Componentes del dominio de la infraestructura TIC para los servicios de interoperabilidad entre servicios farmacéuticos y operador logístico

Realizado por el Ministerio de Salud, IESS, ISSFA, ISSPOL, Ministerio de Defensa Nacional, Ministerio de las Telecomunicaciones, ARCSA y SERCOP, con el apoyo del Banco Interamericano de Desarrollo.

Ecuador, diciembre de 2020

CONTENIDO

1 RESUMEN EJECUTIVO

1.1 ANTECEDENTES

El 05 de mayo de 2020, el presidente de la República de Ecuador expidió el Decreto Ejecutivo No. 1033, a través del cual reforma parcialmente el Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública, particularmente la sección referida a compra de fármacos. Con este Decreto se eliminan las normas previas existentes en el Reglamento y se reemplaza por nuevos procesos y regulaciones para la contratación de fármacos y bienes estratégicos de salud, los cuales constituyen todo tipo de bien determinado por la Autoridad Sanitaria Nacional, en el marco de sus competencias, que sea necesario y se encuentre relacionado directamente con la prestación de servicios de salud.

Considerando el crecimiento que ha experimentado la transformación digital y la adopción de la resolución digital de salud por la OMS en 2018, se ha priorizado el uso de tecnologías digitales para promover la cobertura de salud en línea. En este contexto, el MSP, con asistencia técnica del BID, prevé la elaboración de una Agenda Digital en Salud con la priorización de proyectos de digitalización del sector a corto, mediano y largo plazo, con la finalidad de incrementar la eficiencia, efectividad y acceso del Sistema Nacional de Salud.

El proyecto de articulación de las compras públicas del sector salud es uno de ellos. Liderado por el Gobierno, busca tener un procedimiento de compra centralizada y optimizar la distribución, almacenamiento y entrega de fármacos y bienes estratégicos para el Sistema Público de Salud, con el fin de asegurar el acceso de la población a éstos, requieren de un esfuerzo interinstitucional de la Red Pública Integral de Salud (RPIS) y del Servicio Nacional de Contratación Pública (SERCOP), entre otros involucrados. Uno de estos esfuerzos está relacionado con la adaptación de procesos logísticos, administrativos y asistenciales en estas organizaciones, que conllevarán a adecuaciones, ampliaciones y/o desarrollos de otras capacidades técnicas y funcionales en los aplicativos que hoy soportan los procesos de atención y prestación de servicios asistenciales en los hospitales y centros médicos de la Red Pública.

Este documento, es el resultado del trabajo realizado por los representantes de la RPIS con el apoyo consultivo del BID, en el que mediante análisis de procesos actuales y futuros se identificaron las necesidades de información y de integración que guiarán el desarrollo o adaptación de los sistemas actuales.

1.2 OBJETIVO Y ALCANCE DEL DOCUMENTO

Dentro de la estructura de dimensiones y componentes consideradas en la hoja de ruta de Salud Digital para Ecuador, en consonancia con la norma ISO/TR 14639-2: 2014, se define un marco de componentes clave indispensables dentro del contexto de Salud Digital tales como, personas y cultura, gobierno, **infraestructura,** infoestructura, procesos de salud, uso de la información para la toma de decisiones y mejoramiento de la calidad y la atención:

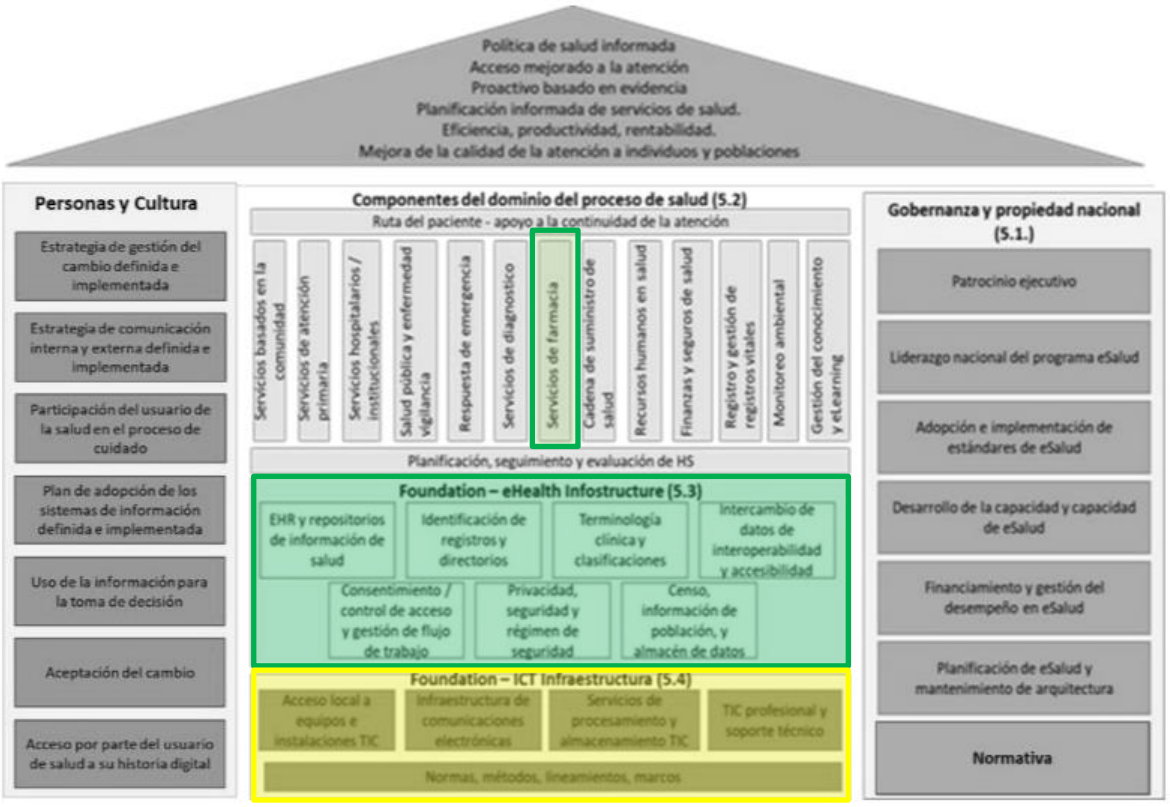

Figura 1: La casa digital - Adaptación del modelo de arquitectura de la salud digital: Fuente: ISO/TR 14639-2, Health informatics - Capacity-based eHealth architecture roadmap

Dentro de las **componentes del dominio de procesos de salud** (5.2) hemos definido los relacionados con el ciclo de atención de farmacia (desde la prescripción hasta la administración), identificando y describiendo los actores, repositorios, mensajes, terminologías, flujos de trabajo, gestión de accesos, políticas de seguridad, privacidad y protección de datos a los que hace referencia el dominio de **infoestructura** (5.3)[1].

En capítulo 2 de este documento se describen las componentes del **dominio de la infraestructura TIC** (5.4 en la gráfica) que define la tecnología informática requerida para soportar los procesos y componentes de interoperabilidad, privacidad y seguridad de la información en las actividades del servicio de farmacia comunitaria y hospitalaria de la red pública de prestación y el operador logístico.

Requerimientos generales de conectividad, almacenamiento, procesamiento, dispositivos y aquellos que son necesarios para que la interoperabilidad técnica, sintáctica y semántica sean viables y los servicios de operación, administración y monitoreo de la infraestructura, que propicien la resiliencia de los sistemas y garanticen la continuidad de la operación, son tratados a manera de guía en este documento

Adicionalmente y como complemento a la definición de la arquitectura de referencia, en el **capítulo 3** describimos las componentes de la plataforma tecnológica que debe habilitarse para lograr la interoperabilidad a nivel de datos y aplicaciones relacionadas con las prescripciones de medicamentos, así como su validación, dispensación y administración, entre el operador logístico y la Red Pública Integral de Salud – RPIS. Estas componentes están detalladas en los apéndices 1 y 2: en el primero, se detalla la arquitectura referencial de componentes requeridos para lograr la implementación de los casos de uso, flujos de trabajo y de intercambio de información detallados

[1] Recomendamos la lectura de los documentos **Arquitectura y guía de implementación de farmacia y Privacidad y Seguridad (P&S) de la información en el Sistema de Farmacia Interoperable para una mejor comprensión de este documento**

en el documento de Arquitectura y guía de implementación de Farmacia y los requisitos de privacidad y seguridad. En el segundo apéndice presentamos la arquitectura de referencia técnica de la interoperabilidad propuesta.

Dado que el SERCOP se encuentra (en el momento de la elaboración del documento) en el proceso de selección del Operador Logístico, fue necesario incluir un capítulo de los requisitos técnicos mínimos de la infraestructura tecnológica. Esta información se encuentra en el apéndice 3.

1.3 JUSTIFICACIÓN

La infraestructura tecnológica es la base que sostiene los sistemas interoperables y representa uno de los componentes que requieren más cuidado en el momento de definir sus capacidades y coberturas. Los altos costos, la diversidad de proveedores y de opciones hacen de esta componente una de las más complejas en el proceso de toma de decisiones de los diferentes actores.

En este sentido se hace necesario contar con una guía que asegure la optimización de los recursos de hardware y software requeridos para lograr la interoperabilidad entre la RPIS y el Operador Logístico y que considere los requisitos no funcionales que pueden afectar el correcto funcionamiento de los servicios y que den continuidad a las características de calidad requeridas en los procesos de intercambio de información clínica y de prescripción entre las entidades de la red.

1.4 REALIZACIÓN DEL DOCUMENTO

La realización del informe ha sido el resultado de un trabajo de colaboración en el que se ha contado con la contribución de un nutrido grupo de representantes del Ministerio de Salud Pública, el Instituto Ecuatoriano de Seguridad Social, Hospital de Especialidades Fuerzas Armadas, Instituto de Seguridad Social de las Fuerzas Armadas, el Instituto de Seguridad Social de la Policía Nacional, el Servicio Nacional de Contratación Pública, la Agencia Nacional de Regulación, Control y Vigilancia Sanitaria y el Ministerio de Telecomunicaciones y Sociedad de la Información del Ecuador.

A través de diferentes mesas de trabajo y con el apoyo de la consultoría del BID, se han aportado opiniones y conocimiento desde los diferentes agentes y sectores involucrados. La contribución de estos expertos se realizó en mesas de trabajo desarrolladas entre agosto y octubre de 2020 de manera virtual.

2 SIGLAS Y ACRÓNIMOS

Para un mejor entendimiento del documento, describimos a continuación algunos conceptos clave que usaremos durante el desarrollo de este:

ARCSA: La Agencia Nacional de Regulación, Control y Vigilancia Sanitaria (Arcsa), es la entidad pública adscrita al Ministerio de Salud Pública (MSP) que se encarga de controlar y vigilar las condiciones higiénico – sanitarias de los productos de uso y consumo humano, además de brindar servicios que facilitan la obtención de permisos de funcionamiento y Notificaciones Sanitarias.

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones

API es una abreviatura de Application Programming Interfaces, (interfaz de programación de aplicaciones). Se trata de un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones, permitiendo la comunicación entre dos aplicaciones de software a través de un conjunto de reglas. Es una especificación formal que establece cómo un módulo de un software se comunica o interactúa con otro para cumplir una o muchas funciones.

Arquitectura de información: Plan detallado de la manera en que los sistemas y usuarios de una organización almacenan, organizan y utilizan la información. Permite a las organizaciones captar la estructura de su información y cómo los sistemas y usuarios producen e interactúan con esta información en todos sus flujos y procesos de trabajo.

Autoridad de Registro Una entidad autorizada para la asignación, registro y administración de OIDs dentro de un contexto

Autenticación de usuario empresarial (EUA): Define un medio para establecer un nombre por usuario que luego se puede utilizar en todos los dispositivos y software que participan en este perfil de integración.

Bien estratégico en salud: los constituyen todo tipo de bien determinado por la Autoridad Sanitaria Nacional en el marco de sus competencias, que sea necesario y se encuentre relacionado directamente con la prestación de servicios de salud.

Business Process Execution Language (BPEL). Un estándar de la Organization for the Advancement of Structured Information Standards (OASIS) de un lenguaje que puede ser ejecutado y sirve para especificar acciones dentro de los procesos de negocio de las organizaciones mediante servicios web. Permite especificar procesos integrados entre estos servicios provistos por distintos sistemas de información.

Business Process Definition Metamodel (BPMD). Es un estándar del Object Management Group (OMG) con la capacidad de representar y modelar procesos de negocio, independientemente de la notación o metodología. Para lograrlo se utiliza un metamodelo, que es una especie de vocabulario de procesos con conexiones bien definidas entre términos y conceptos. Utiliza notación XML para representar los procesos.

CEN/ISO 13606 es el estándar CEN/ISO para la comunicación de documentos clínicos digitales entre sistemas de historia clínica electrónica o entre ellos y repositorios de información clínica centralizados. El estándar está dividido en cinco partes: modelo de referencia, intercambio de arquetipos, vocabularios y terminología, seguridad y especificación de las interfaces.

CDA: Arquitectura de Documento Clínico en inglés (Clinical Document Architecture): El CDA es una norma de marcado de documentos que especifica la estructura y la semántica de los documentos clínicos. Un documento CDA es un objeto de información definida y completa que puede incluir textos, imágenes, sonidos y otros contenidos multimedia.

Certificado digital: Documento electrónico mediante el cual se acredita la vinculación entre la identidad de un individuo o una entidad y una clave pública.

Consistent Time (CT) – Estampa de tiempo: define mecanismos para sincronizar la base de tiempo entre múltiples actores y computadoras. Varios perfiles de infraestructura, seguridad y adquisición requieren el uso de una base de tiempo constante en varios equipos.

Datos abiertos: Todos aquellos datos de dominio público, son accesibles, están descritos, son reutilizables, completos y están disponibles oportunamente. Pueden ser utilizados, compartidos y aprovechados libremente por cualquier persona, en cualquier lugar y con cualquier finalidad.

Directorio remoto es un conjunto de objetos que están organizados de forma jerárquica, tales como nombre claves direcciones, etc. Estos objetos estarán disponibles por una serie de cliente conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que los utilicen.

DMZ son las siglas en inglés de Demilitarized Zone o red perimetral, es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, web por ejemplo. Y son precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre la DMZ y la red interna, como una conexión de datos entre un servidor web y una base de datos protegida situada en la red interna.

DWH (Almacén de datos): Sistema de información que compagina los datos de una amplia gama de fuentes dentro de una organización. Los almacenes de datos se usan como repositorios centralizados de datos para fines analíticos y de información

Electronic Data Interchange (EDI) de la American National Standards Institute (ANSI, 1979). Es el formato para intercambiar documentos electrónicos entre sistemas informáticos. Su objetivo es representar documentación electrónica en reemplazo al papel.

Enterprise Service Bus (ESB): Es un componente de integración al cual se conectan los diferentes servicios y a través del cual fluyen los mensajes que permiten que ellos interactúen. Es un elemento que puede rutear inteligentemente cada requerimiento al componente que lo requiere, tiene la capacidad de reformatear los datos para adaptarlos a los diferentes aplicativos participantes y provee además facilidades de manejo de eventos relacionados con el intercambio de información.

EMPI: Enterprise Master Patient Index: Es un indice maestro de paciente también conocido como EMPI (Enterprise Master Index), es un índice de pacientes de toda la institución) Al paciente se le asigna un identificador único que se utiliza para referirse a este paciente en toda la institución. El objetivo es asegurar que cada paciente está representado una sola vez a través de todos los sistemas de software utilizados dentro de la organización.

El perfil IHE de referencias cruzadas de identidad del paciente (PIX) admite la referencia cruzada de identificadores de pacientes de varios dominios de identificadores de pacientes. Estos identificadores de pacientes con referencias cruzadas pueden ser utilizados por los sistemas de "consumidores de identidad" para correlacionar la información sobre un solo paciente de fuentes que "conocen" al paciente mediante diferentes identificadores. Esto permite que un médico tenga una vista más completa de la información del paciente.

El perfil IHE de Consulta de datos demográficos del paciente (PDQ) proporciona formas para que múltiples aplicaciones distribuidas consulten un servidor de información del paciente para obtener una lista de pacientes, según los criterios de búsqueda definidos por el usuario, y recuperar la información demográfica de un paciente (y, opcionalmente, la visita o relacionada con la visita) información directamente en la aplicación.

El perfil IHE de intercambio de documentos entre empresas (XDS) facilita el registro, la distribución y el acceso a través de las empresas de salud de los registros médicos electrónicos de los pacientes. XDS asume que la granularidad en la que se comparte la información clínica entre entidades se encuentra en el nivel de un documento. El perfil XDS define la especificación para el intercambio de documentos entre empresas de atención médica que van desde una práctica privada hasta una instalación de cuidados intensivos para pacientes hospitalizados.

El perfil IHE de integración de ATNA (Audit Trail and Node Authentication) se define mediante IHE (Integrating the Healthcare Enterprise). El Perfil de integración de ATNA se utiliza para definir las medidas de seguridad que, junto con la política de seguridad y los procedimientos, dan soporte a la confidencialidad de la información del paciente, la integridad de los datos y la responsabilidad del usuario. El Perfil de integración de ATNA abarca varios aspectos de la seguridad, incluida la seguridad a nivel de transporte (utilizando, por ejemplo, TLS y WS-Security) y también la auditoría de los sucesos. El Perfil de integración de ATNA define los sucesos de auditoría, los roles del sistema asociados (denominados *actores*), un formato XML común para describir los sucesos y las opciones de transporte para la entrega de mensajes.

El perfil de afirmación de usuario entre empresas (XUA): proporciona un medio para comunicar afirmaciones sobre la identidad de un principal autenticado (usuario, aplicación, sistema ...) en transacciones que cruzan los límites de la empresa.

Ethernet es un protocolo de capa de enlace (capa 2 del modelo Open System Interconnection u OSI) que permite a dos dispositivos conectados a través de un enlace (cable) intercambiar datos de protocolos de capas superiores.

eXtensible Markup Language (XML) de World Wide Web Consortium (W3C). Metalenguaje extensible basado en etiquetas en texto plano que sirve para representar datos estructurados. XML no define un formato particular, es más bien una forma de definir formatos (por ejemplo SOAP se basa en XML). A su vez, estos formatos particulares sirven como sintaxis para el intercambio de información entre aplicaciones, en general corriendo en diferentes computadoras.

FHIR: Recursos de interoperabilidad rápida para la atención de salud: Norma para el intercambio electrónico de información para la atención de salud.

File Transfer Protocol (FTP). Es el protocolo por excelencia para la transferencia de archivos entre computadoras conectadas en una red TCP (como lo es Internet). Está diseñado para obtener la máxima velocidad de conexión, pues los archivos representan grandes cantidades de datos.

Firewall (Cortafuegos, pared de fuego): Sistema de seguridad que protege una red contra ataques externos (ej: hackers), provenientes de otra red (ej: Internet). Impide la comunicación directa entre computadoras de la red y computadoras de redes externas y, por tanto, el acceso de intrusos. Esas comunicaciones son enrutadas a través de un servidor proxy que decide que mensaje o archivo es seguro dejar pasar a la red protegida.

Gestión de identidades: Se refiere a la autenticación y la autorización de las personas para obtener acceso a diferentes recursos digitales (sistemas y aplicaciones).

Historia Clínica Electrónica: Información médica de un paciente que se conserva directamente en computadoras y contiene notas e información recopilada por y para los médicos clínicos en el consultorio, clínica u hospital, que los proveedores de atención de salud utilizan principalmente para diagnóstico y tratamiento. Los expedientes médicos electrónicos son más valiosos que los expedientes impresos porque permiten a los proveedores hacer seguimiento de los datos en el tiempo, determinar qué pacientes requieren visitas preventivas y tamizaje, dar seguimiento a los pacientes y mejorar la calidad de la atención de salud.

HL7: Health Level Seven, por su sigla en inglés, son un conjunto de estándares que facilitan el intercambio de información clínica. Utiliza modelado dado por UML y lenguaje XML.

HL7 v2 es un estándar de mensajería basado en el formato EDI para el intercambio de mensajes entre sistemas de información computarizados en salud. Las últimas versiones incluyen mensajería en formato XML.

HL7 v3 es un estándar de mensajería basado en el modelo de referencia de HL7 (Reference Informative Model o RIM) y el formato XML. Los mensajes de HL7 v3 están divididos en dominios como contabilidad y facturación, asistencia sanitaria, reclamos y reembolso, soporte a las decisiones clínicas, arquitectura de documento clínico, genómica clínica, afirmaciones clínicas, laboratorio, órdenes y reportes de salud pública, entre otros.

HL7 RIM es un modelo de información de referencia de HL7 v3. Su objetivo es servir de base para la definición consistente de mensajes HL7 v3 para la comunicación de información clínica, administrativa y contable.

HyperText Transfer Protocol (HTTP). Este protocolo permite transferir recursos (archivos, texto, imágenes, videos, sonidos, etc.) en Internet. Está basado en el modelo pedido/respuesta donde a cada pedido que realiza una computadora cliente a un servidor, este envía un mensaje en respuesta que puede incluir los recursos solicitados.

Hypertext Markup Language (HTML) de World Wide Web Consortium (W3C), el formato de documentos multimedia en Internet. Es un formato basado en etiquetas que puede ser leído por un humano. Estas etiquetas sirven para organizar el contenido de los documentos y darles un formato. Permite incluir distintos tipos de contenidos multimedia a través de referencias (URLs), y también vincular documentos entre sí. Las últimas familias de documentos HTML y XHTML (HTML1-1991, HTML5-201X) son también documentos XML.

IHE: Integrating the Healthcare Enterprise, es una iniciativa de empresas y profesionales en Salud con el objetivo de optimizar, mejorar y clarificar la comunicación entre los sistemas informáticos en Salud. IHE define un conjunto de perfiles técnicos para implementar la comunicación entre sistemas en diversos ámbitos como laboratorio, imagenología, cardiología y coordinación de cuidado del paciente, entre otros.

IHE IT Infrastructure (ITI): Identifica un subconjunto de los componentes funcionales del ámbito de la salud, denominados actores IHE, y especifica sus interacciones en términos de un conjunto de transacciones coordinadas y basadas en estándares.

Interoperabilidad: Habilidad de dos o más sistemas para intercambiar información y utilizar entre estos mismos la información.

JavaScript Object Notation (JSON) de Internet Engineering Task Force (IETF). Es un formato muy popular en Internet para representar objetos estructurados. El principal fundamento para usar JSON en lugar de XML es que para representar una misma estructura es mucho más liviano (lo que es una necesidad en redes con poco ancho de banda).

LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, o en inglés Lightweight Directory Access Protocol). Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

MINTEL: Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) es una organización del Estado de Ecuador, para definir y coordinar la política de Telecomunicaciones que

promueva la masificación de las Tecnologías de la Información y Comunicación en el territorio ecuatoriano.

Mensaje: Modo en que se intercambia la información entre sistemas informáticos. Su sintaxis está dada por el estándar de mensajería HL7, en el cual se detalla el lenguaje, la estructura, la codificación, etc.

Medicamento: Un medicamento es uno o más fármacos, integrados en una forma farmacéutica, presentado para expendio y uso industrial o clínico, y destinado para su utilización en las personas o en los animales, dotado de propiedades que permitan el mejor efecto farmacológico de sus componentes con el fin de prevenir, aliviar o mejorar el estado de salud de las personas enfermas, o para modificar estados fisiológicos.

Metadatos en salud: Los metadatos (datos acerca de datos) se requieren para poder interpretar, transferir o utilizar datos adecuadamente. Existen diferentes tipos de metadatos, según su finalidad (metadatos estadísticos, metadatos para publicación, etc.).

MLLP: Minimum Lower Layer Protocol: se utiliza para transferir mensajes de la industria de la salud, como los mensajes HL7. El objetivo de MLLP es el de proveer una interface entre una aplicación HL7 y el nivel de transporte que asegure un mínimo de overhead. Esta característica, junto a su gran base implantada en el ámbito sanitario, han sido las condiciones por las que se ha habilitado este protocolo.

MPLS - La conmutación de etiquetas multiprotocolo o (del inglés Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Normas HL7: Normas que rigen el intercambio de datos para asegurar la interoperabilidad entre plataformas. Procesos y características que se requieren para permitir el acceso, la gestión y el intercambio de datos entre diferentes sistemas (por ejemplo, entre instrumentos de laboratorio y sistemas de gestión de la información), redes o comunidades. Por ejemplo: HL7, FHIRE, LOINC, SDMX (norma de datos estadísticos y metadatos).

PKI - Una infraestructura de clave pública (en inglés: Public Key Infrastructure –PKI–) es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.

Prescripción médica: Orden generada por el profesional de la salud para la formulación de medicamentos.

Registro electrónico de salud (EHR): Registro electrónico longitudinal de la información de los pacientes generada por uno o más encuentros en cualquier entorno de atención de la salud. Los médicos clínicos autorizados que atienden a un paciente pueden obtener acceso a la información para atender a ese paciente. Los registros electrónicos de salud también permiten compartir información con otros proveedores país.

Simple Mail Transfer Protocol (SMTP). Es un protocolo basado en mensajes de texto plano para enviar correos electrónicos. Permitió la implementación del correo electrónico a gran escala.

Simple Object Access Protocol (SOAP). Un protocolo que acepta que objetos en diferentes sistemas puedan comunicarse entre sí mediante el intercambio de mensajes XML sobre HTTP. Es uno de los protocolos que permiten implementar servicios web.

TCP/IP son los protocolos más usados en el mundo. TCP es un protocolo de transporte (capa 4 del modelo OSI) que permite crear conexiones lógicas sobre una red IP entre dos computadoras físicamente distantes. IP es un protocolo de capa de red (capa 3 del modelo OSI). Estos protocolos posibilitaron la implementación de Internet.

REST es una interfaz para conectar varios sistemas basados en el protocolo HTTP (uno de los protocolos más antiguos) y nos sirve para obtener y generar datos y operaciones, devolviendo esos datos en formatos muy específicos, como XML y JSON. El formato más usado en la actualidad es el formato JSON, ya que es más ligero y legible en comparación al formato XML. Elegir uno será cuestión de la lógica y necesidades de cada proyecto.

RPIS: Red Pública Integral de Salud. Las entidades prestadoras de servicios de salud en Ecuador que pertenecen a la RPIS conformada por el Ministerio de Salud son:

- IESS (Instituto Ecuatoriano de Seguridad Social)
- ISSFA (Instituto de Seguridad Social de las Fuerzas Armadas)
- ISSPOL (Instituto de Seguridad Social de la Policía Nacional)
- RED PÚBLICA COMPLEMENTARIA

SAML: Acrónimo de Security Assertion Markup Language. Entorno basado en XML diseñado para facilitar el intercambio de información de autenticación y autorización entre los diferentes componentes de la infraestructura de seguridad informática. Define los componentes necesarios para garantizar que cualquier aplicación u entorno pueda intercambiar la información sobre autenticación (identificación de usuarios) y autorización (control de acceso). La adopción de este estándar podría ser un gran paso para facilitar la adopción de los entornos de single sign-on (identificación única del usuario en un único punto, independiente de la aplicación utilizada).

SAN: Storage Area Network: Soluciones de almacenamiento para grandes cantidades de datos. Gestiona de manera central la capacidad de almacenamiento de redes de servidores para mejorar la velocidad de los procesos.

SERCOP: El Servicio Nacional de Contratación Pública, Sercop, es la entidad rectora del Sistema Nacional de Contratación Pública (SNCP), responsable de desarrollar y administrar el Sistema Oficial de Contratación Pública del Ecuador y de establecer las políticas y condiciones en la materia, a nivel nacional.

VPN (en inglés Virtual Private Network) es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet, es decir, la Red Privada Virtual permite que estos dispositivos estén conectados entre sí a través de internet de una forma segura, la cual garantiza la integridad y la confidencialidad de la información que se encuentra en dichos dispositivos.

Web Service Definition Language (WSDL). El formato eXtensible Markup Language (XML) para describir servicios web como un conjunto de interfaces que operan sobre mensajes conteniendo información orientada a documentos o procesos.

XML Schema. Es un lenguaje utilizado para definir estructuras de XML y restricciones sobre los datos que contendrán; asimismo, define usos particulares del formato XML. Web Service Definition Language (WSDL) lo utiliza para definir formatos de servicios web y los objetos que se intercambian vía SOAP.

X.509 es un formato estándar para certificados de clave pública, documentos digitales que asocian de forma segura pares de claves criptográficas con identidades como sitios web, individuos u organizaciones.

3 COMPONENTES DEL DOMINIO DE INFRAESTRUCTURA TIC

En este dominio identificamos tres elementos fundamentales:

3.1 EQUIPOS INFORMÁTICOS

Contempla todos los elementos de infraestructura necesarios para el despliegue y ejecución de los programas, plataformas, servidores de aplicaciones y contenedores, así como los entornos de desarrollo y calidad, las aplicaciones empaquetadas, las máquinas virtuales que se encuentran en el hardware y que son necesarios para lograr la interoperabilidad entre los sistemas de la Red y el operador logístico.

Dentro de esta categoría, se incluye:

- La infraestructura de software y hardware y sus componentes en tiempo de ejecución y tiempo de diseño.
- Los elementos de alojamiento operativo y tiempo de ejecución de los componentes de los sistemas físicos subyacentes.
- Los activos necesarios para dar soporte a la funcionalidad de los servicios, incluyendo aplicaciones empaquetadas o personalizadas, nuevos servicios, servicios creados a través de la composición o la orquestación, y servicios de infraestructura, entre otros.

Esta infraestructura debe estar alojada en centros de datos seguros que cumplan con el estándar ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Centers), el cual define los lineamientos que se deben seguir para clasificarlos en función de los distintos grados de disponibilidad que se pretende alcanzar, esto es, la redundancia necesaria en cada una de sus componentes (telecomunicaciones, arquitectura, eléctrico y mecánico) para lograr grados de disponibilidad que van hasta el 99.995%.

Con base en las recomendaciones del Uptime Institute, se establecen cuatro niveles (tiers) que corresponden con cuatro grados de disponibilidad: cuanto más elevado sea el nivel, mayor será la disponibilidad.

Se recomienda que el centro de datos que albergue la infraestructura de la interoperabilidad esté clasificado como mínimo en nivel III (mantenimiento concurrente), cuyas características se describen a continuación:

- Las capacidades de un centro de datos de este nivel le permiten realizar cualquier actividad planeada (p. ej. mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, y adición o eliminación de elementos) y pruebas de componentes de infraestructura o sistemas, entre otras, sin interrumpir la operación.
- Para aquellas infraestructuras que utilizan sistemas de enfriamiento por agua se requiere un conjunto doble de tuberías.
- Debe existir suficiente capacidad y doble línea de distribución de los componentes, de modo que se pueda hacer mantenimiento o conducir pruebas en una línea, mientras que la otra atiende la totalidad de la carga.
- En este nivel, todavía es posible que se presenten interrupciones por causa de errores de operación o fallas espontáneas en la infraestructura.
- La carga máxima en los sistemas en situaciones críticas es del 90%.

- Muchos cetros de datos de nivel III se diseñan para poder ascender al nivel IV (tolerante a fallos), cuando los requerimientos del negocio justifiquen el costo. Aquí la tasa de disponibilidad máxima del es del 99,982% del tiempo.

En el nivel IV, además de tener la capacidad de realizar cualquier actividad planeada sin interrupciones de carga críticas, tiene funcionalidades de tolerancia a fallas que permiten que la infraestructura continúe operando incluso en presencia de un evento crítico no planeado. En este caso se requieren dos líneas de distribución simultáneamente activas, típicamente en una configuración System + System; eléctricamente esto significa dos sistemas de UPS independientes, cada uno con un nivel de redundancia N+1. La tasa de disponibilidad máxima en este nivel es del 99,995% del tiempo.

De acuerdo con la normativa vigente en Ecuador (acuerdo ministerial 030-2019) los centros de datos deben considerar mecanismos alternativos de prestación de servicios o de gestión de infraestructura, como son los Centro de Datos Virtualizados, que consideran un conjunto de soluciones de TI (aplicaciones, datos, runtime, middleware, sistema operativo, virtualización, servidores, almacenamiento, red) gestionados a modo "servicio" como solución empaquetada que pueden ser gestionadas internamente o por terceros.

3.2 REDES DE COMUNICACIÓN

Las redes son un instrumento clave para la obtención de la plataforma de Salud Digital. La infraestructura de conectividad posibilita que los organismos trabajen de forma integrada, bajo un marco técnico seguro para el intercambio de información. Son el elemento básico para la interoperabilidad pues a través de ellas se transporta la información generada y compartida por los actores.

Ecuador cuenta actualmente con la Red Nacional Gubernamental, la infraestructura de transmisión de datos implementada en el territorio ecuatoriano por la CNT EP (Corporación Nacional de Telecomunicaciones), que presta servicios de enlace datos, Internet e incluye componentes de seguridad y redundancia, exclusivo para las entidades públicas, cumpliendo con los requisitos básicos de una red de alta velocidad de fibra óptica, privada y segura. Adicionalmente, usar los servicios de la red gubernamental para la conectividad segura entre los sistemas de información de las instituciones, es una de las condiciones generales que deben proveer los centros de datos seguros a los que hace referencia el acuerdo ministerial 030 del 2019.

3.3 OPERACIÓN Y MANTENIMIENTO DE TI

Comprende el conjunto de procedimientos que garantizan un tiempo prolongado de actividad para los componentes mencionados en los puntos anteriores (hardware, software y los recursos de red), por lo tanto, es un aspecto crítico para los sistemas que interoperan.

La administración y operación de los sistemas que interoperan exige desarrollar procesos óptimos de gestión, operación, monitoreo y mantenimiento para asegurar su disponibilidad, continuidad y seguridad bajo los acuerdos de niveles de servicio establecidos entre las partes.

Dado que este proyecto involucra a las entidades de la red pública y al operador logístico, se sugiere que los recursos destinados a las actividades de operación y mantenimiento de la plataforma puedan acordarse, compartirse, validarse y distribuirse articuladamente para lograr la sostenibilidad de los sistemas en el tiempo. Algunos de los aspectos que deben considerarse en esta componente dentro del dominio de infraestructura, son:

- Antes de poner en marcha el sistema de intercambio de información, se deben definir acuerdos de niveles de servicio entre los participantes de la interoperabilidad y con los proveedores que dan soporte a los componentes críticos del centro de datos y demás componentes de la infraestructura, quienes deben ofrecer cobertura en un régimen de 7 días/24 horas/365 días/año.
- Considerar el crecimiento de la infraestructura con base en el volumen de los datos compartidos, es un aspecto importante para considerar para que se mantengan los niveles de servicio definidos.
- Dado la rápida evolución de la tecnología, se debe considerar como parte del mantenimiento, además de las licencias, las actualizaciones necesarias para disminuir, en la medida de lo posible, el riesgo de obsolescencia tecnológica.
- Debe hacerse una revisión sistemática del desempeño de los servicios de soporte y mantenimiento y ajustarlos en la medida de la evolución y la adaptación de los requisitos de la interoperabilidad. Cuando sea necesario, aumentar la capacidad del personal de tecnología para responder a fallas imprevistas del sistema con posibles consecuencias adversas.
- Se recomienda contar con un sistema de gestión y monitoreo centralizado y con las herramientas necesarias que permitan alertar fallas en componentes críticos.

4 COMPONENTES TECNOLÓGICAS DE LA PLATAFORMA DE INTEROPERABILIDAD EN EL DOMINIO DE FARMACIA

Toda plataforma TIC requiere la solución previa de algunas funcionalidades de infraestructura, tales como:

- **Seguridad:** usuarios, autenticación y control de acceso
- **Enrutamiento y transformación de mensajes** (ESB/Bus de interoperabilidad)
- Implementación **de estándares sobre interoperabilidad** y usabilidad
- Mecanismos de **continuación y acceso a datos**
- Acceso a la información **(portal)**
- **Conectividad** en diferentes niveles
- Herramientas de **gestión y administración**
- **Gobierno**
- **Privacidad y la protección** de datos.

Estas funcionalidades básicas, deben ser proporcionados por la plataforma de Salud Digital de Ecuador, que para la fase inicial (Fase I) de interoperabilidad que cubrirá los casos de uso de intercambio en el dominio de farmacia comunitaria, debe estructurarse en tres capas: una física y dos lógicas. La capa física estará formada por la nube, la cual deberá soportar toda la infraestructura tecnológica de la plataforma y las capas lógicas compuestas por la capa de Aplicaciones y la Plataforma de Interoperabilidad: la primera orientada a usuarios finales y la segunda a servicios de integración:

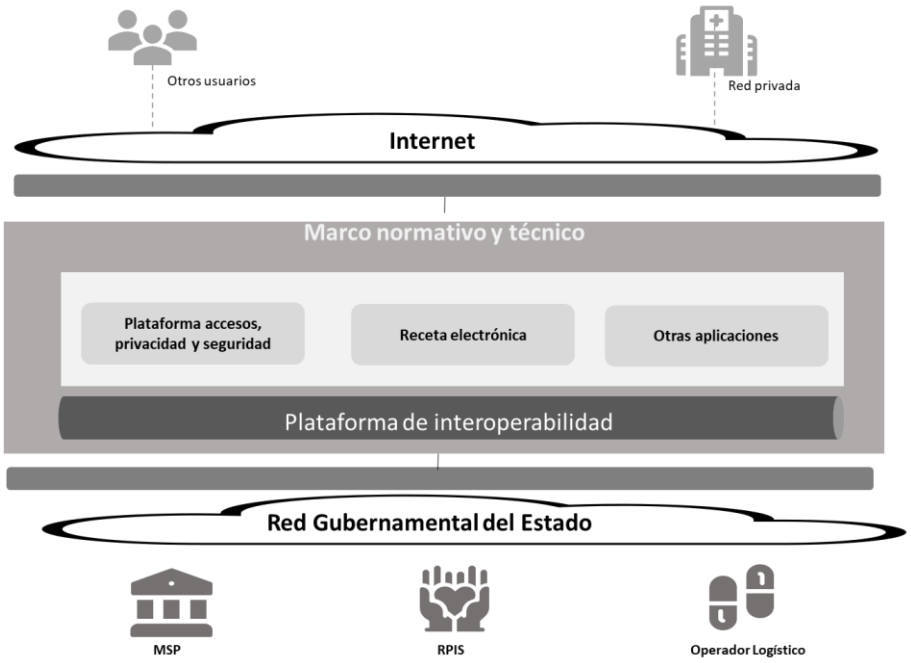

Figura 2: Propuesta plataforma de salud digital Ecuador (Fase I)

Para esta fase, la propuesta de plataforma de salud digital para Ecuador tiene tres componentes:

4.1 LA PLATAFORMA DE INTEROPERABILIDAD:

La plataforma de interoperabilidad integra los sistemas de la RPIS y operador logístico a nivel de back-end. Tiene dos capas: una de seguridad y otra de interoperabilidad (semántico y técnico). La interoperabilidad técnica se resuelve mediante el uso de un Enterprise Service Bus (ESB) y la semántica se resuelve mediante una serie de definiciones de metadatos (Registry), que permiten simplificar el intercambio de datos y ofrecer servicios de valor agregado sobre el mismo.

La plataforma de Interoperabilidad de salud deberá cumplir con todos los componentes y estándares de la industria, promoviendo y facilitando el intercambio de datos e información electrónica mediante la formulación y ejecución de proyectos conjuntos de interoperabilidad. Para nuestro caso, iniciaremos con el intercambio de información en el ámbito de farmacia, pero debe ser extensible a otras áreas como la Historia Clínica Electrónica, Inmunizaciones, Gestión de facturación y cuentas médicas, entre otras.

El contexto de prescripción y dispensación electrónica requiere el cumplimiento de reglas de interoperabilidad y reglas de integridad de datos. Las primeras reglas están respaldadas por los tres niveles principales de interoperabilidad: interoperabilidad organizacional, interoperabilidad semántica e interoperabilidad técnica.

- La **integridad de los datos** se basa en reglas y políticas de auditoría, trazabilidad, identidad, confiabilidad y verificación automática.

- **Interoperabilidad organizacional** se basa en dos elementos: diseño basado en el concepto de dominio de afinidad y normativa a nivel país y a nivel específico del Ministerio de Salud. Los diseños se basan en el concepto de dominio de afinidad, el cual se refiere a una serie de proveedores de atención médica que comparten algunas políticas dentro de un entorno de cooperación, utilizando una infraestructura compartida. Para nuestro caso, se sugiere la creación de un solo dominio de afinidad para la Red Pública y el Operador logístico.

  Considerando que este modelo fue diseñado para un sistema de ámbito nacional, se requiere la gobernanza de este dominio, con el fin de establecer y asegurar reglas o políticas compartidas que los proveedores de salud se comprometen a cumplir. Algunas de las políticas a definir son las siguientes: reglas organizacionales (legales, roles y estructurales, básicamente establecidos por el MSP), reglas operativas (por ejemplo, SLA, políticas de respaldo y recuperación, modificación y eliminación de datos médicos y administrativos), reglas de registro de dominio, políticas de autenticación y acceso, políticas de privacidad, consentimiento y auditoría.

- **Interoperabilidad semántica** se basa en la definición y gestión de los formatos de documentos aceptados por los repositorios, así como en términos y vocabulario. Además, también se basa en la implementación de servicios terminológicos, según un marco controlado con acceso distribuido.

- **Interoperabilidad técnica** se basa en la adopción de algunos estándares e instrumentos proporcionados por la plataforma de interoperabilidad que incluye estándares y perfiles definidos establecidos por HL7 e IHE, e implementados en instrumentos específicos como ESB o bus de interoperabilidad, EMPI, XDS y otros que se describen a continuación:

  - El **motor de integración** está formado por el **BUS de Interoperabilidad**, para procesar mensajes específicos de protocolos de salud, cumpliendo con las normativas legales y reglamentarias vigentes, así como estándares internacionales. Desempeña el papel de

transformar, validar, enrutar, integrar y realizar acciones de difusión en los mensajes recibidos de las aplicaciones de salud. Dentro de este motor, se configuran varios puertos de origen y destino para llevar a cabo procesos de intercambio de datos. Los mensajes se emiten y envían desde y hacia las aplicaciones que se integrarán, según distintos protocolos de comunicación (TCP / IP, HTTP, SOAP, WS *, REST, MLLP) y diferentes formatos de mensajería (HL7 V2.x, HL7 V3, FHIR, DICOM , X12, XML, EbXML, EDI, texto delimitado). Después de recibir el mensaje de un puerto, se identifica y procesa sintácticamente. Los mensajes se dirigen dentro del motor y se pueden validar y / o transformar. Una vez transformado el mensaje, puede enviarse a otro puerto de destino, según cierto formato y protocolo. Como cualquier ESB, proporciona funcionalidades para administrar y monitorear el servicio y el tráfico.

- La **aplicación (appliance/artefacto)** que corresponde a la solución tecnológica que resuelve las necesidades del intercambio y la integración de mensajes. Puede ser un artefacto formado por hardware y software que implementa capas de servicios e interfaces de usuario. Estará conformado por dos componentes: uno está ubicado en el Data center central (software) y el otro físico (software y hardware) está ubicado en los sitios del proveedor. Algunas de las funcionalidades de este tipo de artefactos, son:

  Localmente, para cada proveedor:

  - Conector, que resuelve conectividad, autenticación y acceso a la plataforma de salud digital;
  - Motor de mensajería que proporciona capacidades de publicación / suscripción
  - Capacidades para el almacenamiento persistente de documentos, así como la capacidad de indexación para una búsqueda rápida (registro y depósito de documentos XDS).
  - Abstracción y encapsulación de servicios para la gestión de identificación única de pacientes (EMPI)
  - Retención de mensajes en caso de interrupción de servicios/gestión de colas, enrutamiento de mensajes
  - Funcionalidades para uso local de firma digital.
  - Funciones de transformación (por ejemplo, para transformar a CDA aquellos documentos que contengan los datos mínimos requeridos, pero que no cumplan con los estándares de formato);
  - Adaptadores específicos de acuerdo con los requisitos del sistema no estándar

Otras componentes relevantes de la plataforma de salud digital:

- El **EMPI** (Enterprise Master Patient Index) Módulo para la gestión de la identificación única de pacientes que prove un registro central de los pacientes y sus características demográficas, gestiona entradas duplicadas, localiza registros, usa mensajería de los perfiles PIX/PDQ de HIE y algoritmos determinísticos para la búsqueda de registros similares y búsquedas fonéticas.

- Autenticación y autorización: Gestión de políticas y controles de acceso a través de componentes de autenticación y autorización. La implementación del mecanismo concreto de interacción de los servicios web expuestos debe cumplir con todos los aspectos relacionados ´la Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos para garantizar la validez a nivel de acuerdo comercial de esta interacción. Concretamente se deben adoptar mecanismos de autenticación

basados en certificados digitales X509 que identifiquen a los terceros formalmente. Los clientes externos deben utilizar certificados de emitidos por las entidades o centros de confianza (TrustCenter) acreditadas ante el ARCOTEL, como autoridades de certificación aprobadas en Ecuador.

- **Sistema de auditoría:** Generación de eventos de auditoria (importación, exportación o consulta de información médica o sensible protegida) y el almacenamiento en repositorios que proveen información para seguimiento y trazabilidad de registros.

- **Sistema de auditoría:** Generación de eventos de auditoria (importación, exportación o consulta de información médica o sensible protegida) y el almacenamiento en repositorios que proveen información para seguimiento y trazabilidad de registros.

- Las **funciones de negocio** propias del intercambio de información entre las entidades de la Red Pública y el Operador Logístico, que se originan en el acto médico de la prescripción de medicamento y/o el requerimiento de un bien estratégico, la validación de la prescripción en términos de pertinencia, dosis, interacciones, toxicidad, alergias y demás variables que puedan causar posibles eventos asociados con la prescripción, la dispensación de medicamentos y bienes estratégicos de acuerdo a parámetros de prescripción y validación y la administración del medicamento al paciente.

4.2 LAS COMPONENTES DE CONECTIVIDAD

Provee los servicios básicos para la interconexión de sistemas y mecanismos básicos para facilitar la transferencia de información. Contiene los elementos de hardware y software que componen la red y los enlaces físicos de comunicaciones utilizados por los sistemas.

En este contexto, la red se convierte en el instrumento clave dentro de la plataforma de salud digital. La infraestructura de conectividad posibilita que los organismos trabajen de forma integrada, bajo un marco técnico seguro para el intercambio de información; como se mencionó en el punto 2.2 de este documento, se sugiere utilizar la Red Gubernamental del Estado ya que cumple con los requisitos básicos de una red de alta velocidad de fibra óptica (infraestructura MPLS), privada y segura que cuenta con velocidades desde de 10 a 100Mbps

4.3 EL MARCO NORMATIVO Y TÉCNICO

En esta componente de la plataforma de salud digital están los marcos jurídicos y las disposiciones legales y regulatorias aplicables al sector salud, como por ejemplo las relacionadas con el acceso a datos, identificación de ciudadanos, protección de datos personales, firma electrónica, datos abiertos y otros que se detallan en el apéndice 4 de este documento. Todas estas disposiciones deben ser tomadas en cuenta en el momento de la adquisición de infraestructura, plataformas y servicios y en los procesos de instalación e implementación de estas.

Una descripción detallada de las componentes de la plataforma de salud digital para la primera fase de la interoperabilidad se presenta en el apéndice 1 de este documento.

5 ARQUITECTURA DE DESPLIEGUE

A continuación, una arquitectura de despliegue que puede tomarse como referencia para la implementación de la plataforma de interoperabilidad. Las decisiones de arquitectura, las decisiones de plataforma y proveedor seleccionado impactan directamente la infraestructura y su despliegue. Tomar la información a continuación, solo de manera referencial:

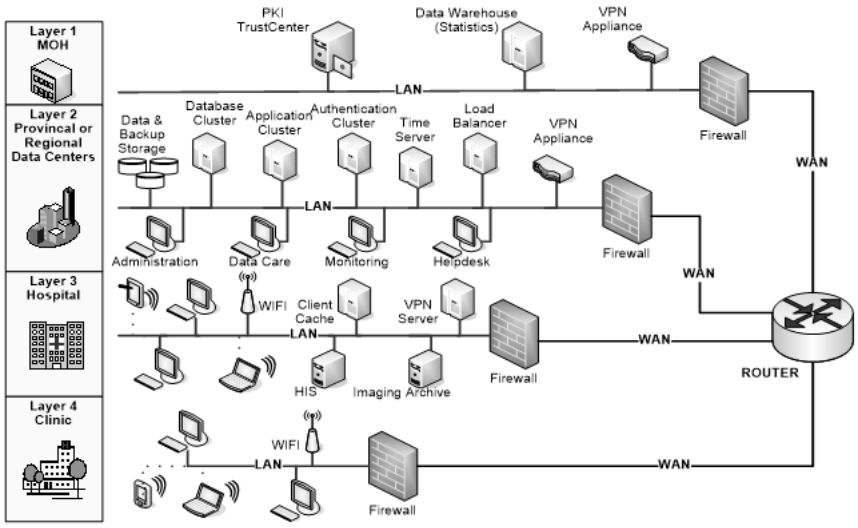

Figura 3: Arquitectura REFERENCIAL de despliegue (fuente: elaboración propia)

En este modelo, de 4 Layers (Layer 1 Ministerio de Salud – MOH, Layer 2 Datacenter provincial o regional, Layer 3 Hospital y Layer 4 centro médico o en nuestro caso, una farmacia comunitaria) tiene en cada capa, las siguientes componentes:

- **Layer 1: Ministerio de salud**
  - Firewall para proteger la red interna
  - Dispositivo VPN para una conexión segura a los centros de datos
  - DWH (Data Warehouse) recopila información de los centros de datos para análisis estadísticos. Inicialmente será utilizado por el operador logístico como herramienta para determinar las necesidades de compra o de producción que se requiere de un medicamento o bien estratégico, generar estadísticas de uso de medicamentos controlados o restringidos, demandas insatisfechas, entre otros.
  - Portal para el asegurador, prestador, operador logístico, ciudadano (fase futura)
  - Trustcenter (Centro de confianza) para proporcionar una PKI o generación de certificado digital: Además de emitir certificados, el centro de confianza desarrolla infraestructuras de clave pública (PKI) para las organizaciones que interoperan. La autenticación se basa en el uso de certificados; todo mensaje debe ir autenticado haciendo uso de un token tipo X.509 (X.509 Certificate Token). La generación de este token proporciona un mecanismo valido de autenticación y se basa en la posesión de un certificado con su llave pública y privada. En Ecuador, las entidades acreditadas ante ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones), que son las autoridades de certificación aprobadas en Ecuador para todo intercambio con terceros, dadas las normas y leyes vigentes de la legislación ecuatoriana
  - Registro (Metadata) de los documentos clínicos Electrónicos
  - Master Patient Index infrastructure

- Herramienta de Analítica para el procesamiento de información y toma de decisiones (fase futura).

- **Layer 2: Centros de Datos Nacional/Regional o Provincial**
  - Firewall para proteger la red interna
  - Balanceadores para distribuir la carga de trabajo
  - Clúster de dispositivos VPN para garantizar:
    - Conexiones seguras con todos los clientes (por ejemplo, clínicas, Ministerio de Salud, operador logístico)
    - Conexiones seguras a otros centros de datos
    - Registro de auditoría
    - Escalabilidad para mantener el rendimiento y la disponibilidad
  - Clúster de equilibrador o balanceador de carga para:
    - Mayor rendimiento y disponibilidad
    - Failover
    - Fácil escalabilidad
  - Clúster de servidores de tiempo para mantener las marcas de tiempo correctas (IHE: CT)
  - Clúster de autenticación (IHE: EUA, XUA)
  - Clúster de Repositorios de Documentos Clínicos (XDS)
  - Clúster de aplicaciones
  - Clúster de base de datos
  - Almacenamiento de datos y copias de seguridad (por ejemplo, SAN)
  - Estaciones de trabajo para uso administrativo y operativo

- **Layer 3: Hospitales de la red**
  - Firewall para proteger la red interna
  - Servidor VPN para una conexión segura al centro de datos
  - Proxi server cache para un alto rendimiento y una transferencia de datos confiable: se debe garantizar un ancho de banda disponible de (entre 10 y 100 Mbps) entre el hospital y el centro de datos
  - Appliance de salud
  - Clientes web para acceder al portal (inicialmente solo para lista de recetas activas con potencial de crecimiento hacia la Historia Clínica Electrónica Nacional) a través de HTTPS

- **Layer 4: Centros de salud / Farmacias comunitarias**
  - Firewall para proteger la red interna
  - Clientes web para acceder al portal de la Historia clínica nacional/Repositorios de prescripción o dispensación vía HTTPS.

La infraestructura definida debe tener capacidad para implementar la solución e integrar sitios de atención médica de la RPIS, considerando como mínimo:

- MSP: 1939 Centros de Salud y 135 Hospitales.
- F.F.A.A: 78 Centros de Salud y 1 Centro de Especialidades.
- Policía Nacional: 42 Centros de Salud y 2 Hospitales.
- IESS: 659 Seguro Campesino, 48 Centros de Salud y 53 Hospitales.

Con alrededor de 3000 usuarios (como base), considerando al menos 20 sistemas de información dentro de los cuales son en de uso común en las entidades, los siguientes: PRAS (MSP), AS/400 (IESS), Innovativa (ISSFA), IntegraSalud, Hosvital (ISSPOL)

Debe tener capacidad para gestionar un volumen de transacciones mínimo o superior al que se especifica en la siguiente tabla:

INSTITUCIONES	PROMEDIO MENSUAL (2018-2019)	CANTIDAD PROMEDIO RECETAS FISICAS DIARIO (2018-2019)	CANTIDAD DE RECETAS ELECTRONICAS (Considerando 1 y 2 ítems por receta)	CANTIDAD DE PETICIONES BASE DIARIAS BUS ESTIMADAS
FFAA	5.336	178	356	711
IESS	3.179.739	105.991	143.883	287.767
ISSPOL	21.336	711	975	1.950
MSP	7.147.659	238.255	443.828	887.657
Total general	10.354.070	**345.136**	**589.042**	**1.178.085**

- La estimación anterior se la realizó utilizando los datos proporcionados por las entidades de la RPIS, para el volumen de recetas producidas en promedio entre 2018-2019 dentro de 2353 establecimientos de salud. Resaltando que no se cuenta con datos estadísticos para 584 establecimiento de salud, los cuales representan un 24,82% del total. Por lo que es importante considerar para la volumetría de recetas diarias este número, que corresponde principalmente a entidades que no reportaron datos o no tienen receta electrónica.
- La estimación de ítems por receta es un valor aproximado, ya que, en función de la entidad y tipo de establecimiento, puede haber mínimo 1 ítem por receta, y no puede tener un valor máximo (n ítems). Para los cálculos se utilizó un promedio de 2 ítems por receta para centros y 1 ítem por receta para hospitales.
- La cantidad de peticiones básicas (de la receta) como mínimo pueden ser dos, se incluye una consulta de la receta (validada) para ejecutar el proceso de dispensación, así como un registro por parte de quien ejecuta la dispensación (en este caso el Operador Logístico). Se deben considerar de manera adicional las peticiones relacionadas a autenticación y autorización (Ejemplo: generación de un Token).
- Se debe considerar que el peso aproximado de una receta electrónica con 10 medicamentos es de 1.6-2.5KB. Por lo que se debe tener presente el dimensionamiento de almacenamiento necesario para albergar los registros durante 10 años.

APENDICE 1 – DETALLE DE LAS COMPONENTES DE LA PLATAFORMA

Partiendo de la arquitectura de integración propuesta por la mesa de trabajo y basados en las definiciones del capítulo 3 de este documento, describimos a continuación las componentes de la plataforma tecnológica sugerida para que se logre el objetivo del intercambio entre la RPIS y el operador logístico:

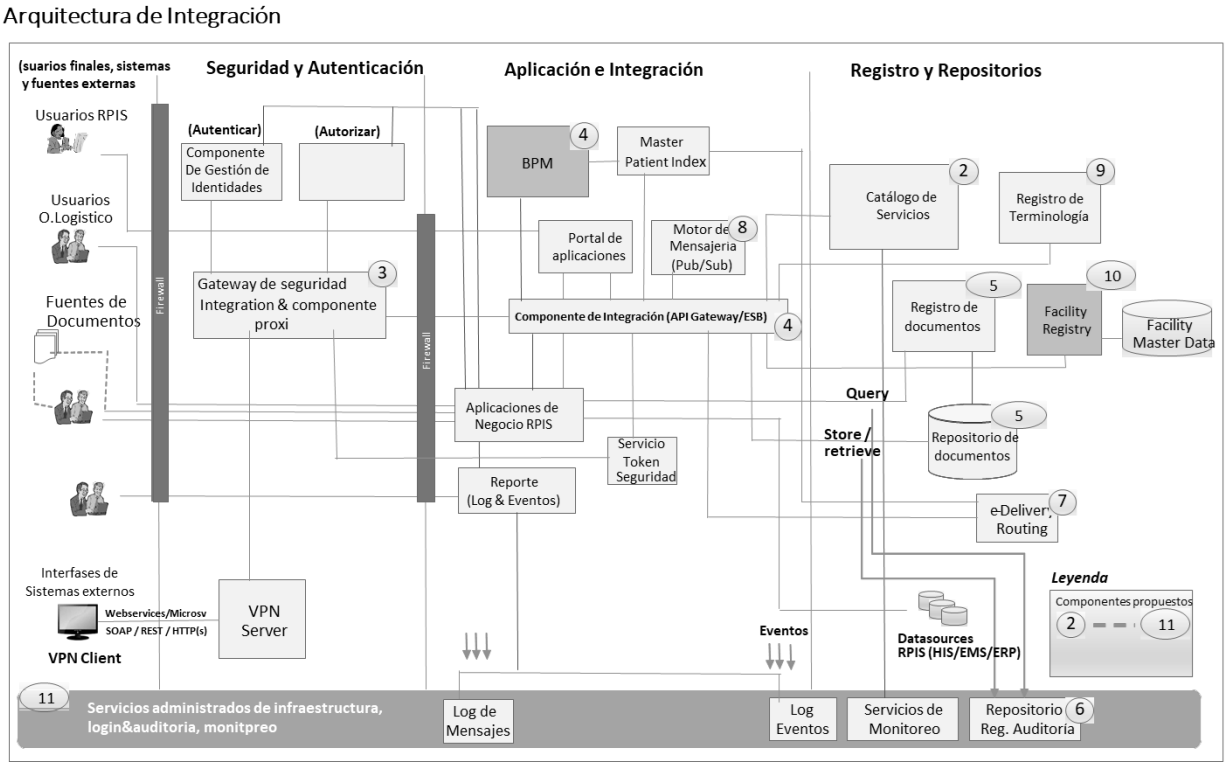

Figura 4: Arquitectura de componentes (fuente: elaboración propia)

Si bien la arquitectura es conceptual, proporciona una base de comprensión de las capacidades deseadas organizadas por una descripción conceptual de los componentes de la solución, que describimos a continuación:

Número y nombre del componente	Breve descripción y referencia cruzada a la sección que proporciona detalles específicos de implementación
(2) Registro y repositorio de servicios empresariales (catálogo de servicios)	Este componente proporciona capacidades que respaldan la gestión del ciclo de vida del servicio (SOA) para varias fases, como modelar, ensamblar, implementar y administrar. Proporciona visibilidad y gobernanza del servicio de diseño y tiempo de ejecución y servidores como un registro y repositorio empresarial de servicios.
(3) Componente de puerta de enlace de seguridad, integración y proxy inverso	Este componente sirve como puerta de enlace de servicios web y proporciona servicios de seguridad e integración en el perímetro de la organización. Proporciona gestión centralizada de políticas y niveles de servicio para el cumplimiento de las políticas de la organización. Este componente interactúa con los componentes de gestión de acceso e identidad para proporcionar capacidades de

Número y nombre del componente	Breve descripción y referencia cruzada a la sección que proporciona detalles específicos de implementación
	autenticación, autorización y auditoría para el tráfico de servicios web.
(4) Componente de integración de servicios (ESB) (4) Gestión de procesos comerciales	Estos componentes abordan las responsabilidades principales de los aspectos de integración y orquestación de servicios. El componente de integración de servicios proporciona funcionalidades como la transformación de mensajes, el enriquecimiento de mensajes, la conmutación de protocolos y la invocación del punto final del servicio. El componente Business Process Management proporciona capacidades de orquestación de servicios.
(5) Depósito y registro de documentos	Estos dos componentes proporcionan las capacidades para el almacenamiento persistente de documentos, así como la capacidad de indexación para una búsqueda rápida (registro y depósito de documentos XDS).
(6) Repositorio de registros de auditoría	Este componente proporciona capacidades para proporcionar un repositorio de Audit Trail e interfaces con el repositorio según el perfil IHE ATNA y las especificaciones de transacción ITI. Este componente se utiliza para almacenar registros de eventos de auditoría.
(7) enrutamiento de entrega electrónica	Este componente proporciona capacidades para habilitar un repositorio y las interfaces de servicio correspondientes para permitir la configuración de la entrega a los proveedores de resultados de laboratorio, informes clínicos y otros contenidos para su distribución. Permite la configuración de opciones de entrega según el tipo y la naturaleza del contenido, como pacientes hospitalizados o ambulatorios, ubicaciones de servicios, función del proveedor y aspectos similares.
(8) Motor de mensajería	El componente del motor de mensajería proporciona capacidades de publicación / suscripción.
(9) Registro de terminología	Este componente proporciona las capacidades, las interfaces de usuario y de servicio para establecer un aspecto de Gestión de vocabulario.
(10) Registro de instalaciones	Este componente proporciona las capacidades para gestionar las identidades de las ubicaciones de prestación de servicios.
(11) Capa de gestión de servicios de TI	Esta capa proporciona varios componentes para agregar e informar de eventos y registros de mensajes de todo el sistema.
(12) Master Patient Index	Módulo para la gestión de la identificación única de pacientes por medio de un EMPI, Enterprise Managment Patient Index. El MPI prove un registro central de los pacientes y sus características demográficas, gestionar entradas duplicadas, localizaregistros, usa mensajería de los perfiles PIX/PDQ de HIE y algoritmos determinísticos para la búsqueda de registros similares y búsquedas fonéticas.

El bus de interoperabilidad debe cumplir características mínimas, cómo muestra la siguiente gráfica:

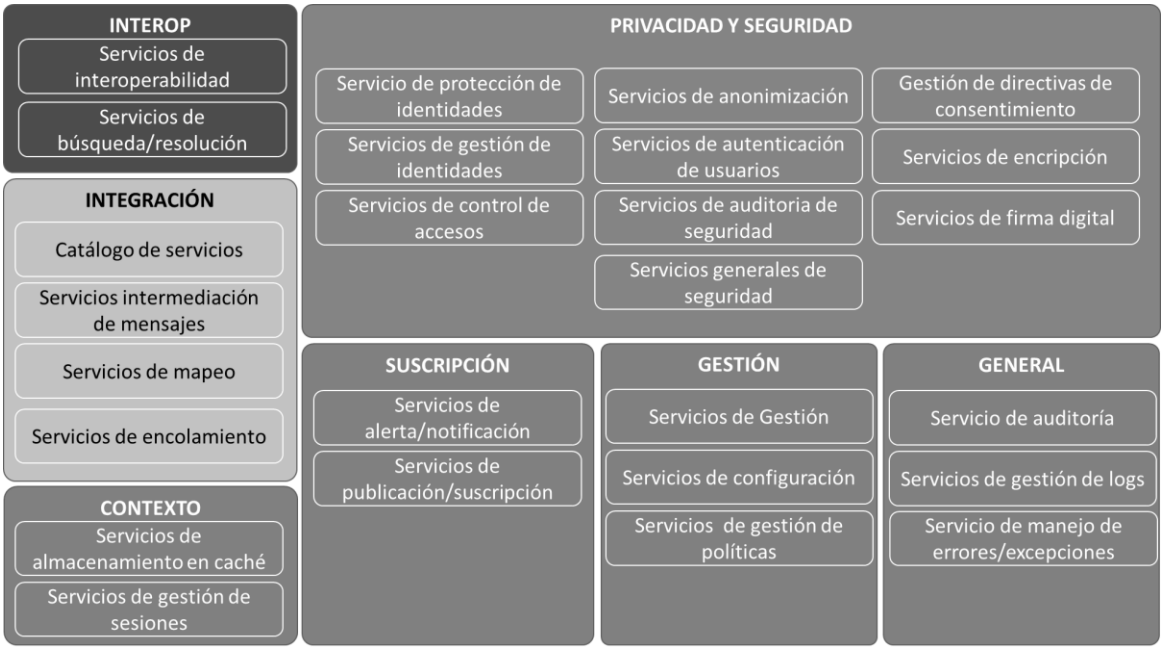

Figura 5: Caracterísiticas mínimas del Bus de interoperabildiad (fuente: elaboración propia)

APENDICE 2 – ARQUITECTURA DE REFERENCIA TÉCNICA

A continuación, un diagrama que muestra la comunicación entre los principales componentes de infraestructura, tecnología y la relación con los sistemas de información de los hospitales que hacen parte de la red pública de prestadores de salud

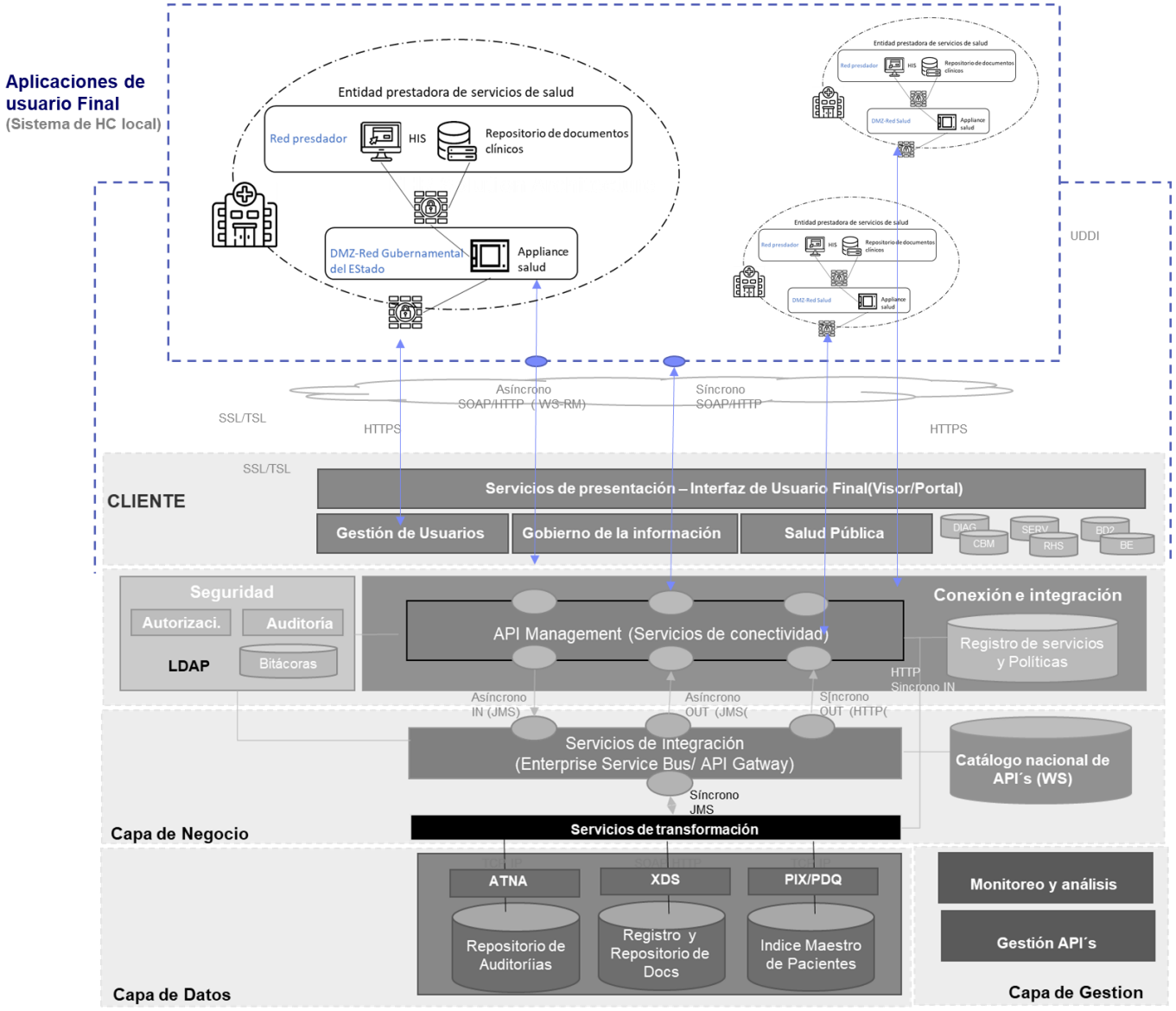

Figura 6: Arquitectura técnica referencial (fuente: elaboración propia)

Describimos a continuación la función que cumple cada uno de los componentes representados en la arquitectura de referencia propuesta:

- Ecuador cuenta actualmente con una red estatal de comunicación de datos, "Red Gubernamental del Estado" (RGE), que proporciona la infraestructura de conectividad necesaria para vincular a las entidades de la red pública de salud y al operador logístico, de forma segura, con niveles adecuados de servicio, seguridad informática y alta disponibilidad.

Como se puede observar en la Figura 6 la RGE termina en una "DMZ (red perimetral) que está físicamente en un una entidad de la red pública de prestaciones de salud y/o en las sedes del operador logístico. La RGE se extiende a través de conexiones con redes de salud locales existentes (red de salud pública, redes de proveedores privados y acceso público a internet para usuarios y proveedores).

- Dado que la Red Pública Integral de Salud está compuesta de múltiples proveedores de atención médica, proponemos una arquitectura con basada en un modelo federado de registros médicos electrónicos, de tal manera que todos los integrantes de la red sean responsables de administrar y proporcionar la custodia de los registros médicos de sus afiliados al mismo tiempo que se cubre la necesidad de tener una vista completa de la información relacionada con la prescripción de medicamentos y bienes estratégicos, cuando y donde sea necesario (escalable a la Historia Clínica Electrónica Nacional).

- La arquitectura considera los componentes de software necesarios para brindar los principales servicios del Ministerio de salud relacionados con: la salud de las personas, los servicios de salud (tablas maestras, los diccionarios y terminología y los sistemas de notificación.

- El contexto prescripción-dispensación electrónica requiere el cumplimiento de **reglas de interoperabilidad y reglas de integridad de datos**. Las primeras reglas están respaldadas por los tres niveles principales de interoperabilidad: interoperabilidad organizacional, interoperabilidad semántica e interoperabilidad técnica. La integridad de los datos se basa en reglas y políticas de auditoría, trazabilidad, identidad, confiabilidad y verificación automática.

- El modelo de autenticación y autorización se basa en la federación de identidades y, por tanto, en la fiabilidad. Este utiliza tokens SAML firmados con certificados X509 para ser el único punto de acceso a diferentes servicios. Para lograrlo, cada proveedor y consumidor de servicios tiene una sucursal en el **directorio LDAP** de la plataforma de interoperabilidad. En este directorio se definen los roles existentes de la organización, que luego se utilizarán para autorizar el consumo de servicios. Esta autorización se puede lograr con una granularidad más fina: en la medida de una operación de servicio web. Los roles específicos utilizados por las aplicaciones de salud se gestionarán dentro de las aplicaciones respectivas.

- Este modelo de arquitectura propuesto es de ámbito nacional, por lo tanto se requiere de la gobernanza de este dominio, con el fin de establecer y asegurar **reglas o políticas** compartidas que las entidades de la red se comprometen a cumplir: reglas organizacionales, reglas operativas (SLA´s, políticas de respaldo y recuperación, modificación y eliminación de datos médicos y administrativos, por ejemplo), reglas de registro de dominio, políticas de autenticación y acceso, políticas de privacidad, consentimiento, revisión de cuentas.

- La interoperabilidad semántica se basa en la definición y gestión de formatos de documentos aceptados por los repositorios, así como **en términos y vocabulario**. Además, también se basa en la implementación de **servicios terminológicos,** de acuerdo con un marco controlado con acceso limitado y distribuido

- La interoperabilidad técnica se basa en la adopción de algunos estándares e instrumentos provistos por la plataforma de interoperabilidad que se amplían para incluir estándares y perfiles definidos establecidos por HL7 e IHE, e implementado en instrumentos específicos como **ESB** de salud**, EMPI, XDS** y otros perfiles de interoperabilidad.

- El motor de integración está formado por el ESB de interoperabilidad, para procesar mensajes específicos de protocolos de salud. Desempeña el papel de transformar, validar, enrutar, integrar y realizar acciones de difusión en los mensajes recibidos de las aplicaciones de salud. Dentro de este motor, se configuran varios puertos de origen y destino para llevar a cabo procesos de intercambio de datos. Los mensajes se emiten y envían desde y hacia las aplicaciones que se integrarán, según diferentes protocolos de comunicación (TCP / IP, HTTP, SOAP, WS *, REST, MLLP) y diferentes formatos de mensajería (HL7 V2.x, HL7 V3, DICOM , X12, XML, EbXML, EDI, delimitado)

- La tabla maestra de pacientes, versión empresarial (EMPI), contiene información actualizada de la identificación de diferentes individuos para suministrar el dominio de afinidad. Esto permite que cada proveedor mantenga su identificación actual y comparta información médica (lista de prescripciones activas, Histórica Clínica Electrónica, etc.) a través de un registro XDS local, administrado por el proveedor, que se copia en el Registro Nacional de Información Médica (Registry). Este registro también se ubica dentro de la plataforma, y recibe la información proporcionada por los registros locales que lleva cada proveedor.

- Para mantener actualizada la información de prescripciones-dispensaciones y documentos clínicos relacionados y para minimizar la recopilación de datos durante la visita del paciente, los prestadores de la red pública tendrán un servicio de **Publicación y suscripción.** Pueden suscribirse a este servicio para recibir informes sobre hechos médicos ocurridos dentro del sistema relacionados con sus afiliados.

APENDICE 3 – CARACTERÍSTICAS Y REQUISITOS MÍNIMOS DE LA INFRAESTRUCTURA (BASE PARA LICITACIONES O ESTUDIOS DE MERCADO)

Característica
El proveedor deberá hacerse cargo de la provisión, instalación y puesta en marcha de infraestructura necesaria para desplegar la solución propuesta (Procesador, memoria y almacenamiento) así como su administración hasta que la solución sea transferida al MSP, de acuerdo con la normativa ecuatoriana vigente y alineado a la planificación del proyecto.
El proveedor deberá realizar el dimensionamiento para el dominio de infraestructura, teniendo en cuenta que los componentes deben estar en alta disponibilidad, de: ● Sistema de balanceo ● Servidores de aplicación ● Servidores de la capa de servicios ● Servidores de Base de Datos / Back end ● Volumetría de crecimiento
Se deben proveer sistemas hiperconvengentes de tal manera que se eliminen las incidencias de la gestión de la TI tradicional agrupando servicios de centro de datos como el servidor, el almacenamiento y la red, y permite que se gestionen en una única aplicación. Este Sistema hiperconvengente debe considerar: ● Nodos hiperconvergentes ● Virtualización de cómputo ● Virtualización de almacenamiento ● Gestión de la virtualización
Todos los equipos que provea deberán ser nuevos de fábrica (no remanufacturados) ni reparadas ninguna de sus partes. El año de fabricación deberá ser al menos el 2021, incluyendo cada uno de los componentes. Para cumplir este requerimiento deberá emitir un certificado por parte del fabricante.
Todas las componentes de infraestructura deberán ser instaladas por el fabricante, en conjunto con el proveedor de acuerdo con las mejoras prácticas.
El soporte del Sistema Hiperconvergente debe ser entregado en forma unificada: hardware de los nodos, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión a través de un servicio de soporte integral y unificado. Adjuntar certificado emitido por el fabricante
Las actualizaciones de software, firmware, parches/fixes deben ser certificadas y entregadas por el fabricante en forma integrada y considerando todos los componentes de red, computo, almacenamiento y virtualización. El proveedor deberá obtener del fabricante parches/fixes cada seis meses, así como detalles de parches/fixes soportados y su procedimiento de aplicación. No podrán ser aplicadas actualizaciones y/o parches por separado que no hayan sido pre-validados por el fabricante

Toda la infraestructura y sus componentes de red, cómputo, almacenamiento y virtualización deberá ser con esquema de alta redundancia N+1. Adjuntar el certificado respectivo
El proveedor deberá garantizar al MSP que a través de la entrega de un certificado el fabricante ofrece y certifica un esquema de atención directa de llamadas y problemas que deberá ser provisto desde un centro de soporte unificado, desde donde deberán asistirse todos los problemas asociados a los componentes de red, computo, almacenamiento y virtualización, durante el tiempo que dure la garantía en la modalidad 7x24x 365 con un tiempo de respuesta en sitio máximo de 4 horas para solventar inconvenientes.
La infraestructura deberá incluir todo el licenciamiento e instalación del software Hipervisor que permita el cumplimiento de todo lo requerido. El proveedor deberá detallar la cantidad, versión de todo el licenciamiento necesario para cumplir con el objeto de la contratación
El sistema debe contar con una aplicación de soporte que reporte el estado del equipo al fabricante en forma automática. El proveedor deberá detallar las características técnicas de aplicación de soporte propuesta.
Los nodos hiperconvergentes deberán contar mínimo con: ● Software de administración. ● Software de monitoreo. ● Software de reportería
El Sistema Hiperconvergente debe incluir el licenciamiento/suscripción para la plataforma de virtualización de acuerdo con el número de procesadores por nodo que dimensione el proveedor, quien además deberá detallar las especificaciones de licenciamiento/suscripciones propuestas. Todo licenciamiento debe ser establecido a nombre del Ministerio de Salud Pública del Ecuador.
Se debe instalar en los respectivos servidores la última versión liberada y soportada por el fabricante del Sistema hiérconvergente. (adjuntar certificado)
El Sistema hiperconvergente debe incluir y venir precargado de fábrica con el hipervisor, de modo de minimizar los tiempos de puesta en marcha y debe ser 100% compatibles plataformas de virtualización (VMWARE).
El fabricante del Sistema Hiperconvergente debe proveer el soporte integrado de la capa de virtualización de cómputo.
El Hipervisor debe disponer de funcionalidades de alta disponibilidad.
La solución deberá permitir entregar estadísticas completas sobre las máquinas virtuales, como consumos de CPU, RAM y Almacenamiento, así como los IOPs de lectura/escritura y latencias.
El sistema hiperconvergente debe incluir un software integrado de virtualización de almacenamiento. El proveedor deberá detallar las especificaciones de software integrado.
El fabricante del Sistema hiperconvergente debe proveer el soporte integrado de la capa de virtualización de almacenamiento.

La administración de la virtualización de almacenamiento debe ser integrada a la administración de servidores virtuales y no ser una consola independiente.
El sistema de almacenamiento debe manejar como políticas características mínimas como: ● Desempeño ● Nivel de protección ● Calidad de Servicio Estas características deben tener la granularidad de máquina virtuales.
Garantía de fabrica: debe ser de 3 años
Garantía extendida por 2 años: es el servicio pagado post garantía de fábrica
Durante la vida útil del equipamiento se deberá garantizar soporte por cinco (5) años en la modalidad 7x24x4 (7días a la semana, 24 horas y 4 horas que aseguren la operatividad de la plataforma) acorde al SLA TABLA DE VIDA ÚTIL Y % DE COSTO DEL MANTENIMIENTO Y FRECUENCIA DEL MANTENIMIENTO
El fabricante del Sistema hiperconvergente debe proveer el soporte integrado acorde al SLA de estas aplicaciones de servicios de almacenamiento, mientras dure la garantía técnica de la solución.
En cuanto a capacidades del Sistema hiperconvergente, se debe proveer la funcionalidad de alarmas preventivas y automáticas en caso de falla de componentes del sistema a través de correo electrónico.
La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada en los nodos que componen la solución, manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información.
El proveedor deberá incluir todos los catálogos de los equipos ofertados en formato digital.
El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de microcódigo (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.
El proveedor, como parte de adquisición del equipamiento, proporcionará un pool de 80 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica), sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el

Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte): ● Hasta 2 horas máximo de tiempo de respuesta para iniciar la solución de incidentes con prioridad alta si el tipo de soporte es remoto y/o telefónico ● Hasta 3-4 horas de tiempo de respuesta para iniciar solución de incidentes con prioridad alta si el soporte se hace en sitio ● De 5 a 6 horas para iniciar solución de problemas a incidentes con prioridad Moderada, en cualquiera de las modalidades de soporte (sitio, remoto o telefónico) ● Hasta 24 horas para iniciar solución a incidentes de complejidad Baja, en cualquiera de las modalidades del soporte (sitio, telefónico y/o remoto)
El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas: El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

Prioridad	Descripción	Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente	Modalidad de comunicación	Tiempo máximo de diagnóstico del incidente o problema	Forma de Trabajo, para diagnóstico o solución	Tiempo de Cambio de Repuestos y solución a incidentes.
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	4 horas posteriores al resultado del diagnóstico
Media	Herramienta continúa en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	12 horas posteriores al resultado del diagnóstico
Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico

El proveedor deberá incluir la solución de hardware de respaldos, librería de cintas LTO y servidor para instalación del orquestador. El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales hojas técnicas de los servicios o software asociado al servicio, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.

El proveedor deberá incluir una solución de almacenamiento “Stage” para respaldos: El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales hojas técnicas de los servicios o software asociado al servicio, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.

El proveedor deberá incluir el software de orquestación de respaldos, indicando marca y versión. Debe ser la última versión del software disponible por el fabricante. Debe incluir la instalación y configuración de la solución ofertada conforme a las recomendaciones y buenas prácticas

definidas por el fabricante del producto. Deberá soportar las últimas versiones disponibles de los hipervisores, al menos VMWare vSphere 6.5
El Proveedor deberá incluir la configuración de las tareas de respaldo automatizadas para las máquinas virtuales que la DNTIC determine y que se encontrarán desplegadas dentro de la solución Hiperconvergente requerida en este documento. El Proveedor deberá ejecutar pruebas de generación y recuperación de los respaldos, con la finalidad de evidenciar el correcto funcionamiento de la solución y consistencia de los datos generados dentro del proceso de respaldo
La solución deberá incluir funcionalidades de respaldo (backup) y replicación integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada
La solución deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar degradación en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.
La solución de respaldos deberá ser una solución altamente eficaz y preparada para el futuro integrándose en forma extensiva, con las APIs de los fabricantes de infraestructura virtualizada, para la protección de datos.
La solución deberá poder realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una replicación más frecuente.
La solución deberá permitir la recuperación instantánea de las máquinas virtuales, así mismo deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.
El Proveedor será responsable de aplicar/instalar las últimas actualizaciones estables liberadas por el fabricante del producto, en coordinación con la DNTIC del MSP y máximo un mes después de su lanzamiento oficial, mientras dure el periodo de garantía técnica y soporte de fabricante (incluido el periodo de extensión de la garantía técnica y soporte). Todas las actividades descritas en este párrafo no implicarán costos adicionales para el MSP.
El proveedor deberá incluir solución de equipos de seguridad informática tipo firewall de seguridad perimetral de siguiente generación con características de prevención de amenazas avanzadas y de día cero, filtrado web, control de aplicaciones, que incluya instalación, configuración para la gestión de accesos y permisos de los usuarios del Ministerio de Salud Pública y sus políticas de seguridad.
Por la criticidad del equipo, el fabricante del producto ofertado, debe estar en el cuadrante de líderes de Gartner (últimos 5 publicados), para

“Enterprise Network Firewall” o “Firewalls de Redes Empresariales”. (adjuntar documento o link para su verificación). El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls
En proveedor deberá relacionar el diagrama de Hardware y Software de la solución. (Equipos, sistemas operativos, bases de datos, capa media, capa de aplicación y demás componentes que se considere)
La arquitectura propuesta por el proveedor deberá ser escalable (vertical y horizontalmente) garantizando la funcionalidad (Elasticidad).
La configuración y arquitectura de sistemas de la solución implantada deberá estar certificada oficialmente por el fabricante. Se deberá poder validar la legalidad de todos los componentes utilizados en, o por la solución. Si el proveedor es un prestador de servicios oficial de dichos componentes de software, la certificación oficial del proveedor será suficiente.
Se deberá especificar, en caso tal de que el flujo de datos entre los sistemas de MSP y el o los repositorios, que hagan parte de la solución propuesta, se realice hacia o desde nubes públicas, si existen condiciones particulares para la descarga de los dichos datos.
Deberá permitir la monitorización de los diferentes eventos y la definición de alertas proactivas y reactivas. Se deben especificar las componentes particulares a monitorizar adiciona a la memoria, procesador, disco y red.
Deberá estar dimensionada, a nivel de hardware, licencias y software, para todas las funcionalidades definidas en este documento y los requisitos tecnológicos y de seguridad de la información. El proveedor será el responsable de la gestión de la capacidad de la solución a lo largo de la ejecución del contrato (y sus prórrogas).
El proveedor deberá indicar la arquitectura a nivel de infraestructura tecnológica sobre la cual recomienda la implementación de la solución, teniendo presente la elasticidad, flexibilidad, funcionalidad y eficiencia que se busca en el uso de los recursos de hardware y software base.
Soluciones dimensionadas en arquitecturas con contenedores para los casos que el proveedor considere, pueden ser presentadas.
La arquitectura propuesta debe incorporar el concepto de “duplicidad física y lógica” para evitar puntos únicos de fallos, mejorando con ello los parámetros de continuidad y disponibilidad de los servicios ofertados. Se debe garantizar el funcionamiento del producto en componentes de infraestructura en alta disponibilidad.

La solución tecnológica propuesta no sólo debe posibilitar la prestación de los servicios bajo el alcance requeridos, sino que establece además un marco tecnológico adaptable a necesidades futuras de ampliación del modelo.
La solución deberá garantizar el desempeño indiferente del número de usuarios que hagan uso de ella, por lo tanto, se debe especificar los umbrales que manejaría el proveedor para los componentes de cómputo (memoria, procesador y disco)
Se debe garantizar la funcionalidad de la solución en versiones de sistema operativo vigente y su constante actualización de acuerdo con la evolución de este.
Es necesario especificar los diferentes ambientes que debe contemplar la solución con las características y capacidades necesarias que garanticen el funcionamiento eficiente de la plataforma.
Teniendo en cuenta la continuidad de servicio que se debe garantizar frente a esta solución, el proveedor deberá presentar las alternativas de contingencia recomendadas cubriendo todas las capas tecnológicas que componen la solución y esquemas de replicación respectivos.
El proveedor deberá mantener actualizados todos los componentes de hardware a nivel de firmware y componentes de software base de la solución implementada. Así mismo, debe garantizar la compatibilidad de la solución/producto con las actualizaciones que se apliquen a nivel de infraestructura tecnológica (firmware, parches, por ejemplo). Debe anexar las matrices de compatibilidad respectivas.
Los accesos remotos del proveedor deberán usar únicamente la infraestructura de acceso remoto (VPNs) del MSP.
El MSP se reserva el derecho en el momento que lo considere de auditar la seguridad de la infraestructura, plataformas y aplicaciones entregadas como parte del desarrollo de la solución propuesta por el contratista.
Los usuarios finales de RPIS, cuentan con sistema operativo Windows en sus puestos de trabajo, en versiones soportadas por el fabricante Microsoft, la o las aplicaciones que conformen la solución deben tener en cuenta que deben correr sobre estas estaciones de trabajo.
La solución web que se provea, deberá ser capaz de operar sobre los navegadores Internet Explorer y Edge de Microsoft, Chrome y Firefox, en las versiones que la RPIS tenga controladas, es decir, que el proveedor debe validar cuales son las versiones permitidas o soportadas en las entidades de la red; de no existir versiones especificadas por la RPIS, la o las aplicaciones que soportan la solución, deberán mantenerse en constante evolución a la par de los navegadores, sin que esto repercuta en valores adicionales. La solución que se plantee deberá ser responsive,

es decir, que permita su carga, uso y funcionalidad sin pérdida de calidad o de funciones, desde cualquier dispositivo móvil o de escritorio.
Si la solución que se provea requiere de componentes adicionales como complementos, extensiones o plugins, el proveedor será el encargado de asumir los costos a los que haya lugar por su uso y su implementación en los clientes que usen la aplicación o en la creación del componente de distribución, en conjunto con las instrucciones para distribuirlo para el área de operaciones.

APENDICE 4 – MARCO NORMATIVO Y TÉCNICO APLICABLE

Art. 360.- El sistema garantizará, a través de las instituciones que lo conforman, la promoción de la salud, prevención y atención integral, familiar y comunitaria, con base en la atención primaria de salud, articulará los diferentes niveles de atención y promoverá la complementariedad con las medicinas ancestrales y alternativas. La red pública integral de salud será parte del sistema nacional de salud y estará conformada por el conjunto articulado de establecimientos estatales, de la seguridad social y otros proveedores que pertenecen al Estado; con vínculos jurídicos, operativos y de complementariedad.

Art. 361.-El Estado ejercerá la rectoría del sistema, a través de la autoridad sanitaria nacional, quien será responsable de formular la política nacional de salud y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector.

Art. 362.- *(…)* *"Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes, los servicios públicos establecidos estatales de salud serán universales y gratuitos en todos los niveles de atención y comprenderán los procedimientos de diagnóstico, tratamiento, medicamentos y rehabilitación necesarios".*

Art. 363 numeral 7: "Garantizar la disponibilidad y acceso a medicamentos de calidad, seguros y eficaces, regular su comercialización y promover la producción nacional y la utilización de medicamentos genéricos que respondan a las necesidades epidemiológicas de la población. En el acceso a (sic) medicamentos, los intereses de la salud pública prevalecerán sobre los económicos y comerciales".

La Ley Orgánica de Salud, en su artículo 4, dispone: "La autoridad sanitaria nacional es el Ministerio de Salud Pública, entidad a la que corresponde el ejercicio de las funciones de rectoría en salud; así como la responsabilidad de la aplicación, control y vigilancia del cumplimiento de esta ley; y, las normas que dicte para su plena vigencia serán obligatorias".

El Modelo de Atención Integral en Salud (MAIS), establece como uno de sus objetivos estratégicos, el fortalecimiento de la organización territorial de los establecimientos de la Red Pública Integral de Salud, (RPIS), y la ampliación de la oferta a través de la estructuración de redes zonales y distritales que permitan brindar una atención integral e integrada.

Mediante Acuerdo Ministerial 0084 del 30 de octubre del 2020 que menciona:

- Aprobar y autorizar la publicación de la Norma Técnica *"Historia clínica única electrónica"*. y del Manual *"Historia clínica única electrónica".*
- *Disponer que la norma técnica y el manual que con este acuerdo ministerial se aprueban, y sean aplicados con carácter obligatorio por todo el Sistema nacional de Salud.*

Mediante Acuerdo Ministerial 0084 del 13 de noviembre del 2020 que menciona:

- *Art. 1.- Disponer que los profesionales de la salud que laboran en los establecimientos de salud del Sistema Nacional de Salud, utilicen de manera obligatoria la firma electrónica en los documentos clínicos electrónicos que se generen en el ejercicio de sus funciones.*
- *Art 4.- El uso de la firma electrónica en los documentos clínicos electrónicos se aplicará en el marco de la interoperabilidad, entendida esta como la capacidad de los diversos sistemas*

de salud para interactuar con objetivos consensuados y comunes, enmarcado en los estándares de información y protección de datos.

El Acuerdo de la Contraloría General del Estado Nro. 39, publicado en el Registro Oficial Suplemento 87 de 14 de diciembre de 2009, denominado: "*Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que disponga de recursos públicos*" en el grupo 410 "*Tecnología de la Información*" numeral 8 define: "*La unidad de tecnología de la información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización" y literal número 2 "La Unidad de Tecnología de Información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos*".

Mediante **Decreto Ejecutivo No. 1033** para la Adquisición de Fármacos y Otros Bienes Estratégicos en Salud, publicado el 5 de mayo de 2020, en las que se menciona:

- La Red Pública Integral de Salud será parte del Sistema Nacional de Salud y estará conformada por el conjunto articulado de establecimientos estatales, de la seguridad social y con otros proveedores que pertenecen al Estado, con vínculos jurídicos, operativos y de complementariedad.

Decreto 1384 de MINTEL menciona en:

- *Artículo 1: Establecer como política pública el desarrollo de la interoperabilidad gubernamental, que consiste en el esfuerzo mancomunado y permanente de todas las entidades de la Administración Central, dependiente e institucional para compartir e intercambiar entre ellas, por medio de las tecnologías de la información y comunicación, datos e información electrónicos que son necesarios en la prestación de los trámites y servicios ciudadanos que prestan las entidades, así como en la gestión interna e interinstitucional.*
- *Artículo 2.- La interoperabilidad gubernamental entre todas las entidades de la Administración Pública: Central, dependiente e institucional será gestionada y normada por el conjunto de principios, políticas, procesos, procedimientos y estándares en los ámbitos operativo, conceptual y tecnológico que para el efecto dicte la Secretaría Nacional de la Administración Pública.*

Acuerdo Ministerial 1062 se menciona:

- *Art. 4.- La Plataforma de Interoperabilidad está conformada por:*
  - *El Portal Web de Interoperabilidad;*
  - *Los Lenguajes de intercambio de información;*
  - *El Bus de Servicios Gubernamentales (BSG) de la SNAP y otros Buses de Datos generados por las entidades de la ACPID **(...);***
  - *El Catálogo Nacional de Servicios Web Gubernamentales; y,*
  - *Los Sistemas de Información.*

- *Art. 5.- Las entidades de la Administración Pública Central Institucional y Dependiente de la Función Ejecutiva, promoverán y facilitarán el intercambio de datos e información*

electrónica mediante la formulación y ejecución de proyectos conjuntos de interoperabilidad.

Dichos proyectos serán enviados, para revisión de la Secretaría Nacional de la Administración Pública, a fin de garantizar que se desarrollen dentro de las directrices y estándares que especifica la Norma Técnica de Interoperabilidad.

Capítulo V Interoperabilidad Tecnológica

5.2 Obligaciones

1. *Definir la arquitectura de referencia de Interoperabilidad Gubernamental en base a la Arquitectura Orientada a Servicios (En idioma inglés Service-Oriented Architecture - SOA).*
2. *Administrar, operar y mantener la Plataforma Tecnológica de Interoperabilidad Gubernamental.*
3. *Administrar y facilitar la publicación de los servicios informáticos provistos por entidades públicas en el Portal Web de Interoperabilidad.*

Resolución de la DINARDAP 5

Capítulo I

Generalidades

Art. 3.- Ámbito de aplicación. - La presente Resolución será de cumplimiento obligatorio para las siguientes entidades ***que administren una o varias plataformas de servicios de interoperabilidad****:*

1. *Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral,*
2. *Las entidades que tienen a su cargo la seguridad social (…);*

Art. 5.- Obligación de integración. *- Las entidades contempladas en el artículo 3 de la presente Resolución que administren plataformas de servicios de interoperabilidad deberán obligatoriamente integrarse a la Federación de Plataformas de Servicios de Interoperabilidad administrado por la Dirección Nacional de Registro de Datos Públicos.*

Una vez realizada la integración de una Plataforma de Servicios de Interoperabilidad, su catálogo de datos o servicios pasará a formar parte del catálogo único de datos o servicios del Sistema Nacional de Registro de Datos Públicos.

Las entidades que no se hayan integrado o no se encuentren en proceso de integración de sus plataformas de servicios de interoperabilidad a la Federación de Plataformas de Servicios de Interoperabilidad no podrán prestar servicios de interoperabilidad externa.

El **Acuerdo Ministerial Nro. 025-2019**, de fecha 20 de septiembre de 2019, publicado en el Registro Oficial Edición Especial 228 de 10 de enero de 2020, expedido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expide el Esquema Gubernamental de Seguridad de la Información (EGSI) V2.0 en la sección relativa a la Gestión de la Capacidad, señala que se debe realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.

En el marco del Programa Multifase de Mejora de la Calidad en la Prestación de Servicios Sociales Fase I (EC-L1227), el 7 de septiembre de 2018 se celebra entre la REPÚBLICA DEL ECUADOR y el BANCO INTERAMERICANO DE DESARROLLO el contrato de préstamo BID No. 4364 /OC-EC, en donde el Banco otorga un préstamo al Ecuador para la financiación y ejecución del Programa, cuyo objetivo general es contribuir a mejorar la calidad en la prestación de servicios sociales en Ecuador, particularmente en los sectores de educación y salud; siendo el Ministerio de Salud Pública una de las entidades priorizadas para el financiamiento y responsable de la ejecución del Componente Nro. 3 “Mejora de la Calidad en la Prestación de Servicios de Salud”.

Con base en lo establecido en el Reglamento Operativo aprobado por el Banco Interamericano de Desarrollo, se estipula en la sección: "VIII. ASPECTOS PARTICULARES PARA LA EJECUCIÓN DEL COMPONENTE–MSP." "8.1 Los responsables de la ejecución de las actividades asignadas para la ejecución del MSP, serán las áreas responsables de la ejecución de los proyectos de inversión relacionados con los Productos establecidos en la MDR, los cuales se apoyarán en el EDG-MSP." "En la Tabla No. 11 responsables de la ejecución de las actividades del Programa asignadas al MSP", "Producto 3.2.- Equipamiento priorizado para la digitalización en salud (bienes)" como Área Requirente se encuentra la "Dirección Nacional de Tecnologías de la Información".

Mediante el **Acuerdo Ministerial 0324-2019** en disposición transitoria menciona: *“(…) la Coordinación General Administrativa Financiera y la Coordinación General de Planificación y Gestión Estratégica a través de la Dirección Nacional de Gestión de Procesos elaborarán el flujo del proceso para determinar las competencias con sus responsables para la ejecución del Contrato de Préstamo No. 4364/0C-EC, en sus fases preparatoria precontractual, contractual y post contractual…”, en tal virtud y de acuerdo a los memorandos MSP-SNGCSS-BID-2019-0342-M de fecha 29 de marzo de 2019 y MSP-CGAF-2019-0579-M, de fecha 4 de abril de 2019, se aprueba y se socializa que, la DNTIC es el área técnica competente para emitir el informe de necesidad.*

El estatuto orgánico sustitutivo de gestión organizacional por procesos del Ministerio de Salud Pública emitido el 31 de marzo de 2014, en el título V "**Estructura orgánica descriptiva" Capítulo III "Procesos habilitantes de Asesoría" Art. 20 "**Gestión estratégica" describe que la Dirección Nacional de Tecnologías de la Información y Comunicación entre sus atribuciones y responsabilidades se encuentra:

- "*Supervisar la ejecución de los diferentes proyectos a nivel nacional en el área de redes, desarrollo informático y mantenimiento de toda la infraestructura tecnológica al servicio del Ministerio de Salud Pública".*
- *“Dirigir la implementación de normas y estándares tecnológicos para las diferentes unidades de salud;”.*

La Dirección Nacional de Tecnologías de la Información y Comunicaciones tiene las siguientes atribuciones en el Estatuto Orgánico Sustitutivo de Gestión Organizacional por Procesos del Ministerio de Salud Pública:

Administrar, gestionar y supervisar el uso adecuado de la tecnología informática (TIC´s); y,

- Administrar eficiente y eficazmente los recursos informáticos del Ministerio de Salud Pública.

Acuerdo Ministerial 1062

Acuerda:

Expedir la Norma Técnica de Interoperabilidad Gubernamental:

Art. 1.- Disponer el uso obligatorio de las directrices y estándares contenidos en la Norma Técnica de Interoperabilidad Gubernamental, en iniciativas y proyectos que tengan como finalidad la construcción y/o implantación de programas de software gubernamental; sea por ejecución directa por parte de las instituciones que conforman la Administración Pública Central Institucional y Dependiente de la Función Ejecutiva (APCID), o desarrollados a través de procesos de contratación pública.

APENDICE 4 – REFERENCIAS BIBLIOGRÁFICAS

- ISO Standard. Federated health record13606-1:2008 https://www.iso.org/obp/ui/#iso:std:40784:en
- IHE. IT Infrastructure Technical Framework - ITI TF-1:10. http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI _TF_Vol1.pdf
- AGESIC. PDI User guide. http://www.agesic.gub.uy/innovaportal/v/3543/9/agesic/gu ia-de-uso-.html
- INFOWAY.https://infowayconnects.infowayinforoute.ca/index.php/resources/technicaldocuments/architecture
- NEHTA. Personally Controlled Electronic Health Record (PCEHR). https://www.nehta.gov.au/implementationresources
- AHMAC Electronic Prescribing Working Group Meeting Papers for 24 July 2018.
- AHMAC Electronic Prescribing Working Group Meeting Papers for 13 December 2018.
- ATS 4888.1 – 2013 available at https://infostore.saiglobal.com/en-au/Standards/ATS-4888-1-2013119976_SAIG_AS_AS_251436/
- Marco Europeo de Interoperabilidad. 2017. Obtenido de https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.
- Seguridad y políticas y control para sistemas de información federal y organizaciones. Publicación especial NIST 800-53 del Instituto de Estándares y Tecnología. Obtenido de: https://www.nist.gov/publications/security-and-privacycontrols-federal-information-systems-and-organizations-including. Ross, R. S. 2015.
- The Open Group. 2015. Marco de Referencia para Arquitecturas Abiertas (TOGAF) Edición 9.2 Obtenido de: https://publications.opengroup.org/c182?_ga=2.148823923.555217292.1562958922-1863878398.1562867869.