positivos. El proyecto permitió a los departamentos de salud pública recibir asistencia técnica para enviar resultados de laboratorio en formatos HL7 (2.5.1, 2.3.1 o 2.3.z) y CSV a la plataforma AIMS para que el personal de los CDC pueda acceder a ellos a través del portal CELR.

Figura 9. Lago de datos para el informe electrónico de laboratorio del COVID-19 (CELR)



Órdenes y resultados de pruebas electrónicas (ETOR)

AIMS facilita el intercambio de órdenes y resultados de pruebas electrónicas entre organizaciones sanitarias y laboratorios de salud pública. Las pruebas universales de detección neonatal (una prueba universal obligatoria a nivel federal para detectar afecciones congénitas, genéticas y metabólicas no detectables de otra manera al nacer) fueron su primer caso de uso. AIMS DETOR facilita el intercambio de órdenes y resultados de pruebas entre organizaciones sanitarias y laboratorios de salud pública, así como la presentación obligatoria de informes a las autoridades sanitarias. ETOR resuelve desafíos de codificación y terminología en muchos sistemas dispares para permitir el intercambio de datos basado en estándares entre todas las partes involucradas.

Figura 10. Programa de órdenes y resultados de pruebas electrónicas de APHL (ETOR): fase 1

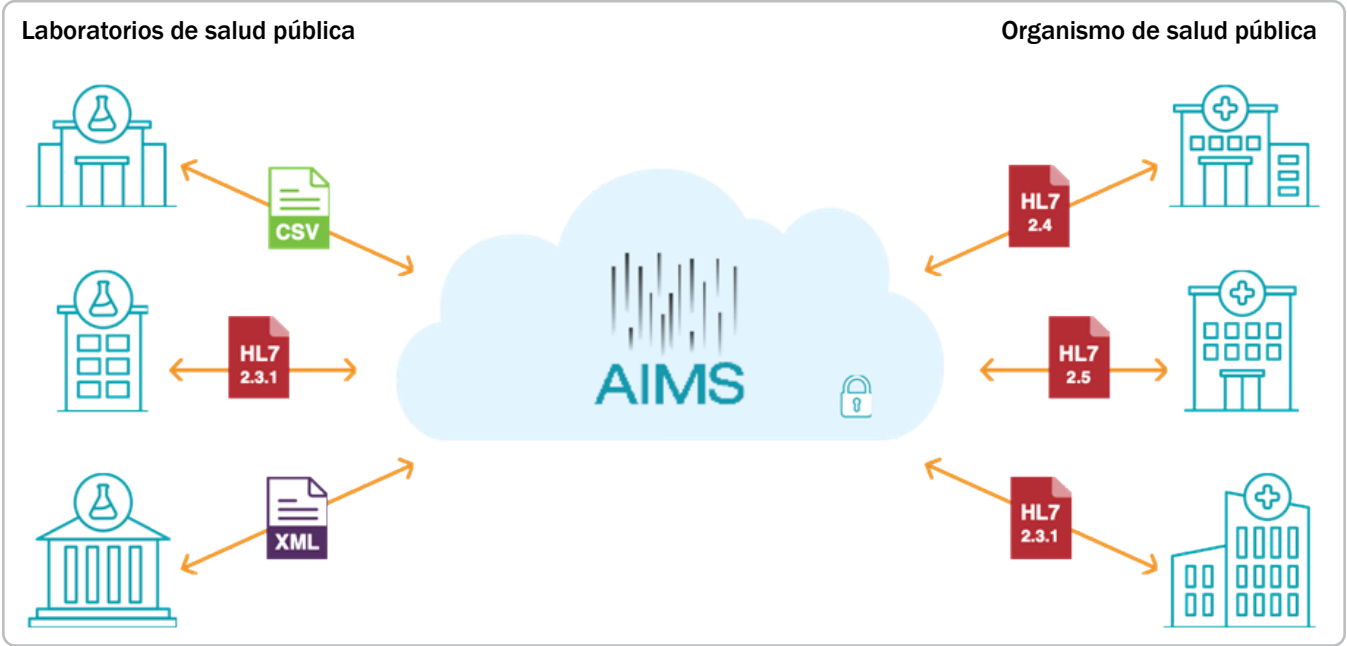
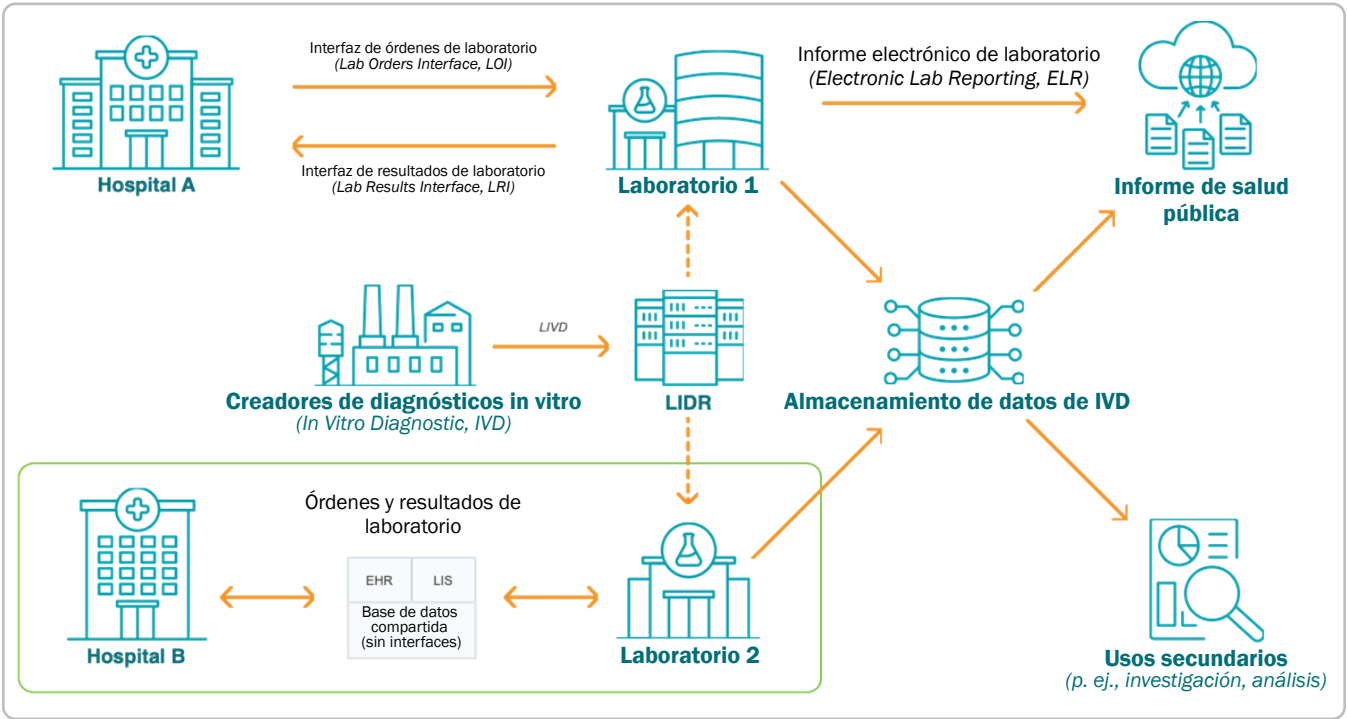


Figura 11. Programa de órdenes y resultados de pruebas electrónicas de APHL (ETOR): fase 2



COVIDSTATEDX

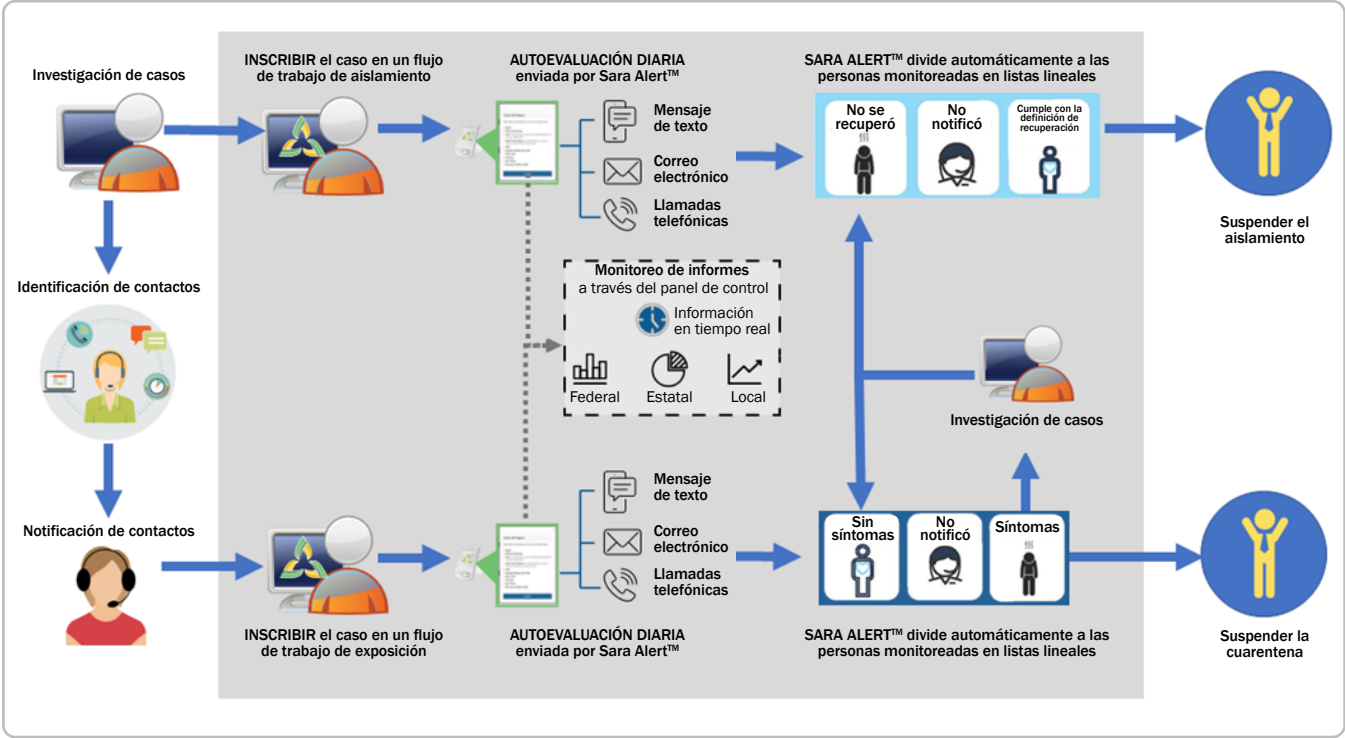
Durante la pandemia de COVID-19, AIMS facilitó el intercambio regional interestatal de datos de viajes, vacunación y registros de defunción relacionados con COVID-19 entre tres estados y la capital nacional, una región metropolitana con considerable movimiento regular a través de las fronteras estatales. Este intercambio de datos creó un mayor conocimiento de la situación de la región que el que se obtendría con los datos de un solo estado.

Sara Alert

El monitoreo diario de síntomas por parte del personal de salud pública de personas potencialmente expuestas al virus COVID-19 fue una actividad que requería muchos recursos. Sara Alert, una herramienta de vigilancia de la salud pública creada por MITRE y alojada en AIMS, proporcionó a los funcionarios de salud pública de múltiples jurisdicciones apoyo automatizado para la vigilancia de COVID-19, tanto para el control de la exposición como del aislamiento, lo que facilitó la comunicación con las personas inscritas a través de distintas plataformas (dispositivos móviles, computadora de escritorio, mensajes de texto o de voz), aumentó el conocimiento de la situación y permitió identificar los casos que requerían seguimiento.

En 2021, Sara Alert se utilizó en 20 jurisdicciones de salud pública de EE. UU. Los datos de 11 de esas jurisdicciones, que cubren a una población de 22 millones de habitantes, mostraron que se controlaba a más de 12,000 personas al día para detectar síntomas de COVID-19.

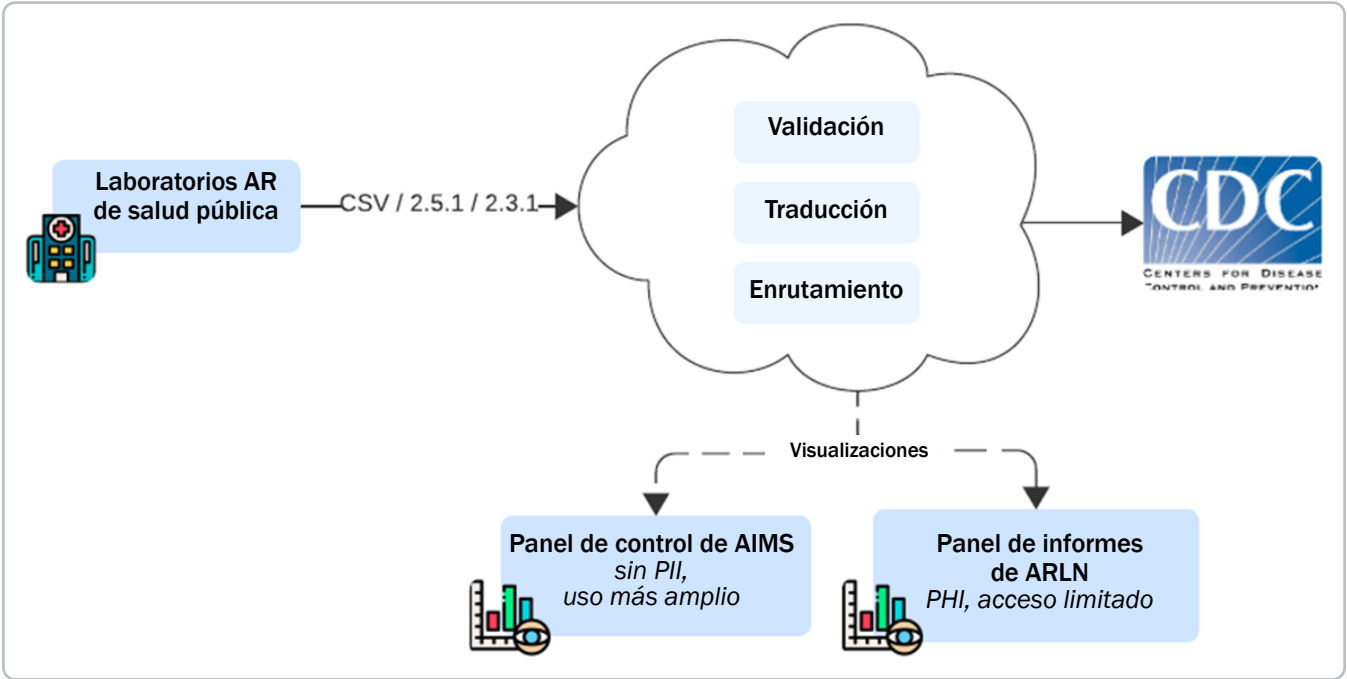
Figura 12. Flujo de trabajo de Sara Alert



Red de Laboratorios de Resistencia a los Antimicrobianos (Antimicrobial Resistance Laboratory Network, ARLN)

AIMS mejora la capacidad de los laboratorios de salud pública de Estados Unidos para identificar con rapidez las amenazas emergentes y novedosas de resistencia a los antimicrobianos. Los laboratorios de salud pública de la ARLN utilizan el enrutamiento inteligente de mensajes de la plataforma AIMS para enviar los resultados de resistencia a los antimicrobianos a los CDC para su análisis.

Figura 13. Red de Laboratorios de Resistencia a los Antimicrobianos (ARLN)



El Modelo de AIMS

Tras analizar la funcionalidad básica, las ventajas, los casos de uso y la evolución de la plataforma AIMS en [La Historia de AIMS \(pág. 7\)](#), esta sección detalla los componentes técnicos fundamentales que proporcionan las funciones de la plataforma. Las siguientes subsecciones representan cómo AIMS se ajusta a las prácticas recomendadas del sector para los sistemas informáticos sanitarios a gran escala, divididas en tres áreas fundamentales: tecnología, gestión de datos y partes interesadas y operaciones. Para que cualquier sistema centralizado de intercambio de datos tenga éxito, es primordial garantizar que estas áreas estén alineadas y centradas en las necesidades de las partes interesadas y sus operaciones.

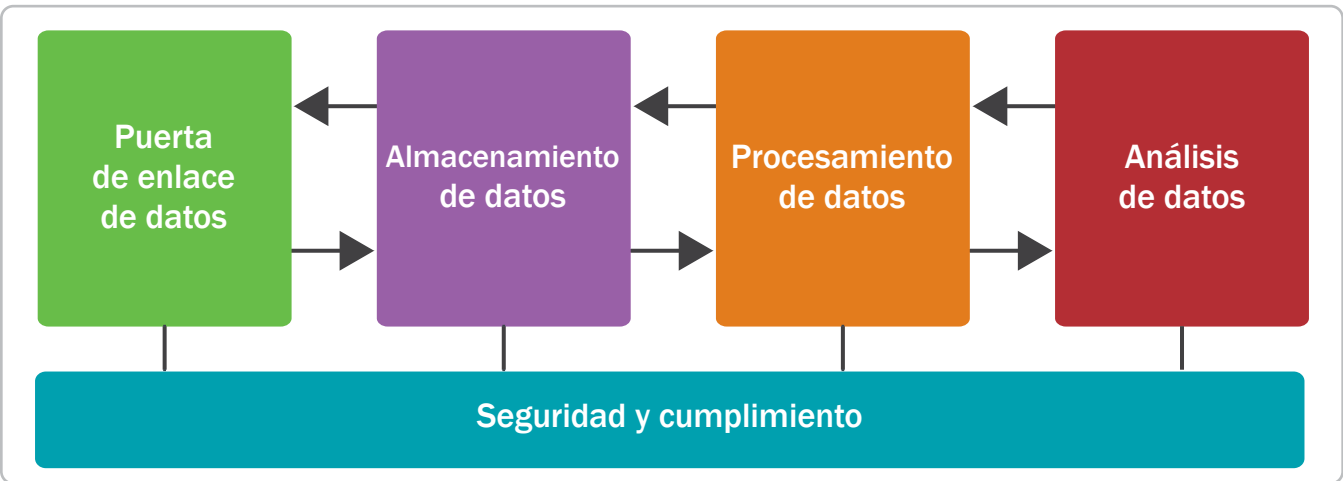
Esta sección describe cada una de las áreas fundamentales, con un enfoque particular en la tecnología y sus requisitos funcionales. La sección final, [Implementación de un Sistema de Intercambio de Datos Centralizado \(pág. 32\)](#), sirve de guía para aprender a implementar la tecnología.



Tecnología

La tecnología que se utiliza para la plataforma AIMS es una infraestructura sofisticada que se basa en la nube y está diseñada para facilitar el intercambio fluido de datos de salud pública a través de una red diversa de sistemas de atención médica y de laboratorio. Al aprovechar tecnología de vanguardia y los protocolos de intercambio de datos estándar de la industria, AIMS garantiza una comunicación y una interoperabilidad en tiempo real sólida, segura, escalable y eficiente entre las entidades de salud pública. Esta parte reúne 15 años de historia de una compleja plataforma informática sanitaria en componentes básicos “obligatorios”, **centrándose en las capacidades funcionales de la tecnología**. Este “modelo” es deliberadamente de primer nivel y está estructurado en segmentos consumibles para que la plataforma AIMS pueda replicarse con éxito. La siguiente estructura conceptual de primer nivel abarca los componentes técnicos necesarios para ofrecer la funcionalidad básica de la plataforma AIMS.

Figura 14. Modelo técnico de primer nivel para la plataforma AIMS



Seguridad y cumplimiento

La seguridad y el cumplimiento son esenciales para proteger los datos sanitarios sensibles y garantizar que se manejen de manera adecuada. Las medidas de seguridad, como el cifrado y los controles de acceso, garantizan que solo las personas que están autorizadas puedan ver los datos. “Cumplimiento” significa seguir normas y los reglamentos específicos, como la Ley de Transferibilidad y Responsabilidad del Seguro de Salud (Health Insurance Portability and Accountability Act, HIPAA) en Estados Unidos, para garantizar que la plataforma cumple los requisitos legales de privacidad de los datos. Juntos, la seguridad y el cumplimiento de la normativa ayudan a prevenir las filtraciones de datos, proteger la privacidad de las personas y fomentar la confianza entre las organizaciones de salud pública al garantizar que los datos se gestionan de forma segura y responsable. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

- **Cifrado:** AIMS implementa mecanismos sólidos de cifrado, tanto para datos en reposo como en tránsito. Esto incluye el uso del protocolo de seguridad de la capa de transporte (Transport Layer Security, TLS) para proporcionar canales de comunicación seguros y el estándar de cifrado avanzado (Advanced Encryption Standard, AES) para datos almacenados.
- **Gestión de identidad y acceso (Identity and Access Management, IAM):** la plataforma aprovecha los servicios de IAM (por ejemplo, AWS IAM) para controlar el acceso a los recursos según las funciones y las políticas. El control de acceso basado en roles (Role-based access control, RBAC) garantiza que solo los usuarios autorizados puedan acceder a datos sensibles o realizar acciones específicas dentro de la plataforma.
- **Marcos de cumplimiento:** la plataforma AIMS está diseñada para cumplir varios marcos normativos, incluidos NIST* e HIPAA en Estados Unidos. Esto implica aplicar controles de seguridad, realizar auditorías periódicas y mantener registros detallados e informes de auditoría para demostrar el cumplimiento de los requisitos legales y reglamentarios.
- **Autenticación y federación de usuarios:** AIMS es compatible con el inicio de sesión único (single sign-on, SSO) y la autenticación federada, lo que permite a los usuarios de distintas organizaciones acceder de forma segura a la plataforma utilizando sus credenciales existentes. Esto suele gestionarse mediante la integración con proveedores de identidad (por ejemplo, Active Directory, SSO basado en SAML).

Infraestructura

la infraestructura es la columna vertebral de la plataforma y garantiza la seguridad del flujo de datos y la estabilidad del sistema. Incluye servidores, redes y sistemas en la nube que se adaptan a la demanda y se recuperan rápidamente de los problemas. Mediante la integración de prácticas de operaciones de desarrollo (Development Operations, DevOps), se automatiza la implementación de código de software y la gestión de infraestructuras, lo que permite realizar actualizaciones eficientes y obtener un rendimiento del sistema con capacidad de respuesta. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

Alojamiento en la nube

- **Plataforma como servicio (Platform as a Service, PaaS):** AIMS funciona según un modelo de plataforma como servicio basado en la nube, haciendo uso de proveedores de servicios en la nube como Amazon Web Services (AWS) para su infraestructura subyacente. Este modelo de operación permite que la plataforma se despreocupe del manejo del hardware subyacente y se enfoque en aspectos a nivel de aplicación como el procesamiento de datos, la integración y la seguridad.
- **Escalamiento flexible:** el uso de la infraestructura de la nube permite un escalamiento flexible, lo que permite a la plataforma ajustar automáticamente los recursos informáticos y de almacenamiento en función de la demanda.

* [Marco de privacidad y ciberseguridad del NIST](#)

Esto es crucial para manejar grandes volúmenes variables de datos de salud pública, como durante brotes de enfermedades u otras emergencias de salud pública.

- **Alta disponibilidad y redundancia:** la plataforma está diseñada para ofrecer alta disponibilidad con mecanismos de conmutación por error y redundancia en varias regiones geográficas. Esto garantiza que, aunque una región se vea interrumpida, la plataforma pueda seguir funcionando desde otra, minimizando el tiempo de inactividad.

Nube híbrida e integración local

- **Integración de sistemas heredados:** las puertas de enlace de datos locales y las soluciones de middleware facilitan la integración de sistemas heredados con los servicios basados en la nube de AIMS, lo que permite la sincronización y gestión segura y eficiente de datos.
- **Residencia de datos y cumplimiento:** el enfoque de nube híbrida utiliza almacenamiento local de datos sensibles, también cumple con normas locales y aprovecha la escalabilidad de la nube para operaciones menos confidenciales.
- **Mayor seguridad y rendimiento:** los componentes críticos pueden funcionar localmente para necesidades de baja latencia o mayor seguridad, integrándose de manera fluida en la infraestructura de la nube para capacidades más amplias.
- **Gestión de costos:** el procesamiento local de tareas que utilizan una gran cantidad de datos reduce los costos de transferencia y puede ayudar a sustituir altas demandas de cómputo antes de moverlos a la nube para realizar análisis adicionales.
- **Implementación de contenedores:** el uso de tecnologías de contenedores como Docker y orquestadores como Kubernetes permite empaquetar e implementar aplicaciones de forma coherente tanto en la nube como en entornos locales. Este enfoque admite una escalabilidad sin problemas, mejora la velocidad de implementación y mantiene la coherencia operativa en toda la infraestructura híbrida, lo que mejora la capacidad de la plataforma para gestionar las cargas de trabajo de forma flexible y segura independientemente de su ubicación de implementación.

Control y observación

- **Registro centralizado:** la plataforma emplea sistemas de registro centralizados (por ejemplo, ELK Stack- Elasticsearch, Logstash, Kibana) para agregar registros de varios servicios y componentes. Esto permite la supervisión en tiempo real y facilita la resolución de problemas al ofrecer una visión completa de la actividad del sistema y los flujos de datos.
- **Control y alertas:** AIMS utiliza herramientas de control (por ejemplo, Prometheus, Grafana, AWS CloudWatch) para realizar un seguimiento de la salud y el rendimiento de su infraestructura y servicios. Las alertas se configuran para notificar a los administradores cualquier anomalía, como interrupciones del servicio o degradación del rendimiento, lo que permite una respuesta y resolución rápidas.
- **Controles de salud y supervisión de SLA:** se realizan comprobaciones automáticas del estado de los servicios críticos para garantizar su correcto funcionamiento. Los acuerdos de nivel de servicio (Service Level Agreements, SLA) se supervisan para garantizar que la plataforma cumpla sus compromisos de tiempo de actividad y rendimiento.

Automatización y DevOps

- **La infraestructura como código (Infrastructure as Code, IaC):** AIMS utiliza herramientas de infraestructura como código (IaC), por ejemplo, Terraform, AWS CloudFormation, para automatizar la implementación y la gestión de su infraestructura. Esto garantiza su consistencia y repetición, y facilita la escalabilidad de los recursos de la plataforma.

- **Canales CI/CD:** la plataforma utiliza canales de integración y entrega continuos (Continuous Integration/Continuous Deployment, CI/CD) para automatizar las pruebas, la integración y la implementación de nuevos códigos. Esto reduce el tiempo de implementación de las actualizaciones y garantiza que los cambios se prueben exhaustivamente antes de ponerlos en marcha.
- **Contenerización y orquestación:** AIMS utiliza la contenerización (por ejemplo, Docker) y la orquestación (por ejemplo, Kubernetes) para gestionar sus servicios en una arquitectura de microservicios. Este enfoque permite la implementación de servicios modulares, escalables y resilientes.

Portal de datos

El componente de las puertas de enlace de datos actúa como punto de acceso central que garantiza que solo los datos autorizados entren y salgan de la plataforma, a través de la aplicación de controles de cifrado y acceso para mantener la seguridad. La puerta de enlace de datos gestiona la conexión segura de los socios de intercambio de datos y permite que sus mensajes fluyan por el sistema: canales seguros y datos en movimiento. Cada socio de intercambio de datos tiene una dirección y una puerta de entrada en la plataforma para gestionar el flujo de mensajes a través de su canal conectado. Si las conexiones se gestionan de manera eficiente y centralizada, se favorece el intercambio de datos confiables y seguros entre varios sistemas. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

- **Incorporación de socios:** la plataforma incluye herramientas y procesos para la incorporación de nuevos socios, lo que garantiza que sus sistemas puedan conectarse de forma segura a AIMS y cumplan los estándares de datos requeridos. Esto puede implicar la configuración de API, el establecimiento de canales de comunicación seguros y la validación de formatos de datos.
- **Bus de servicios empresariales (ESB):** la plataforma AIMS utiliza una arquitectura de bus de servicios empresariales (ESB), que actúa como eje central para integrar diversos sistemas y aplicaciones de salud pública. El ESB facilita el enrutamiento, la transformación y la orquestación de mensajes entre sistemas, lo que garantiza que los datos se entreguen en el formato correcto y a los destinos adecuados.
- **HL7, FHIR y otros estándares:** la plataforma es compatible con múltiples estándares de intercambio de datos sanitarios, como HL7 (Health Level 7) y FHIR (Fast Healthcare Interoperability Resources). Esto permite una comunicación fluida entre distintos sistemas de atención médica, laboratorios y organismos de salud pública.
- **Puerta de enlace de API:** AIMS incluye una puerta de enlace de API que gestiona la exposición de las API basadas en RESTful y SOAP, y proporciona un acceso seguro a los servicios de la plataforma. La puerta de enlace de API gestiona el tráfico de API, aplica la limitación de velocidad y proporciona mecanismos de autenticación y autorización para garantizar un acceso seguro y controlado a los datos y servicios.

Archivo de datos

El objetivo del componente de almacenamiento de datos es guardar, gestionar y realizar copias de seguridad de los datos de forma segura para su uso futuro, lo que garantiza que sean fácilmente accesibles cuando se necesiten. Los datos sin procesar de los mensajes se almacenan temporalmente para garantizar una transferencia segura y, una vez procesados por completo, se eliminan del sistema. Los metadatos relacionados con el procesamiento de mensajes se almacenan durante períodos más largos para facilitar el seguimiento del ciclo de vida del intercambio de datos a fin de respaldar la auditabilidad y el cumplimiento. Existen medidas de redundancia y copia de seguridad para proteger los datos durante el tránsito y evitar pérdidas en caso de fallas del sistema. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

- **Sistemas de bases de datos:** AIMS utiliza una combinación de bases de datos relacionales (por ejemplo, PostgreSQL, MySQL) y NoSQL (por ejemplo, MongoDB, DynamoDB) para almacenar datos estructurados y no estructurados. La elección de la base de datos depende de la naturaleza de los datos: las bases de datos

relacionales suelen utilizarse para datos transaccionales y las bases de datos NoSQL para el almacenamiento flexible de datos a gran escala.

- **Lagos de datos y almacenamiento:** la plataforma puede integrarse con lagos de datos (por ejemplo, AWS S3) o almacenes de datos (por ejemplo, Amazon Redshift) para permitir el almacenamiento y análisis a largo plazo. Esto permite agregar y analizar grandes volúmenes de datos de salud pública, lo que facilita la investigación y la toma de decisiones.
- **Recuperación en caso de accidentes y continuidad de las actividades:** la plataforma AIMS incluye planes de recuperación y continuidad de la actividad, con sistemas redundantes y copias de seguridad periódicas para garantizar que los datos no se pierdan en caso de interrupción o accidentes. Esto garantiza que las funciones de salud pública puedan continuar sin interrupción, incluso en situaciones adversas.

Procesamiento de datos

El objetivo del componente de tratamiento de datos es limpiar, organizar y transformar los datos sin procesar en un formato estandarizado y utilizable. Este proceso garantiza que los datos sean precisos, coherentes y no contengan errores, lo que los hace confiables para enviarlos a otros socios de intercambio de datos. Esto incluye todo, desde la estandarización, el enriquecimiento, la transformación, el enrutamiento inteligente y mucho más. El procesamiento de datos es el paso crítico en torno a la limpieza y la traducción de datos una vez que la plataforma recibe un mensaje, de modo que otros socios de intercambio de datos lo puedan enrutar y utilizar eficazmente. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

- **Colas de mensajes y estructura orientada a eventos:** la plataforma utiliza colas de mensajes (por ejemplo, AWS SQS o Apache Kafka) para desacoplar sistemas y permitir la comunicación asíncrona. Esta estructura orientada a eventos permite el procesamiento en tiempo real de los datos a medida que fluyen a través de la plataforma, lo que garantiza la entrega y el procesamiento oportuno de la información de salud pública.
- **Motores de interfaz y herramientas de transformación:** AIMS utiliza motores de interfaz como Mirth para gestionar transformaciones e integraciones de datos, brindando canales sólidos y configurables que manejan flujos de datos complejos y garantizan la integridad de los datos. Estas herramientas se complementan con servicios de transformación de datos dentro del ESB o mediante procesadores externos, lo que facilita las conversiones entre diversos formatos de datos (por ejemplo, de HL7 v2 a FHIR), que son cruciales para la interoperabilidad del sistema.
- **Orquestación:** la plataforma utiliza motores de orquestación (por ejemplo, Apache Camel o AWS Step Functions) para gestionar flujos de trabajo complejos en los que intervienen múltiples sistemas y fuentes de datos. La orquestación garantiza que los datos se procesen en el orden correcto y que se completen todos los pasos necesarios antes de que lleguen a su destino final.

Análisis de datos

El componente de análisis de datos se encarga de examinar e interpretar los datos procesados para descubrir patrones, tendencias y perspectivas que ayuden a informar las decisiones. Incluye herramientas estadísticas, algoritmos y, en ocasiones, aprendizaje automático para analizar datos y generar informes, perspectivas o predicciones sobre las actividades de intercambio de datos y el rendimiento del sistema. Estas herramientas permiten a los usuarios supervisar el tráfico de mensajes, identificar tendencias y realizar un seguimiento del estado del sistema en tiempo real. Los paneles visuales y los informes personalizados ofrecen una vista clara de métricas clave, como el volumen de mensajes, los tiempos de procesamiento y las tasas de error, lo que permite una mejor toma de decisiones y una resolución proactiva de problemas. La plataforma AIMS cumple estos requisitos funcionales a través de lo siguiente:

- **Análisis en tiempo real y visualización de seguimiento de mensajes:** AIMS admite el análisis de datos en tiempo real mediante el uso de plataformas de transmisión de datos (por ejemplo, Apache Kafka Streams, AWS Kinesis,

OpenSearch, Elasticsearch). Esto permite a los funcionarios de salud pública obtener información inmediata a partir de los datos que reciben, lo que facilita la toma de decisiones en el momento oportuno.

- **Herramientas de realización de informes:** la plataforma se integra con herramientas de realización de informes (por ejemplo, Tableau, Power BI) que permiten a los usuarios crear y visualizar informes personalizados. Estas herramientas están conectadas a las fuentes de datos dentro de AIMS y proporcionan información actualizada y visualizaciones de análisis.

Gobernanza de datos

La gobernanza de datos es la segunda de las tres áreas fundamentales. El objetivo de la gobernanza de datos es generar confianza en torno a la calidad de los datos. La gobernanza de datos es esencial en la plataforma AIMS, ya que garantiza que los datos que se intercambian y gestionan dentro de la plataforma sean precisos, seguros y cumplan las normas. DAMA International ha codificado las prácticas recomendadas relacionadas con la gobernanza de datos como metodología en *Data Management Body of Knowledge (DMBOK2)*.^{*} La alineación de estas prácticas de gobernanza con el marco DMBOK mejora la capacidad de la plataforma para gestionar los datos como un activo estratégico. La gobernanza de datos impacta en la plataforma AIMS en las siguientes áreas:

Gestión de la calidad de los datos

- **Precisión y coherencia:** los marcos de gobernanza de datos establecen estándares para su calidad y garantizan que los datos que se intercambian a través de AIMS sean precisos, coherentes y fiables. Esto es fundamental para la toma de decisiones en el ámbito de la salud pública, donde los errores en los datos pueden llevar a conclusiones incorrectas o a respuestas tardías.
- **Validación de datos:** las políticas de gobernanza garantizan que los datos se validen antes de su intercambio, lo que reduce la probabilidad de errores y garantiza que todas las partes interesadas puedan usar la información.

Seguridad de los datos y privacidad

- **Control de acceso:** las políticas de gobernanza de datos definen quién puede acceder a datos específicos dentro de la plataforma AIMS. Esto incluye controles de acceso basados en funciones que garantizan que solo el personal autorizado pueda ver o manipular datos confidenciales.
- **Cumplimiento de las normas:** la plataforma AIMS debe cumplir diversas normativas, como HIPAA en Estados Unidos. La gobernanza de datos garantiza que todos los procesos de tratamiento de datos cumplan estos requisitos normativos, lo que protege la privacidad de los pacientes y la información confidencial.
- **Protocolos de seguridad y cifrado:** los marcos de gobernanza exigen la utilización de protocolos de cifrado y de seguridad para proteger los datos durante su transmisión y almacenamiento para que ninguna persona sin acceso pueda acceder.

Administración de datos

- **Propiedad y responsabilidad:** la gobernanza de datos asigna una propiedad clara de los datos, lo que garantiza que haya administradores designados responsables de gestionar, mantener y garantizar la calidad de los datos en AIMS. Esto ayuda a mantener la responsabilidad y a garantizar que los datos se manejen correctamente.
- **Seguimiento automatizado del linaje:** herramientas y tecnologías que capturan y documentan el linaje de los datos de forma automática. Esto reduce el esfuerzo manual requerido para los administradores de datos y garantiza que la información de linaje se capture de forma coherente.

^{*} DAMA International, The DAMA Guide to the Data Management Body of Knowledge (DMBOK2), 2nd ed., Technics Publications, 2017, Chapter 3: Data Governance, págs. 45 a 66.

- **Gestión del ciclo de vida:** las políticas de gobernanza definen cómo se gestionan los datos a lo largo de su ciclo de vida, desde su creación y transmisión hasta que se almacenan y eliminan. Esto garantiza que los datos estén siempre disponibles y se eliminen cuando ya no se necesiten.

Interoperabilidad y estandarización

- **Cumplimiento de los estándares:** la gobernanza de datos garantiza que los datos intercambiados a través de AIMS cumplan los estándares del sector (por ejemplo, HL7). Esta estandarización es crucial para la interoperabilidad, ya que permite que distintos sistemas de salud pública se comuniquen con eficacia.
- **Gestión de metadatos:** los marcos de gobernanza también administran los metadatos, y aportan contexto y significado a los datos. Esto ayuda a garantizar que los distintos sistemas y partes interesadas interpreten correctamente los datos.

Gestión de riesgos y respuesta a incidentes

- **Evaluación de riesgos:** la gobernanza de datos incluye evaluaciones de riesgo continuas para identificar posibles vulnerabilidades en los procesos de tratamiento de datos. Este enfoque proactivo ayuda a mitigar los riesgos antes de que se conviertan en problemas importantes.
- **Respuesta a incidentes:** las políticas de gobernanza definen cómo deben gestionarse las vulneraciones de datos u otros incidentes. Esto incluye protocolos claros para responder a incidentes de seguridad, notificar a las partes afectadas y restaurar la integridad de los datos.

Cumplimiento y auditoría

- **Registros de auditoría:** la gobernanza de datos exige la creación de registros de auditoría para saber quién ha accedido a los datos o los ha modificado y cuándo lo ha hecho. Esto es crucial para la rendición de cuentas y para identificar el origen de cualquier problema que surja.
- **Auditorías regulares:** se realizan para garantizar que se siguen las políticas de gobernanza de datos y que la plataforma AIMS sigue cumpliendo todas las leyes y normativas vigentes.

Uso ético de los datos

- **Transparencia:** la gobernanza de datos fomenta la transparencia en el uso de los datos, lo que garantiza que todas las partes interesadas comprendan la finalidad y el alcance de la recopilación y el uso de estos.
- **Consideraciones éticas:** los marcos de gobernanza garantizan que los datos se utilicen de forma ética y protegen los derechos de las personas para que no se haga un uso indebido de los datos.

La gobernanza de datos dentro de la plataforma AIMS está estrechamente alineada con el marco DMBOK que apoya la integridad, la seguridad y el uso de los datos de salud pública. Esta alineación garantiza que las prácticas de gobernanza de datos en AIMS sean sólidas, coherentes y conformes con las prácticas recomendadas del sector, permitiendo así intervenciones eficaces de salud pública y la elaboración de políticas.

Partes interesadas y operaciones

Las partes interesadas y las operaciones constituyen la tercera y última área fundamental. Una vez construida, una plataforma de intercambio centralizado de datos requiere apoyo continuo para incorporar usuarios al sistema, garantizar su correcto funcionamiento y proporcionar asistencia a las partes interesadas del sistema, incluidos los usuarios finales, entres reguladores, proveedores y socios de intercambio de datos. En las siguientes subsecciones, se describe

en primer lugar un marco de prestación de servicios utilizado por AIMS para garantizar la alta calidad de las operaciones, seguido de los servicios básicos prestados.

Marco de gestión de la prestación de servicios

La gestión de la prestación de servicios (service delivery management, SDM) es el proceso de supervisión y coordinación de la prestación de servicios a los clientes. El objetivo de SDM es cumplir en todo momento las expectativas del cliente en cuanto a plazos, costos, calidad y rendimiento.

Para AIMS, esto significa que el servicio en el que confían los socios de intercambio de datos para enviar y recibir información se presta de manera confiable. Si hay interrupciones en el flujo de datos, el servicio se restaura en un tiempo aceptable, se analiza la causa raíz, se publica documentación sobre el problema a las partes interesadas y se planifican y ejecutan acciones preventivas para prevenir futuros incidentes.

La prestación de servicios a través de la Biblioteca de Infraestructura de Tecnologías de la Información (Information Technology Infrastructure Library, ITIL) y la Gestión de Servicios de TI (IT Service Management, ITSM) es un enfoque estructurado para gestionar los servicios de TI y garantizar que satisfagan las necesidades de la empresa. Implica un conjunto de prácticas para diseñar, brindar, gestionar y mejorar los servicios de TI dentro de una organización, orientadas a garantizar que los servicios de TI se alineen con las metas empresariales.

Componentes clave de la prestación de servicios de ITIL e ITSM

- **Estrategia del servicio:** define las necesidades empresariales de los servicios de TI y cómo contribuirán con los objetivos empresariales. Involucra la gestión de la oferta de servicios, la gestión de la demanda y la gestión financiera.
- **Diseño del servicio:** se centra en el diseño de nuevos servicios informáticos o en la modificación de los existentes para satisfacer las necesidades de la empresa. Abarca aspectos como la gestión de la capacidad, la gestión de la disponibilidad, la gestión del nivel de servicio y la seguridad informática.
- **Transición del servicio:** garantiza que los servicios nuevos o modificados se transfieran al entorno operativo sin problemas y sin causar interrupciones. Incluye la gestión de cambios, la gestión e implementación de versiones y la gestión de activos y configuraciones del servicio.
- **Operación del servicio:** se ocupa de la prestación diaria de servicios de TI garantizando que se cumplan los niveles de servicio acordados. Esto incluye la gestión de incidentes, la gestión de problemas, la gestión de eventos, el cumplimiento de solicitudes y la gestión de accesos.
- **Mejora continua del servicio (Continual Service Improvement, CSI):** se centra en mejorar la eficacia y la eficiencia de los servicios informáticos en función de los comentarios, las métricas de servicio y los datos de rendimiento. CSI busca oportunidades para mejorar la calidad del servicio a lo largo del tiempo.

Procesos clave en la prestación de servicios de ITIL e ITSM

- **Gestión de incidentes:** se encarga de gestionar y resolver incidentes (interrupciones no planificadas o reducciones en la calidad del servicio) para restaurar el servicio lo más rápido posible.
- **Gestión de problemas:** se trata de identificar la raíz de lo que está causando el incidente y prevenir que vuelva a ocurrir.
- **Gestión de cambios:** regula el proceso de implementación de cambios en los servicios de TI, minimizando las interrupciones.
- **Gestión de niveles de servicio (Service Level Management, SLM):** garantiza que todos los servicios se brinden dentro de los estándares de rendimiento acordados (SLA).

- **Gestión de configuración:** realiza un seguimiento de las configuraciones de todos los activos de TI y garantiza la disponibilidad de información precisa para respaldar otros procesos de ITSM.
- **Gestión de capacidad:** garantiza que la infraestructura de TI sea capaz de satisfacer las demandas actuales y futuras de la empresa.
- **Gestión de disponibilidad:** garantiza que los servicios de TI estén disponibles en los momentos necesarios según los SLA.
- **Gestión financiera para servicios de TI:** involucra la elaboración de presupuestos, la contabilidad y el cobro de los servicios de TI.
- **Gestión de continuidad de los servicios de TI:** se centra en la gestión de riesgos para garantizar que los servicios informáticos puedan reanudarse tras un accidente o un incidente grave.

Beneficios de la prestación de servicios de ITIL e ITSM

- **Alineación con las necesidades de la empresa:** garantiza que los servicios de TI apoyen directamente los objetivos del negocio.
- **Aumento de la eficiencia:** los procesos optimizados reducen el esfuerzo doble y aumentan la productividad.
- **Mejora de la calidad del servicio:** a través de procesos estructurados, los servicios de TI cumplen con los estándares de calidad acordados.
- **Mejora de la gestión de riesgos:** ayuda a anticipar posibles interrupciones y minimizar su impacto.
- **Control de costos:** ayuda a tener una visión más clara de los costos de los servicios de TI y a gestionar los presupuestos de manera más efectiva.
- **Mejora de la satisfacción del cliente:** una prestación de servicios consistente ayuda a que los usuarios y clientes estén más satisfechos.

Servicios principales

Mantenimiento y operaciones de la plataforma

AIMS cuenta con un equipo interdisciplinario de ingenieros, técnicos, gerentes de proyectos y analistas que apoyan las operaciones continuas de la plataforma. El mantenimiento y las operaciones de la plataforma AIMS incluye corrección de fallas del sistema operativo, gestión de vulnerabilidades, configuración y ajuste continuo de alertas y alarmas, operaciones de infraestructura, supervisión de certificados, automatización de procesos de operaciones en producción, gestión de identidad y acceso, actividades de recuperación ante accidentes de infraestructura, monitoreo de interfaces del motor de integración Mirth, seguridad de configuraciones, seguridad de bases de datos, creación y mantenimiento de políticas de ciclo de vida, gestión de detección de intrusiones, resolución de errores en aplicaciones y gestión de cambios.

El equipo responsable del mantenimiento de las operaciones en curso de la plataforma de intercambio debe definir y documentar qué individuos o equipos son responsables de identificar eventos o problemas, quiénes son responsables de su resolución y a quiénes se debe consultar o informar al respecto. Estas asignaciones pueden representarse en una [matriz de asignación de responsabilidades \(RACI\)](#).

Asistencia al usuario final

El equipo de asistencia de producción de AIMS asiste a sus socios de intercambio de datos para reforzar su uso constante de la plataforma. El equipo controla un sistema de tickets para responder a las solicitudes de los clientes y comunica la información relevante por correo electrónico, como los períodos de inactividad por mantenimiento o las interrupciones del servicio. Un sistema de tickets para estandarizar, gestionar y seguir la tramitación y resolución de las

solicitudes de asistencia es una herramienta esencial para el apoyo continuo de un sistema sólido de intercambio de datos, al igual que una herramienta para automatizar las comunicaciones masivas con los usuarios finales.

Los usuarios de AIMS acceden al sistema de tickets a través de un portal o por correo electrónico. El envío por correo electrónico es una opción sencilla para los servicios de asistencia menos complejos. A medida que la complejidad de AIMS crecía, surgió la necesidad de dirigir a los usuarios al portal de asistencia para estandarizar las entradas.

La presentación a través del portal permite al equipo de AIMS requerir un conjunto básico de información para la solicitud y permite a los usuarios clasificar su presentación como un incidente (tiempo de inactividad, problemas que requieren solución) o una solicitud (consulta o pregunta, servicio menos urgente). Estas categorizaciones permiten el reparto a diferentes equipos en función de la urgencia y la experiencia en la materia requerida y dan lugar a una resolución más eficiente.

Figura 15. Menú de solicitudes de servicio

Comuníquese con nosotros sobre lo siguiente

Solicitudes de servicio

¿En qué lo podemos ayudar?

Cuestiones generales
Informar un problema, solicitar un cambio.

Actualizar un certificado
Renovación, revocación o emisión de certificados.

Solicitud de CMDB
Nueva adición, configuración o modificaciones en los elementos de CMDB y configuración.

Validación de datos
Asistencia en la validación de entradas de datos, realización de verificaciones de integridad y resolución de discrepancias.

Solicitud de despliegue
Implementación de actualizaciones del sistema, modificaciones de configuración y parches en los servicios que se alojan en AIMS.

Solicitud general
Es una versión general de las solicitudes de servicio.

Jira o Confluence
Nueva adición, configuración o modificaciones en los proyectos Jira y espacios de Confluence.

Nueva solicitud de incorporación (New Onboarding Request, Non-eCR)
Solicitud de incorporación de Non-eCR en nuevos HCO, PHA y PHL.

Figura 16. Menú del centro de asistencia de AIMS

Centro de asistencia de AIMS y de APHL

Centro de asistencia de AIMS

Bienvenido al portal del servicio de atención al cliente del AIMS!

- Puede realizar su consulta desde las siguientes opciones.
- No publique **PHI ni PII** en **ninguna** solicitud, comentario, ni lo incluya en archivos adjuntos.
- Haga clic aquí para obtener más información sobre cómo utilizar el portal.

Comuníquese con nosotros sobre lo siguiente

Cuestiones generales
Informar un problema, solicitar un cambio.

Informes electrónicos de casos (eCR)
Asistencia técnica de eCR, requisito de notificación obligatoria de eCR (ayuda del usuario de RCKMS), funciones y mejoras de eCR RCKMS, contenido de eCR RCKMS, incorporación de eCR: organismos de salud pública (PHAS), funciones y mejoras de eCR, información y recursos de eCR, políticas legales de eCR, distribución de informes y vigilancia electrónica de eCR (eRSD).

Gestión del usuario del panel de control de monitoreo de eCR de PHA
Desactivar la cuenta del panel de control de monitoreo de eCR de PHA, nueva cuenta del panel de control de monitoreo de eCR de PHA, resetear contraseña de la cuenta del panel de control de monitoreo de eCR de PHA.

Solicitudes de servicio
Crear un certificado nuevo, actualizar certificado, solicitar base de datos de gestión de configuración (configuration management database, CMDB), validación de datos, solicitud de desarrollo, solicitud general, Jira o Confluence, nueva solicitud de incorporación (No eCR), solicitud incompleta, actualización del catálogo de servicios, usuario y control de acceso, renovación de acceso a AIMS.

Asistencia técnica

APHL colabora con el CDC para ofrecer asistencia técnica a organismos de salud pública y laboratorios, conectando los sistemas de gestión de información de laboratorios (Laboratory Information Management Systems, LIMS) y de gestión de datos a la plataforma AIMS. El programa de asistencia técnica brinda apoyo temporal de expertos en la materia a entidades de salud pública a quienes la contratación de personal permanente no les resulta económicamente viable o sostenible. Las áreas de asistencia técnica incluyen lo siguiente:

- **Extracción y migración de datos:** asistencia para extraer datos de los LIMS locales y garantizar que estén en un formato compatible para su migración a la plataforma de intercambio de datos. Los expertos en asistencia técnica ofrecen herramientas y técnicas especializadas para facilitar la migración de datos de manera fluida, con mínima interrupción de las operaciones en curso.
- **Estandarización e integración de datos:** asistencia para garantizar que los datos de distintos LIMS locales se estandaricen e integren en la plataforma de intercambio de datos, preservando la integridad y consistencia de la información. Los expertos en asistencia técnica asesoran sobre los procesos de mapeo y transformación de datos para alinear diferentes estructuras y formatos de datos.
- **Soluciones y asistencia personalizados:** asistencia para ofrecer soluciones a medida que aborden los desafíos específicos que enfrentan los LIMS locales en diferentes regiones. Los expertos en asistencia técnica brindan apoyo práctico y resuelven problemas durante el proceso de extracción y migración de datos.
- **Capacitación y desarrollo de capacidades:** asistencia para capacitar al personal local en nuevos procesos y herramientas para la extracción y gestión de datos en el nuevo entorno. Los expertos en asistencia técnica apoyan a los socios de intercambio de datos para desarrollar la capacidad local de gestionar y mantener el nuevo sistema de manera efectiva y sostenible.
- **Protección de la seguridad y privacidad de los datos:** asistencia para implementar medidas de seguridad sólidas durante la extracción y migración de datos, protegiendo la información confidencial de salud pública y garantizando el cumplimiento de las normativas y estándares pertinentes a lo largo del proceso de manejo de datos.

Implementación de un Sistema de Intercambio de Datos Centralizado: Consideraciones de Diseño y Prácticas Recomendadas

El objetivo de esta sección es ofrecer al lector consideraciones de diseño y prácticas recomendadas al planificar intercambios centralizados de datos de salud pública para satisfacer sus propias necesidades. La organización de esta sección refleja la del “[El Modelo de AIMS](#)” (pág. 21), que brinda información sobre cada área fundamental: **tecnología, gobernanza de datos, partes interesadas y operaciones**, así como árboles de decisiones detallados para guiar al lector en la toma de decisiones. Se brinda atención especial al área de tecnología para ayudar al lector a abordar las necesidades de sus partes interesadas y establecer su propio intercambio de datos de salud pública.

Tecnología

Esta sección abarca cada uno de los componentes introducidos en el modelo técnico de alto nivel de la plataforma AIMS, incluye árboles de decisiones, consideraciones y guías. Los árboles de decisiones se utilizan para mostrar los pasos que el lector puede seguir y así identificar las necesidades no funcionales para implementar cada uno de los componentes tecnológicos requeridos en su país. Los requisitos no funcionales se enfocan en describir cómo debe llevarse a cabo el trabajo para que el sistema funcione de una manera que se pueda utilizar y sostener en el tiempo. La leyenda codificada por colores que se utiliza en cada uno de los árboles de decisiones es la siguiente:

Figura 17. Leyenda del árbol de decisiones

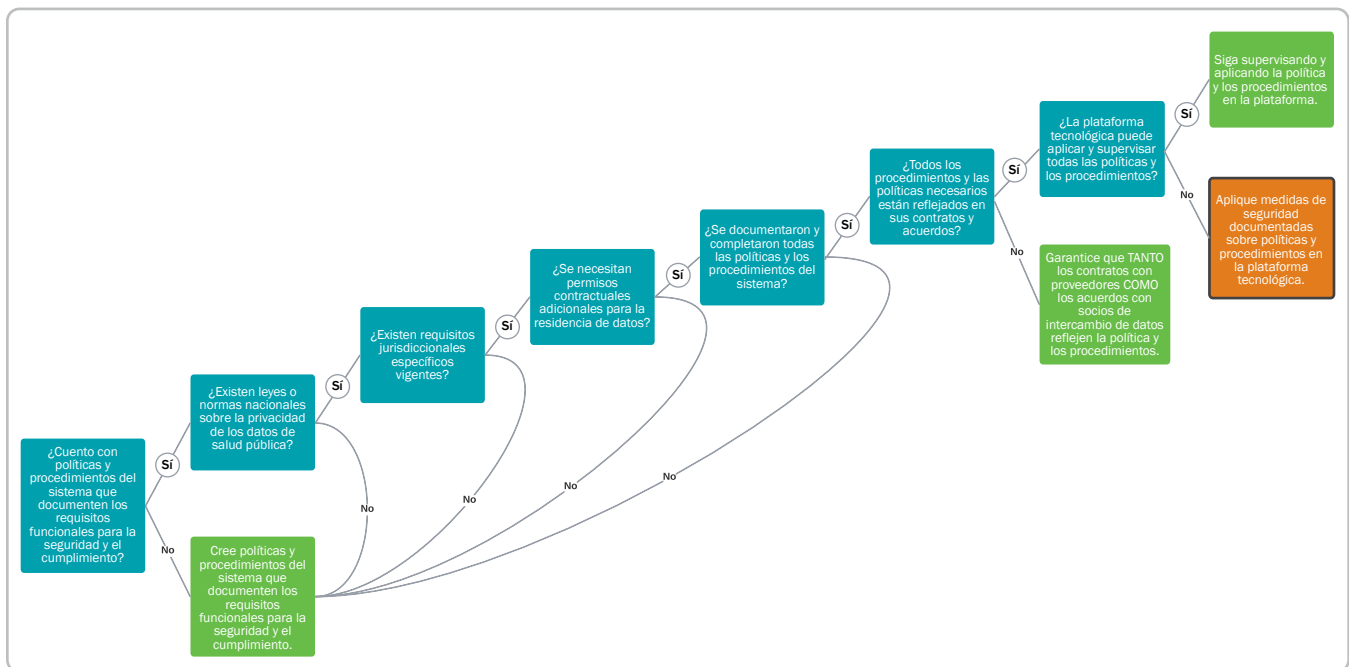


Seguridad y cumplimiento

La seguridad y el cumplimiento, como se mencionó en “El Modelo de AIMS” (pág. 21), son esenciales para proteger los datos sanitarios confidenciales y garantizar que se manejen de manera adecuada. Las medidas de seguridad, como el cifrado, garantizan que solo las personas que están autorizadas puedan ver los datos. “Cumplimiento” significa seguir normas y los reglamentos específicos, como HIPAA, para garantizar que la plataforma cumpla los requisitos legales de privacidad de los datos.

Diagrama de decisiones

Figura 18. ¿Cómo implementar controles de seguridad y cumplimiento para el intercambio de datos de salud pública?



Consideraciones

La siguiente lista proporciona consideraciones clave que serán útiles para ayudar al lector a alinear las necesidades de seguridad y cumplimiento con las necesidades no funcionales de su intercambio de datos de salud pública. El cumplimiento de las leyes de residencia y localización de datos es crucial.

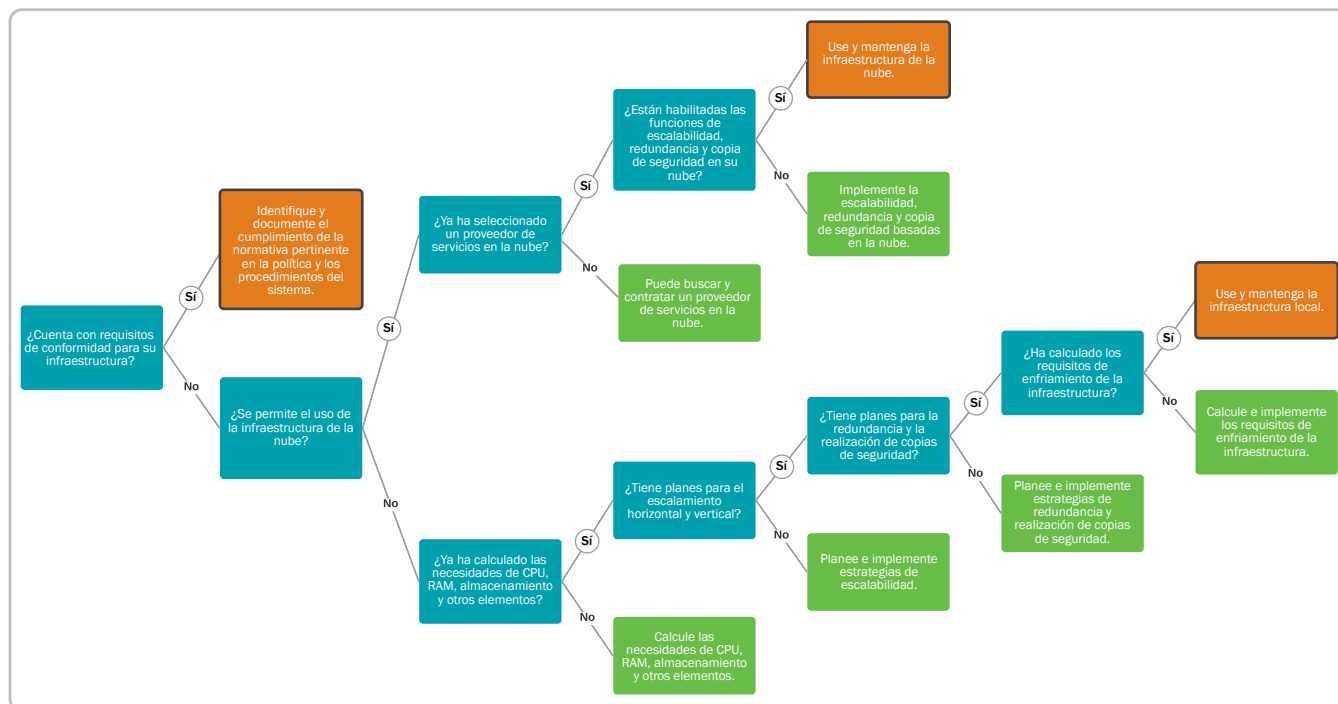
- **Normativas específicas de la jurisdicción:** comprender y cumplir las leyes que exigen que los datos se almacenen dentro de límites geográficos específicos.
- **Requisitos de privacidad:** garantizar que los proveedores de la nube cumplan con las normativas como, GDPR, HIPAA y otras leyes de protección de datos.
- **Acuerdos contractuales:** incluir los requisitos de residencia de datos en los contratos con proveedores de la nube para garantizar el cumplimiento.

Infraestructura

Como ya se mencionó en “El Modelo de AIMS” (pág. 21), la infraestructura es la columna vertebral del intercambio de datos de salud pública y proporciona un flujo de datos confiable y estabilidad del sistema. Incluye servidores, redes y sistemas en la nube que se adaptan a la demanda y se recuperan rápidamente de los problemas. Debe integrar prácticas de operaciones de desarrollo (DevOps), donde se automatiza la implementación de código de software y la gestión de infraestructuras, lo que permite actualizaciones eficientes y un rendimiento del sistema con capacidad de respuesta.

Diagrama de decisiones

Figura 19. ¿Cómo implementar la infraestructura para el intercambio de datos de salud pública?



Consideraciones

Las organizaciones deben considerar varios factores al decidir entre soluciones locales, en la nube privada y en la nube pública.

- **Cumplimiento:** garantizar el cumplimiento de las normativas y los estándares relevantes para la privacidad y seguridad de los datos.
- **Seguridad:** evaluar las medidas de seguridad ofrecidas por entornos de nube comercial, nube privada o locales.
- **Costo:** comparar el costo total de propiedad, que abarca inversiones iniciales, mantenimiento continuo y gastos operativos.
- **Escalabilidad:** evaluar la capacidad de ajustar los recursos hacia arriba o hacia abajo según la demanda. La capacidad de ajustar hacia arriba para responder a un tráfico intenso en situaciones emergentes y hacia abajo para ahorrar costos una vez que dichas situaciones han disminuido. En la nube, esto puede ser tan fácil como seleccionar algunas opciones en el panel de administración. Si no está en la nube, se puede utilizar una arquitectura que permita la contenerización (por ejemplo, Kubernetes).
- **Flexibilidad:** considerar la flexibilidad para acceder a los datos de forma remota y apoyar la colaboración.

Guías para la nube local o privada

Si se implementa una nube local o privada, la estructura incluirá una combinación de máquinas virtuales (servidores) y una estrategia de contenedores para las capacidades del componente. Esto se puede considerar si se utilizan los siguientes pasos de cálculo de capacidad:

1. Estimar los requisitos de cómputo

- Requisitos del CPU:
 - ◆ Sobrecarga de la contenerización: estimar la sobrecarga del CPU para la orquestación de contenedores (por ejemplo, Kubernetes) y la virtualización (por ejemplo, KVM, VMware).
 - ◆ Requisitos de la carga de trabajo: calcular el uso promedio y máximo del CPU para las aplicaciones que se estarán ejecutando. Esto abarca el CPU mínimo necesario por contenedor, multiplicado por la cantidad de contenedores.
 - ◆ Capacidad de reserva: se puede añadir una reserva (por lo general entre 20 y 30 %) para manejar picos inesperados en el uso y facilitar el escalamiento futuro.
 - ◆ Núcleos totales del CPU: el total de núcleos que se necesitan del CPU = (número de CPU por contenedor x número de contenedores) + sobrecarga + reserva.
- Requisitos de la memoria RAM:
 - ◆ Necesidades de memoria de la aplicación: determinar los requisitos de la memoria RAM para cada aplicación y contenedor basándose en datos históricos o pruebas de referencia.
 - ◆ Sobrecarga: incluir la sobrecarga de memoria para la plataforma de orquestación de contenedores y la virtualización.
 - ◆ Capacidad de reserva: similar al CPU, también se puede añadir una reserva a la RAM.
 - ◆ RAM total: el total de RAM que se necesita = (RAM por contenedor x número de contenedores) + sobrecarga + reserva.

2. Estimar los requisitos de almacenamiento

- Volumen de almacenamiento para los datos:
 - ◆ Calcular la cantidad total de datos que las aplicaciones generarán, almacenarán y procesarán. Incluir datos estructurados (bases de datos) y datos no estructurados.
 - ◆ Incluir las necesidades de almacenamiento para registros, copias de seguridad y cualquier política de retención de datos.
 - ◆ Considerar la redundancia de datos y los factores de replicación (por ejemplo, configuración RAID, factor de replicación en almacenamiento distribuido).
- Operaciones de entrada y salida por segundo (Input/Output Operations Per Second, IOPS):
 - ◆ Determinar los requisitos de IOPS basándose en las operaciones de lectura y escritura de las cargas de trabajo.
 - ◆ Considerar los requisitos de velocidad para los discos (por ejemplo, SSD vs. HDD) y los niveles de almacenamiento.
- Tipo de almacenamiento:
 - ◆ Evaluar la necesidad de almacenamiento en bloques, almacenamiento de archivos y almacenamiento de objetos según los requisitos de aplicación.
 - ◆ Las soluciones de código abierto como Ceph, GlusterFS u otras pueden ser adecuadas para una nube privada.

3. Requisitos de la red

- Ancho de banda:
 - ◆ Estimar el ancho de banda de red necesario en función de la tasa de transferencia de datos entre contenedores, máquinas virtuales y sistemas externos.
 - ◆ Incluir el ancho de banda necesario para actividades de copia de seguridad, replicación y migración de datos.
- Latencia:
 - ◆ Calcular la latencia aceptable para diferentes tipos de tráfico (por ejemplo, comunicación interna del clúster, solicitudes de usuarios).
 - ◆ Considerar el impacto de latencia de la red en el rendimiento de las aplicaciones.
- Topología de la red: Determinar si utilizará redes definidas por software (software-defined networking, SDN) o configuraciones de red tradicionales. Para las SDN se necesitará una sobrecarga adicional.

4. Virtualización y sobrecarga de la contenerización

- Sobrecarga del hipervisor: calcular la sobrecarga de recursos asociada con el hipervisor.
- Sobrecarga de orquestación de contenedores: determinar los recursos adicionales requeridos por el sistema de orquestación de contenedores (por ejemplo, recursos del plano de control en Kubernetes).
- Disminución del rendimiento: estimar la posible disminución del rendimiento al ejecutar contenedores dentro de máquinas virtuales en comparación con ejecutarlos en hardware físico.

5. Escalabilidad y alta disponibilidad

- Escalamiento: brindar una guía sobre cómo calcular los recursos de escalamiento horizontal y vertical en función del crecimiento esperado.
- Redundancia: estimar los recursos adicionales requeridos para la alta disponibilidad (por ejemplo, configuraciones activas-pasivas, balanceo de carga).

6. Eficiencia en el uso de los recursos

- Asignación de recursos: recomendar métodos para optimizar la asignación de recursos, como las tasas de un sobre compromiso para CPU y memoria en entornos virtuales.
- Escalamiento automático: considerar los requisitos de recursos para implementar el escalamiento automático según la carga.

7. Requisitos de energía y refrigeración

Si los recursos locales se utilizarán mucho, se debe calcular el consumo de energía y los requisitos de refrigeración del centro de datos en función de las necesidades estimadas de cómputo y almacenamiento.

8. Ejemplo del modelo de cálculo

- CPU y RAM:
 - ◆ Suponga que cada contenedor necesita 2 vCPUs y 4GB de RAM.
 - ◆ La capa de orquestación necesita el 10 % del total de los recursos de cómputo y memoria.
 - ◆ Planea ejecutar 20 contenedores.
 - ◆ La reserva se establece en un 25 %
 - ◆ Cálculo:
 - ◇ Núcleos totales del CPU = $(2 \text{ vCPUs} \times 20 \text{ contenedores}) \times 1.10 \text{ (sobrecarga)} \times 1.25 \text{ (reserva)} = 55 \text{ vCPUs}$.
 - ◇ Núcleos totales de RAM = $(4 \text{ GB de RAM} \times 20 \text{ contenedores}) \times 1.10 \text{ (sobrecarga)} \times 1.25 \text{ (reserva)} = 110 \text{ GB RAM}$.

- ◆ Almacenamiento:
 - ◇ Asuma que cada contenedor necesita 50 GB de almacenamiento y necesita un factor de replicación de 3.
 - ◇ El almacenamiento de registros y copias de seguridad añaden un 20 % adicional de sobrecarga.
 - ◇ Cálculo: Almacenamiento total = (50 GB x 20 contenedores) x 3 (replicación) x 1.20 (sobrecarga) = 3,600 GB (3.6 TB).

9. Recomendaciones de herramientas y plataformas

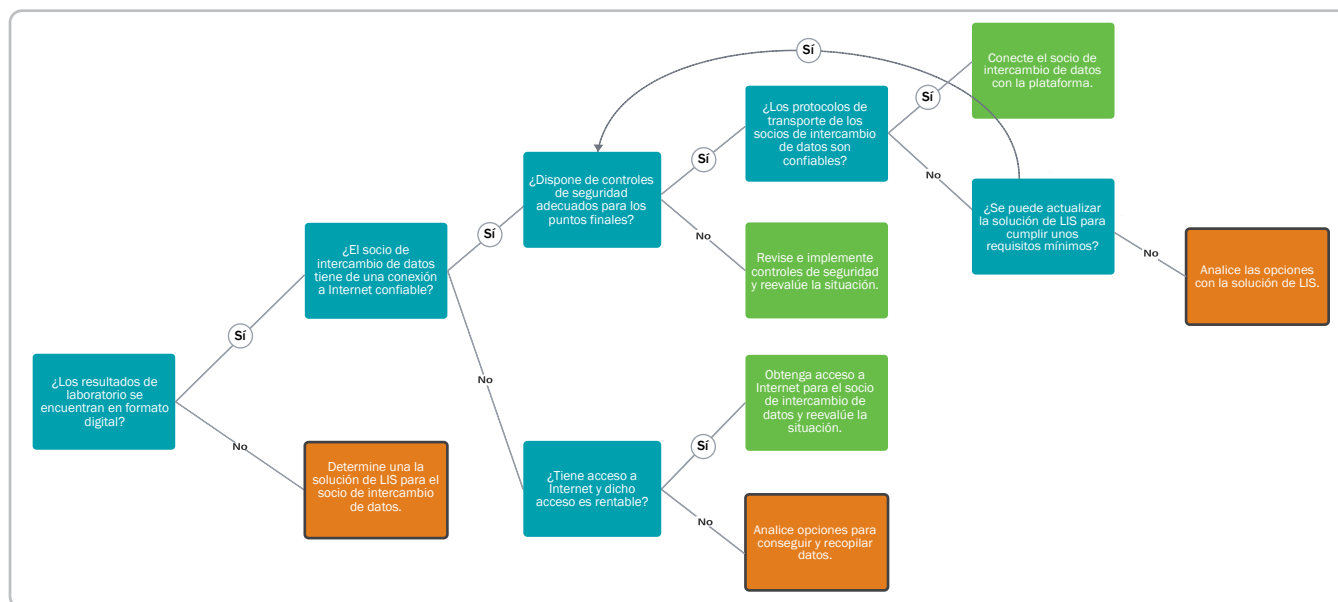
- **Orquestación de contenedores:** Kubernetes, OpenShift.
- **Virtualización:** KVM, Xen, VMware (si no es estrictamente de código abierto).
- **Almacenamiento:** Ceph, GlusterFS para almacenamiento distribuido.
- **Control y gestión:** Prometheus, Grafana para control; Ansible, Terraform para gestión de infraestructura.

Puerta de enlace de datos

Como ya se mencionó en el [Modelo de AIMS](#), el componente de puertas de enlace de datos actúa como punto de acceso central que garantiza que solo los datos autorizados entren y salgan del intercambio de datos de salud pública, aplicando controles de cifrado y acceso para mantener la seguridad. La puerta de enlace de datos gestiona la conexión segura de los socios de intercambio de datos y permite que sus mensajes fluyan por el sistema.

Diagrama de decisiones

Figura 20. ¿Cómo conecto un socio de intercambio de datos con el intercambio de datos de salud pública?



Consideraciones

La siguiente lista proporciona consideraciones clave que serán útiles para ayudar al lector a alinear el funcionamiento del componente de la puerta de enlace de datos con las necesidades no funcionales de su intercambio de datos de salud pública:

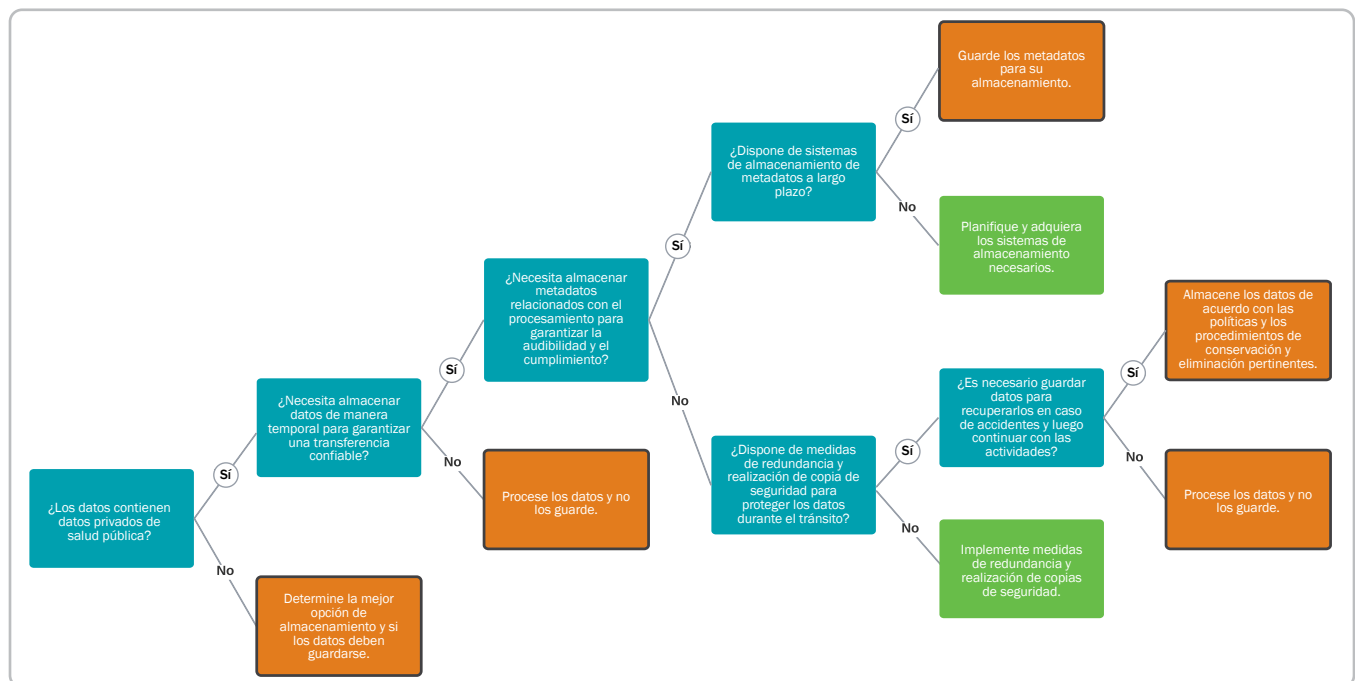
- El motor de interfaz Mirth se puede utilizar tanto en entornos locales como en la nube para facilitar el manejo de datos que hacen posible la interoperabilidad. Mirth ofrece un conjunto de funciones básicas que permite construir una interfaz entre dos sistemas con tan solo diez líneas de código, en comparación con las miles de línea en Java u otro lenguaje de programación estándar. Si se implementa en la nube, compare Mirth con las opciones de integración que ofrece el proveedor de servicios en la nube.
- Formato de datos
 - Consistencia: los formatos de datos estandarizados garantizan que los datos se estructuren de manera consistente, lo que permite una integración y un intercambio fluido entre diferentes sistemas y organizaciones. Los formatos de datos consistentes permiten el procesamiento y análisis automatizados, lo que reduce el riesgo de errores y mejora la eficiencia.
 - Interoperabilidad: con formatos estandarizados, los datos de diversas fuentes se pueden combinar y comparar fácilmente. Esto es esencial para que los organismos de salud pública agreguen datos de múltiples jurisdicciones para con el fin de vigilar y analizar por completo las tendencias en salud pública.
 - Escalabilidad: los formatos estandarizados facilitan la escalabilidad de los sistemas de información en salud pública. A medida que más estados y organizaciones adoptan formatos comunes, se facilita la expansión de la red y la incorporación de fuentes de datos adicionales sin necesidad de una reconfiguración significativa.

Almacenamiento de datos

El componente de almacenamiento de datos, según se detalla en el [Modelo de AIMS](#), debe almacenar y gestionar los datos, y hacer copias de seguridad de estos, de forma segura para su posterior uso. Además, debe garantizar su acceso cuando se necesiten. Los datos sin procesar de los mensajes se almacenan temporalmente para garantizar una transferencia y un procesamiento seguros. Además, los metadatos relacionados con el procesamiento de mensajes se almacenan durante períodos más largos para facilitar el seguimiento del ciclo de vida del intercambio de datos a fin de respaldar la auditabilidad y el cumplimiento. Por último, se deben implementar medidas de redundancia y copia de seguridad para proteger los datos durante el tránsito y evitar pérdidas en caso de fallas del sistema.

Diagrama de decisiones

Figura 21. ¿Cómo debo almacenar y gestionar los datos en el intercambio de datos de salud pública?



Consideraciones

La siguiente lista proporciona consideraciones clave que serán útiles para ayudar al lector a alinear el funcionamiento del almacenamiento de datos con las necesidades no funcionales de su intercambio de datos de salud pública:

- Gestión del ciclo de vida de los datos:
 - Implementar políticas de retención, archivo y eliminación de datos para gestionar el almacenamiento de manera efectiva y cumplir con los requisitos legales.
 - Utilizar herramientas automatizadas para aplicar políticas del ciclo de vida de los datos y optimizar el uso del almacenamiento.
- Rendimiento:
 - Elegir soluciones de almacenamiento que ofrezcan los IOPS requeridos para las aplicaciones, equilibrando los costos y el rendimiento.
 - Considerar opciones de almacenamiento por niveles (por ejemplo, SSD para necesidades de alto rendimiento, HDD para archivo) con el fin de optimizar tanto el costo como la velocidad.

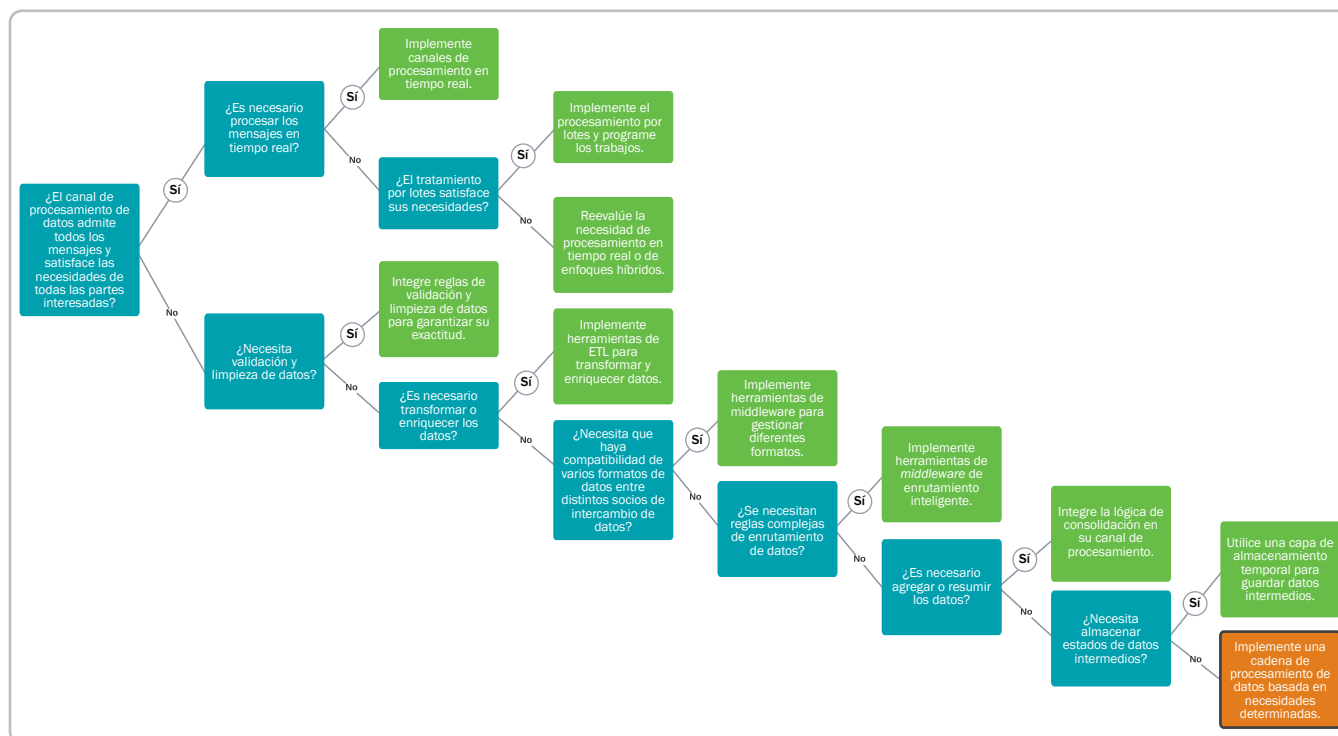
- Escalabilidad:
 - Utilizar soluciones de almacenamiento en la nube escalables (por ejemplo, Amazon S3) que permitan ampliar la capacidad de almacenamiento sin una inversión inicial significativa.
 - En el caso del almacenamiento local, considerar la expansión futura mediante unidades de almacenamiento modulares o sistemas de almacenamiento agrupados.
- Seguridad de los datos:
 - Cifrar todos los datos almacenados mediante los algoritmos de cifrado estándar de la industria para proteger la información confidencial.
 - Implementar controles de acceso para garantizar que solo el personal autorizado pueda acceder a conjuntos de datos específicos.
- Redundancia y copia de seguridad:
 - Diseñar sistemas de almacenamiento redundantes con conmutación por error automática para garantizar la disponibilidad de datos en caso de fallas de hardware.
 - Hacer copias de seguridad periódicas de los datos importantes y almacenar las copias de seguridad en ubicaciones geográficamente diversas para prevenir la pérdida de datos.

Procesamiento de datos

Según se detalla en el [Modelo de AIMS](#), el componente de procesamiento de datos tiene la función de limpiar, organizar y transformar los datos sin procesar en un formato normalizado y utilizable. Esto incluye todo, desde la estandarización, el enriquecimiento, la transformación, el enrutamiento inteligente y mucho más. Este componente garantiza que los datos sean precisos, coherentes y estén libres de errores, lo que los hace confiables para el enrutamiento y el uso por parte de otros socios de intercambio de datos en la plataforma.

Árbol de decisiones

Figura 22. ¿Cómo se puede facilitar el intercambio de mensajes entre socios de intercambio de datos en diferentes sistemas y entornos mediante la plataforma?



Consideraciones

La siguiente lista ofrece consideraciones clave que ayudarán al lector a alinear la funcionalidad del componente de procesamiento de datos con las necesidades no funcionales de su intercambio de datos de salud pública:

- **Procesamiento de mensajes en tiempo real y por lotes:** para crear canales de procesamiento en tiempo real, se pueden utilizar tecnologías como Apache Kafka, Apache Flink o AWS Kinesis para gestionar flujos de datos. Si la transferencia de datos en tiempo real no es necesaria, se puede implementar el procesamiento por lotes utilizando herramientas como Apache Hadoop, Apache Spark o procesos ETL tradicionales (extraer, transformar y cargar). Planificar las tareas en horas de menor actividad para optimizar el uso de recursos. Reevaluar la necesidad de procesamiento en tiempo real o de enfoques híbridos.
- **Validación y limpieza de datos:** integrar reglas de validación de datos y procesos de limpieza desde las primeras etapas del procesamiento de canales. Utilizar herramientas de calidad de datos como Talend, Informatica o scripts personalizados para garantizar la precisión de los datos.
- **Transformación o enriquecimiento de datos:** utilizar procesos ETL (extraer, transformar, cargar) para transformar y enriquecer los datos. Considerar la utilización de plataformas como Mirth Connect, Apache NiFi, Talend o herramientas personalizadas de transformación de datos.
- **Compatibilidad con múltiples formatos de datos:** implementar middleware o herramientas de conversión para gestionar diferentes formatos (por ejemplo, JSON, XML, HL7). Utilizar un motor de procesamiento flexible que pueda adaptarse a diferentes tipos de datos.
- **Reglas de enrutamiento de datos complejos:** utilizar enrutamiento inteligente con middleware como Mirth Connect, Apache Camel o enrutamiento personalizado. Siempre asegurarse de que el enrutamiento sea flexible y se pueda adaptar a los cambios en los requisitos del negocio.
- **Consolidación de datos y procesamiento de resúmenes:** incorporar la lógica de consolidación en los canales de procesamiento. Utilizar herramientas como Apache Spark, Flink o scripts personalizados para consolidar y resumir datos.
- **Almacenar estados intermedios de datos:** utilizar una capa de almacenamiento temporal (por ejemplo, Redis, bases de datos en memoria) para retener datos intermedios. Garantizar que estos datos se cifren y gestionen de acuerdo con los requisitos de cumplimiento.
- **Seguridad y cumplimiento durante el procesamiento:** garantizar que todos los componentes de procesamiento de datos cumplan con las normativas relevantes (por ejemplo, HIPAA, GDPR). Implementar cifrado de extremo a extremo y mantener registros de auditoría detallados.
- **Implementar un diseño basado en eventos:** utilizar listas de prioridades para hacer que el sistema sea menos vulnerable a fallas durante picos de demanda (consultar el componente de [procesamiento de datos](#) dentro del modelo decAIMS)
- **Implementar OpenSearch o Elasticsearch:** un componente clave para la inteligencia y la gestión de datos. Si la infraestructura es adecuada para configurarlo desde las etapas iniciales del desarrollo, permitirá la creación de paneles que faciliten el monitoreo en tiempo real e histórico de las transacciones de datos, ofreciendo evidencia concreta de las acciones de la plataforma y mostrando cómo se han utilizado los fondos destinados al proyecto.
- **Vocabulario**
 - Terminología uniforme: el vocabulario estandarizado garantiza que se utilicen los mismos términos de manera consistente en diferentes sistemas y regiones. Esta uniformidad es fundamental para la interpretación y el análisis precisos de los datos. Por ejemplo, el uso consistente de nombres de enfermedades, síntomas y protocolos de tratamiento permite un seguimiento y comparación precisos.
 - Comunicación clara: el vocabulario estandarizado mejora la comunicación entre los profesionales de la salud pública. Cuando se utilizan los mismos términos, se reducen los malentendidos y los datos transmitidos entre diferentes jurisdicciones se pueden interpretar de manera correcta.

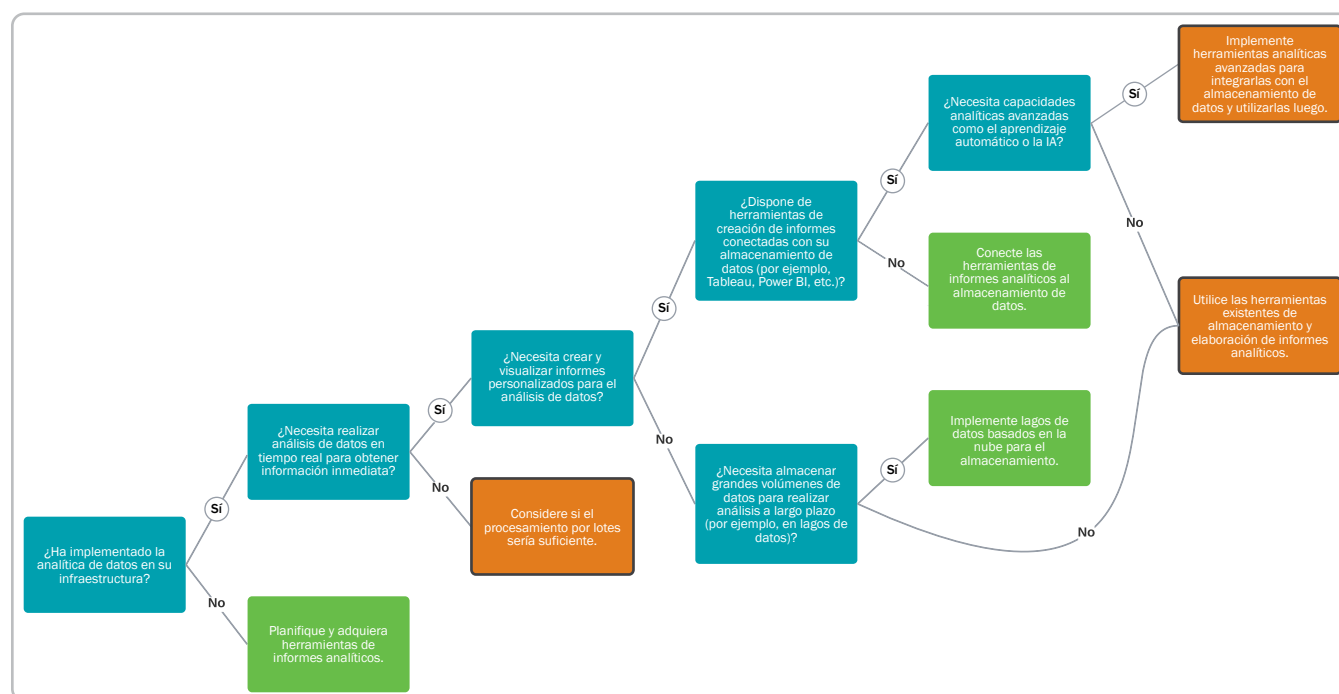
- Integración de datos: con un vocabulario en común, la integración de datos de diferentes sistemas se vuelve más sencilla. Esto es importante para combinar datos clínicos, resultados de laboratorio e información epidemiológica, ya que permite una comprensión más completa de los problemas de salud pública.

Análisis de datos

Como se mencionó en el [Modelo de AIMS](#), el componente de análisis de datos se encarga de examinar e interpretar los datos procesados para descubrir patrones, tendencias y perspectivas que ayuden a informar las decisiones. Debería contemplar herramientas estadísticas, algoritmos y tal vez aprendizaje automático para analizar datos y producir informes, análisis o predicciones sobre las actividades de intercambio de datos y el rendimiento del sistema. Estas herramientas deben permitir a las partes interesadas supervisar el tráfico de mensajes, identificar tendencias y realizar un seguimiento del estado del sistema en tiempo real para el intercambio de datos de salud pública.

Árbol de decisiones

Figura 23. ¿Cómo debo implementar y utilizar los análisis de datos en el intercambio de datos de salud pública?



Consideraciones

La siguiente lista ofrece consideraciones clave que ayudarán al lector a alinear la funcionalidad del componente de análisis de datos con las necesidades no funcionales de su intercambio de datos de salud pública:

- **Lagos de datos:** pueden almacenar grandes cantidades de datos estructurados y no estructurados, y tienen capacidad para diferentes casos de uso analíticos.
- **Análisis avanzados:** las capacidades avanzadas de análisis, que incluyen aprendizaje automático e inteligencia artificial, pueden proporcionar información valiosa sobre el flujo de datos y su contenido.
- **Integración:** la interoperabilidad de los datos almacenados y el análisis avanzado con aplicaciones secundarias pueden brindar información a nivel operativo o de aplicación.

- **Integración con otros sistemas:** garantizar una conectividad fluida con fuentes de datos, sistemas de almacenamiento y herramientas de informes para un flujo de datos sin contratiempos.
- **Automatización:** automatizar tareas repetitivas, como la generación de informes y alertas, para aumentar la eficiencia y reducir el trabajo manual.
- **Control de acceso del usuario:** definir roles y permisos para restringir el acceso a análisis o informes confidenciales en función de los roles de los usuarios.

Gobernanza de datos

La gobernanza de datos se representa mejor a través de las operaciones de gestión de datos empresariales, diseñados para mejorar el cumplimiento normativo, mitigar riesgos, aumentar la eficiencia operativa, elevar la calidad de los datos y maximizar el valor de los activos de datos. DAMA International ha codificado las prácticas recomendadas relacionadas con la gobernanza de datos empresariales en *Data Management Body of Knowledge (DMBOK2)*.*

Objetivos y consideraciones

- **Operaciones de gestión de datos:** se recomienda establecer una Oficina de Gobernanza de Datos (Data Governance Office, DGO) para supervisar las políticas, los estándares y el cumplimiento de la gobernanza de datos a fin de garantizar su alineación con los objetivos organizacionales.
- **Establecer políticas internas:** desde la perspectiva de establecer políticas internas sobre cómo se recopilan, almacenan, procesan y eliminan los datos, AIMS establece reglas sobre la duración de la persistencia de los datos en los sistemas que los transmiten, basándose en reglas comerciales y en las leyes de almacenamiento de datos relevantes de HIPAA. Por ejemplo, los mensajes de eCR que se entreguen a AIMS se eliminarán después de 7 días si no se toman y procesan. Varios casos de uso de ELR requieren y permiten mantener los datos durante 30 días.
- **Automatización de esas políticas:** desde la perspectiva de limitar el acceso a los datos y controlar lo que las personas pueden hacer con ellos, AIMS utiliza un servicio en la nube llamado Cloud Custodian para implementar y gestionar políticas como código en un entorno de AWS. Esta herramienta ofrece beneficios integrales en términos de seguridad, cumplimiento, gestión de costos y eficiencia operativa. Facilita un enfoque proactivo para la gestión en la nube que es escalable, flexible y se alinea con las prácticas modernas de gobernanza de datos.

En el caso de las instituciones que operan en las instalaciones, se recomienda que adopten las prácticas recomendadas de Cloud Custodian, aunque esto implique realizar algunas operaciones manuales. El beneficio principal de las prácticas de políticas como código que son automatizadas, repetibles y controladas por versiones es la eliminación de la interacción humana, lo que puede conducir a errores, como eliminar datos que no corresponden u omitir ejecuciones de código.

Manuales o automatizadas, las prácticas recomendadas que puede seguir una institución son las siguientes:

- **Eliminación de elementos no utilizados:** identificar y eliminar usuarios y claves inactivos, instancias detenidas, volúmenes desconectados, secretos inactivos y, en general, cualquier recurso que no se esté utilizando. Estas políticas deben estar estructuradas para identificar, alertar, deshabilitar, volver a alertar y, eventualmente, eliminar según los plazos establecidos.
- **Aplicación de registros:** monitorear y hacer cumplir ciertos requisitos de registro, como los registros de nube privada virtual (Virtual Private Cloud, VPC), registros de acceso, etc., para prevenir desviaciones y garantizar la visibilidad.
- **Etiquetado:** etiquetado automático o manual y la imposición de incluir otras etiquetas para estandarizar el etiquetado en cuentas y entornos, facilitando así el desglose y análisis de costos, propiedad y propósito de los recursos.

* DAMA International, The DAMA Guide to the Data Management Body of Knowledge (DMBOK2), 2nd ed., Technics Publications, 2017, Chapter 14: Data Management Operations, págs. 373 a 389.

- **Capacitación y concienciación:** implementar programas de capacitación y concienciación periódicos para educar a las partes interesadas sobre las prácticas recomendada de gobernanza de datos, los requisitos de cumplimiento y los roles en la gestión de datos.
- **Financiación y sustentabilidad:** obtener la financiación necesaria para las iniciativas de gestión de datos y garantizar su sostenibilidad a largo plazo alineando recursos con prioridades estratégicas y demostrando el retorno de la inversión.
- **Compromiso de las partes interesadas:** fomentar la colaboración entre todas las partes interesadas, como las unidades de negocio, TI, propietarios de datos y socios externos, para alinear los esfuerzos de gestión de datos con las necesidades organizacionales y construir una cultura basada en datos.

Las siguientes son algunas consideraciones clave que pueden influir en las decisiones y prioridades de la gestión de datos:

- **Cumplimiento normativo:** garantizar que las prácticas de gestión de datos cumplan con las leyes y normativas pertinentes (por ejemplo, GDPR, HIPAA) para evitar sanciones legales y mantener la confianza.
- **Gestión de riesgo:** reducir los riesgos relacionados con filtraciones, pérdidas y uso indebido de los datos mediante la implementación de medidas de gobernanza, seguridad y privacidad de datos.
- **Eficiencia operacional:** optimizar los procesos relacionados con los datos, reducir la redundancia y mejorar el acceso a datos de alta calidad, lo que potencia el rendimiento general de la empresa.
- **Mejora de la calidad de los datos:** centrarse en mantener datos de alta calidad que sean precisos, coherentes y confiables para respaldar la toma de decisiones efectiva y las actividades operativas.
- **Valor y análisis de los activos de datos:** maximizar el valor de los activos de datos a través de análisis avanzados, inteligencia e información que impulsan la innovación, la estrategia y la mejora de la salud pública.

Partes interesadas y operaciones

Componentes fundamentales para respaldar cualquier nueva plataforma de intercambio de datos

- **Consideración de la posibilidad de formar un equipo interno de integración:** es un buen recurso para la interoperabilidad. Los ingenieros de integración desempeñan un papel central en AIMS.
- **Planificación de una amplia asistencia técnica (technical assistance, TA):** este es un elemento indispensable para la implementación y el éxito, además de ser un requisito de asistencia continuo. Cada nuevo socio de intercambio de datos necesitará TA para establecer la conexión. Los socios necesitarán TA para cada nueva función que se implemente en la plataforma.
- **Planificación del establecimiento de un equipo de SDM:** el equipo de SDM desempeñará un papel fundamental para garantizar que los servicios proporcionados por la plataforma se brinden a los socios de intercambio de manera confiable y consistente, que se resuelvan rápidamente las interrupciones en el flujo de datos y que se tomen las medidas correctivas adecuadas para prevenir su recurrencia.
- **Ofrecimiento de asistencia de producción a los usuarios finales:** considerar la posibilidad de crear un equipo de asistencia especializado y optimizar sus esfuerzos implementando un sistema de tickets para gestionar de manera eficiente la resolución de problemas y garantizar la comunicación con los socios de intercambio de datos.
- **Equipo técnico multifuncional para mantenimiento y operaciones** se necesitará un equipo interdisciplinario que incluya habilidades de gestión de proyectos, ingeniería, asistencia técnica y más, para mantener y gestionar con éxito una plataforma de intercambio de datos.

Promoción y persuasión

Al igual que en cualquier proyecto complejo que requiera el apoyo de un gran número de partes interesadas, muchas de las cuales probablemente tendrán dudas sobre el impacto de sistemas y métodos desconocidos en su propia carga de trabajo, el establecimiento de una plataforma de intercambio de datos se verá enormemente acelerado si es respaldada por una o más personas que puedan asumir el papel de defensor o patrocinador.

Esta defensa inicial puede ser necesaria durante un período prolongado. En los primeros días de AIMS, se tuvo que contactar y convencer personalmente a los líderes de los laboratorios de salud pública estatales, uno por uno, sobre los beneficios de la nueva plataforma. Una vez que los líderes comenzaron a unirse, el siguiente obstáculo fue persuadir a su propio personal de seguridad que no confiaban en la seguridad de los sistemas propuestos. Esos nuevos sistemas se crearon, se probaron y debieron superar una amplia gama de desafíos técnicos (por ejemplo, integrar los datos de LIMS en mensajes HL7).

El proceso de expansión a más laboratorios de salud pública estatales ganó impulso a medida que AIMS comenzó a abordar de manera integral los problemas que enfrentaban los laboratorios. Con el tiempo, los beneficios de la plataforma se volvieron más tangibles, lo que llevó al desarrollo de confianza. El crecimiento se aceleró enormemente cuando AIMS comenzó a ofrecer asistencia técnica formal a las jurisdicciones.

Una buena comunicación es fundamental en esta campaña para fomentar la aceptación y participación de las partes interesadas en todos los niveles. En particular, es importante la enunciación clara de los beneficios del intercambio de datos interjurisdiccional, que incluye lo siguiente:

- **Mejora de la calidad de los datos:** los formatos de datos y vocabularios estandarizados mejoran la calidad de los datos recopilados y compartidos. Esto hace que la vigilancia de la salud pública y la toma de decisiones sean más confiables, ya que los datos de distintas jurisdicciones se pueden agrupar y analizar con seguridad.
- **Mejora de la coordinación de respuesta:** en emergencias de salud pública, como brotes de enfermedades o desastres naturales, las respuestas rápidas y coordinadas son fundamentales. Los datos estandarizados permiten compartir e interpretar rápidamente información crítica entre jurisdicciones, lo que hace que las intervenciones sean más efectivas y oportunas.
- **Cumplimiento normativo:** muchas iniciativas de salud pública requieren el cumplimiento de normativas federales y estándares de presentación de informes. Los formatos de datos y vocabularios estandarizados garantizan que los datos compartidos entre jurisdicciones cumplan con estos requisitos normativos, y evitan complicaciones legales y procedimentales.
- **Optimización de recursos:** con datos estandarizados, las jurisdicciones pueden compartir recursos de manera más efectiva. Por ejemplo, las herramientas y plataformas de análisis de datos desarrolladas en una jurisdicción pueden ser adoptadas fácilmente por otras, lo que reduce los esfuerzos dobles y fomenta la colaboración.
- **Investigación de la salud pública:** los datos estandarizados permiten llevar a cabo iniciativas de investigación en varias jurisdiccionales, lo que permite contar con conjuntos de datos más grandes y diversos. Esto aumenta la validez y la generalización de los resultados de la investigación, lo que, a su vez, contribuye a estrategias e intervenciones de salud pública más efectivas.

Fomento de la aceptación de las partes interesadas

Obtener el apoyo y la aprobación para alojar una plataforma de intercambio centralizado de datos generalmente requiere varios pasos clave.

- **Compromiso de las partes interesadas:** involucrar a las partes interesadas clave desde el principio del proceso de planificación para abordar inquietudes y recopilar aportes.

- **Demostración de los beneficios:** explicar de manera clara las ventajas de una plataforma de intercambio centralizado de datos frente a los sistemas antiguos, como la eficiencia, el ahorro de costos, la escalabilidad y la mejora en la seguridad.
- **Evaluación de riesgos:** realizar evaluaciones de riesgos exhaustivas y abordar posibles problemas de seguridad y cumplimiento.
- **Proyectos piloto:** implementar proyectos piloto para demostrar la viabilidad y los beneficios de alojar una plataforma de intercambio de datos a pequeña escala.
- **Comunicación continua:** mantener canales de comunicación abiertos con las partes interesadas durante todo el proceso para generar confianza y abordar cualquier inquietud que surja.

Fomentar la confianza con los socios de intercambio de datos

fomentar la confianza con los socios de intercambio de datos es esencial para su participación continua en el sistema. Con el tiempo, el equipo de intercambio centralizado de datos puede generar confianza con los socios y demostrar una sólida experiencia y una trayectoria comprobada en el área. Demostrar los potenciales beneficios y éxitos de alojar una plataforma de intercambio de datos en entornos similares genera confianza. Resaltar estudios de caso o ejemplos de implementaciones exitosas en otras jurisdicciones o regiones puede reforzar la credibilidad. Las estrategias para fomentar la confianza con los socios de intercambio de datos son las siguientes:

- **Comunicación clara de los beneficios:** es fundamental comunicar de manera efectiva las ventajas de una plataforma de intercambio de datos, como una mayor accesibilidad a la información, escalabilidad, ahorro de costos y mejores resultados en salud pública. Compartir una visión clara y convincente y la manera en que se alinea con los objetivos de salud pública de las jurisdicciones puede fomentar la aceptación.
- **Transparencia y compromiso:** involucrar a las partes interesadas en diálogos abiertos, abordar sus inquietudes y proporcionar información transparente sobre el proceso puede generar confianza. Es esencial que las partes interesadas se involucren desde el principio y que se sientan parte del proceso de la toma de decisiones.
- **Seguridad y cumplimiento:** enfatizar las sólidas medidas de seguridad y el cumplimiento de las normativas pertinentes (por ejemplo, HIPAA) que puede ofrecer una plataforma de este tipo. Proporcionar información detallada sobre cómo se mantiene la privacidad y la seguridad de los datos puede aliviar las preocupaciones y generar confianza.

Participación crítica: equipos de seguridad de IT

Es fundamental contar con la comprensión y el compromiso de participación continua de los equipos de seguridad de TI de cada socio de intercambio de datos. Las siguientes son algunas estrategias para fomentar esta participación:

- **Involucrar la seguridad de TI desde el principio:** los equipos de seguridad de TI deben participar desde el inicio del proyecto para garantizar que se aborden sus inquietudes y requisitos. Involucrarlos desde el inicio ayuda a detectar posibles desafíos de seguridad y a desarrollar soluciones para reducir los riesgos.
- **Realizar evaluaciones de seguridad exhaustivas:** realizar evaluaciones de seguridad exhaustivas de la infraestructura y los servicios planificados de la plataforma.
- **Ofrecer personalización y control:** garantizar que los equipos de seguridad de TI tengan control sobre las configuraciones de seguridad, como controles de acceso, cifrado y monitoreo. Ofrecer opciones de personalización para cumplir con las políticas y los requisitos de seguridad específicos de la organización.
- **Ofrecer capacitación y asistencia continuos:** ofrecer sesiones de capacitación para los equipos de seguridad de TI para que se familiaricen con las prácticas recomendadas de seguridad relacionadas con la solución de alojamiento elegida. Brindar apoyo continuo y actualizaciones para abordar nuevas amenazas y vulnerabilidades de seguridad.

Apéndices

Cronología del desarrollo de AIMS

2008	• AIMS se creó para eliminar la presentación de informes en papel de los resultados de la gripe de los laboratorios de salud pública estatal y territorial al CDC. • Se transmitió el primer mensaje de vigilancia de la gripe al CDC. • Se escalaron los servidores físicos de centros de datos con el fin de tener capacidad para las cargas de datos futuras.
2010	Se brindó asistencia técnica a los estados y servicios de integración, vocabulario y gestión de proyectos. Como resultado, aumentó la adopción de AIMS por parte de los estados.
2013	Se completó la primera auditoría conforme a la Ley Federal de Gestión de la Seguridad de la Información (Federal Information Security Management Act, FISMA) y se demostró el cumplimiento de los principales estándares de privacidad y seguridad para el manejo de datos confidenciales.
2014	AIMS migró a la nube y se aprovecharon los servicios nativos de Amazon Web Services (AWS), con un enfoque en la escalabilidad y la continuidad de las operaciones a nivel nacional.
2016	• Se transmitió el millonésimo mensaje de forma segura. • Se incorporó el primer laboratorio privado (Quest Diagnostics) para enviar informes de laboratorio electrónicos a los organismos de salud pública de todo el país de manera segura. • Se creó un clúster de computación bioinformática en AWS para el programa de detección molecular avanzada (Advanced Molecular Detection, AMD) de gripe del CDC.
2017	• STEVE 2.0, la aplicación de intercambio de datos de estadísticas vitales del país se lanza en AIMS.
2018	• Se transmitieron los primeros mensajes del CDC a los estados, estableciendo un intercambio de datos bidireccional entre AIMS y el CDC. • Se lanzó el primer hospital en AIMS, Houston Methodist. Esto marcó el inicio del proyecto de Informe electrónico de casos (eCR), el proyecto más grande de AIMS hasta la fecha.
2019	• Se creó un panel que permite el monitoreo en tiempo real del flujo de mensajes por parte de los usuarios. • Se completó la primera interfaz con un país extranjero (Chile) para el intercambio de datos de vacunación contra la gripe. • Se creó la Oficina de Gestión de Proyectos (Project Management Office, PMO), lo que aumentó el enfoque en la excelencia operativa. • Se implementó el intercambio de datos InterPartner, que permitió a los socios de intercambio de datos de AIMS intercambiar información de manera segura con un mínimo de asistencia o interacción con el personal técnico de AIMS. Este momento indica el comienzo de un crecimiento orgánico notable en el intercambio de datos entre estados.
2020	• Se logra mucho apoyo para el intercambio de datos nacional sobre COVID-19, así como actividades de gestión que brindan asistencia a la Casa Blanca, el CDC y los estados de todo el país. • El CDC declara a AIMS como autoridad de salud pública.
2021	• Se ampliaron los casos de uso de intercambio de datos para incluir datos del registro de cáncer. • Se lanzó una iniciativa nacional de transporte de intercambio de datos para migrar a los organismos de salud pública de la tecnología de transporte heredada (PHINMS) a AWS S3; se mejoraron las velocidades de transporte, la escalabilidad y la confiabilidad, especialmente durante el COVID-19.

2022	• Se inició el proyecto Mirth Resilience, diseñado para modernizar la infraestructura de AIMS y permitir una escalabilidad más sólida de las interfaces en todos los casos de uso de la plataforma. • El Portal de vacunación (IZ Gateway) alojado en AIMS brinda una solución tecnológica e infraestructura que facilita el intercambio de datos de inmunización entre estados y el CDC.
2023	• Se inició el proyecto de Órdenes y Resultados de Pruebas Electrónicas (Electronic Test Orders and Results, ETOR) para desarrollar tecnologías que permitan a las organizaciones sanitarias enviar órdenes y recibir resultados de los laboratorios de salud pública de manera electrónica. • La Red de Acción Mundial en el Ámbito Sanitario (GAIHN-HAI) se lanza en AIMS, la cual involucra a expertos en salud pública nacionales, regionales y globales para desarrollar capacidades que permitan detectar, prevenir y responder a amenazas de enfermedades infecciosas en una amplia variedad de entornos de atención médica.
2024	• Se completó la renovación de Jira Service Desk, lo que mejoró la facilidad y eficiencia de los servicios de asistencia al cliente. • Se lanzó el proyecto de Órdenes y Resultados de Pruebas Electrónicas con el primer socio, Orlando Health, para la realización de las pruebas de detección neonatal. • Se lanzaron paneles de control de informes de casos electrónicos accesibles a todos los organismos de salud pública de EE. UU. y sus territorios. • Se realizó la primera transición de los datos del CDC a DEX, con el objetivo de optimizar la forma en que los datos de salud pública llegan al CDC. • Se completó la conexión con eHealth Exchange QHIN para permitir que el eCR aproveche el Marco y Acuerdo Común de Intercambio Confiable (Trusted Exchange Framework and Common Agreement, TEFCA).

Mirth en la plataforma AIMS

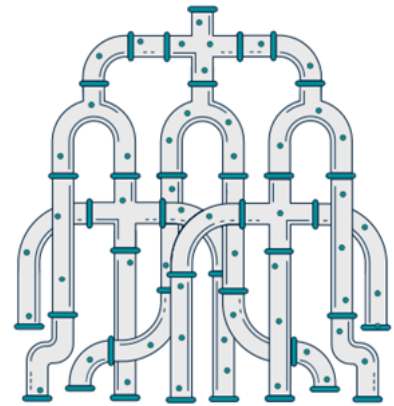
La plataforma AIMS utiliza Mirth como su motor de interfaz. A continuación, se detalla cómo AIMS utiliza el procesamiento paralelo a través de canales e instancias para ofrecer una escalabilidad confiable.

Mirth en la Plataforma AIMS

El flujo de mensajes se obtiene en la plataforma AIMS gracias a Mirth, un motor de integración de código abierto que enruta los mensajes a través de muchas series de canales interconectados. Muchas aplicaciones de AIMS, como el Informe electrónico de casos (eCR), ELR Centralizada, CELR, STEVE, DAART, registros de cáncer, entre otras, dependen de Mirth para el transporte de mensajes.

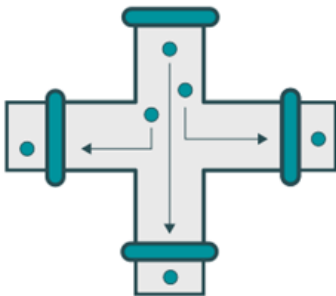
La red de canales interconectados de Mirth se puede imaginar cómo una serie de canales programados para dirigir los mensajes por vías definidas en función de su tamaño, contenido y uso previsto.

El uso de Mirth en la plataforma AIMS se diseñó para escalar de múltiples formas con el fin de evitar colas, retrasos y fallas en el transporte de mensajes cuando aumenta su volumen en AIMS. Mirth cuenta con las siguientes capas de funcionalidad que permiten a AIMS escalar en respuesta a los aumentos del volumen y protegerse contra las fallas:



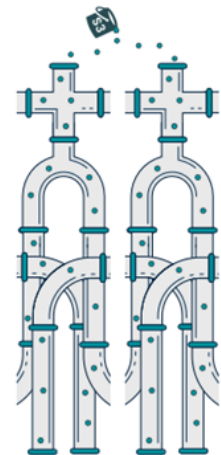
1. Procesamiento paralelo en un único canal

Un único canal en Mirth puede ejecutar varios comandos o procesos a la vez.



2. Canales paralelos

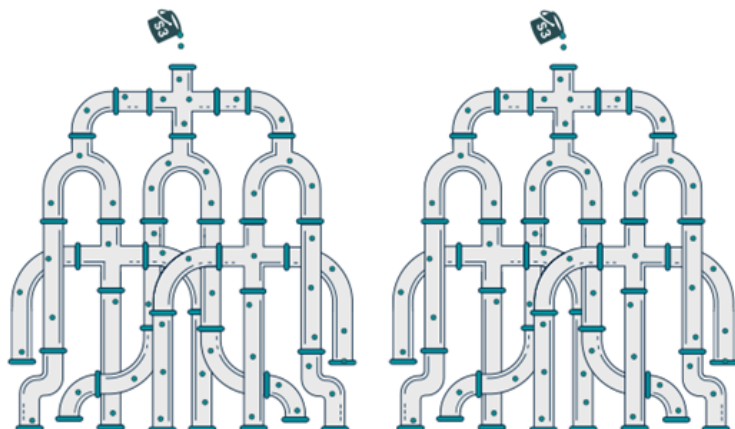
Cuando el canal único de Mirth alcanza limitaciones en el número o tamaño de los mensajes que puede procesar, podemos introducir canales paralelos para repartir el procesamiento de mensajes y aliviar cualquier posible cola o acumulación de mensajes. Estos canales paralelos son idénticos y realizan las mismas funciones. Sirven para disminuir el tiempo de procesamiento de los mensajes a medida que aumenta su volumen. Muchas aplicaciones en AIMS se procesan a través de canales paralelos.



3. Instancias de Mirth en paralelo

Cuando los volúmenes de mensajes son tan grandes que el procesamiento paralelo y los canales paralelos no son suficientes, se puede duplicar toda la instancia de Mirth. Se crea una instancia Mirth idéntica y paralela que duplica el volumen de mensajes que la plataforma AIMS puede procesar para una aplicación.

Con estas capas de escalabilidad, la plataforma AIMS procesa más de 450,000 mensajes diarios con confianza y seguridad.



Políticas y procedimientos ilustrativos

Al igual que en cualquier emprendimiento importante, la gestión de proyectos será esencial para guiar con éxito un nuevo intercambio de datos a través de todas las etapas de su conceptualización y diseño, lo que garantiza la aprobación y el compromiso, el desarrollo y la implementación, así como la asistencia técnica y el soporte en las fases de desarrollo continuo. La documentación es una herramienta clave para gestionar esfuerzos complejos y garantiza que las medidas necesarias se comprendan e implementen de manera correcta y oportuna. Además, debido a la naturaleza confidencial de los datos de salud pública que se almacenan y se intercambian, el establecimiento de políticas de seguridad y el mantenimiento de la documentación correspondiente serán probablemente requisitos legales significativos para su operación. Esta sección brinda una selección representativa de algunos de los tipos de políticas, procedimientos y documentación que se implementa en AIMS.

Estructura e infraestructura

Visualización de datos y paneles de control

- Mantenimiento del historial de las aplicaciones. Toma de decisiones importantes, cambios en el enfoque, etc.
- Documentación sobre las herramientas utilizadas. Si se trata de un servicio externo, adición de detalles del contrato, fechas de renovación, costo y contacto del representante.
- Proceso de actualización y mantenimiento.
- Guía(s) del usuario para aplicaciones.

Un plan que detalla los proyectos que los líderes desean para mantener y mejorar la plataforma, junto con un proceso de control de cambios para analizar lo siguiente:

- Riesgos;
- Beneficios;
- Costos;
- Partes interesadas;
- Prioridad ante otras iniciativas.

Documentación de todos los servicios o ubicaciones de servidores, redundancias, limitación de capacidad, mecanismos de conmutación por error, etc.

Estándares, seguridad y cumplimiento

La seguridad y el cumplimiento de la infraestructura de intercambio de datos debe incluir lo siguiente:

- Documentación de auditoría.
- Acuerdos contractuales, como SLA, acuerdos de uso de datos (Data Use Agreement, DUA), acuerdos maestros de servicios (Master Service Agreements, MSA), acuerdos de socio comercial (Business Associate Agreements, BAA), etc.
- Cumplimiento de las actividades programadas.
- Artefactos de los proveedores de servicio.

Figura 23. Ejemplo de estructura de matriz de decisiones para evaluar y aprobar proyectos

Estado	PARA PROPONER
Impacto	ALTO / MEDIO / BAJO
Creador	@ usted
Encargado de autorización	@ quien debe aprobar esta iniciativa, (si lo desconoce, deje la opción en blanco)
Contribuidores	@ personas de esta página que pueden ayudarlo o brindarle información
Personas notificadas	@ personas que no están en los grupos anteriores, pero deben ser notificadas acerca de las actualizaciones de esta aprobación, (recibirán mensajes de correo electrónico cuando se actualice esta página)
Fecha de vencimiento	Fecha en la que espera que se revise, (escriba / + fecha y, a continuación, introduzca una fecha)
Prioridad	Número
Equipo asignado	Integración, desarrollo, apoyo a la producción... etc.
Resultado	Una breve reseña sobre la situación actual: por ejemplo, "se iniciará la semana del 7 de enero" o "se revisará el 16 de septiembre."
Justificación	P. ej.: • Actualización necesaria • Deuda técnica • Mejora y eficiencia en los procesos • Innovación

La documentación debe incluir lo siguiente:

- Documentación de auditoría pública; los resultados de una auditoría podrían incluir lo siguiente:
 - Plan de Evaluación de Seguridad: un documento que contiene un plan de pruebas para evaluar los controles de seguridad de AIMS. Este plan es elaborado por una organización de evaluación externa para beneficio de los anfitriones y propietarios de AIMS.
 - Informe de resumen ejecutivo: un documento elaborado para la alta gerencia que ofrece un resumen conciso de la revisión general.
 - Informe completo: incluye todos los criterios detallados y las respuestas, junto con recomendaciones específicas que se deben abordar antes del siguiente ciclo de acreditación.
- Documentos de la política de AIMS.
 - Procedimiento de etiquetado de recursos de AWS.*
 - Documentos de planificación de contingencias y resultados de ejercicios.
 - ◆ Documento de ejercicios del plan de contingencia.
 - ◆ Lista de verificación para la conmutación por error de aplicaciones.
 - ◆ Ejercicio de simulación de respuesta a los incidentes.
 - ◆ Proceso y lista de verificación para la selección de sistemas y proveedores, por ejemplo:
 - ◇ Evaluación de proveedores de servicios de identidad.
 - ◇ Evaluación de proveedores de Gestión de Seguridad de la Información y Eventos (Security Information and Event Management, SIEM).
 - ◇ Captura electrónica de datos.
 - ◇ Evaluación de soluciones de plataforma de identidad.
 - ◇ Plataforma de seguridad y servicio de asesoramiento de caza de amenazas.
 - ◇ Evaluación de proveedores del lenguaje de evaluación de controles de seguridad abiertos (Open Security Controls Assessment Language, OSCAL).
 - ◇ Evaluación y curso de capacitación sobre seguridad y concienciación.
 - ◆ Procedimiento de incorporación de miembros del equipo.
 - ◆ Revisiones de preparación para producción.
 - Documentos de procedimientos de plataforma desarrollados en AIMS.
 - ◆ Procedimiento de la familia de controles NIST 800-53 del Instituto Nacional de Estándares y Tecnología.
 - ◆ Procedimiento de control de acceso. Política y procedimiento de control de acceso móvil.
 - ◆ Procedimiento de auditoría y responsabilidad.
 - ◆ Procedimiento de conciencia y capacitación.
 - ◆ Procedimiento de gestión de configuración.
 - ◆ Procedimiento del plan de contingencia.
 - ◆ Procedimiento de identificación y autenticación.
 - ◆ Procedimiento de respuesta a incidentes.
 - ◆ Procedimiento de mantenimiento: proveedor de servicios en la nube (CSP) heredado.
 - ◆ Procedimiento de protección de medios (CSP heredado).
 - ◆ Política de planificación.
 - ◆ Procedimiento del personal de seguridad.
 - ◆ Procedimiento de designación de riesgo de posición. Procedimiento de protección física y ambiental (CSP heredado).
 - ◆ Procedimiento de evaluación de riesgos.

* Proceso o procedimiento específico de la nube (un equivalente local puede ser relevante).

- ◆ Procedimiento de evaluación de la seguridad y autorización. Estrategia de monitoreo continuo y procedimiento.
- ◆ Procedimiento de protección del sistema y las comunicaciones. Procedimiento de protección de límites.
- ◆ Procedimiento de integración del sistema y la información.
- ◆ Procedimiento de adquisición de sistemas y servicios.
- ◆ Comisión de redes de salud electrónica y acreditación (Electronic Healthcare Network and Accreditation Commission, EHNAC).
- Programa de actividades de auditoría.

Gobernanza y política de datos

Procesos para establecer procedimientos de gestión de datos que mantengan la seguridad, la privacidad, la precisión y el uso de los datos a lo largo del ciclo de vida de la información.

Se debe realizar lo siguiente con los socios de intercambio de datos:

- Comenzar conversaciones y abrir foros (ejemplos):
 - Foro de Interoperabilidad: control de calidad (Data quality assurance, DQA).
 - Discusión de control de calidad (Quality Assurance, QA).
- Seleccionar y capacitar un pequeño grupo de socios innovadores para formar una junta de gestión y establecer reglas o recomendaciones para todo el cuerpo de socios comerciales. Realizar revisiones mensuales o trimestrales de los estándares con ese grupo.
- Proveer recursos accesibles publicados (ejemplos):
 - Programas de control de calidad y estandarización de laboratorios del CDC ([cdc.gov](https://www.cdc.gov)).
 - Colaborar para mejorar la calidad de los datos de ciencia ciudadana: guía para agencias gubernamentales.
 - Marco y Acuerdo Común de Intercambio Confiable (TEFCA) | HealthIT.gov.
 - Discusión de la comunidad de control de calidad (aphl.org).
 - Guía de implementación Schematron.
 - Schematron de calidad de datos (ejemplo): Los representantes de salud pública han expresado su deseo de mejorar la calidad de los datos de EHR disponibles a través de eCR. Los esquemas Schematron de la Guía de implementación (Implementation Guide, IG) no son suficientes para evaluar y garantizar la calidad de los datos. Para abordar estas inquietudes, el grupo de trabajo de Control de Calidad (QA) convocó a más de 31 Agencias de Salud Pública (PHA) para desarrollar reglas de calidad de datos relacionadas con la validez e integridad de los eICR. Antes de la creación del grupo de trabajo de QA, los esfuerzos se centraban en verificar los archivos XML entrantes para garantizar su conformidad con los estándares de CDA y en apoyar las necesidades de determinación de declaración obligatoria de RCKMS.
 - Herramienta de mapeo de datos. Notas de las versiones.
 - Divisor de fuentes.
 - Ejemplos de plantillas de estándares de documentos o datos.
- Alojar un repositorio de documentación accesible internamente (ejemplos): Diccionario de datos para índices o bases de datos.

Mantenimiento y operaciones

Una base de conocimientos, accesible públicamente por cualquier ingeniero que trabaje en la plataforma, con documentación que describa procesos y procedimientos como los siguientes:

- Procesos
 - Procedimientos del coordinador de proyectos.
 - ◆ Proceso sobre cómo iniciar una nueva iniciativa de mantenimiento.
 - ◆ Implementación del proceso de documentación para todas las aplicaciones alojadas en la plataforma.
 - Centro de asistencia o procedimientos del servicio al cliente.
 - ◆ Gestión de identidad y acceso.
 - ◇ Procedimiento de revisión de solicitudes de acceso y flujo de trabajo de aprobación para herramientas de gestión de identidades y accesos.
 - ◇ Plantilla de formulario de solicitud de acceso a la red y flujo de trabajo de aprobación.
 - ◇ Procedimientos de flujo de trabajo de acceso específicos para cada aplicación.
 - ◆ Procedimiento operativo estándar del centro de asistencia de AIMS (AIMSSD): selección
 - ◆ Procedimiento operativo estándar del centro de asistencia: selección.
 - ◆ Proceso de la “regla de 3 contactos.”
 - ◆ Proceso y plantilla de correo electrónico externo de la “regla de 3 contactos.”
 - ◆ Horario extendido.
 - ◆ Revisiones diarias del panel de control: proceso.
 - ◆ Asistencia de creación de alarmas de Splunk On Call (9-5).
 - ◆ Actualizaciones de certificados.
 - ◆ Inclusión de contactos y respuesta: selección.
 - ◆ Distribución de actualizaciones semanales para tickets: proceso.
 - ◆ Creación de un ticket para alertas de SQS en Jira o por correo electrónico: proceso.
 - ◆ Creación de una cuenta en el portal de clientes de APHL: proceso.
 - ◆ Solicitud de asistencia técnica.
 - ◆ Envío de solicitudes de cambio.
- Guías técnicas.
 - Solución de resolución de problemas de FREERadius MFA para AWS Workspaces: proceso*
 - Reprocesamiento de mensajes por lotes con errores e incompatibilidad de tiempos en Opensearch: proceso.
 - Problema con la cola de SQS: fallas en la eliminación.*
 - Configuración de monitoreo de CheckMK: proceso.
 - Guía de configuración de conexión S3 para Mirth.*
 - Canales SFTP en Mirth.
 - Reseteo de contraseña de AD.
 - Reindexación de Elasticsearch.
 - Instalación e implementación de Datadog: proceso.
 - Active Directory y aprovisionamiento de acceso de usuario.
 - Solución de problemas de red privada virtual (Virtual Private Network, VPN).
 - Solución de problemas de S3 Transport de AIMS.*
 - Proceso de reinicio de Mirth en producción 4, 5 o 6.
 - Actualización de certificado autofirmado de Rhapsody.

* Proceso o procedimiento específico de la nube (un equivalente local puede ser relevante).

Gestión de la prestación de servicios

Un espacio diseñado para rastrear y gestionar meticulosamente todos los aspectos relacionados con la prestación de servicios en la plataforma. El objetivo principal de este espacio es crear una plataforma centralizada donde los miembros del equipo puedan acceder a actualizaciones, compartir ideas y colaborar en la resolución de problemas relacionados con la prestación de servicios. Esto no solo mejorará la transparencia, sino que también fomentará la responsabilidad y mejorará la eficiencia en toda la cadena de prestación de servicios.

Estos procesos deben seguir las prácticas recomendadas de [ITIL v4 e ITSM](#).

- Cumplimiento de niveles de servicio: esta página debe albergar datos relacionados con la disponibilidad, el tiempo de presentación de informes de incidentes y el tiempo de resolución de solicitudes de cambio en los SLA. Las prácticas recomendadas incluyen la automatización del cálculo de los SLA, lo que garantiza informes precisos y actualizados, así como transparencia y eficiencia.
- Definir y documentar los objetivos y valores mínimos para el SLA de tiempo de notificación, tiempo de resolución y tiempo de presentación de informes.
- Definir y documentar la disponibilidad, el tiempo de presentación de informes, notificación y resolución de incidentes; el tiempo de notificación y resolución de solicitudes de cambio; el tiempo de notificación y resolución de solicitudes administrativas.
- Brindar y documentar revisiones mensuales del servicio para evaluar rigurosamente la calidad, la eficiencia y la efectividad de nuestros mecanismos de prestación de servicios con los siguientes fines:
 - Agilizar la comunicación entre los miembros del equipo.
 - Mejorar la responsabilidad y la transparencia.
 - Facilitar la toma de decisiones basada en datos.
 - Fomentar la mejora continua en la prestación de servicios.
- Procedimientos del coordinador de prestación de servicios.
 - Detallar el procedimiento operativo estándar para preparar un informe de incidentes relacionado con un incidente que involucre una aplicación alojada en AIMS.
 - Detallar el procedimiento operativo estándar para preparar una versión de software para una aplicación alojada en AIMS.
 - Detallar el procedimiento operativo estándar para preparar una investigación de problemas para una aplicación alojada en AIMS.

Asistencia técnica (TA) e incorporación

- Una carpeta maestra de recursos de asistencia técnica donde los usuarios pueden acceder a lo que necesiten en cada etapa de la incorporación:
 - Implementación previa;
 - Planificación;
 - Validación y pruebas;
 - Producción puesta en marcha;
 - Evaluación;
 - Mantenimiento;
- Preguntas frecuentes, por ejemplo:
 - ¿Qué se detalla en TA?
 - ¿Qué se ofrece?
 - ¿Quiénes reúnen los requisitos?
 - ¿Cómo la solicitan los usuarios que reúnen los requisitos?

- Expectativas de velocidad de TA.
- Cómo verificar el estado (tickets, sitio web, otro).
- Herramientas y recursos:
 - Paquetes de código;
 - Fragmentos personalizados;
 - Un lugar donde los usuarios pueden publicar herramientas y recursos para sus colegas (una especie de mercado de código abierto).

Implicación de las partes interesadas

- Dar a los usuarios acceso a una wiki de contenido público, como Confluence, con carpetas específicas para ellos.
- Llamada semanal con un foro abierto para todas las PHA y los laboratorios de salud pública (Public Health Laboratories, PHL) de los 55 estados, donde las preguntas o los problemas se envían con anticipación y se discuten en grupo, al estilo de un seminario web. Las notas y las grabaciones se publican y son accesibles de manera asíncrona para todos los participantes.

Estrategia y liderazgo

- Junta de Control de Cambios (Change Control Board, CCB).
- Capacitar a un grupo pequeño pero diverso de líderes para mantener una visión estratégica de la plataforma. Todas las decisiones sobre proyectos, infraestructura y gastos deben estar alineadas con esa visión.

Comunicaciones y marketing

- Comunicaciones a los usuarios existentes y a los socios de intercambio de datos:
 - Procedimiento operativo estándar del centro de asistencia: selección.
 - Proceso de la “regla de 3 contactos”.
 - Proceso y plantilla de correo electrónico externo de la “regla de 3 contactos.”
 - Procedimiento operativo estándar de aviso de 2 semanas, 2 días y posterior a la finalización sobre el mantenimiento y el tiempo de inactividad.
 - Materiales de marca y plantillas de correo electrónico para elaborar notificaciones.
- Comunicaciones a contactos suscritos o que han optado por participar. Boletín informativo semanal.

Consideraciones sobre el alojamiento en la nube

Atracciones de la nube

Al seguir las prácticas adoptadas ampliamente por gobiernos y empresas de todos los tipos y tamaños, muchas organizaciones de salud pública han realizado la transición a la nube desde servidores físicos locales. Estos servidores estaban típicamente ubicados en las instalaciones de las organizaciones o en centros de datos alojados. Este tipo de configuración a menudo implica desventajas como las siguientes:

- **Necesidad de gran mantenimiento:** se requieren actualizaciones, copias de seguridad y reemplazos de hardware periódicos.
- **Flexibilidad limitada:** aumentar la capacidad requiere comprar e instalar nuevo hardware, lo cual es costoso y consume tiempo.
- **Vulnerabilidad a las amenazas físicas:** los servidores locales son susceptibles a daños por desastres naturales, cortes de energía y otras amenazas físicas.

Desafíos de mantenimiento de recursos locales

La gestión de servidores físicos locales presenta desafíos significativos, como los siguientes:

- **Gestión que requiere mucha mano de obra:** el personal de TI dedica un tiempo considerable a tareas de mantenimiento rutinarias, lo que les resta capacidad para centrarse en iniciativas estratégicas.
- **Problemas de escalabilidad:** aumentar la capacidad de almacenamiento o procesamiento requiere una inversión de capital significativa y tiempo de espera para la adquisición e instalación.
- **Accesibilidad limitada:** el acceso a los datos suele estar restringido a ubicaciones locales, lo que dificulta el trabajo remoto y la colaboración.
- **Riesgo elevado de pérdida de datos:** las fallas o errores de los servidores físicos pueden dar lugar a una pérdida significativa de datos si no se realizan copias de seguridad adecuadas.

Impulso para la migración

Varios factores motivan la decisión de migrar a la nube.

- **Necesidad de escalabilidad:** las organizaciones de salud pública requieren una solución más flexible y escalable para manejar volúmenes de datos crecientes y demandas en aumento.
- **Consideración de los costos:** las soluciones en la nube a menudo ofrecen modelos de precios más rentables, lo que reduce la necesidad de grandes inversiones iniciales en hardware.
- **Interés por una mejor colaboración:** las plataformas en la nube facilitan un mejor intercambio de datos y una mayor colaboración entre las partes interesadas de salud pública.
- **Enfoque en la innovación:** migrar a la nube permite al personal de TI centrarse en proyectos innovadores en lugar de en el mantenimiento rutinario.

Beneficios de estar registrado en la nube

El alojamiento en la nube trae numerosos beneficios.

- **Escalabilidad:** Las soluciones en la nube ofrecen la capacidad de escalar fácilmente hacia arriba o hacia abajo según la demanda y garantiza que los recursos se ajusten a las necesidades.
- **Rentabilidad:** el modelo de pago por uso reduce los gastos de capital y optimiza los costos operativos.

- **Accesibilidad:** las plataformas en la nube facilitan el acceso remoto a los datos, lo que apoya modalidades de trabajo flexibles y mejora la colaboración.
- **Fiabilidad:** los proveedores de la nube ofrecen soluciones sólidas de respaldo y recuperación ante accidentes, lo que reduce el riesgo de pérdida de datos.
- **Seguridad:** los principales proveedores de la nube han implementado medidas de seguridad avanzadas, a menudo superiores a las de las soluciones locales.
- **Innovación:** las plataformas en la nube son compatibles con análisis avanzados, aprendizaje automático y otras tecnologías innovadoras, lo que permite intervenciones en salud pública más efectivas.

Selección de un proveedor de servicios en la nube

Elegir el proveedor de servicios en la nube adecuado implica una investigación apropiada.

- **Evaluar la reputación del proveedor:** tener en cuenta la trayectoria y la fiabilidad de los proveedores potenciales.
- **Evaluar las ofertas de servicios:** asegurarse de que los servicios del proveedor coincidan con las necesidades de la organización, incluida la compatibilidad con formatos de datos específicos y herramientas de análisis.
- **Revisar las medidas de seguridad:** verificar las certificaciones de seguridad del proveedor y su cumplimiento con los estándares relevantes.
- **Analizar los costos:** comparar los modelos de precios y el costo total de propiedad entre diferentes proveedores.

Figura 24. Consideraciones para soluciones en la nube vs. soluciones locales

	Nube	Local
Cumplimiento	• Las normativas específicas de la jurisdicción pueden exigir que los datos se almacenen dentro de límites geográficos específicos. • Puede ser necesario cumplir con las normativas locales de privacidad vigentes, como GDPR, HIPAA y otras leyes de protección de datos.	
Seguridad	• Prioridad número 1 de los principales proveedores de servicios en la nube. • Estándares de seguridad respaldados por auditorías independientes.	Garantizar la seguridad puede representar el 50 % de la carga de trabajo.
Costo Total de costos de propiedad, que abarca inversiones iniciales, mantenimiento continuo y gastos operativos.	• Pagar solo por los servicios que se utilizan, evitando gastos fijos (como hardware y sitio). • Con los grandes proveedores de servicios en la nube, las economías de escala obtienen una reducción de costos.	Pagar por adelantado la infraestructura física, el hardware, el software y el mantenimiento.

	Nube	Local
Escalabilidad Capacidad para ajustar los recursos hacia arriba o hacia abajo según la demanda variable.	- Se permite el aprovisionamiento de solo la cantidad de recursos que realmente se necesitan. Escalar los recursos hacia arriba o hacia abajo para aumentar y reducir la capacidad a medida que cambian las necesidades. - Las opciones de almacenamiento en la nube escalables resuelven muchos problemas de interoperabilidad relacionados con las limitaciones de tamaño de archivo y volumen.	- Estimar los recursos necesarios con anticipación puede dar lugar a una capacidad insuficiente o excesiva. - Aumentar la capacidad es costoso y requiere mucho trabajo, implica la compra y el aprovisionamiento de hardware físico adicional, así como la instalación de software en el sitio.
Agilidad Capacidad para agregar o eliminar fácilmente infraestructura o aplicaciones.	- El acceso sencillo a una amplia variedad de tecnologías que se pueden implementar en minutos impulsa la innovación. - La capacidad para agregar o eliminar rápidamente infraestructura facilita las pruebas.	Para probar nuevas aplicaciones, puede ser necesario comprar y obtener hardware físico adicional e instalar software en el sitio.
Asistencia Asistencia técnica para resolver problemas.	Gran equipo de asistencia disponible las 24 horas del día, los 7 días de la semana, para responder a problemas.	Personal de asistencia limitado para responder a problemas.
Mantenimiento	El mantenimiento de la infraestructura lo realiza el proveedor de servicios en la nube.	Se requieren actualizaciones, copias de seguridad y reemplazos de hardware periódicos.
Riesgo de interrupción del servicio o pérdida de datos	Los proveedores de servicios en la nube dependen de una infraestructura redundante y geográficamente distribuida para minimizar riesgos.	- Susceptibilidad a daños por desastres naturales, cortes de energía y otras amenazas físicas. - Las fallas de los servidores físicos podrían dar lugar a una pérdida significativa de datos si no se realizan copias de seguridad adecuadas.
Compatibilidad con funciones avanzadas Lago de datos, análisis avanzados e integración.	- Los lagos de datos en la nube permiten almacenar grandes cantidades de datos estructurados y no estructurados, y tienen capacidad para diferentes casos de uso analíticos. - Las capacidades de análisis avanzadas de las plataformas en la nube incluyen aprendizaje automático e inteligencia artificial para obtener información de los datos. - Permite una integración fluida con las herramientas y los sistemas existentes para maximizar el valor de los análisis basados en la nube.	

Terminología

APHL: Asociación de Laboratorios de Salud Pública (Association of Public Health Laboratories, APHL), una organización de membresía de los Estados Unidos que representa a los laboratorios que protegen la salud y la seguridad del público. En colaboración con sus miembros, APHL avanza en los sistemas y prácticas de laboratorio, promueve políticas que apoyan comunidades saludables, actúa como un enlace entre los laboratorios y las agencias federales e internacionales y garantiza que la red de laboratorios disponga de información científica actual y consistente para estar preparada ante brotes y otras emergencias de salud pública.

Computación en la nube: la práctica de utilizar una red de servidores remotos alojados en Internet para almacenar, gestionar y procesar datos, en lugar de un servidor local.

Sistemas de Información en Salud (Health Information Systems, HIS): cualquier sistema que captura, almacena, gestiona o transmite información relacionada con la salud de los individuos o las actividades de las organizaciones que trabajan en el sector de la salud.

Nube híbrida: un entorno de computación en la nube que utiliza una mezcla de servicios de nube privada en las instalaciones y servicios de nube pública de terceros, con orquestación entre las dos plataformas.

Integración: la combinación de procesos técnicos y empresariales utilizados para combinar datos de fuentes dispares en información significativa y valiosa. Una solución completa de integración de datos proporciona datos confiables de una variedad de fuentes

Sistemas de Información de Laboratorio (Laboratory Information Systems, LIS): sistema de software que registra, gestiona y almacena datos para laboratorios clínicos. Un LIS siempre fue más eficiente en enviar órdenes de pruebas de laboratorio a los instrumentos, rastrear dichas órdenes y luego registrar los resultados, generalmente en una base de datos que se puede buscar.

Mirth: Mirth Connect es un motor de integración multiplataforma que se utiliza en la industria de la salud y permite la gestión de información mediante el envío bidireccional de muchos tipos de mensajes.

Nube privada: un tipo de computación en la nube que ofrece ventajas similares a la nube pública, como la escalabilidad y el autoservicio, pero a través de una estructura privada. A diferencia de las nubes públicas, que brindan servicios a múltiples organizaciones, una nube privada está dedicada a una sola organización.

Nube y nube pública: un tipo de nube basada en el modelo estándar de computación en la nube, en el que un proveedor de servicios pone recursos, como servidores, aplicaciones y almacenamiento a disposición del público en general a través de Internet.

Ruvos: socio técnico de APHL para la plataforma AIMS. Los expertos técnicos de Ruvos fueron fundamentales en el diseño inicial, la estructura y la construcción de la plataforma AIMS, así como en su migración a la nube, escalabilidad y desarrollo continuos.

TEFCA: Marco y Acuerdo Común de Intercambio Confiable (Trusted Exchange Framework and Common Agreement, TEFCA). Creado por la Oficina del Coordinador Nacional (Office of the National Coordinator, ONC) de Tecnología de la Salud para convertirse en un sistema de organizaciones interconectadas llamadas Redes de Información de Salud Calificadas (Qualified Health Information Networks, QHIN) que mejoran el intercambio de datos de salud a nivel nacional. En resumen, esto es una red de redes que se diseñó para mejorar la interoperabilidad en la atención médica.



Association of Public Health Laboratories

La Asociación de Laboratorios de Salud Pública (APHL) trabaja para reforzar los sistemas de laboratorio al servicio de la salud pública en Estados Unidos y en todo el mundo. Los laboratorios miembros de la APHL protegen la salud pública mediante el seguimiento y la detección de enfermedades infecciosas y transmitidas por los alimentos, contaminantes ambientales, agentes terroristas, trastornos genéticos en recién nacidos y otras amenazas sanitarias diversas.

7700 Wisconsin Avenue, Suite 1000 Bethesda, MD 20814 | 240.485.2745 | www.aphl.org

Este documento fue redactado por Ruvo, LLC, socio técnico a largo plazo de la Asociación de Laboratorios de Salud Pública (Association of Public Health Laboratories), como parte del Acuerdo de Orden de Trabajo n.º 56401-700-800-24-04.

Esta publicación se financió mediante el Acuerdo de Cooperación n.º NU2HGH000080 de los Centros para el Control y la Prevención de Enfermedades (Centers for Disease Control and Prevention, CDC) de EE. UU.

© Derechos de autor 2025, Association of Public Health Laboratories. Todos los derechos reservados