INTEROPERABILIDAD PRESCRIPCIÓN/DISPENSACIÓNRED PÚBLICA INTEGRAL DE SALUD-

LOGÍSTICO

Elaborado por Elisa Zapata,
Consultora
Banco Interamericano de Desarrollo
Ecuador, enero 2021

Tabla de contenido

RECOMENDACIONES FINALES

INTEROPERABILIDAD PRESCRIPCIÓN/DISPENSACIÓN

RED PÚBLICA INTEGRAL DE SALUD-OPERADOR LOGÍSTICO

ECUADOR, ENERO 2021

1. Resumen ejecutivo

Este documento detalla las recomendaciones finales de las mesas de trabajo desarrolladas por el Ministerio de Salud, las entidades de la Red Pública Integral de Salud, el Ministerio de Telecomunicaciones, el Servicio Nacional de Contratación Pública, la Agencia Nacional de Regulación, Control y Vigilancia con el apoyo del Banco Interamericano de Desarrollo. Por lo anterior, se recomienda la lectura de los documentos generados en las mesas de arquitectura, privacidad y seguridad, infraestructura y desarrollo, para una mayor comprensión de las recomendaciones planteadas en el presente documento.

El propósito de este documento es presentar las recomendaciones finales de un Marco de Referencia y Estrategias para la adopción y el uso de sistemas de prescripción, validación, dispensación y administración interoperables e interconectados en la Red Pública Integral de Salud y el Operador Logístico en Ecuador.

Se entiende por Marco de Referencia el grupo de elementos que conforman la base estructural sobre la que se construye un sistema. Para esta consultoría se tuvieron en cuenta elementos de política (políticas nacionales de salud), gestión (clínica, administrativa, logística, de riesgo, de seguridad de la información), normativos (leyes, decretos, resoluciones, y demás, relacionadas con los temas tratados), técnicos (del uso de tecnologías de la información y las comunicaciones en salud), funcionales (funciones de los diferentes actores del sistema de salud, y el apoyo

que los sistemas de HCE y logísticos les ofrece), clínicos (de competencia del prestador de salud) y económicos para la adopción y uso de dichos sistemas a nivel nacional, respetuosos de la privacidad de los ciudadanos y la seguridad de la información.

Estrategias son el conjunto de procesos, pasos y acciones que se deben llevar a cabo en forma definida y ordenada para lograr un propósito o fin determinado. Las recomendaciones presentadas en este documento han sido diseñadas para ser implementadas en forma integral, conjunta, armónica y progresiva, dadas las interdependencias entre los diferentes componentes de las recomendaciones.

Las actividades desarrolladas durante esta consultoría tuvieron como objetivo diseñar la arquitectura de referencia y la guía de implementación de la interoperabilidad en procesos que van desde la prescripción hasta la administración de medicamentos, diseño de la arquitectura de seguridad y privacidad y de infraestructura tecnológica requerida para la implementación de componentes definidos. Durante las actividades realizadas en las mesas de trabajo se obtuvo el diseño del Marco de Referencia y las Estrategias que conforman el paquete de recomendaciones presentadas en este documento. El diseño de este marco de referencia y estrategias estuvo guiado por los requerimientos específicos del Decreto Ejecutivo 1033 (adquisición de fármacos y bienes estratégicos en Ecuador), de las experiencias internacionales en cuanto a la adopción y uso de sistemas de información en salud interoperables e interconectados, y el contexto nacional de las políticas nacionales de salud y de las TIC en el país.

En consecuencia, las recomendaciones presentadas en este documento se han definido de la siguiente manera:

1. Creación de un programa de e-Salud en Ecuador cuyo objetivo principal sea la coordinación del conjunto de acciones de gobierno, incluyendo leyes, resoluciones, decretos, directivos, regulaciones, programas, proyectos y otras acciones normativas, políticas, jurídicas, o de otra índole, que definen la dirección y acción que el país y sus instituciones de salud públicas y privadas deben tomar con respecto a las Tecnologías de la Información y la Comunicación (TICs) que, a modo de herramientas, se emplean en el entorno sanitario en

materia de prevención, diagnóstico, tratamiento, seguimiento, así como en la gestión de la salud.

2. Se sugiere crear un dominio de afinidad para las entidades de la red pública; esto facilita las decisiones de gobierno, de definición de políticas comunes (privacidad, seguridad, autenticación, auditoría, catálogos, uso de metadata, formatos y presentación de datos clínicos, etc.) y gestión de infraestructura común de repositorios y registro.
3. La arquitectura de la solución debe estar basada en modelos federados, pero con gobernanza (cada institución produce sus datos e interopera con un ente rector federado).
4. La información de medicamentos y bienes estratégicos debe interoperar a través de un Bus de Servicios robusto que permita intercambiar información entre los sistemas de prescripción, validación, dispensación y administración de medicamentos y que tenga capacidad de escalar para soportar en un futuro la interoperabilidad de otros datos de salud, como por ejemplo la Historia Clínica Electrónica.
5. Actualmente en el sector salud no existe un mecanismo de identificación única dentro de los diferentes dominios de atención médica, necesarios durante el intercambio de información, por lo cual recomendamos la implementación un esquema y registro de usuarios/pacientes nacional –Enterprise Master Patient Index (EMPI). Esta componente dentro de la arquitectura de interoperabilidad planteada permite el registro, modificación, sincronización y fusión inteligente de los datos del paciente almacenado en los diferentes sistemas de información de las entidades de la red de prestación. El MPI permite validar de forma rápida y fiable el paciente que se está tratando en la entidad, proporcionando además mecanismos para evitar la creación de registros duplicados.
6. Algunos factores como la persistencia de los objetos representados en los flujos de trabajo de los casos de uso de intercambio de información de medicamentos, por el gobierno de la información, por el grado de interactividad de los flujos de trabajo, por la gestión de estados de la prescripción, entre otros factores que se explican con más detalle en este documento, se recomienda usar mensajes para la interoperabilidad, en lugar de documentos.
7. Además de los pacientes, los vocabularios, las instituciones, las prescripciones, los documentos electrónicos y otros objetos de interés dentro del ámbito de la

salud y las tecnologías de la información deben tener un mecanismo de identificación única dentro de los diferentes dominios de atención médica. Para estos fines, la organización HL7 Internacional mediante el uso de estándares ISO, recomienda el uso de identificadores conocidos como OIDs (Object Identifiers). Detallamos en este documento de recomendaciones las mejores prácticas para su uso, dentro del proyecto de interoperabilidad de prescripción de medicamentos y bienes estratégicos.

8. Se deben establecer Políticas de Gestión de la Seguridad, Ciberseguridad y Privacidad de la Información y los lineamientos necesarios para construir un Sistema de Información de Farmacia interoperable seguro y protector de la privacidad.
9. Se debe contar con infraestructura tecnológica alojada en centros de datos seguros situados en el territorio nacional, de acuerdo con las normativas legales y reglamentarias vigentes, cumpliendo con estándares internacionales de seguridad, disponibilidad, confiabilidad e integridad requeridos.

En el capítulo 3 de este documento detallamos a continuación, cada una de estas recomendaciones.

2.Siglas y acrónimos

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

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

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.

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

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.

Actor humano: individuo (médico, farmacéutico, enfermera) que suele utilizar un actor del sistema para realizar una actividad en el ámbito de la farmacia electrónica.

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.

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.

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

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.

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

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

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.

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.

CNMB: Cuadro Nacional de Medicamentos Básicos

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).

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.).

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

HL7 v2.x: 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.

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.

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.

MPI: Master Patient Index. El MPI es un indice maestro de paciente también conocido como EMPI (Enterprise Master Index), es un índice de pacientes de toda la institución)

Es una base de datos que se utiliza a través de una organización de salud para mantener los datos demográficos y médicos esenciales y actuales sobre los pacientes atendidos y gestionados dentro de sus distintos departamentos. 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.

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.

SNOMED-CT significa Nomenclatura Sistematizada de Medicina – Términos Clínicos por sus siglas en inglés. Tiene como propósito ambicioso proporcionarnos todos los conceptos que alguna vez se hayan expresado en el dominio de la medicina en forma no ambigua, es decir, sin riesgo de confusión.

En la actualidad es el vocabulario más rico que existe para codificar hallazgos clínicos, enfermedades, procedimientos, etc. Cubre todo el espectro del dominio de la salud gracias a sus más de 300.000 conceptos, junto con la capacidad de combinarlos y relacionarlos.

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.

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

La conmutación de etiquetas multiprotocolo o **MPLS (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.

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.

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

Una conexión 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.

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.

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.

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.

Un **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.

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).

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.

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.

LAN: Acrónimo de Local Area Network. Grupo de computadoras y otros dispositivos compartidos (como impresoras, módems, grandes discos duros) y dispersos en un área relativamente limitada conectados por enlaces de comunicaciones que permiten a un dispositivo interactuar con cualquier otro en la red.

WAN: Acrónimo de Wide Area Network en inglés. Una red de área amplia, o WAN es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

SLA: Acrónimo de" Service Level Agreement" que significa Acuerdo de nivel de servicio o Garantía de nivel de servicio. Se trata de un contrato firmado entre las partes involucradas en una negociación que determina cuáles son las responsabilidades de cada uno en relación con los servicios contratados.

3. Detalle de las recomendaciones planteadas

La mesa de trabajo interdisciplinaria conformada por representantes técnicos y funcionales de la Red Pública Integral de Salud, funcionarios del Ministerio de Telecomunicaciones, Control Sanitario (ARSA), SERCOP y el Ministerio de Salud con apoyo del Banco Interamericano de Desarrollo ha consensuado en el diseño de una plataforma tecnológica con una arquitectura escalable, que permitirá el intercambio de mensajes entre procesos de prescripción y dispensación y se constituye en la base para escalar hacia iniciativas de interoperabilidad futuras, como es la Historia Clínica Electrónica Nacional. La arquitectura considera las políticas públicas enfocadas a la ciudadanía, contribuyendo a mejorar su calidad de vida, asegurando debidamente la seguridad de la información y protección de datos personales.

Presentamos en este documento las conclusiones del equipo de arquitectura, privacidad y seguridad e infraestructura que son parte del proceso de construcción durante las fases de implementación de procesos y plataformas que soporten las transacciones entre el operador logístico y los centros de prestación de la red.

Las siguientes recomendaciones se proponen, principalmente, para que las entidades de la Red Pública, el Operador Logístico y los dirigentes del sector salud en Ecuador, las consideren como la base para la adaptación de procesos, tecnología y cultura de las organizaciones ante los cambios que presupone el nuevo modelo de compras públicas, las cuales se realizarán de forma centralizada a través del repertorio virtual de medicamentos como forma prioritaria de adquisición de fármacos y bienes estratégicos en salud y que tiene como requisito inicial haber suscrito un contrato de servicios de almacenamiento, distribución y entrega de fármacos o bienes estratégicos, con el operador logístico.

Recomendación 1: Iniciativa de e-Salud de Ecuador:

La efectiva implantación de e-Salud en un entorno complejo como es el de la sanidad requiere: visión, compromiso, liderazgo a los más altos niveles, agenda bien fundamentada y un conjunto de participantes activos y capaces en la base. No es esperable que una estrategia e-Salud en el sector sanitario —que básicamente significa la intercomunicabilidad e interoperabilidad del sistema— pueda ponerse en marcha sin el liderazgo de la autoridad sanitaria al más alto nivel y desde una perspectiva de política de estado despejando incertidumbres y alineando esfuerzos.

No es esperable que una estrategia de este alcance pueda implantarse por un conjunto de proveedores aislados y fragmentados, sin que exista un marco impulsor del proceso desde el propio sistema sanitario. Es por esta razón que consideramos de alta relevancia la creación de un programa ad-hoc en el país, con un equipo de trabajo dedicado en donde convergen los actores implicados y que tenga como objetivo fundamental alinear esfuerzos promover el uso de las Tecnologías de Información y las Comunicaciones (TIC) en el sector de la salud del Ecuador.

Este programa tendrá adicionalmente, la responsabilidad de la definición de estándares y lineamientos de informática médica y el establecimiento del contexto técnico y regulatorio habilitante para hacer posible y segura la historia clínica electrónica nacional.

Debe tener un modelo de gobierno compartido y participativo que represente a los diferentes actores claves del ecosistema de salud, que defina lineamientos estratégicos a través de los cuales se pueda desarrollar una infraestructura de sistemas validados, interoperables y de fácil uso para la educación sanitaria, la prevención de las enfermedades y la asistencia médica, con el fin de avanzar hacia la creación de infraestructuras de una manera coherente que le permita al estado, utilizar la tecnología para alcanzar sus objetivos sanitarios.

Recomendación 2: Un solo dominio de afinidad para la RPIS

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 la RPIS se compromete a cumplir. Algunas de las políticas

a definir son las siguientes: reglas organizacionales (legales, roles y estructurales, básicamente establecidos por el Sistema de Salud), 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, auditoría. Esto facilitará el trabajo en conjunto y la utilización de un agregado común de políticas e infraestructuras para compartir documentos e información clínica de los pacientes e interactuar con el operador logístico.

Recomendación 3: Un modelo federado de registros y repositorios de prescripciones electrónicas

El modelo debe garantizar a las entidades administrar y brindar la custodia de los registros médicos de sus afiliados y al mismo tiempo tener una vista completa de las prescripciones, validaciones, dispensación y administración de medicamentos cuando y donde sea necesario.

En este tipo de interoperabilidad, cada institución producirá sus datos e interopera con un ente rector federado; este ente rector canaliza las transacciones hacia la institución consumidora que solicita los datos y también genera transacciones de actualización de información de una institución a otra.

Recomendación 4: Bus de interoperabilidad

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

i) Seguridad (usuarios autenticación y control de acceso);
ii) Enrutamiento y transformación de mensajes (ESB);
iii) Implementación de estándares sobre interoperabilidad y usabilidad;
iv) Mecanismos de continuación y acceso a datos;
v) Lista acceso a la información (portal);
vi) Conectividad en diferentes niveles;
vii) Herramientas de gestión y administración;

viii) Gobernanza;

ix) Garantizar la privacidad y la protección de datos.

El documento “Arquitectura de Infraestructura” fue desarrollada por esta mesa de trabajo y contiene información detallada de los requerimientos técnicos descritos en este punto.

Recomendación 5: Identificación unívoca de personas en Ecuador

La identificación correcta de las personas es un elemento clave en los entornos de salud compartida; Lograr una HCE nacional depende no sólo del grado de informatización y de madurez que tengan los distintos sistemas de información clínicos, sino de la correcta implementación, gestión y auditoría permanente de sus respectivos Índices Maestros de Pacientes (en inglés: Master Patient Index, MPI), fundamentales para asegurar la identificación unívoca de las personas. Este debe considerarse un requisito previo a la implementación de cualquier Historia Clínica Electrónica e inclusive en esta primera fase de interoperabilidad de farmacia comunitaria y hospitalaria.

La problemática de la duplicación de los registros de identidad de los pacientes en el país tiene consecuencias negativas en la salud. La identificación errónea de personas puede producir la pérdida de información o mala praxis, como, por ejemplo, la no detección de alergias medicamentosas que puede llevar a un error médico.

Las duplicaciones se producen comúnmente por errores humanos en la entrada manual de datos que no son detectados por los sistemas de información y por la posible multiplicidad de números de documentos como la cédula o el documento identidad sin atributos que garantice su unicidad (tipos de documento, número de documentos, país de emisión, por ejemplo).

En Ecuador, los sistemas utilizan como identificador único de personas a números como el documento nacional de identidad. Está probado que estos identificadores no son suficientes para identificar unívocamente a una persona. Cada centro de la red de prestación que hace parte de la RPIS tiene su propio identificador de paciente sin existir control sobre la duplicación de los datos de identificación

relacionados con este. Estos registros con los datos básicos de las personas luego abren la posibilidad de que existan historias clínicas duplicadas.

Por la importancia que tiene este elemento dentro de la arquitectura de interoperabilidad de historia clínica electrónica, sugerimos altamente la elaboración detallada de la implementación de la **Guía de Identificación de Personas en el dominio de Salud de Ecuador**.

Para más información sobre la importancia de implementar un esquema y registro de usuarios/pacientes nacionales – Enterprise Master Patient Index (EMPI) en Ecuador, ver Anexo A

Recomendación 6: La Mensajería HL7 como Estándar de Interoperabilidad en Farmacia

Se sugiere la implementación de mensajería estándar HL7 como método de intercambio de información e instrumento de interoperabilidad en Farmacia, adaptado a la realidad del sector salud en Ecuador.

En el documento "**GUÍA TÉCNICA PARA LA INTEROPERABILIDAD DE LA RPIS CON EL OPERADOR LOGÍSTICO EN EL PROCESO DE COMPRAS DE FÁRMACOS Y BIENES ESTRATÉGICOS EN SALUD**" generado por la mesa de arquitectura, nos centramos en los principales datos intercambiados en el área farmacéutica y tomamos como referencia la versión de mensajería 2.9 de HL7. Esta versión proporciona una serie de mensajes específicos para el dominio de Farmacia, los cuales se encuentran descritos en el capítulo 4 "Order Entry" del estándar, dentro del apartado "Pharmacy/Treatment Trigger Events & Messages". De manera similar y para conseguir un modelo de interoperabilidad completa sugerimos el uso de determinados vocabularios controlados para utilizar dentro de la mensajería como el Nomenclador CNMB (Cuadro Nacional de Medicamentos Básicos) para la codificación de Medicamentos y Principios Activos, La codificación de términos clínicos SNOMED CT (Systematized Nomenclature of Medicine) del College of American Pathologists para la categorización de la parte del cuerpo en que se sitúa la vía de administración y otros datos locales como Profesionales, Farmacias, Establecimientos de Salud, Financiadores.

Recomendación 7: Gestión de OIDs:

Actualmente en el sector salud no existe un mecanismo de identificación única dentro de los diferentes dominios de atención médica, necesarios durante el intercambio de información, no sólo para identificar de manera única a personas, sino también vocabularios, catálogos, instituciones, documentos electrónicos y otros objetos de interés dentro del ámbito de la salud y las tecnologías de la información. Para estos fines, la organización HL7 Internacional mediante el uso de estándares ISO, ha considerado el uso de identificadores conocidos como OIDs (Object Identifiers). Se recomienda que el MSP sea la Autoridad de Asignación Local para la asignación de OIDs en el ámbito de la interoperabilidad de la historia clínica electrónica nacional.

De acuerdo con los estándares, cada OID es creado y registrado por una Autoridad de Asignación local (Ecuador), o internacional en la materia. Cada una de estas autoridades podrá asignar nuevos OID a partir del delegado por las autoridades. Finalmente, una de estas autoridades asigna un único número que corresponde a un nodo en el árbol. Este nodo puede representar una autoridad de registro (en cuyo caso existe un OID que identifica la autoridad) o una instancia de un objeto.

Tomando como base los procedimientos que organizaciones internacionales han establecido para el registro y asignación de OIDs, el Ministerio de Telecomunicaciones y Sociedad de la información (MINTEL) en su calidad de autoridad de asignación de OIDs para Ecuador en el Sistema Nacional de Salud, y el Ministerio de Salud Pública (MSP) como responsable de vigilar el cumplimiento de la Norma Técnica “Historia Clínica Única Electrónica” y como entidad competente en la materia, serán los responsables de validar las solicitud que de OIDs haga cualquier entidad jurídica o persona solicitante. MINTEL será el organismo habilitado para asignar, registrar y publicar los OIDs que considere pertinentes.

MINTEL asignará todos los OID requeridos en el ámbito nacional con fines de intercambio de información en salud, por ejemplo: sistemas de información, vocabularios, identificadores de personas, etc. Con esto se trata de identificar al

sistema y no a cada documento o registro emitido por dicho sistema, es decir, habrá un único OID para identificar al catálogo “Clave Única de Establecimientos de Salud”, más no un OID por cada establecimiento de salud que exista.

Para la atención de solicitudes de nuevos OIDs, el MINTEL hará un análisis exhaustivo que permita determinar si un OID ya existe uno previamente asignado con las mismas características, pero emitido a través de otras fuentes. MINTEL hará públicos los OID en su página de internet www. https://www.telecomunicaciones.gob.ec. La norma ISO cuenta con tres diferentes formas para la representación de un OID, no obstante, el Ministerio de telecomunicaciones, utilizará para la asignación de los identificadores OID, cadenas de caracteres y el valor de esta cadena es lo único que se comunicaría y lo único que el receptor debe considerar. Existen dos razones principales por las cuales, un prestador de servicios de salud u organización desarrolladora de software en salud en su calidad de solicitante debe pedir al MINTEL la asignación de un OID:

- Solicitar un OID que sea de dominio público. Un ejemplo de esta situación, es la solicitud del registro de un OID para la credencial de elector, el cual es un documento de identificación a nivel nacional. –
- Utilizar un OID como un Namespace para identificadores propios del prestador de servicios de salud. En la práctica, cada solicitante a partir del OID que el MSP le asigne, debe generar su propia estrategia de implementación de OIDs en su organización (ver capítulo de sugerencias en el manejo de OIDs), debiendo observar las recomendaciones de esta Guía de Intercambio de Información y mejores prácticas establecidas por los estándares en la generación de OIDs. Un ejemplo es el caso en el que una institución de salud solicite un OID para implementar OIDs que identifiquen a sus diferentes Sistemas de Información de Registros Electrónicos, áreas de servicio, identificadores de órdenes médicas y prescripciones y vocabularios locales.

Es importante reiterar que bajo ninguna circunstancia un OID debe ser cambiado para identificar un objeto diferente al que se le asignó de origen, es decir, los OID no son reciclables.

Uso de los OIDs

El uso específico de OIDs en cada escenario de intercambio de información o especificación técnica, deberá detallarse en su correspondiente Guía de Intercambio de Información.

Los diferentes tipos de identificadores y usos de los mismos que se requieren de manera obligatoria en las diferentes ediciones normativas de estándares como HL7 CDA R2 y HL7 Versión 3 se detallan mediante ejemplos prácticos y reales a continuación, con la finalidad de proporcionar una guía práctica de uso de OIDs en el ámbito de la salud y sus estándares. Los OID se resaltarán con formato de Negritas. Los OIDs que se muestren en cada uno de los ejemplos son de muestra con fines ilustrativos y no son reales. Para más información sobre los diferentes tipos de OIDs para el sector salud, ver Anexo B: Detalles sobre el uso y tipos de OIDs

Recomendación 8: Privacidad y seguridad

Como parte de los esfuerzos realizados por las mesas de trabajo para crear una arquitectura conceptual de privacidad y seguridad para la infraestructura de interoperabilidad de prescripción/dispensación de medicamentos y bienes estratégicos se buscó inicialmente determinar los requisitos necesarios para garantizar una infraestructura segura y que proteja la privacidad, así como los requisitos mínimos de privacidad y seguridad para las entidades de la red pública y el operador logístico que conectarán sus sistemas HIS/EMR/ERP a la Infostructura de interoperabilidad de recetas y dispensaciones.

Cada requisito clasificado como administrativo (los que involucran políticas, acuerdos contractuales y procedimientos), técnico (los que exigen la arquitectura y el despliegue de sistemas de información) o ambos, deben ser considerados como parte de la configuración y administración de las implementaciones de la infraestructura de prescripción y dispensación interoperable. El incumplimiento de ellos puede tener un impacto grave y perjudicial en la privacidad y seguridad de los datos de atención médica en los repositorios de la Infoestructura. Es importante considerar que las salvaguardias técnicas pueden funcionar sin problemas, pero la

privacidad del paciente aún puede verse comprometida si el sistema es administrado por personas que carecen de la capacitación necesaria para garantizar su funcionamiento adecuado y seguro; si sus usuarios no comprenden la naturaleza confidencial de la información a la que acceden y manejan podría verse comprometido el funcionamiento seguro y protector de la privacidad del sistema.

Otras recomendaciones relacionadas con la privacidad y seguridad se relacionan a continuación:

- Es necesario que las organizaciones desarrollen una política de privacidad, la cual debe identificar cómo la organización cumple con los requisitos de privacidad de la red de prestación o dispensación a la que pertenecen y debe ponerse a disposición del público.
- Cada entidad debe identificar a una persona responsable del cumplimiento de la organización con los requisitos de privacidad legales y basados en políticas y para responder a las consultas y quejas de privacidad del personal y el público (generalmente llamado “oficial de privacidad”).
- Las organizaciones deben proteger la información de salud personal que ponen a disposición de las personas que tengan acceso a la información de salud personal o la procese en nombre de la organización; Las organizaciones deben utilizar medios contractuales o de otro tipo para proporcionar un nivel de protección comparable mientras un tercero procesa la información.
- Las organizaciones deberán ser abiertas sobre sus políticas y prácticas con respecto al manejo de la información personal (esta información debe estar fácilmente disponible para las personas); y la información debe estar disponible sobre los siguientes temas en una forma que sea generalmente comprensible:
    - El nombre / cargo y la dirección de la persona a quien se pueden enviar las quejas y consultas;
    - Los medios para obtener acceso a la información personal;
    - Una descripción de la información personal en poder de la organización y una descripción general de su uso;
    - Una copia de cualquier folleto u otra información que explique los estándares, políticas y procedimientos de la organización; y Una

descripción de la información personal puesta a disposición de organizaciones relacionadas.

- Se requiere consentimiento para la recopilación de información personal y el uso o divulgación posterior de esta información, a menos que la recopilación sea requerida o autorizada para realizarse sin consentimiento por ley; generalmente, cuando se requiere consentimiento, puede ser implícito o expreso. En determinadas circunstancias, sin embargo, se requiere específicamente el consentimiento expreso. Consentimiento expreso significa que se solicita expresamente a una persona y se le otorga su permiso para recopilar, usar o divulgar su información médica personal antes de que se lleve a cabo la recopilación, el uso o la divulgación de información. A menudo, esto se logra mediante un formulario de consentimiento por escrito firmado por la persona. El consentimiento expreso también se puede obtener verbalmente. Consentimiento tácito, por el contrario, significa que los proveedores de atención médica pueden asumir que una persona da su consentimiento para la recopilación, uso o divulgación de su información médica personal para la prestación de servicios y tratamiento de atención médica.

- La infoestructura deberá tener funcionalidad que apoye la captura e implementación de directivas de consentimiento y proporcionar un marco adecuado para representar la gama de directivas de consentimiento de acuerdo con las mejores prácticas (previniendo el acceso de usuarios específicos, evitando el acceso a tipos de registros específicos, por ejemplo). Adicionalmente, debe proveer estándares de mensajes de consentimiento para respaldar los requisitos de consentimiento de la Infraestructura de interoperabilidad y garantizar que las directivas de consentimiento se gestionen de manera eficaz.

- Las organizaciones harán todos los esfuerzos razonables para garantizar que se informe a la persona sobre los fines para los que se utilizará y divulgará la información;

- Las organizaciones no requerirán que un individuo dé su consentimiento para la recopilación, uso o divulgación de información más allá de lo requerido para cumplir con los propósitos legítimos y explícitamente especificados;

- Las formas y métodos para obtener el consentimiento pueden variar y se basan, en parte, en expectativas razonables del individuo;

- El individuo puede retirar su consentimiento en cualquier momento, sujeto a restricciones legales o contractuales; cuando una persona retira su consentimiento, la organización debe informarle sobre las implicaciones de esta decisión.

- Las organizaciones no deberán recopilar información personal de forma indiscriminada. Tanto la cantidad como el tipo de información personal recopilada se limitará a lo que sea necesario para cumplir con el propósito de la prescripción, validación y dispensación de medicamentos y bienes estratégicos.

- Las organizaciones deben desarrollar pautas e implementar procesos relacionados con la retención de información personal, incluidos los períodos de retención mínimo y máximo; Las organizaciones solo deben retener la información utilizada para tomar una decisión sobre un individuo el tiempo suficiente para permitirle acceder a la información; la legislación ecuatoriana determinó 7 años como el período mínimo de retención de datos personales.
- Las organizaciones deben poder destruir, borrar o hacer anónima la información que ya no necesitan para cumplir con el propósito de la información.

- Las organizaciones generalmente solo pueden recopilar, usar y divulgar información de salud personal con el consentimiento del paciente a menos que la ley permita o exija lo contrario. Según este modelo, las organizaciones pueden asumir que tienen el consentimiento implícito del paciente para divulgar información médica personal con fines de atención médica y tratamiento (es decir, compartir información dentro del círculo de atención de

un paciente), excepto si la organización es consciente de que la persona ha retenido explícitamente o retirado dicho consentimiento. Además de la atención médica, existe una variedad de "usos secundarios" legítimos para obtener información médica personal, incluida la mejora de la calidad, la investigación de la salud y la vigilancia de la salud pública. Por lo general, la ley permite que estos usos secundarios ocurran sin el consentimiento del paciente, siempre que se cumplan las condiciones específicas (por ejemplo, la aprobación de la junta de ética de la investigación, se proporcione el aviso apropiado, etc.).

- La medida en que la información personal sea precisa, completa y actualizada dependerá del uso de la información y será lo suficientemente precisa, completa y actualizada para minimizar la posibilidad de que se utilice información inapropiada para tomar una decisión. sobre el individuo; La infraestructura de interoperabilidad deberá incluir mecanismos para mantener la precisión de la información de salud personal que contiene y permitir la corrección de datos que se determinen que son inexactos.

- Las garantías de seguridad protegerán la información personal contra pérdida o robo, así como acceso, divulgación, copia, uso o modificación no autorizados;

- La información se protegerá independientemente del formato en el que se mantenga;

- La naturaleza de las salvaguardas variará dependiendo de la sensibilidad de la información. La información más sensible estará salvaguardada por un mayor nivel de protección;

- Los métodos de protección deben incluir medidas físicas, organizativas y tecnológicas;

- Las organizaciones deben concientizar a los usuarios de la importancia de mantener la confidencialidad de la información;

- Se debe tener cuidado para evitar el acceso no autorizado a la información durante la eliminación o destrucción

- Los mecanismos de seguridad provistos por la infraestructura de interoperabilidad deberán proveer funcionalidad para controlar el acceso arbitrario a los registros de los pacientes por parte de proveedores de atención médica u operador logístico que no estén relacionados con la prescripción o dispensación de medicamentos y bienes estratégicos, proteger adecuadamente la información y mantener la disponibilidad de los sistemas críticos de infraestructura ante perturbaciones ambientales, desastres o ataques de denegación de servicio.

- A nivel de seguridad se recomienda que las aplicaciones de usuario, debe preservar las restricciones de los sistemas origen: los sistemas origen enviarán toda la información que se defina y el nivel de seguridad sobre la misma. Los requisitos de seguridad a implantar serán los establecidos para sistemas de nivel alto en el marco legal vigente, así como las Políticas, Normas, Estándares y Lineamientos de Seguridad de la RPIS y las leyes de protección de datos vigentes en Ecuador.

- Todas las componentes de la infraestructura (repositorio, portal, aplicaciones, etc.) deberá cumplir con las dimensiones: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad en el procesamiento, almacenamiento y transporte de la información.

Recomendación 9: Infraestructura:

Los sistemas informáticos deben estar alojados en centros de datos seguros situados en territorio nacional, de acuerdo a las normativas legales y reglamentarias vigentes, cumpliendo con estándares internacionales de tal manera que se garanticen los niveles de disponibilidad, confiabilidad e integridad requeridos y que cumplan al menos con los siguientes requerimientos:

- **Telecomunicaciones:**

Los sistemas críticos de telecomunicaciones, cableado, firewall, IPS, routers, switches LAN y switches SAN deben ser redundantes.

- **Arquitectura y Estructura:** El sistema estructural del edificio debe ser de acero o de hormigón. Como mínimo, la estructura del edificio debe estar clasificado como mínimo de Tier III, diseñado para soportar cargas de viento de acuerdo con los códigos de construcción aplicables para la ubicación en cuestión y de conformidad con las disposiciones de las estructuras designadas como instalaciones esenciales (por ejemplo, construcción de Clasificación III del Código Internacional de la Construcción). La razón fundamental para que se haga una distinción entre estos dos subdominios radica en lo siguiente:
    - Debe prever protección contra los principales eventos físicos, intencionales o accidentales, naturales o artificiales, que podrían causar una falla en el mismo.
    - Es requerido control de acceso físico, muros exteriores sin ventana, seguridad perimetral, CCTV y protección contra incendio.

- **Electricidad:**
    - Se debe contar con un sistema generador de energía eléctrica con capacidad suficiente para abastecer todo el centro de datos.
    - Se debe contar con sistemas de alimentación ininterrumpida redundantes.
    - Se deben implementar unidades de distribución de energía (PDU) redundantes.
    - Para energizar los racks se deben implementar circuitos eléctricos redundantes y de tal manera que el fallo de uno de ellos no afecte a más de un rack.
- **Mecánica:**
    - El sistema de climatización debe implementarse con varias unidades de aire acondicionado cuya capacidad de refrigeración combinada mantenga constante la temperatura del espacio crítico y la humedad relativa a las condiciones de diseño.

- El sistema de climatización debe contar con una redundancia que garantice los niveles de temperatura y humedad relativa en caso de falla o mantenimiento de uno de sus componentes.
- Los sistemas de aire acondicionado deben estar diseñados para un funcionamiento continuo 7 días/24 horas/365 días/año.
- El sistema de climatización debe ser alimentado por el generador de energía eléctrica.

- **Control de Acceso y Protección del Centro de Datos:**
  - Se deberá contar con mecanismos de gestión que aseguren la protección y salvaguarda de los componentes físicos y lógicos, incluyendo entre otros la seguridad física, de la red de datos, de la infraestructura, así como protección contra incendios, desastres naturales o riesgos por fallas humanas.
- **Requerimientos de gestión y operación:**
  - Gestión de monitoreo: Se recomienda contar con un sistema de gestión y monitoreo centralizado y con las herramientas necesarias que permitan alertar fallas en componentes críticos.
  - Disponibilidad y niveles de servicio: Se deben definir acuerdos de niveles de servicio con los proveedores que den soporte a los componentes críticos del centro de datos y deben ofrecer cobertura en un régimen de 7 días/24 horas/365 días/año.
- **Ciberseguridad:**

  Los requisitos detallados en el documento de “Privacidad y Seguridad (P&S) de la información en el Sistema de Farmacia Interoperable (PIS)” desarrollado en las mesas de trabajo de arquitectura deben ser considerados, así como las normativas de cada institución que contemple en la ejecución del presente documento

  Se debe contar con la infraestructura tecnológica adecuada para cumplir con los requisitos expresados anteriormente, ya que los datos que se intercambiarán a través de la plataforma de interoperabilidad son un activo nacional y deben estar alojados en centros de datos seguros.

- La plataforma de salud digital 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 de la plataforma. En esta capa física se implementará lo siguiente: La infraestructura como Servicio (IaaS) y Plataforma como servicio (PaaS). Esto permitirá seleccionar la mejor forma de administrar la infraestructura de la solución, optimizando los recursos físicos.
- Las capas lógicas compuesta por la capa de Aplicaciones (Saas) y la Plataforma de Interoperabilidad, hacen referencia a dos visiones de este proyecto: una está orientada a usuarios finales (capa de Aplicaciones) y la otra está orientada a servicios de integración para sistemas de los centros de atención de la red (Plataforma de Interoperabilidad).
- El centro de datos donde se aloje la solución de interoperabilidad debe cumplir un conjunto de requisitos que garanticen su disponibilidad, detallado en Anexo C: Recomendaciones para la ciberseguridad de centros de datos

4. Conclusiones

Las recomendaciones del marco de referencia y estrategias presentadas en este documento buscan fundamentalmente y en forma prioritaria, secuencial y progresiva lograr cumplir 5 grandes metas: Adopción, Uso, Interoperabilidad, Interconectividad e Intercambio de Información. Específicamente, se busca avanzar en forma rápida, la adopción y el uso significativo de sistemas de prescripción, validación, dispensación y administración de medicamentos y bienes estratégicos interoperables e interconectados a nivel nacional, por todos los prestadores de la red pública de salud y el operador logístico, de tal manera que logren los siguientes objetivos:

- Que haya una adopción general, a nivel de todos los prestadores de la red pública de salud del país, de sistemas de HCE que incluyan de manera automatizada y segura los procesos de prescripción y administración electrónica de medicamentos e insumos requeridos en procesos de atención. Que estos sistemas cumplan con unos requisitos mínimos de funcionalidad y estándares electrónicos y que sean seguros y respetuosos de la privacidad del ciudadano.
- Que se establezcan los requisitos básicos de interoperabilidad que los sistemas de información de los centros de la red deben cumplir para interactuar en forma efectiva, oportuna y segura con otros sistemas de historia clínica, con los sistemas de información del operador logístico, con los sistemas de salud pública del país y otros componentes del ecosistema de salud del Ecuador.
- Que se definan los requisitos de interconectividad y de intercambio de información de dichos sistemas para crear una “infoestructura” de salud que asegure el flujo de información multidireccional entre los diferentes actores del ecosistema de salud en forma efectiva, eficiente, apropiada, oportuna y segura

Anexo A: **La Importancia de implementar un esquema y registro de usuarios/pacientes nacional –Enterprise Master Patient Index (EMPI) en Ecuador**

El sector de la asistencia sanitaria en el país se mueve hacia un futuro en el que el intercambio electrónico de información sanitaria será habitual. A medida que nos vamos acercando a este nuevo escenario, existe una mayor necesidad de identificar con exactitud las personas en las distintas jurisdicciones o ámbitos de actuación, para que los proveedores de servicios sanitarios puedan tener una sólida base en la que compartir información sanitaria de pacientes y ofrecer un tratamiento más seguro y rentable.

Por los errores e inconsistencias presentados en la mesa de arquitectura, relacionados con la identificación actual de los pacientes en los sistemas de información, podríamos pensar que la utilización de cualquier número de documento nacional (por ej. DNI o Cédula de Identidad) no alcanza como identificador único de personas. Se describieron varios casos que afirman que ninguna entidad ha demostrado tener suficiente confianza en usar la identificación actual como identificador unívoco del paciente.

Algunas de las limitaciones del número de DNI o Cédula de identidad como identificadores únicos para la salud tienen que ver con la existencia de personas que no cuentan con DNI; por ejemplo, las personas indocumentadas, los recién nacidos (previo a su inscripción), los extranjeros que no lo hayan tramitado, turistas, etc. y aun así necesitan ser representados en un padrón asistencial para ser atendidos en los diferentes efectores del sistema de salud ecuatoriano.

Además, los errores humanos de tipeo y las inconsistencias en los procedimientos de registro son las causas más frecuentes de errores en la asignación de identidad en un registro de Pacientes. Por lo tanto, es necesario contar con un mejor servicio de identificación de personas.

El uso de tecnologías más sofisticadas es fundamental para mejorar la coincidencia de pacientes. Sin embargo, el error humano no se eliminará por completo. Por lo tanto, el establecimiento de políticas y procedimientos (como estándares en la

identificación o rutinas de búsqueda) a seguir por todo el personal es fundamental para la integridad general de los datos. Capacitar al personal en las políticas y procedimientos estándar resultará en menor creación de duplicados en el registro cara a cara con el paciente, y una detección y fusión de registros duplicados más exacta en el proceso de auditoría. Además, monitorear, analizar las tendencias e identificar los errores que ocurren son formas proactivas para identificar problemas de integridad de los datos.

En resumen, el problema de la Identificación Unívoca de Pacientes no está en encontrar un identificador único, ya que ninguno ha demostrado ser perfecto, sino en contar con un proceso estandarizado que asegure un conjunto mínimo de datos que permita la identificación unívoca, con un sistema de auditoría que controle la calidad de los datos, minimizando la posibilidad de errores.

Estándares internacionales de Servicios de Identificación

Los servicios de identificación de personas generan una única lista de personas (Master Patient Index o MPI) dentro de una misma institución o a través de múltiples organizaciones o sistemas de salud, evitando la duplicidad de registros clínicos. El desarrollo del MPI o Tabla Maestra de Personas (que puede incluir a los Pacientes y también al Personal de Salud) está íntimamente relacionado con el rediseño de algunos procesos que aseguren la identificación unívoca de personas en el sistema.

Todo el circuito de identificación de personas (o pacientes) para la creación de un MPI confiable puede dividirse en 3 procesos:

- **Identificación y búsqueda de candidatos:** Servicios centralizados para la identificación de pacientes
- **Registro:** Procesos para la acreditación de la identidad de pacientes
- **Auditoría de calidad:** Auditoría de calidad de datos, procesos y operadores

Es un requisito primordial que cada paciente esté identificado en el MPI local antes de la apertura de su Historia Clínica Electrónica.

Existe un estándar para la identificación unívoca de pacientes mediante un EMPI, provisto por IHE. El perfil **PIX (Patient Identifier Cross-Reference)** soporta la referencia cruzada de identificadores de pacientes que pertenecen a múltiples dominios de identificación. Esta referencia cruzada de identificadores puede ser usada por un servicio de consulta de identificación, con el fin de correlacionar información de un paciente sin importar si este tiene distintos identificadores en diferentes dominios, permitiéndole al personal de salud tener una vista más amplia de la información del paciente. El perfil PIXm (Patient Identifier Cross-Reference for Mobile) es semejante a PIX pero a través de una interfaz RESTful liviana, aprovechando tecnologías fácilmente disponibles para aplicaciones móviles y aplicaciones web ligeras. Bajo este estándar, el Federador es un PIX Manager, es decir, un gestor central de referencias cruzadas de identificadores de pacientes.

Conjunto Mínimo de Datos

Para poder identificar correctamente a cada paciente a nivel nacional, los MPI jurisdiccionales deben recolectar un conjunto estandarizado de datos. El Federador recibe esos datos para buscar, comparar y detectar si se trata del mismo paciente que se registró en distintos dominios.

Sólo se almacenan en el nivel central constantes validadas e inalterables (o modificables en pocos casos) de las personas que forman parte de los dominios y que permanecen en ese estado a lo largo del tiempo. Es decir, un conjunto mínimo de datos que permite identificar unívocamente al paciente. A este conjunto de datos se los llama Set Permanente o Set Mínimo de Datos y está compuesto básicamente por:

- Primer nombre
- Otros nombres
- Primer apellido
- Otros apellidos
- Tipo de documento

- Número de documento
- Sexo
- Fecha de Nacimiento

Por su parte, los registros de pacientes locales almacenan otros datos de los individuos (denominado Set Ampliado), que contempla más información necesaria para la atención y gestión sanitaria local. Esta información no es compartida con los demás dominios ni con el Federador. El Set Ampliado puede incluir información personal como apellido materno, de contacto como dirección, teléfonos, email, y también variables demográficas como etnia, religión u otras que sean necesarias para la atención de salud en ese dominio, pero que por ser datos sensibles no son compartidos, salvo expresa autorización del paciente.

Proceso de registro usando MPI

Poner en marcha un índice maestro de pacientes (MPI) presupone un cambio en los procesos de atención habituales en las entidades de la red, para lo cual es necesario contar con estrategias adecuadas de capacitación al recurso humano involucrado en actividades de registro de pacientes, realizar una adecuada gestión de cambio organizacional y generar estrategias de comunicación para que el afiliado/paciente presente siempre su identificación personal cuando accede a un establecimiento de salud.

El proceso de registro tiene como principal función evitar el ingreso duplicado o fragmentado de la información de los individuos, como así también validar la calidad de la información ingresada en el modelo de conocimiento.

Para que cada entidad de la RPIS pueda sumarse a la red de Interoperabilidad en salud, debe primero adecuar tecnológicamente su maestro de pacientes y seguir el proceso recomendado de Identificación de Pacientes. Desde un punto de vista general, en la siguiente Figura se esquematizan y luego se describen los pasos que debe cumplir.

Buscar un paciente:

El Identificador único del paciente se puede buscar en el MPI, proporcionando datos demográficos del paciente y / o identificadores de pacientes (el ejemplo muestra la consulta por identificador / consulta PIX).

Se presenta una lista de pacientes adecuados que coinciden con los criterios de búsqueda y se puede seleccionar un paciente para su procesamiento posterior. Nota: Dependiendo de la configuración, solo se devuelven los pacientes de un dominio específico, p. Ej. el dominio de afinidad de XDS, que contiene los ID para la gestión de documentos.

Insertar / Admitir Paciente

Los datos demográficos del paciente e identificadores pueden ser ingresados de manera interactiva.

Los datos son enviados al repositorio central de Índice de Pacientes, donde son validados.

Un identificador para el dominio de afinidad XDS (Cross-Enterprise Document Sharing) es automáticamente creado, si éste no existe

En caso de que el paciente coincida con otro existente en el maestro, éste es vinculado o insertado automáticamente a una lista de potenciales duplicados, que pueden ser gestionados en procesos posteriores.

Actualizar Paciente

Los datos demográficos de un paciente pueden ser modificados y enviados al Master Patient Index en cualquier momento.

Gestión de pacientes duplicados

- En el proceso de inserción de pacientes, el sistema identifica los registros potencialmente duplicados y los lleva a una lista
- Esta lista puede ser gestionada de manera interactiva

- Los pacientes pueden ser fusionados en caso de que se verifique la duplicidad.
- o los pacientes pueden ser marcados como únicos, por lo tanto, no van a coincidir de nuevo
- Los pacientes pueden separarse nuevamente, si fueron fusionados erróneamente.

Por la importancia que tiene este elemento dentro de la arquitectura de interoperabilidad de historia clínica electrónica, sugerimos altamente la elaboración detallada de la implementación de la **Guía de Identificación de Personas en el dominio de Salud de Ecuador**.

Anexo B: detalles sobre tipos y usos de OIDs en el sector de salud

i. Documentos

Dentro de la especificación normativa de HL7 CDA, existen muchos elementos en el archivo estructurado que se debe conformar, desde el identificador del documento en sí, hasta el sistema de identificación de profesionales de la salud, pasando por vocabularios o terminologías como LOINC. A continuación, se presenta el ejemplo de la sección de encabezado de un CDA:

Este ejemplo muestra el OID registrado internacionalmente para la identificación del R-MIM de CDA, así como el OID de un sistema de identificación de documentos, el cual asigna un valor a cada documento creado, que para fines del documento se definió como FOLIO ÚNICO DOCUMENTO.

ii. Pacientes

En Ecuador existen varios sistemas de identificación de pacientes, siendo ésta, únicamente la fuente de identificación de los pacientes que asisten a las diferentes instituciones prestadoras de servicios de salud, es decir, el sistema de afiliación que identifica a los pacientes dentro de cada institución, podría ser independiente del sistema de laboratorio, de farmacia, expediente clínico, etc.

CURP: Clave única de registro de población (Ejemplo).

iii. Profesionales de la salud

Podemos identificar como profesionales de la salud a todas aquellas personas que ejercen una profesión, actividad técnica, auxiliar o de especialidad en salud, quedando sujeta a lo establecido en las disposiciones jurídicas aplicables para el ejercicio de dicha actividad, luego entonces tenemos como profesionales de la salud a personal: médico, enfermería, laboratorio, auxiliares, especialistas, etc. Todos estos profesionales necesitan ser identificados dentro de un documento clínico (notas médicas, recetas, resultados de laboratorio, etc.). Existe dentro de la normatividad vigente en materia de expediente clínico nacional una serie de lineamientos que requieren que datos de identificación del profesional de la

salud sean plasmados en una serie de documentos de manera obligatoria

El ejemplo mostrado anteriormente, se ejemplifica el uso de OID para la identificación de profesionales de la salud, que en el caso de Ecuador pueden ser identificados mediante el Registro Médico Profesional, que es un documento legalmente aceptado para la práctica médica. Así mismo, este profesional de la salud puede ser identificado por su Cédula de Identidad y el establecimiento de salud donde presta sus servicios

iv. Lugares o ubicaciones geográficas

Existe información requerida dentro de algunos documentos electrónicos que requieren especificar el lugar dentro de las instalaciones del establecimiento de salud en el que el paciente fue atendido (ejemplo, dispensación hospitalaria). Para este caso, cada organización de salud debe identificar mediante OIDs todos sus "Puntos de Asistencia" (áreas físicas o lugares) donde realiza actividades dentro de sus establecimientos, con el fin de poder contemplar el nivel de granularidad requerido en determinados documentos clínicos que reportan la información generada por dichas actividades en determinados “Puntos de Asistencia”.

v. Organizaciones

En Ecuador existe la normatividad que exige el uso de determinados identificadores para los establecimientos de salud. Algunos establecimientos de salud registrados en documentos electrónicos o mensajes podrían necesitar tener alguna clave local para identificarse, a falta de algún identificador global externo. En estos casos, los identificadores locales deben contar con un OID único que les sirva para identificar el Namespace de identificadores locales de ese establecimiento de salud, es decir, un OID que haga las veces de nodo raíz para ese establecimiento de salud y a partir del cual, se desprendan los demás identificadores a utilizar dentro de su ámbito y contexto local. A continuación, se presenta el ejemplo de una organización de salud siendo identificada mediante un OID y su Clave Única de Identificación del Establecimiento de Salud:

vi. Dispositivos y aplicaciones

Es igual de importante la asignación de OIDs a sistemas de información, principalmente cuando éstos, como herramientas colaborativas, forman parte del proceso de atención médica. Existen casos prácticos en los que dispositivos realizan el procesamiento de una muestra de laboratorio y emiten los resultados de manera automatizada, siendo estos resultados fuente de información para sistemas externos como un Expediente Clínico Electrónico, en esta situación, es necesario identificar el dispositivo origen y el sistema destino, para mantener control y seguridad sobre los flujos de información. Existen incluso situaciones en la que los dispositivos asociados con la prestación de los servicios de salud no sean necesariamente electrónicos, a continuación, se presenta un ejemplo de una entrada dentro de un documento HL7 CDA R2 en el que al paciente se le asigna una silla de ruedas.

vii. Vocabularios

Los OIDs también son utilizados para identificar vocabularios y terminologías internacionales y locales (entre los que destacan los catálogos). Son de gran utilidad en la codificación de documentos electrónicos HL7 CDA y mensajería de HL7 V2.x y V3. Es importante en este sentido tener cuidado de no asignar OIDs a vocabularios que ya cuentan con el mismo. A continuación, se muestra una tabla con algunos vocabularios que cuentan ya con un OID global.

viii. Procesos

Un expediente clínico representa el registro longitudinal de todos los contactos de un paciente con un prestador de servicios de salud, para resolver sus problemas de salud como sus necesidades de apoyo. Con el primer contacto se genera la apertura del expediente clínico y los demás contactos sucesivos alimentan dentro de una serie temporal dicho registro longitudinal. Cada contacto, abre y cierra a su vez un expediente de asistencia que requiere un

identificador OID para enlazar todas las actuaciones que generará el proceso asistencial y referenciar su reporte en los documentos clínicos pertinentes.

ix. Templates

Los Templates (o Plantillas) también pueden ser identificados mediante OIDs. Se recomienda que cada Template posea su propio OID y no se utilicen extensiones. A continuación, se muestra un ejemplo de un documento estructurado que utiliza Templates, entre otros como los de IHE, mismos que son identificados con sus correspondientes OIDs.

Resumen

Como se ha observado en las secciones previas, existen múltiples y variadas formas de hacer uso adecuado de los identificadores OID. Así mismo, se observa y denota la importancia que juegan dentro del intercambio de información entre EMR´s. Sin embargo, las mostradas, no son todas las posibles aplicaciones que pueden tener los OIDs, existen aún algunas otras como: identificación de Secciones (Sections), Entradas (Entries), Órdenes (Orders), Encuentros (Encounters) y Referencias Externas (External References) dentro de documentos electrónicos estructurados, mensajería, etc.

Anexo C: Recomendaciones para Ciberseguridad de Centros de Datos

- El centro de datos será el centro neurálgico donde se ubicarán las componentes tecnológicas, de control y de comunicaciones requeridos para que los establecimientos de salud de la RPIS y el Operador Logístico puedan realizar el intercambio de información en los procesos de prescripción, validación y dispensación de medicamentos y bienes estratégicos, por lo que no deberán interrumpirse en ninguna circunstancia. Para garantizar esta situación, se debe implementar una infraestructura redundante.

- Se podrá hacer cualquier labor de mantenimiento a cualquier equipo sin que ello afecte a la continuidad del servicio crítico. Se recomienda tomar la topología TIER III, la cual permite mantenimientos concurrentes sin que sean necesarios apagados para dichos mantenimientos.
- 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
- Se deben implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas, de tal manera que se minimice el riesgo de acceso no autorizado a los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos) y proteger las instalaciones y equipos contra robos, daños o mal uso.
- Implementar controles ambientales en los centros de datos y áreas relacionadas, garantizando la continuidad de las operaciones y reducir los efectos causados por desastres humanos o naturales a través de la implementación de controles ambientales en los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos).
- Debe definirse una política de seguridad del equipamiento. Dicha política puede contener, entre otros, los siguientes puntos: medidas de protección y ubicación del equipamiento crítico de la organización, controles para la protección de amenazas físicas y/o ambientales, mecanismos de monitoreo de condiciones ambientales, medidas para el manejo del equipamiento fuera de las instalaciones de la organización, etc.
- Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos, con el objetivo de lograr una adecuada administración de los componentes críticos alojados en sitios o centros de datos
- Se debe contar con herramientas de monitoreo que implementan protocolos como SNMP, ICMP, HTTP, consulta de apertura de puertos TCP. Las mismas herramientas deben permitir definir umbrales y enviar alarmas por mail, en

tiempo real en un cuadro de mando. Es deseable contar con herramientas para cruzamiento de información de diversas fuentes que permitan emitir alertas preventivas. Se debe establecer una estrategia de recolección de la información, evitando un único punto de falla.

- Se deben gestionar las vulnerabilidades técnicas con el fin de prevenir y mitigar el riesgo de explotación de vulnerabilidades técnicas en los sistemas.
- Gestionar la capacidad de los servicios y recursos que se encuentran operativos: Asegurar que la capacidad de servicios de TI y la infraestructura de TI, sean capaces de cumplir con los objetivos acordados de capacidad y desempeño de manera puntual y efectiva.
- Definir entornos separados para desarrollo, pruebas y producción, con lo que se busca reducir los riesgos de accesos no autorizados o realización de cambios no autorizados en producción, evitar modificaciones no deseadas de archivos o sistemas, evitar fallas de los sistemas.
- Controlar software malicioso, asegurando que la información y los sistemas informáticos que la procesan se encuentren protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros)
- Respaldar la información y realizar pruebas de restauración periódicas, con el objetivo de preservar la información de la organización o en poder de ésta y poder restaurarla en tiempo y forma en caso de necesidad. Se debe definir una política de respaldos donde se detalle claramente los requisitos que posee la organización con relación a las copias de la información y sistemas.
- Se deben conocer los eventos relevantes que se suceden en una aplicación o sistema, por ejemplo, inicios de sesión, fallas en los sistemas, eventos de seguridad, etc. Asegurar la protección de los registros de eventos contra modificaciones y/o accesos no autorizados y asegurar los registros de auditoría.
- Se debe definir una política de auditoría y registro de eventos que incorpore procedimientos para la gestión y protección de los registros de eventos. Se debería contar con un procedimiento asociado a la política donde se identifiquen los eventos de los activos a monitorear y se establezcan umbrales tolerables para estos (por ejemplo, tiempo de espera para una aplicación Web, etc.). Se deben identificar las herramientas que se utilizarán para realizar el monitoreo.

- Gestionar la instalación de software: Se recomienda definir procedimientos sobre la instalación de software y difundirlo a los usuarios y/o todo aquel interesado que se considere pertinente
- Se debe asegurar la protección de la información en las redes: Debe existir segregación a nivel de servicios de información para lo cual debe definirse una política de segregación de redes donde se contemplen al menos los siguientes puntos: Definición de los perímetros de cada dominio o segmento mediante, por ejemplo: firewalls o routers de filtrado, definiendo el tráfico por defecto entre segmentos, definición de alertas de tráfico no autorizado y alineación con la política y procedimientos de gestión de incidentes y monitoreo. Se debe contar con diagrama/s de red actualizado/s
- Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización, con el objetivo de mantener la seguridad de la información que se intercambia o transfiere dentro de la organización y con cualquier entidad externa a la misma. Establecer el marco en el cual se intercambiará información desde y con la organización.
- Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software: Dentro de la metodología de gestión de proyectos de sistemas de información, debe contemplarse los requisitos de seguridad de la información, formando parte de la especificación de requisitos para un nuevo sistema o bien modificaciones en los sistemas existentes. Es recomendable establecer los requisitos de seguridad en etapas tempranas para lograr sistemas más eficaces y eficientes.
- Se deben definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos. Contar con acuerdos de niveles de servicios que permitan nivelar las expectativas y responder con la calidad establecida y en los tiempos establecidos
- Todo sistema, servicio y equipamiento crítico del centro de datos debe contar con soporte de mantenimiento y recambio de partes o, en su defecto, con un plan acción en caso de falla. Se debe establecer el régimen de cobertura para los servicios críticos de acuerdo a las necesidades de la organización. La administración de infraestructura del centro de datos requiere atención en modalidad 7x24 (o la que mejor se adapte a las necesidades del negocio).

- Se debe establecer un procedimiento de supervisión de los niveles de desempeño del servicio, en concordancia con los SLAs y los contratos. Debe evaluarse la posibilidad de realizar auditorías de los proveedores y, en función de sus resultados, reevaluar riesgos frente a cambios en los servicios de los proveedores.
- Se debe planificar la gestión de los incidentes de seguridad de la información de tal manera que se pueda prevenir y mitigar el impacto de los incidentes de seguridad de la información. Se debe definir una política de gestión de incidentes de seguridad de la información
- La organización debe ser capaz de lograr una adecuada evaluación de daños (imagen, económicos, operativos, legales, etc.) conjuntamente con una evaluación de costo y esfuerzo para la recuperación. En caso de que corresponda, se debe ejecutar el plan de recuperación y contingencia, para lo cual debe establecer los mecanismos para recuperarse luego de un incidente
- Debe contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.
- Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia. Se deben implementar mecanismos que aseguren el adecuado funcionamiento de la red ante un posible fallo de equipamiento crítico de telecomunicaciones. Esto puede resolverse mediante redundancia, protocolos, etc.