Privacidad y Seguridad (P&S) de la información en el Sistema de Farmacia Interoperable (PIS)

MESA ARQUITECTURA RPIS

Ecuador, noviembre 2020

1. TABLA DE CONTENIDOS

DERECHOS RESERVADOS

1. INTRODUCCION

Este documento describe la arquitectura conceptual necesaria para garantizar que se cumplan los requisitos de privacidad y seguridad (P&S) para un sistema de farmacia interoperable e incluye una descripción de los servicios de TI que se convertirán en componentes centrales de la estructura de información de registros médicos electrónicos de Ecuador.

1.1. OBJETIVO

Este informe tiene varios objetivos:

1. Definir conceptos de conexiones confiables para el intercambio de mensajes entre la RPIS y el operador logístico;
2. Delinear los activos de información que deben protegerse y el nivel de seguridad que debe cumplirse;
3. Especificar los principios de diseño que se aplicarán a la arquitectura conceptual P&S;
4. Proporcionar una visión interjurisdiccional de los servicios específicos de privacidad y seguridad en apoyo de red de farmacias comunitarias y hospitalarias interoperables; y
5. Servir como documento de referencia para la comunidad ecuatoriana de tecnologías de la información de la salud.

1.2. ALCANCE

El alcance de este trabajo incluye todo lo siguiente:

1. Una delimitación de los activos de información que deben protegerse y la sensibilidad de cada activo en términos de confidencialidad, integridad y disponibilidad;
2. Un análisis y recomendación de todos los servicios de seguridad P&S que se necesitan para construir un **Sistema de Información de Farmacia (PIS)** interoperable seguro y protector de la privacidad. Los servicios incluyen los que necesita el propio Sistema de Farmacia y los que especifican puntos de conexión con servicios externos, como los sistemas de punto de servicio (POS) y los usuarios del PIS (proveedores de atención médica, personal de asistencia sanitaria, operador logístico, etc.)
3. Ejemplos de flujo de procesos para los principales componentes arquitectónicos;
4. Todo lo siguiente se describirá en detalle:
    a. **Identificación de usuario**: establecer una identidad válida y única para cada usuario de PIS;
    b. **Autenticación**: validar la identidad de los usuarios o dispositivos de PIS en cada acceso al sistema, transacción o mensaje

c. **Control de acceso (gestión de privilegios y autorización de usuarios):** protegiendo la confidencialidad e integridad de los activos de información de PIS al evitar el acceso y uso no autorizados.
d. **Protección de la identidad y seudonimización**: mecanismos de separación, al mayor en la medida de lo posible, de la información personal que identifica de forma única al paciente / personas a partir de información sanitaria relacionada con el tratamiento, diagnóstico, etc.
e. **Anonimización:** Asegurar que los datos agregados estén disponibles para la investigación y la vigilancia de la salud pública que proteja la privacidad de los pacientes / personas en la mayor medida posible.
f. **Confidencialidad:** garantizar que la información no esté disponible o divulgada a personas, entidades o procesos no autorizados.
g. **Integridad del sistema y de los datos**: Asegurarse de que el contenido de cada transacción o mensaje no se haya alterado o destruido de manera no autorizada.
h. **Disponibilidad:** garantizar que los activos de información estén siempre disponibles de manera oportuna y confiable cuando los usuarios y dispositivos autorizados de PIS los necesiten.
i. **Auditoría y Control**: establecer la responsabilidad del procesamiento de transacciones mediante la creación de un registro permanente del historial de transacciones y mensajes.

Este documento no hace recomendaciones sobre tecnologías, proveedores o productos específicos.

La seguridad de la red es una responsabilidad jurisdiccional y no se discutirá en este documento. La arquitectura de P&S no depende de los servicios o protocolos de seguridad de la red para mantener la confidencialidad o integridad de la información personal de los pacientes, que atraviesa cualquier red a la que esté conectado el PIS.

La seguridad del servidor, la administración de vulnerabilidades y la administración de cambios también son responsabilidades jurisdiccionales y, si bien son esenciales para la seguridad general, no se discutirán en este documento.

1.3. SUPUESTOS

A lo largo del documento, las suposiciones están resaltadas y numeradas consecutivamente para facilitar la referencia. Si en el futuro uno o más de estos supuestos ya no se cumplen, el impacto en la arquitectura necesitará una revisión cuidadosa y la arquitectura en sí puede necesitar una revisión.

- Todo el PIS se construirá sobre una arquitectura orientada a servicios basada en mensajes.

- Los custodios de la información médica serán responsables de la seguridad de cualquier información médica personal (PHI) descargada del PIS a sus sistemas de punto de servicio (EMR/HIS). Una vez que el PIS ha proporcionado la información solicitada a un sistema local, el custodio / fideicomisario de ese sistema asume la responsabilidad de custodia para mantener la privacidad y seguridad de la información.
- Los sistemas HIS/EMR que se conectan al PIS deben cumplir de manera demostrable con las políticas y estándares de seguridad publicados y aprobados por la autoridad jurisdiccional de la Salud (MSP), responsable del funcionamiento del PIS en una jurisdicción determinada.
- Las implementaciones del PIS existen dentro de un modelo uniforme de alta confianza. Puede que no ocurra lo mismo con los sistemas HIS/EMR que se conectan al PIS.
- Se implementarán prácticas rigurosas de gestión de cambios y gestión de vulnerabilidades para redes, hardware y software (por ejemplo, firewalls, gestión de parches).
- La seguridad del malware se ejecutará en todos los servidores de PIS.
- No todos los servicios de P&S descritos en este documento estarán operativos en la implementación de la PIS en todas las jurisdicciones, ya que algunos no son actualmente requeridos por las obligaciones legislativas de cada jurisdicción. Todos los servicios de PIS estarán operativos en al menos algunas jurisdicciones.
- La infraestructura de mensajería de servicios comunes de PIS se diseñará para permitir el acuse de recibo del mensaje.
- Para garantizar que los proveedores de atención médica confíen en el sistema de mensajería que brindan los servicios comunes de PIS, los servicios comunes de PIS intentarán incansablemente la entrega de mensajes hasta que se acuse recibo o hasta que el servicio de notificación de servicios comunes de PIS notifique con éxito a una entidad apropiada sobre la falla en la entrega de mensajes.
- Cada implementación de la PIS almacenará la información médica personal (PHI) bajo el gobierno de la jurisdicción de implementación.

2. GLOSARIO Y ABREVIATURAS

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

- **Autenticación** - corroboración de que la fuente de los datos es la declarada, basada en la información utilizada para establecer la validez de una identidad declarada (ISO 7498-2)
- **Token de autenticación** - Un token de autenticación es una cadena u objeto codificado en binario y protegido criptográficamente que contiene información mínima del usuario, una marca de tiempo y una fecha de vencimiento. La PIS la crea después de haber autenticado a un usuario por primera vez como parte del proceso de inicio de sesión. Este token luego se devuelve al sistema del usuario para ser

utilizado para el acceso posterior a las funciones de EHR durante esa sesión sin que el usuario tenga que volver a iniciar sesión.

- **Disponibilidad** - la propiedad de ser accesible y utilizable a pedido de una entidad autorizada (ISO 7498-2)
- **Arquitectura conceptual** - Una arquitectura conceptual proporciona una vista de los servicios clave de alto nivel y los repositorios de datos y dónde se alojarán en la empresa. La arquitectura conceptual de PIS describe los diversos sistemas que deben existir para permitir la creación de un Sistema de Farmacias ambulatorias y hospitalarias interoperables. Una arquitectura conceptual no hace suposiciones sobre la ubicación física de los servidores o servicios.
- **Confidencialidad** - la propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados (ISO 7498-2).
- **Consentimiento presunto** - En el contexto de un requisito legal, significa que no importa si el paciente / persona realmente ha dado su consentimiento; la ley permite que las organizaciones actúen como si el paciente o la persona hubieran dado su consentimiento;
- **Estado futuro deseado de la arquitectura conceptual P&S** - una arquitectura P&S madura donde se ha implementado una estructura de información EHR integrada y totalmente interoperable en todas (o la mayoría) de las jurisdicciones sanitarias de Ecuador. El estado futuro deseado presupone que la mayoría de los sistemas EMR/HIS en uso se han construido, actualizado o complementado para integrarse sin problemas con el PIS. Idealmente, este estado futuro se logrará dentro de varios años, aunque el retiro del servicio de los sistemas heredados obsoletos, sabemos que no es una tarea fácil de lograr en la atención médica de manera oportuna.
- **Divulgación de PHI** - significa poner a disposición información médica personal o divulgarla a otro custodio de información médica, fideicomisario oa otra persona, pero no incluye el uso de la información.
- **Colección de PHI** - significa recopilar, adquirir, recibir u obtener información médica personal por cualquier medio de cualquier fuente.
- **Repositorio de dominio** - " Un repositorio de dominio es un componente de un PIS que almacena, gestiona y conserva un subconjunto clínico específico de datos, normalmente a nivel jurisdiccional. Estos también pueden ser sistemas operativos a nivel de dominio para la jurisdicción determinada. Los dominios de datos clave reconocidos como parte de una HCE son los medicamentos, el laboratorio y las imágenes de diagnóstico , por ejemplo.
- **Gestión de usuarios de confianza de PIS**. —Registro de usuario (es decir, administración de identidad), administración de privilegios (inscripción para acceder a servicios específicos de PIS) y autenticación de usuario.
- **Historia clínica electrónica** - un registro electrónico que proporciona a cada individuo en Ecuador un registro de por vida seguro y privado de su historial médico clave y su atención dentro del sistema de salud. El registro está disponible electrónicamente para los proveedores de atención médica autorizados y para el individuo en cualquier lugar y en cualquier momento para respaldar una atención de alta calidad. En una infraestructura de registro electrónico de salud, el EHR es el componente central que almacena, mantiene y administra información clínica sobre pacientes / personas. La extensión de la información clínica sustentada por el

componente EHR puede variar en función de la presencia o ausencia de repositorios de dominio en una jurisdicción determinada.

- **Infraestructura de historia clínica electrónica (EHRi)** - una colección de componentes comunes y reutilizables en apoyo de un conjunto diverso de aplicaciones de gestión de información sanitaria. Consiste en soluciones de software para EHR, definiciones de datos para EHR y estándares de mensajería para EHR.
- **Consentimiento expreso -** Un acuerdo voluntario con lo que se está haciendo o propuesto que es inequívoco y no requiere ninguna inferencia por parte de la organización que solicita el consentimiento.
- **Custodio de información médica** - una persona u organización que recopila, usa o divulga información de salud personal con fines de atención y tratamiento, planificación y administración del sistema de salud o investigación de salud.
- **Integridad -** la propiedad de que los datos no han sido alterados o destruidos de forma no autorizada (ISO 7498-2)
- **Estados provisionales de la arquitectura conceptual P&S** - estados de transición de la arquitectura P&S que admitirá una variedad de métodos para la autenticación de usuarios, control de acceso, gestión de directivas de consentimiento y otros procesos comerciales. Algunos de estos métodos pueden ser menos que ideales en términos de costos y procesos comerciales eficientes, pero son compatibles debido a la obvia necesidad de respaldar y hacer la transición de los sistemas heredados de uso generalizado dentro de la atención médica.
- **Enmascaramiento** - Enmascaramiento es un término que se usa para describir el proceso de restringir el acceso o la transferencia de **PHI**. Por lo general, el enmascaramiento se aplica en la fuente de datos y puede ser anulado, según lo permita la ley, por el custodio que accede (por ejemplo, en situaciones de emergencia de salud).
- **Gestión organizacional de usuarios de confianza.** —La presencia dentro de una organización de atención médica del registro de usuarios (es decir, gestión de identidad), control de acceso y autenticación de usuarios (como lo realiza un sistema EMR/HIS o portal clínico administrado por la organización); todo llevado a cabo con un grado de rigor que permitiría al PIS confiar en los identificadores de usuario asociados con las solicitudes de mensajes HL7 recibidas desde el (los) sistema (s) EMR/HIS de la organización o el portal clínico.
- **ID de organización** - un identificador único asignado a una organización que puede representar múltiples ID de instancia de EMR/HIS.
- **Sistema de punto de servicio (POS)** Los sistemas de aplicación clínica (por ejemplo, HIS, EMR, LIS, RIS/PACS, etc.) que operan en los muchos lugares donde se prestan los servicios de atención médica a pacientes / personas. Estos sistemas pueden tener interfaces de computadora humana o ser equipos médicos que generan datos sobre un usuario que luego se ingresan en el EHR. Estos sistemas son las fuentes de toda la información clínica que componen los datos de EHR. También pueden acceder a los datos del EHR cuando está operativo, así como de sus propios almacenes de datos para proporcionar una vista más completa del historial de salud e información actual de un paciente / persona.
- **ID de instancia del sistema POS** (POSSID): un identificador único asignado a una instalación de un sistema POS.

- **Repudio -** negación por parte de una de las entidades involucradas en una comunicación de haber participado en todo o en parte de la comunicación ISO 7498-2).
- **Seguridad -** Mantener la disponibilidad, confidencialidad, integridad y responsabilidad de los activos de información.
- **Datos críticos de seguridad -** Además de proteger la confidencialidad, integridad y disponibilidad de la PHI, los componentes del EHR también deben proteger muchos otros tipos de datos que son críticos para la seguridad general del sistema. Estos datos incluyen:
    - Identificadores y otros detalles de registro de los usuarios del sistema que podrían ayudar a un atacante a hacerse pasar por un usuario legítimo;
    - Datos utilizados durante la autenticación del usuario;
    - Datos de gestión de privilegios de usuario utilizados en autorización y control de acceso para determinar qué acciones puede realizar un usuario individual y a qué datos puede acceder el usuario;
    - Datos de configuración para firewalls, sistemas de detección de intrusos y otros recursos de software y hardware utilizados para proteger los componentes del EHR; y
    - Claves criptográficas privadas o secretas utilizadas para cifrar o descifrar datos o para generar firmas digitales.

Abreviaturas:

P&S: Privacidad y Seguridad

PIS: Sistema de información de farmacia

HCE: Historia clínica electrónica

CIS: Sistema de información Clínica

EHR: Historia Clínica Electrónica Interoperable

ANS: Servicio de anonimización

CDMS: Servicio de gestión de directivas de consentimiento

DSS: Servicio de firma digital

ES: Servicio de Encripción

FID: Identificador Federado

ESB: Componente fundamental de la arquitectura que provee una capa de acceso a la información de salud

IMS: Servicio de gestión de identidades

IPS: Servicio de protección de identidades

P&SCA: Arquitectura conceptual de Privacidad y Seguridad

PHI: Información personal de salud

PID: Identificador público

POS: Punto de Servicio

POSSID: Identificador de instancia de sistema de punto de servicio (POS)

PSEUDOID: Identificador seudónimo

UAS: Servicio de autenticación de usuarios

3. SEGURIDAD Y PROTECCION DE DATOS CLINICOS

Hace referencia al conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

Atributos de la seguridad de datos clínicos (CIA):

- **Confidencialidad**: La información y/o el acceso a funcionalidades debe estar protegido de accesos no autorizados.
- **Integridad:** La información y/o las funcionalidades no pueden ser modificadas por acceso no autorizados.
- **Disponibilidad:** Garantiza el acceso a la información y/o funciones a los usuarios autorizados bajo diferentes circunstancias, inclusive cuando el sistema se está sometiendo a un ataque.

La información médica es necesaria para poder brindar una buena atención médica. Pero solo aquellos que lo necesiten verán y utilizarán la información.

3.1. NORMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad de la información y seguridad digital.- Según la norma de Historia Clínica Única Electrónica (HCUE) del Ecuador expedido mediante Acuerdo Ministerial 00089-2020 publicado el 13 de noviembre de 2020.

Reglamento de Información Confidencial en Sistema Nacional de Salud expedido mediante **Acuerdo Ministerial 5216** publicado en el Registro Oficial Suplemento Nro. 427 del 29 de enero de 2015.

Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información(8),y los estándares específicos de familia ISO TC215/H7 que es un estándar internacional para los sistemas de información en Salud.

Liderazgo y responsabilidad

En el sector de la salud y la atención, se procesan grandes cantidades de información como base para buenos servicios de salud y atención, investigación e innovación.

La información debe ser procesada para que los servicios de salud y atención se puedan ofrecer de manera responsable y al mismo tiempo salvaguardar la confianza de los ciudadanos en el sector. Una buena seguridad de la información y una buena privacidad son un requisito previo para la digitalización. El sector debe construir y gestionar tecnología, organización y cultura de seguridad sólidas.

Con el desarrollo tecnológico y experiencias de vulnerabilidad de entidades de salud en el mundo, en los últimos años ha habido una mayor atención a la privacidad y seguridad de la información en el sector de la salud y la atención. Como resultado, también se ha creado la necesidad de crear normas modernas y actualizadas para la seguridad y privacidad de la información en el sector de la salud, que sean tecnológicamente neutrales y adaptados a la tecnología actual.

El tema de seguridad debe ser asumida con liderazgo y responsabilidad:

- La alta dirección es responsable de garantizar que la entidad cumpla con los requisitos actuales de seguridad y privacidad de la información
- La alta dirección de la entidad deberá asegurarse de que los roles y funciones se establezcan con los recursos y la competencia suficientes para llevar a cabo las tareas necesarias para cumplir con la responsabilidad
- La entidad decide qué roles y funciones para la seguridad y privacidad de la información son necesarios
- Podríamos pensar que las organizaciones de salud deberían tener su propio director de seguridad de la información u organización de seguridad vinculada a la dirección de la entidad.

3.2. GESTIÓN DEL RIESGO

La RPIS establecerá las medidas técnicas y organizativas adecuadas para gestionar el riesgo de forma satisfactoria. Esto incluye garantizar la confidencialidad, integridad, disponibilidad y solidez de los sistemas de información.

El desarrollo técnico, los costos de implementación y la naturaleza, alcance, propósito y contexto en el que se procesa la información deben tenerse en cuenta al evaluar un nivel aceptable de riesgo. El trabajo con la gestión de riesgos debe tener en cuenta, por ejemplo, el tipo y cantidad de información, el tamaño de la entidad y la complejidad del procesamiento.

La RPIS determinará el nivel de riesgo aceptable en función de los requisitos mínimos de la Norma para la seguridad de la información. La norma debe establecer los siguientes requisitos mínimos generales para la seguridad de la información (confidencialidad, integridad, disponibilidad y solidez):

Requisitos para garantizar la confidencialidad

La RPIS debe salvaguardar el deber de confidencialidad y asegurarse de que personas no autorizadas tengan conocimiento de la información.

- Evitar el acceso no autorizado a información médica y personal y otra información relevante para la seguridad de la información.
- Restringir el acceso del personal autorizado según necesidades de servicio
- Tener una descripción detallada (registros) de todas las personas que han tenido acceso a información médica y personal y otra información importante para la seguridad de la información

Requisitos para garantizar la integridad

La RPIS se asegurará de que la información personal y de salud y otra información relevante para la seguridad de la información esté protegida contra alteraciones o eliminaciones no intencionales o no autorizadas. La integridad es un requisito previo para una buena y sólida atención médica

- Registrar quién ha corregido, registrado, cambiado y eliminado
- Evitar la alteración o eliminación accidental o no autorizada
- Asegurarse de que la información personal y de salud se registre en la persona adecuada
- Asegurarse de que la información médica y personal se ingrese de acuerdo con la codificación y la terminología relevantes.
- Asegurarse de que la información médica y personal sea correcta

Requisitos para garantizar la accesibilidad y la solidez

La RPIS debe asegurarse de que la información médica y personal y otra información relevante para la seguridad de la información esté disponible en el momento adecuado.

- Asegurarse de que la información personal y de salud esté disponible de acuerdo con necesidades de servicio
- Asegurar un funcionamiento sólido y estable de los sistemas de información.
- Asegurar que existen las medidas técnicas y organizativas adecuadas que permitan la prevención, detección, escalabilidad, gestión y recuperación;
- Asegurar que los sistemas de información estén disponibles de acuerdo con requisitos de disponibilidad de la compañía

3.3. PROCESAMIENTO DE DATOS PERSONALES

El tratamiento del paciente presupone el procesamiento de información médica sobre él. a obligación de documentación en el tratamiento de pacientes contribuirá a que los pacientes y usuarios reciban servicios de atención y salud de buena calidad y sea de apoyo para el personal de salud en la prestación de atención médica al paciente individual. La protección de la privacidad del paciente también es importante para la seguridad del paciente,

El sector de la salud tiene varias leyes y regulaciones con reglas especiales sobre el procesamiento de datos de salud y personales.

El deber de confidencialidad del personal de salud es una parte importante de la privacidad y es un requisito previo para la necesaria relación de confianza entre los pacientes y el personal de salud.

Los datos personales solo se pueden procesar cuando la ley lo permite. Todo tratamiento de datos personales debe tener una base legal. En la Ordenanza de privacidad, esto se denomina base de tratamiento.

Antes de que comience el procesamiento de datos personales y de salud e interoperemo, las entidades de la Red Publica deben asegurarse de que tiene una base de procesamiento válida desde la recopilación, el registro, el almacenamiento y la entrega o disponibilización.

3.3.1. DEBERES Y REQUISITOS PARA EL TRATAMIENTO DE DATOS PERSONALES DE SALUD

La RPIS debe facilitar las medidas técnicas y organizativas, para que el inscrito pueda hacer efectivos sus derechos.

Con respecto a los deberes y requisitos tanto de la legislación sobre privacidad destacamos los siguientes:

- **El deber de confidencialidad**

La RPIS se asegurará de que todo el personal que tenga acceso a la información personal y de salud y otra información sujeta al deber de confidencialidad sea consciente de su deber de confidencialidad. Normalmente la violación del deber de confidencialidad es una desviación y está asociada con sanciones administrativas y penales.

- **Información al interesado**

  La RPIS tiene el deber de proporcionar información al interesado de forma concisa, abierta, comprensible y de fácil acceso y en un lenguaje claro y sencillo.

- **Insight**

  El término insight se utiliza en varios contextos. En el de salud, se refiere a que la entidad debe asegurarse de que el interesado pueda acceder a la información registrada sobre sí mismo. Esta información también se aplica al registro de quién y de qué entidad ha adquirido qué información y en qué momento.

  La entidad debe asegurarse de que el interesado pueda conocer qué datos personales sobre sí mismo procesa la entidad. Esto también incluye el conocimiento de quién de otras empresas ha adquirido la información.

- **Corrección y eliminación en el registro sanitario orientado al tratamiento**

  Si la información es incorrecta o engañosa y le resulta onerosa a la persona interesada, o si obviamente no es necesario brindar atención médica, el paciente puede exigir que se elimine la información.

  La corrección se realizará volviendo a ingresar la entrada o agregando una corrección o nota aclaratoria con fecha. La corrección no se realizará mediante la eliminación de información.

  La corrección y eliminación, como regla general, la realizará la persona que haya firmado la información.

  La información introducida sobre la persona equivocada se eliminará a menos que las consideraciones generales indiquen que no se debe eliminar.

- **Hacer que la información esté disponible en el registro sanitario orientado al tratamiento**
  - **El derecho a oponerse a la puesta a disposición y la divulgación**

    El paciente o usuario tiene derecho a oponerse a que la información se divulgue o se ponga a disposición. Esto puede aplicarse a la transferencia o puesta a disposición de información tanto para el propio paciente como para los acompañantes y / o los profesionales sanitarios o a otras entidades. La RPIS tiene la responsabilidad general de garantizar que se protejan los derechos del paciente.

- **Disponibilidad y divulgación de información sanitaria entre entidades**

  A menos que el paciente o el usuario se oponga, el personal de salud deberá proporcionar acceso a la información de salud necesaria y relevante al personal colaborador en la medida necesaria para poder brindar atención médica al paciente de manera responsable.

  Cuando se le da de alta de una institución de salud, el paciente debe tener la oportunidad de indicar a quién debe enviarse la epicrisis.

- **Retención de información personal y de salud**

  La regla principal de la Ordenanza de privacidad es que los datos personales deben almacenarse hasta que se haya cumplido el propósito. Luego, la información debe ¿?? o anonimizarse.

- **Tiempo de almacenamiento al brindar atención médica**

  La información de salud se almacenará hasta que se presuma que ya no será de utilidad para ella debido a la naturaleza de la atención médica. Lo mismo se aplica a la información sobre quién ha tenido acceso o se le ha proporcionado información de salud que está vinculada al nombre o número de identidad (registros) del paciente o usuario.

3.3.2. PRIVACIDAD

La privacidad incorporada es un requisito clave en el intercambio de información. La entidad, tanto el responsable del tratamiento como sus proveedores, debe establecer requisitos y tener en cuenta la privacidad en todas las fases del desarrollo de un sistema o solución. La entidad debe asegurarse de que los sistemas de información cumplan con los principios de privacidad.

3.4. SEGURIDAD DE LA INFORMACIÓN

Este capítulo describe las medidas de seguridad clave. Las medidas de seguridad se seleccionarán sobre la base de evaluaciones de riesgos. La entidad evaluará si es necesario implementar medidas más completas que las descritas en este capítulo.

La mayoría de los requisitos de seguridad se aplican al procesamiento de datos personales y de salud para fines distintos de la prestación de servicios de salud y

atención. La empresa evalúa qué medidas son necesarias (por ejemplo, en control de acceso y registro).

3.4.1. CONTROL DE ACCESOS

La gestión de acceso se trata de cómo se implementa en la entidad los siguientes aspectos:

- Autorización de acceso a los sistemas de información
- Autorización de acceso al registro sanitario orientado al tratamiento, que implica la concesión de permisos para poder leer, registrar, editar, corregir, borrar y / o bloquear información sanitaria y personal
- Autenticación, que asegura la identificación de un usuario autorizado

La entidad debe contar con rutinas de autorización, cambio y terminación del acceso, además de permitir prevenir y afrontar distintos riesgos que pueden presentarse de manera imprevista

Autorización

La entidad es responsable de asegurar que las autorizaciones sean otorgadas, administradas y controladas.

Al otorgar la autorización, se evaluará y salvaguardará el deber legal de confidencialidad.

La autorización otorgada garantizará que el empleado pueda acceder a la información personal y de salud necesaria y relevante de acuerdo con las responsabilidades y tareas del personal, siempre que el deber legal de confidencialidad no lo impida. La autorización se reevaluará cuando haya cambios en las áreas de responsabilidad, condiciones de empleo o ausencias prolongadas.

Autenticación

La autenticación debe garantizar al menos lo siguiente:

- La persona autorizada debe confirmar su identidad de manera segura. La forma segura debe decidirse sobre la base de una evaluación de riesgos.
- Varias personas no deben utilizar los mismos criterios de autenticación.
- La asignación de criterios de autenticación (por ejemplo, nombre de usuario y contraseña) debe realizarse de forma segura.
- El acceso desde la oficina en casa y / o equipos móviles (y redes móviles) debe garantizarse mediante una solución de autenticación segura.
- Todas las contraseñas predeterminadas (configuración de fábrica) de los sistemas y equipos deben cambiarse antes de que comience el procesamiento de los datos personales y de salud.

- Los controles de acceso en red cuenten con la capacidad de identificar una amenaza al sistema, incluso alcanzando a identificar a los responsables de la misma.
- Capacitar a los usuarios de la mejor manera posible acerca de la importancia y el funcionamiento de los distintos tipos de control de acceso de seguridad informática, para que su aplicación sea mucho más certera.

3.4.2. SEGURIDAD FÍSICA Y EQUIPOS DE TIC

Equipo de TIC
Las medidas de seguridad deben evitar que personas no autorizadas accedan a información médica y personal. Esto puede resolverse mediante el control de acceso a las instalaciones con equipo y asegurando el equipo contra el uso indebido o el acceso no autorizado.

Infraestructura
Las medidas de seguridad deben evitar que el personal no autorizado acceda a la infraestructura.

Todos los medios de almacenamiento deben borrarse correctamente cuando se ponen fuera de servicio. En todo caso se debe cumplir con la obligación de archivar la información.

Equipo móvil y oficina en casa
No es posible asegurar las instalaciones para dicho equipo, por lo tanto, el equipo debe asegurarse. Se debe realizar una evaluación de riesgos antes de que se utilicen las soluciones y en caso de cambios que puedan afectar la seguridad de la información. Se establecerán rutinas administrativas para el uso de equipos móviles y oficinas en casa.

La información personal y de salud solo debe almacenarse localmente en el equipo cuando sea necesario en función de las necesidades del servicio, y siempre debe almacenarse encriptada.

Cifrado
Se establecerán medidas técnicas para que toda la comunicación de información personal y de salud fuera del control de la empresa sea encriptada.

Toda comunicación, ya sea por conexión inalámbrica o por líneas, debe estar protegida mediante encriptación.

El cifrado de la información personal y de salud almacenada puede considerarse una medida de seguridad.

Cuando se utilizan redes inalámbricas para el procesamiento de datos personales y de salud, el usuario autorizado debe estar autenticado con una solución de autenticación segura.

3.4.3. OPERACIONES DE TI SEGURAS

Control de configuración

Es un requisito previo que la entidad tenga una visión general del flujo de datos, la comunicación de datos y las integraciones y el control de todos los equipos y software propios utilizados en el procesamiento de datos personales y de salud.
Se debe tener en cuenta lo siguiente:

- La entidad debe asegurarse de que todo el flujo de datos, la comunicación de datos y las integraciones estén mapeados y documentados.
- Solo se utilizarán equipos y software aprobados para el procesamiento de datos personales y de salud. La empresa debe determinar quién tiene la autoridad de aprobación.
- El hardware y el software deben actualizarse para que se sigan las últimas y más actualizadas funciones de seguridad y se utilicen las medidas de seguridad necesarias.
- Deben utilizarse entornos separados para el desarrollo, las pruebas y la producción, de modo que la información personal y de salud utilizada en la prestación de atención médica no se vea afectada por errores en el desarrollo y las pruebas.
- La configuración debe estar protegida contra software malintencionado
- La configuración debe protegerse contra acciones involuntarias.

Gestión de cambios

Todos los cambios significativos para la seguridad de la información en la organización deben documentarse: debe incluir

- Identificación de cambios significativos
- Planificación y pruebas de cambios
- Evaluación de posibles consecuencias
- Formación de usuarios / roles afectados

Copia de seguridad

La gerencia de la entidad debe garantizar la copia de seguridad de la información personal y de salud y otra información que sea necesaria para el restablecimiento de las operaciones normales.

Las copias de seguridad deben mantenerse cerradas y a prueba de fuego y separadas del equipo operativo.

Gestión y manejo de vulnerabilidades técnicas
La gestión y el manejo planes de contingencia

Auditoría de seguridad
El propósito de las auditorías de seguridad es realizar actividades de control y aseguramiento de la calidad de las medidas establecidas y las rutinas establecidas. Debe haber un plan aprobado para auditorías de seguridad.

3.4.4. SEGURIDAD EN LAS COMUNICACIONES

Gestión de la seguridad de la red
La seguridad de la red es una medida clave para garantizar el procesamiento de datos personales y de salud.
La entidad debe definir claramente los requisitos que se aplican a la seguridad de la red, y las medidas que se establezcan deben basarse en una evaluación de riesgos.

Conexión a redes externas
Al conectarse a redes externas, se deben establecer medidas técnicas que aseguren que solo el tráfico permitido expresamente indicado pueda pasar desde el exterior y hacia adentro o viceversa, y que se detenga el resto del tráfico.

Correo electrónico y SMS
La entidad establecerá medidas para evitar que la información de salud, personal y otra información relevante para la seguridad de la información se ponga a disposición mediante correo electrónico y SMS no cifrados u otros canales inseguros.
Si la empresa utiliza canales no cifrados, la empresa debe

- Asegurar mediante medidas técnicas y organizativas que los correos electrónicos no contengan información médica identificable.
- Establecer un registro para comprobar que no se infrinjan las reglas. Las infracciones a las reglas se tratarán como desviaciones y se evaluarán las consecuencias para el personal.
- Evaluar si la información general en SMS y correo electrónico puede dar lugar a una infracción del deber de confidencialidad

Conexión a Internet
La entidad establecerá

- Medidas técnicas que ayudan a prevenir la divulgación no intencional y el acceso no autorizado a la información personal y de salud.
- Registro para comprobar que no se infringen las reglas

4. POLÍTICAS DE PRIVACIDAD Y SEGURIDAD

Antes de que se pueda aplicar cualquier tecnología para hacer cumplir la seguridad o la privacidad, la entidad debe definir las **Políticas de Seguridad y Privacidad** que necesitarán.

Los Perfiles de interoperabilidad están diseñados para ser independientes de las políticas, lo que significa que pueden hacer cumplir casi cualquier política, no hay ninguna restricción para implementarlas.

Estas políticas se componen de muchas capas de políticas externas. Empezando por las políticas de más alto nivel en la comunidad internacional, como la Organización para la Cooperación y el Desarrollo Económico (OCDE). Este nivel más alto también debe respetar los derechos humanos, la ética y las normas.

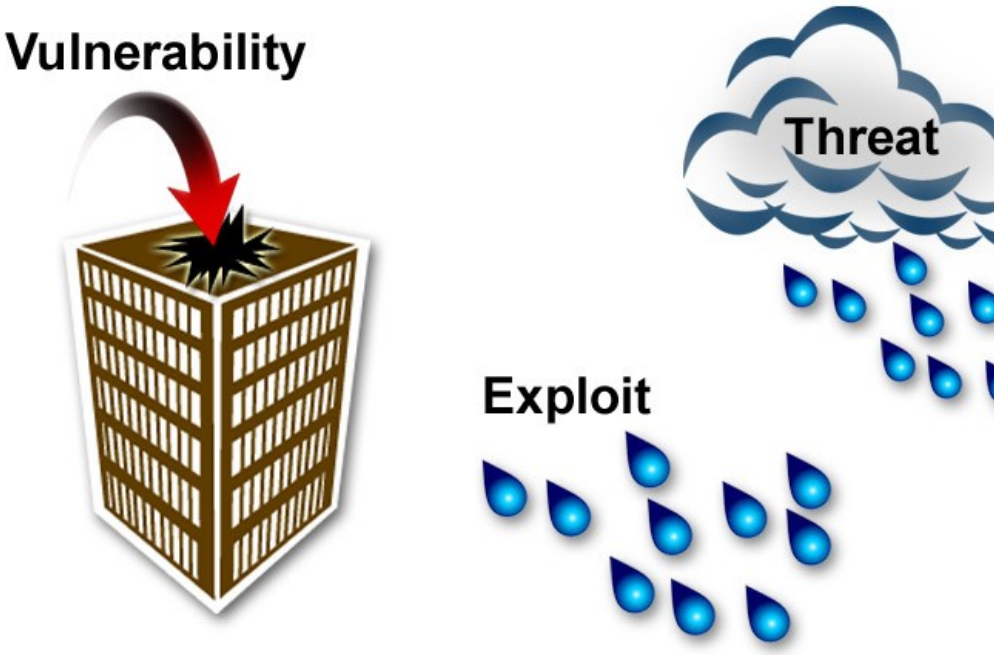
La siguiente capa son las del país, como HIPAA en los EE. UU., EC95 / 46 en Europa y Act 57 en Japón y en Ecuador la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000.

La siguiente capa son las políticas del dominio específico de la industria, en este caso Healthcare. Algunas de las fuentes de esta capa provienen del país, pero también provienen de sociedades profesionales médicas.

Y, finalmente, la entidad debe considerar buenas políticas organizativas, como por ejemplo, las políticas de respaldo y recuperación.

Esta es claramente una descripción general de todas las posibles influencias en las políticas, pero lo importante es aclarar que las políticas deben crearse y redactarse antes de discutir la tecnología. Esto no significa ignorar el hecho de que a veces la tecnología limita las políticas, como veremos más adelante en este documento sobre los Consentimientos de privacidad.

Escenarios de riesgo



La seguridad es el mejor enfoque cuando se utiliza un modelo de evaluación de riesgos que como vimos está enfocado en determinar los riesgos de seguridad, confidencialidad, integridad y disponibilidad.

El nivel de riesgo se mide en términos de una combinación de probabilidad de ocurrencia (probabilidad) y grado de impacto (positivo o negativo) de un evento anticipado.

Imaginémonos el escenario del “agujero en el techo”, el riesgo es que el clima (la amenaza) pueda causar daños a los componentes dentro del edificio, así como al edificio mismo.

Siempre que el informe meteorológico muestre que hay pocas posibilidades de precipitaciones, nuestro nivel de riesgo es bajo.

Sin embargo, este riesgo aumenta a medida que aumenta la probabilidad de lluvias.

Dado que no podemos controlar la amenaza de precipitaciones, mitigamos nuestro riesgo cambiando la vulnerabilidad; arreglamos el agujero en el techo. El costo de arreglar la vulnerabilidad es mucho menor, en este caso, que el daño que causaría la lluvia o la nieve**.**

a) Ejemplos de amenazas: desastre natural, accidente aleatorio, empleado descontento, espionaje de empleados, pirata informático externo indiscriminado, pirata informático externo motivado, externo altamente motivado y financiado.

b) Ejemplos de vulnerabilidades: acceso sin identificación de usuario, acceso sin autenticación de usuario, acceso de usuario a datos que no necesita conocer para su trabajo, interfaz de red abierta.

El riesgo es una evaluación de la probabilidad de que esa amenaza aproveche esa vulnerabilidad. Por lo general, una evaluación de riesgo nos da una probabilidad general de alto, medio y bajo.

El impacto es una evaluación de cuánto daño (daño) resultaría si esa amenaza explotara esa vulnerabilidad (independientemente de cuán improbable sea). Por lo general, una estimación bruta de alto, medio, bajo

4.1. MODELOS DE “ACCOUNTABILITY”

Hay una variación importante de una organización a otra, relacionada con la política que aplican a la rendición de cuentas o “accountability”. Hay dos tipos diferentes de modelos de rendición de cuentas que generalmente se mezclan.

En el modelo de control de acceso, los usuarios simplemente no pueden hacer nada que no deberían hacer.

En el modelo de control de auditoría, el usuario está facultado para ir más allá de lo mínimo que debe hacer por su trabajo, porque hay situaciones en las que se le puede pedir que haga más, por ejemplo, cuando los médicos solo deben acceder a los registros de pacientes a los que están asignados, pero se les da acceso a todos los pacientes para que puedan ayudar más rápidamente con una consulta, atención urgente o incluso una emergencia.

En el sector salud, suele haber una combinación más centrada en los controles de auditoría.

Modelo de control de acceso - Prevención

- Fuertes controles sobre la identificación y autenticación de usuarios
- Control de acceso estricto basado en roles
  - Nadie recibe más derechos de acceso de los que necesita mínimamente
- Típico en un banco

Modelo de control de auditoría - Reacción

- Fuerte control sobre la identificación y autenticación de usuarios
- Control de acceso relajado basado en roles
    - Énfasis en la capacitación y conciencia de la supervisión
    - Dijo lo que normalmente se le permite hacer
    - Con poder para hacer lo correcto cuando sea necesario
- Los registros de auditoría se inspeccionan periódicamente
- Se detecta el abuso y se actúa

Cuidado de la salud: generalmente una mezcla con énfasis en la seguridad del paciente

4.2. POLITICAS DE SEGURIDAD GENERALES PARA LA ARQUITECTURA

El ecosistema distribuido de la arquitectura propuesta para la interoperabilidad entre la RPIS y el operador logístico plantea una serie de retos que deben ser resueltos por las organizaciones en la medida en que sus datos y funcionalidades se hacen disponibles a más aplicaciones y procesos de negocio que pueden encontrarse incluso por fuera de sus fronteras.

La flexibilidad y dinamismo que la adopción de SOA imprime no sólo en términos de negocio sino en términos de TI, permitiendo a las entidades adaptarse con facilidad a condiciones cambiantes, no debe ser afectada por la definición de requerimientos de seguridad que sean implementados de forma rígida y que no puedan ser modificados en la misma medida.

Como parte de las consideraciones de seguridad más relevantes consideramos las siguientes:

- La necesidad de ofrecer interoperabilidad segura de manera que los datos que se comparten a través de los servicios conserven la confidencialidad, integridad y disponibilidad requerida.
- Requerimientos de conexión desde y hacia a otras organizaciones, debidamente administrados, acordados y con la mayor transparencia posible.
- Garantía de cumplimiento de los requerimientos de seguridad que las normatividades y regulaciones internas y externas imponen a las organizaciones.
- La heterogeneidad a nivel tecnológico de los sistemas de la RPIS, entre los que una propuesta basada en servicios busca generar interoperabilidad.
- La diferenciación en los niveles de seguridad requeridos por los servicios cuando son usados de forma independiente o cuando hacen parte de composiciones (orquestaciones, coreografías).
- El manejo independiente de los servicios y la identidad de los consumidores que pueden acceder a ellos.

En este capítulo propondremos las políticas relacionadas de forma general con los retos planteados previamente. Cada política se acompaña de lineamientos, buenas prácticas y estándares que permitan a la RPIS tomar decisiones frente a la identificación y definición de los servicios de seguridad, así como la implementación de los requerimientos de seguridad que como primera medida resuelvan las necesidades de seguridad a nivel corporativo.

Para efectos del presente capítulo las siguientes definiciones serán aplicadas:

- **Política:** Conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Son declaraciones de alto nivel relacionadas en este caso con la protección de información.

  La política perfila las áreas involucradas, indicadores y excepciones y contiene una descripción de alto nivel de los controles que deben ser implementados para proteger la información. Adicionalmente debe hacer referencia a lineamientos y estándares que la soportan.

- **Buena práctica:** Recomendación que ha demostrado en aplicaciones previas buenos resultados en comparación con otras prácticas o actividades.

- **Lineamiento:** Definiciones recomendadas, que no tienen un carácter obligatorio, que ayudan a soportar estándares o sirven como referencia en caso de que no existan estándares aplicables definidos. Deben ser vistos como buenas prácticas que usualmente no son exigidos, pero que son fuertemente recomendados.

- **Estándar:** Documentos que proporcionan requerimientos, especificaciones, guías o características que pueden ser usadas de forma consistente para asegurar que productos, procesos y servicios están ajustados a su propósito. Normalmente son de amplia aceptación y emitidos o respaldados por organizaciones que gozan de reconocimiento a nivel local o internacional. Usualmente contienen controles relacionados con la implementación de hardware, software o tecnología específica.

Considerando las definiciones anteriores, en el presente capítulo se presentan un conjunto de políticas de seguridad agrupadas de acuerdo a cuatro grandes bloques relacionados no solo con los servicios, sino con componentes e infraestructura dentro de una Arquitectura Orientada a Servicios. Los bloques a partir de los cuales se consolidan las políticas son: Alineación con Negocio, Implementación, Operación y Gestión; y corresponden a las secciones planteadas para el entregable de la mesa de arquitectura.

4.2.1. ALINEACION CON EL NEGOCIO

Dentro de la descripción de políticas de seguridad un primer punto a considerar es la necesidad de que las políticas estén alineadas con las necesidades del negocio, que para nuestro caso es permitir el intercambio de información entre las farmacias comunitarias y hospitalarias y entre ellas con el operador logístico. De hecho un

modelo de seguridad se crea y obedece para ofrecerle al negocio los niveles de confianza que se espera de la arquitectura.

4.2.1.1. INTEGRACIÓN DE APLICACIONES

Planteamos una arquitectura con un esquema distribuido para ofrecer capacidades de negocio. Más que de Integración, proponemos un modelo interoperabilidad intrínseca, esto plantea que el software debe ser diseñado y planeado para facilitar la interoperabilidad especialmente entre aplicaciones al interior de las entidades con el operador logístico y entre ellas mismas. El documento de Arquitectura de Seguridad de ISO indica:

> "Los Servicios de Seguridad son funcionalidades que cuando interactúan en un entorno tecnológico, contribuyen a la protección de los recursos de información, asegurando el cumplimiento de las políticas de seguridad de la organización"

A continuación se describen políticas que apoyan la interoperabilidad entre aplicaciones:

Política 1: En la implementación de soluciones basadas en la arquitectura propuesta se debe buscar el cumplimiento de los principios centrales de la seguridad de la información: Disponibilidad, Integridad y Confidencialidad.

La seguridad de la información puede categorizarse a partir de la manera en que los riesgos afectan su confidencialidad, integridad y disponibilidad. La interoperabilidad entre aplicaciones debe considerar todos los aspectos que garanticen que dichos atributos no se vean comprometidos. Para efectos del presente documento se consideran las siguientes definiciones en cada caso:

Disponibilidad: El servicio (proceso, aplicación, sistema) está disponible al consumidor del servicio en el momento requerido.

Confidencialidad: Se define como la protección frente a accesos no autorizados a información confidencial. La confidencialidad cobra mayor relevancia cuando se realiza transferencia de información que no puede hacerse públicamente disponible.

Integridad: Se garantiza que todos los mensajes desde un proveedor llegan inalterados a los consumidores y viceversa.

En la anterior Figura se muestran las características: Disponibilidad, Integridad y Confidencialidad como principios núcleo de la seguridad de la información.

Política 2: El esquema de acceso a los servicios debe implementar un modelo de seguridad si no se ha definido, o extender el modelo actualmente implementado por las aplicaciones que se habilitan como servicios. Este modelo debe orientarse a controlar los nuevos riesgos asociados a la adopción de la arquitectura:

En el esquema tradicional de aplicaciones standalone, la definición de seguridad puede asumir aspectos de seguridad y control interno que no están presentes en la arquitectura propuesta. En muchos casos esta definición interna no es suficiente para lograr los objetivos de seguridad de servicios que pueden ser invocados en diferentes contextos y a diferentes niveles de granularidad: es el caso de servicios y operaciones invocadas desde consumidores con condiciones diferentes, muchas veces en esquemas de composición con delegaciones de identificación complejas y con necesidades de cumplimiento de estándares abiertos, que posiblemente están alejados de los esquemas particulares de definición de seguridad de las aplicaciones existentes.

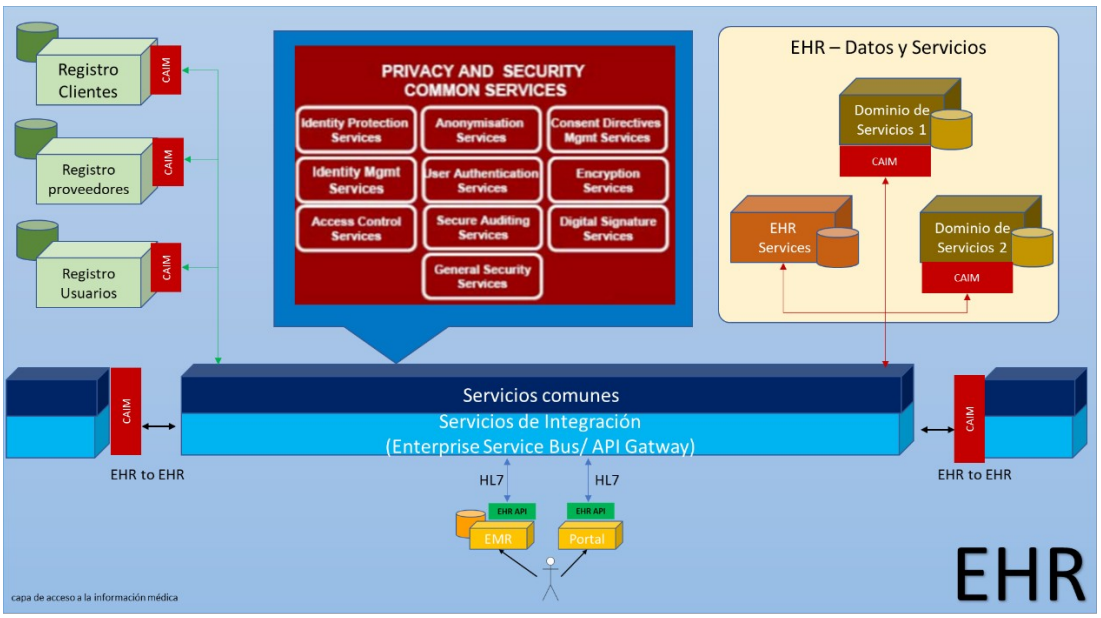
Política 3: Todo servicio expuesto por la infraestructura de la arquitectura debe ofrecer un esquema de control de acceso, de identificación única del usuario, aplicación o tercero que lo consume y de registro de eventos de auditoría de seguridad según su

sensibilidad. Este esquema debe aplicar en ambos sentidos, desde el consumidor al proveedor y desde el proveedor al consumidor.

Cada uno de los servicios expuestos por la infraestructura de la arquitectura representa un activo de información que debe ser protegido según el nivel de importancia y sensibilidad que tenga para el negocio. El uso de dichos servicios debe estar restringido únicamente a los usuarios y aplicaciones que tienen autorización, por lo que la organización debe estar en capacidad de determinar la identidad y el nivel de acceso de quien los usa y de auditar los eventos generados durante su uso.

El conjunto de funcionalidades de seguridad solicitadas por el negocio compone una parte del modelo de seguridad de la arquitectura. Deben manejarse independientemente de los mecanismos técnicos para lograrlos, por ejemplo, la funcionalidad de registro de eventos de auditoría debe distinguirse de la plataforma técnica de envío de eventos. La funcionalidad de negocio se apoya en la funcionalidad técnica pero no es saludable confundir los dos tipos de servicios.

Aunque el tema del modelo de seguridad se describe más adelante, a manera de ejemplo en, el modelo de seguridad, esta diferenciación queda clara en la siguiente Figura:



Donde el modelo define diferentes servicios de seguridad estableciendo cuáles de ellos son requeridos por el negocio. Concretamente en este modelo se definen como servicios de negocio los siguientes:

- Manejo de Identidad y de control de Acceso, de preferencia delegando este control a las soluciones de las entidades ya existentes.
- Cumplimiento regulatorio y de Reporte.
- Protección de datos, Privacidad y Acceso a información (Confidencialidad).
- Gestión de identidades
- Servicios de no repudio durante la interacción.
- Servicios de anonimización y de encripción
- Manejo de Confianza durante la interacción.
- Sistemas y redes seguras.
- Gestión de directivas de consentimiento
- Firma digital

Política 4: Cada uno de los servicios ofrecidos por la infraestructura de la arquitectura debe ser clasificado según su sensibilidad para el negocio por medio de los responsables de datos definidos por la RPIS, valor y riesgo de pérdida de la confidencialidad, integridad o disponibilidad.

No todos los activos de información de la organización tienen el mismo nivel de importancia y sensibilidad para la organización, por lo cual, el esfuerzo por protegerlos debe ser medido y ajustado acorde a los riegos que realmente representa el compromiso de alguno de los requerimientos que plantea la interoperabilidad segura. Con el fin de lograr esta diferenciación es importante hacer una clasificación detallada de cada uno de estos activos según sensibilidad para el negocio, valor y riesgo de pérdida.

El término sensibilidad debe concretarse en dominios de seguridad que permitan definir clasificaciones claras para los servicios.

La clasificación que se plantee puede ser descrita como taxonomías de gobierno que se asocien a los servicios de la arquitectura.

4.2.1.2. INTEGRACIÓN B2B

Política 5: El intercambio de información entre cualquier tercero y la entidad debe basarse en la constitución de una relación de confianza en cuanto a la protección de los activos de información. Dentro de los comités de definición de estas relaciones de confianza deben incorporarse como parte activa a las áreas de seguridad de la información de las partes y a los responsables de los datos definidos por el gobierno de datos de la RPIS.

Se deben documentar de forma detallada cada uno de los acuerdos de comunicación entre la RPIS y terceros en aspectos relevantes a la seguridad de la información. Debe existir siempre claridad sobre los esquemas de seguridad utilizados en dichos intercambios por lo que se debe tener siempre documentación clara de los acuerdos de seguridad informática establecidos entre las dos partes.

Política 6: La autenticidad de un tercero durante una transacción electrónica sobre la plataforma de interoperabilidad debe ser protegida.

Durante el intercambio de información con terceros es importante asegurar el no repudio, es decir, debe asegurarse la autenticidad de cada una de las partes involucradas evitando que alguna de éstas niegue su participación en dicho intercambio.

4.2.1.3. PORTALES DE LA RPIS

Política 7: Debe asegurarse que el acceso a los servicios disponibles en los portales corporativos cuentan con un mecanismo de control de acceso, identificación y autorización único por cada cliente

Esta política detalla los mecanismos de acceso a servicios que utilizan el portal de la RPIS como puerta de acceso a las funcionalidades. Es importante distinguir el portal como mecanismo de acceso que se ofrece a través de interfaces de usuario – GUI. En este caso el portal actúa como consumidor de servicio y la política se concreta en delegar la identidad de usuario del GUI para que los servicios invocados tengan conocimiento del usuario final. Esta parte más que autenticación y autorización en la capa de servicios es autenticación y autorización en la capa de portal y una delegación de identidad hacia las capas de servicios. Otro escenario es cuando el portal sirve como mecanismo para ofrecer las interfaces web, servicios orientados a GUI en un esquema Web 2.0, en este caso se plantea que aunque sean datos obtenidos por invocaciones a servicios de las capas SOA, las operaciones de autenticación y autorización se sigan integrando en el portal.

4.2.2. IMPLEMENTACIÓN

4.2.2.1. ARQUITECTURA

Política 8: La arquitectura debe adoptar e implementar un modelo de seguridad aplicable a todos los servicios del modelo de servicios.

Esta política está asociada con lo expresado en Política 2: El esquema de acceso a los servicios debe implementar un modelo de seguridad, si no se ha definido, o

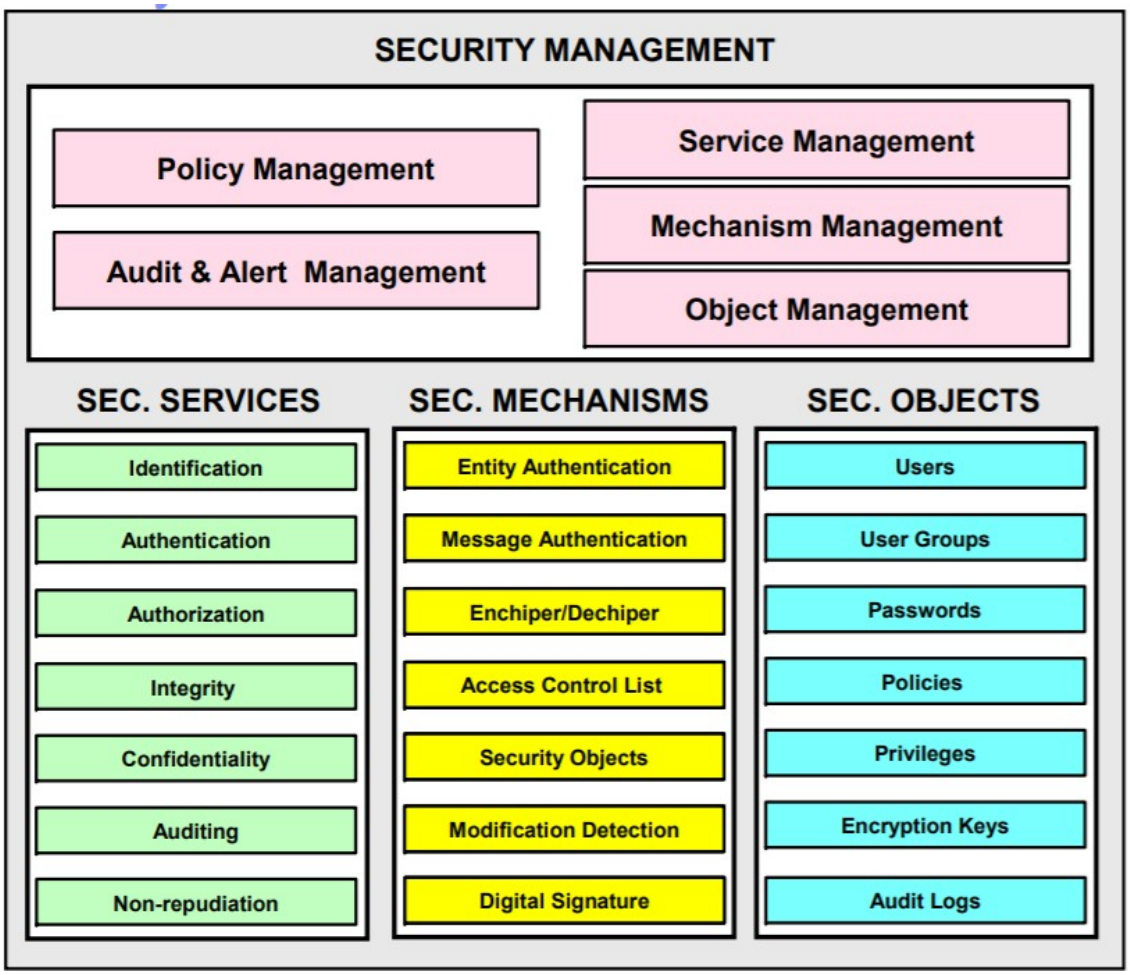
extender el modelo actualmente implementado por las aplicaciones que se habilitan como servicios. Este modelo debe orientarse a controlar los nuevos riesgos asociados a la adopción de la Plataforma de interoperabilidad que se concreta en la adopción de un modelo de seguridad. Este modelo debe seguir los lineamientos de seguridad de la organización y de las definiciones estándares de modelos de seguridad. Concretamente se recomienda adoptar el estándar de seguridad ISO 7498-2 (Arquitectura de seguridad OSI) como marco de referencia para la definición concreta del modelo específico de la organización.

El estándar ISO plantea los siguientes aspectos:

ISO Security Standard 7498-2

El modelo plantea los servicios de seguridad:

- Identificación
- Autenticación
- Autorización
- Integridad
- Confidencialidad
- Auditoría
- No repudio



Política 9: La arquitectura de referencia debe considerar los elementos de seguridad que hayan sido identificados en su definición no funcional.

La arquitectura de referencia define la arquitectura específica que seguirán las implementaciones reales de servicio. Esta definición de referencia plantea la separación de funcionalidades por capas, los patrones que se deben aplicar, los esquemas para lograr soluciones, etc. Esta política indica que adicionalmente la arquitectura de referencia debe plantear patrones de cumplimiento de seguridad y esquemas de solución a los elementos del modelo de seguridad.

4.2.2.2. DISEÑO DEL CATÁLOGO Y DE LOS SERVICIOS

Política 10: Se deben especificar aspectos de seguridad en el diseño del servicio para que sean tenidos en cuenta durante su implementación.

Todo el ciclo de vida del servicio, concretamente el que se refiere al modelamiento y arquitectura del servicio debe considerar los aspectos de seguridad (autenticación, autorización, integridad, confidencialidad, no repudio y auditoría).

4.2.3. OPERACIÓN

4.2.3.1. DISEÑO Y DIMENSIONAMIENTO DE LA INFRAESTRUCTURA

Política 11: Se debe asegurar la aplicación de mecanismos de control durante el diseño, dimensionamiento y activación de la infraestructura , para evitar la pérdida de la integridad, confidencialidad y disponibilidad de la información.

Adicionales a los esquemas de definición de modelo de seguridad para los servicios es importante definir y ejecutar controles de ejecución de las políticas de seguridad que permitan evaluar específicamente los accesos a los servicios ofrecidos.

Se recomienda la generación de reportes de acceso a los servicios, indicando el consumidor y el contexto de invocación (dirección de invocación, mecanismo de reto de autenticación, fecha, etc.). Estos reportes deben ser revisados en busca de accesos no esperados que aunque cumplan las reglas definidas de acceso sugieran operaciones sospechosas. A partir de esta revisión deben plantearse mejoras en la definición de las reglas de acceso.

4.2.3.2. OPERACIÓN DE LA PLATAFORMA

Política 12: Se deben definir las técnicas y mecanismos que aseguren cada uno de los componentes de la infraestructura, a nivel de hardware, software, comunicaciones y sistemas operativos

Es importante asegurar la disponibilidad de la información de forma segura durante la operación y evitar la negación del servicio que pueda causarse por la inadecuada definición y verificación de las políticas de seguridad.

Para asegurar la disponibilidad de la información sin sacrificar la seguridad, es necesario que en el momento de activar la infraestructura para operación, se verifiquen los controles de seguridad en cada uno de los componentes de hardware, software, comunicaciones y se hayan aplicado controles de seguridad a nivel del sistema operativo, de acuerdo con las prácticas listadas en esta sección.

Estos controles son específicos por producto, y cada cual tiene sus mejores prácticas, por lo que deben concretarse cuando los productos y componentes de

la infraestructura sean necesarios por un caso de negocio, adquiridos y con planes de ser integrados al entorno de producción.

4.2.4. GESTIÓN

4.2.4.1. GESTIÓN DEL MODELO DE GOBIERNO

Política 13: Se deben institucionalizar en todos los niveles de la organización, los lineamientos para la definición, diseño, implementación, verificación y control de las políticas del modelo de seguridad

Todas las definiciones de las políticas anteriores (y de los lineamientos para facilitar su cumplimiento) deben lograr la formalidad necesaria que permita lograr los objetivos allí planteados y en consecuencia los de la organización. Esta formalización –que impacta los servicios a lo largo de diferentes momentos y estados e involucra variados roles, se apalanca en las características y funcionalidades que ofrecen componentes (herramientas o soluciones) como el repositorio de metadata o herramientas de apoyo a seguridad como Sistemas de manejo de identidad, Sistemas de manejo y control de políticas, Sistemas de control de acceso, etc.

La institucionalidad buscada –que afecta los procedimientos y procesos definidos para el desarrollo y consumo de servicios - se alcanza transmitiendo de forma clara las políticas y las condiciones de uso de la plataforma de interoperabilidad. Se deben implementar validaciones automáticas que obliguen al cumplimiento de las políticas: tanto en tiempo de diseño como en tiempo de ejecución.

Esta política debe aplicarse con especial énfasis en las fases iniciales de adopción de la Plataforma de interoperabiliad, cuando el riesgo causado por el desconocimiento es mayor y se requiere la interiorización y aplicación de las nuevas políticas introducidas.

5. LINEAMIENTOS DE SEGURIDAD PARA EL INTERCAMBIO DE MENSAJES

5.1. CONSIDERACIONES GENERALES DEL INTERCAMBIO DE INFORMACIÓN

Como hemos mencionado en los supuestos de este documento, y de acuerdo a la recomendación de arquitectura para el intercambio de información de prescripción, dispensación y administración de medicamentos entre la RPIS y el operador logístico, estos serán realizados a través de una arquitectura orientada a servicios basada en mensajes. De acuerdo a la w3c, estos servicios “proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para

presentar información dinámica al usuario. Para proporcionar interoperabilidad y extensibilidad entre estas aplicaciones, y que al mismo tiempo sea posible su combinación para realizar operaciones complejas, es necesaria una arquitectura de referencia estándar." Es decir, su propósito en última instancia es presentar información o actualizarla, y lo hace basado en estándares.

La información intercambiada o almacenada es el activo principal que debe ser protegido por las opciones de seguridad presentes en los servicios de intercambio. Son las características de la información las que guían los elementos de seguridad que deben ser empleados. Teniendo en cuenta lo anterior, se hace uso de la clasificación de seguridad vigente para cada dato, de acuerdo a las prácticas actuales de Gobierno de Datos.

De acuerdo con la Política 10, los elementos de seguridad considerados para los servicios de la RPIS son "autenticación, autorización, integridad, confidencialidad, no repudio y auditoría". Estos elementos deben aplicarse de acuerdo a la información presente en cada servicio y la exposición de la misma a terceros no autorizados, teniendo en cuenta los riesgos a los cuales está expuesta la información por condiciones ambientales tales como la seguridad de los canales empleados.

El acceso a la información solo debe ser posible para aquellos actores que están autorizados para ello, de acuerdo a la definición dada por ISO 27000 para confidencialidad en una traducción aproximada "La información sólo debe ser vista por aquellos que tienen permiso para ello, no debe poder ser accedida por alguien sin el permiso correspondiente." Dado lo anterior todos los servicios deben tener al menos autenticación y autorización. La única posible excepción a lo anterior es que la naturaleza de toda la información de toda la interacción sea información pública, es decir, que pueda ser conocida por cualquiera. Por último, la exigencia de mecanismos de autenticación y autorización está de acuerdo con la Política 3 "Todo servicio expuesto por la infraestructura debe ofrecer un esquema de control de acceso, de identificación única del usuario, aplicación o tercero que lo consume y de registro de eventos de auditoría de seguridad según su sensibilidad. Este esquema debe aplicar en ambo sentidos, desde el consumidor al proveedor y desde el proveedor al consumidor".

La política 4 solicita que "Cada uno de los servicios ofrecidos por la infraestructura debe ser clasificado según su sensibilidad para el negocio, valor y riesgo de pérdida de la confidencialidad, integridad o disponibilidad. "La confidencialidad es el principal aspecto considerado en la clasificación de seguridad vigente para cada dato. Todos los datos confidenciales y sensibles deben estar protegidos mediante técnicas de cifrado. Los semi-públicos pueden no estar cifrados en entornos que el canal no esté expuesto, o sea en la red local de las entidades que hacen parte de la RPIS, pero si deben estarlo si son transportados en una red diferente. Por último, los de carácter público pueden no ser cifrados.

La integridad de la información debe ser asegurada sobre todo cuando la misma provenga de actores externos a la RPIS. La información solo debe ser actualizada por quien tenga permiso explícito para hacerlo y en el momento.

La auditoría debe hacerse en principio sobre todas las interacciones de los servicios web pero no sobre toda la información que viaja en estas interacciones, dependiendo de las necesidades del negocio de cada servicio se debe hacer filtrado de información para auditar únicamente los datos relevantes a nivel de peticiones y de esta forma evitar que la auditoría generada tenga volúmenes de información inmanejables a nivel de almacenamiento y revisión. La cantidad de tiempo que deba retenerse este repositorio de auditoría está determinada por la información en él contenida, cuya definición de nuevo está dada por las políticas vigentes de retención para datos específicos de acuerdo al Gobierno de Datos.

El rastro de auditoria, si está disponible para administradores de plataforma, únicamente debe almacenar los datos semi —públicos o públicos, pero nunca los confidenciales ni siquiera cifrados. Estos datos sí pueden almacenarse en otros repositorios cuyas características mantengan el principio de confidencialidad definido para el dato, es decir; sólo permitan conocer el contenido a quien tiene el permiso explícito para esto. Lo anterior es definido por el Gobierno de Datos de la RPIS.

5.2. CONSIDERACIONES GENERALES DEL INTERCAMBIO CON TERCEROS

Se define que las entidades externas que utilicen servicios expuestos por la RPIS son responsables totalmente del uso que ellas les den a estos servicios. Este compromiso debe ser aceptado por el tercero de forma explícita mediante un contrato legal. La anterior definición es la que habilita los lineamientos a continuación descritos y protegen a la RPIS de que sus servicios sean usados de forma inadecuada.

Para garantizar que esta responsabilidad pueda ser asumida por el tercero, la interacción entre las entidades externas y la RPIS deben proporcionar mecanismos considerados actualmente como válidos y aceptados de no repudio, autenticación, trazabilidad e integridad para los mensajes intercambiados y almacenados. La necesidad y sustento de estos requerimientos se desarrolla a continuación:

- Por la existencia de la Política 5, la cual especifica que "El intercambio de información entre cualquier tercero y la entidad debe basarse en la constitución de una relación de confianza en cuanto a la protección de los activos de información. Dentro de los comités de definición de estas relaciones de confianza deben incorporarse como parte activa a las áreas de seguridad de la información de las partes." Y la Política 6, "La autenticidad de un tercero durante una transacción electrónica sobre la plataforma de interoperabilidad debe ser protegida." Lo anterior nos lleva a hacer uso de mecanismos que garanticen la autenticación del tercero. Es decir, hay que garantizar que se hace uso de un mecanismo por el cual se ejecute una prueba que solo puede ser superada por un tercero valido para hacer uso de los servicios de la RPIS, pero no por cualquier otro. Lo anterior implica el uso tanto de mecanismos de autenticación como de autorización.

- Se debe emplear un mecanismo que permita conocer cuáles fueron las operaciones solicitadas por el tercero o los mensajes por este enviado de forma que este no pueda negar la autenticidad de su petición. Lo anterior protege a la RPIS de terceros que ' pretendan negar sus acciones con el fin de obtener algún beneficio o que pretendan descargar en la RPIS la responsabilidad de asegurar de forma adecuada sus sistemas de cómputo. Así pues, deben incluirse opciones de seguridad para no repudio y trazabilidad.

- Es un riesgo conocido que lo mensajes intercambiados pueden ser alterados por atacantes o entes externos. Debe garantizarse entonces que los mensajes en tránsito y almacenados no han sido modificados desde que fueron originalmente generados en la fuente, ya sea esta la RPIS o el tercero. Lo anterior es la justificación del uso de técnicas de integridad.

- Dada la existencia de operaciones que modifican la información y que no son independientes, se debe adicionar un mecanismo de manejo de **estampas de tiempo**. Lo anterior evita los ataques de repetición y previene adicionalmente los cambios no deseados por mensajes re-enviados por elementos de red intermedios u otros mecanismos presentes en la comunicación.

- En caso de un evento adverso, y también por prácticas aceptadas de seguridad informática, debe almacenarse el llamado y resultado de la ejecución de los servicios. Lo anterior permite hacer búsqueda de eventos particulares o descubrir tendencias que son útiles para diferenciar un uso común de un ataque o un evento extraordinario. El almacenamiento de la interacción no puede exponer información sensible, violación de la confidencialidad de un dato, por lo que el mecanismo de trazabilidad o auditoria debe contemplar opciones para que esta información se mantenga adecuadamente protegida.

5.3. CONSIDERACIONES GENERALES DEL INTERCAMBIO ENTRE SISTEMAS INTERNOS

Son aquellos intercambios de mensajes o llamadas a servicios que se generan completamente dentro del ambiente computacional controlado por una entidad que hace parte de la RPIS, es decir, su centro de datos sin que en ninguna parte de los eventos haya participación de un tercero o ente externo. Más informalmente, son todos los servicios que son consumidos entre aplicaciones o sistemas internos, es decir, tanto el productor como el consumidor son aplicaciones de la entidad que se ejecutan en el entorno computacional de esta.

De acuerdo a la Política 10, "se deben especificar aspectos de seguridad en el diseño del servicio para que sean tenidos en cuenta durante su implementación", estos son

"autenticación, autorización, integridad, confidencialidad, no repudio y auditoría". Si bien los riesgos de seguridad de estos servicios expuestos de forma interna son menores, no son inexistentes. No debe existir ningún servicio en la entidad que no tenga ninguna opción de seguridad, ya que no se identifica que existan servicios o vayan a existir servicios que únicamente hagan manejo de información completamente pública. Los requerimientos de seguridad definidos para los servicios de la RPIS se deben llevar a cabo sin importar quién es el prestador de la infraestructura tecnológica ni la ubicación geográfica de las aplicaciones.

Los consumos de servicios internos deben al menos ser autenticados, es decir; que se garantice que solo son invocados por las aplicaciones y entes que tienen permiso para hacerlo. Igual que para los terceros, lo anterior implica el empleo de mecanismos de autenticación y autorización.

6. MARCOS DE REFERENCIA

El detalle del aseguramiento de los servicios web basados en SOAP debe hacerse basándose en Web Services Policy 1.2 - Attachment, WS-SecurityPolicy 1.2 y OASIS Web Services Security (WSS) TC excepto en la obligatoriedad de uso SHA-1 ya que este algoritmo ya no se considera seguro, se debe hacer uso en cambio SHA-2. Los anteriores estándares hacen uso de XML Encryption, XML Signature y otros estándares que hacen uso de llaves asimétricas y certificados X509. Por supuesto, se recomienda el uso de productos o frameworks que cuenten con el soporte para el manejo de estos estándares mencionados, no se recomienda de ninguna manera la implementación directa total o parcial de los estándares en un desarrollo interno.

Se deben utilizar certificados deemitidos por las entidades acreditadas ante el ARCOTEL, que son las autoridades de certificación aprobadas en Ecuador para todo intercambio con terceros, dadas las normas y leyes vigentes de la legislación ecuatoriana. Para los intercambios internos pueden usarse certificados auto-emitidos. En cualquier caso, solo deben usarse certificados vigentes y hacer uso de ACLs (lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto) donde pueden consultarse los certificados que han sido comprometidos o revocados antes de su periodo de expiración, para abstenerse de su uso para nuevas interacciones.

La autenticación y el no repudio definidos para la RPIS se basan en la utilización de firmas digitales. Una firma digital es una estampa que se adiciona en un mensaje y la misma garantiza la fuente del mensaje. El uso de firmas digitales en el intercambio de información tiene validez legal en Ecuador a nivel nacional según **la ley de Comercio Electrónico, Firmas y Mensajes de Datos** donde se establece que la utilización de firma digital tiene la misma validez que la utilización de una firma manuscrita, siempre y cuando esta firma digital cuente con las características técnicas necesarias para garantizar la validez de la información firmada. Estas características técnicas se encuentran descritas más adelante en este documento.

La utilización de la tecnología de firmas digitales nos permite mitigar los riesgos de suplantación, alteración de información o repudio de la misma, punto en el cual nos apoyamos para enfrentar casos que involucren datos provenientes de intercambios de información utilizando medios electrónicos, los cuales requieren revisión por parte de auditorías o procedimientos de investigación adelantados por las autoridades competentes.

La implementación del mecanismo concreto de interacción de los servicios web expuestos debe cumplir con todos los aspectos relacionados en la **Ley XXXX** 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 acreditadas ante el ARCOTEL**, autoridades de certificación aprobadas en Ecuador.

Por otra parte, la información que se intercambia debe estar protegida durante su tránsito si la misma tiene un carácter de confidencial. Se identifica inicialmente como confidencial toda información del paciente/afiliado relacionada con sus datos personales de ubicación como lo son dirección y teléfono, la información relacionada con tratamientos médicos o historia clínica (por ejemplo, autorizaciones de medicamentos o de exámenes especializados) y por último aquella relacionada con su poder adquisitivo o salario o que a partir de la misma se pueda deducir (como por ejemplo valor mensual descontado por concepto de afiliación). La anterior definición de confidencialidad es ampliada por el modelo de gobierno de datos de la RPIS, el cual define una categoría de seguridad para los diferentes datos y debe ser consultada siempre cuando se trate de determinar opciones de seguridad sobre la información consultada, creada o actualizada a partir de servicios expuestos a terceros.

Por último, los entregados o recibidos por un servicio deben analizarse con el fin de definir si están cubiertos por regulaciones que los enmarcan dentro de la categoría de datos sensibles de conformidad con la Ley Orgánica de Salud y la Ley de Derechos y Amparo al Paciente , obligando a que su tratamiento y acceso restrictivo esté sujeto a la protección de datos personales.

7. CONFIGURACIÓN DE MECANISMOS DE SEGURIDAD

7.1. ASEGURAMIENTO DE HARDWARE Y SOFTWARE DE LA INFRAESTRUCTURA PARA EL INTERCAMBIO DE MENSAJES

La Política 12 menciona que "Se deben definir las técnicas y mecanismos que aseguren cada uno de los componentes de la infraestructura, a nivel de hardware, software, comunicaciones y sistemas operativos.". Lo anterior es fundamental cuando se haga despliegue de un servicio en ambiente productivo. Esta Política debe desarrollarse en procedimientos y lineamientos cuando existan todos los elementos

de hardware y software que intervendrán en el entorno de servicios o cuando uno nuevo sea añadido. A continuación, se detallan algunos aspectos que ayudan al cumplimiento de esta Política 12:

Cada producto tiene una guía de aseguramiento por lo general donde las más completa incluso mencionan aspectos de endurecimiento desde el sistema operativo en adelante. Estas guías deben ser aplicadas. La mayoría de los productos tipo Bus de interoperabilidad se ejecutan sobre un servidor de aplicaciones, el cual a su vez se ejecuta sobre un sistema operativo, ejecutándose este en una plataforma de hardware o en una solución de virtualización. Todos los niveles deben estar asegurados de forma adecuada, o es posible que basándose en falencias de un nivel se puedan generar brechas de seguridad en los siguientes, por ejemplo, modificando un archivo por un esquema inadecuado de permisos sobre la carpeta de instalación del servidor de aplicaciones se pueden eliminar las opciones de seguridad de un servicio. La gráfica muestra los elementos que típicamente deben ser considerados a cada nivel en términos generales, y las consideraciones correspondientes se desarrollan a continuación:

- **Sistema operativo:** Se deben tener cuentas de administración restringidas y auditadas de acuerdo con su función. Así, por ejemplo; se considera deseable que existan cuentas de operador solo con permisos de subir o bajar servicios que representen el servidor de aplicaciones y con opciones de lectura sobre los archivos tipo log.

  La cuenta de administrador en cambio además de los permisos anteriores tiene la posibilidad de leer los diferentes archivos donde se encuentran instalados los productos. Una tercera cuenta es con la que se ejecuta el producto, llamémosla como producto SO, servidor de aplicaciones, y esta cuenta tiene los permisos

necesarios para la ejecución del mismo, por ejemplo, apertura de puertos de rango bajo.

Nótese que ninguna de las anteriores cuentas de usuario es la correspondiente a "super usuario", administrador completo del sistema operativo o root.

- **Servidor de aplicaciones:** Las cuentas propias del producto no deben en lo posible estar deshabilitadas y con una contraseña diferente a la generada por defecto. De acuerdo al producto, deben existir roles donde los permisos de modificación e instalación estén para unos usuarios tipo administrador y otras para usuarios tipo operador donde solo es posible tener una vista de lectura sobre el estado del servidor, mas no modificar o incluso, ver configuraciones que de acuerdo al producto se consideren sensibles. El servidor de aplicaciones solo debe poder ser accedido por las máquinas y hardware que realmente necesitan su acceso y no tras, así pues, debe tener seguridad a nivel de red.

- **BUS de interoperabilidad:** El Bus de Interoperabilidad será provisto por el **Ministerio de Salud** y estará disponible en una plataforma de alta disponibilidad y escalabilidad, con capacidades de bases de datos y servidores de aplicaciones que puedan adaptarse a las necesidades de un escenario nacional que integre todas las regiones y sub-sistemas.

  El BUS de interoperabilidad permite la comunicación entre dominios, no modifica los usos y costumbres en los procesos actuales de almacenamiento de información sanitaria. La información permanece en el repositorio de cada sistema de información, sólo se comunica con otros dominios en caso de existir necesidades concretas avalada por la legislación vigente.

  El bus de interoperabilidad por lo general extiende de los permisos dados sobre el servidor de aplicaciones, sin embargo, debe garantizarse que existen al menos los dos roles anteriores y que si es necesario una interacción con los desarrolladores estos lo hagan a través de un usuario tipo operario o asistido con un administrador. Es claro que los operadores no pueden detener la ejecución de flujos o de recepción de mensajes de un servicio, menos cambiar las opciones con que estos se ejecutan

- **Repositorio de registro de servicios o Registry:** El catálogo de servicios activos debe ser protegido si está presente. Este es vulnerable a cambios malintencionados de los contratos (wsdl, wald) o de las políticas de los mismos. De igual forma, solo las aplicaciones autorizadas deben poder acceder tanto a nivel de consulta como incluso a nivel de red, de ser posible.
- **Base de datos:** No es inusual que las intermediaciones colocadas en un BUS de interoperabilidad hagan uso de una o varias bases de datos, pero en particular pueden usar una para propósitos de lectura de parámetros. Esta base de datos debe estar protegida tanto a nivel de red como a nivel de usuarios, permisos y privilegios.

7.2. ADMINISTRACION DE LLAVES PRIVADAS Y CERTIFICADOS DIGITALES

Como práctica general se usarán al menos dos almacenes de Llaves (keystore) separados, uno para identidad y otra confianza. En el keystore de identidad se almacenarán los pares de llaves privadas y certificados digitales usados por la RPIS y en el keystore de confianza se almacenarán los certificados digitales de las entidades certificadoras y de terceros. De esta manera, los datos sensibles (certificados y llaves privadas) son separados de los datos no sensibles (certificados de entidades de certificadoras) permitiendo aplicar políticas de seguridad diferentes sobre ambos keystores:

- El keystore de identidad y el de confianza se protegen con permisos lectura para el usuario producto SO.
- El keystore de confianza puede distribuirse en la red sin problemas mientras que el de identidad debe encontrarse en una sola ubicación, en particular en el BUS o en el producto donde se aplique la seguridad para los mensajes de salida de la RPIS.
- El password del keystore de identidad debe ser conocido por pocas personas.

Ambos certificados deben configurarse en el producto responsable de la seguridad de los servicios web con el propósito de que puedan ser usados en transacciones con las diferentes opciones de seguridad.

Los certificados incluidos en los keystores deben estar vigentes y se debe hacer uso de ACLs para determinar certificados comprometidos antes de su expiración siempre antes de hacer uso de los mismos.

Esta definición de dos certificados puede verse afectada por limitaciones o forma de uso de los productos específicos que sean seleccionados, por lo que es posible que después de la selección de los mismos deba ajustarse. La de uso de ACLs se considera como una característica altamente deseable.

7.3. ASPECTOS GENERALES DE LA SEGURIDAD DE LOS SERVICIOS

La implementación de los requerimientos de autenticación, integridad y no repudio de servicios se realizará a través de certificados digitales. Se tendrá como mecanismo de confianza el uso de seguridad a nivel de mensaje usando WS-Security.

Si el producto empleado lo permite, se debe hacer uso e Asymmetric binding assertion, como se define en el estándar WS-Policy. Lo anterior obliga a que para el consumo de los servicios tanto el servidor como el cliente deben tener certificados digitales para sus operaciones de seguridad.

La auditoría no hará uso de WS-Security, pero debe contemplar el uso de códigos de integridad, llamados hash, para garantizar la validez del registro. Estos códigos de

integridad deben hacer uso de igual forma de cifrado para evitar que sean fácilmente alterables.

7.4. AUTENTICACIÓN Y AUTORIZACIÓN DE SERVICIOS

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. El certificado (llave privada y pública) debe ser emitido por una autoridad certificadora en la cual el servidor confía. Así pues, los certificados públicos de los clientes deben ser añadidos al keystore correspondiente del servidor, junto con toda su cadena de certificación.

La autorización es un mecanismo que no está cubierto por WS-Security ni por WS-Policy. El producto que haga el manejo de la seguridad debe proporcionar mecanismos para de acuerdo a las credenciales obtenidas en la autenticación determine si cierto cliente tiene o no permiso de ejecución para un servicio específico. La política de consumo también puede ser basado en la IP u otras características conocidas adicionales a las de la identidad proporcionada como complemento.

Para la implementación de la autorización hay diversas opciones, como son desarrollos en el BUS de interoperabilidad seleccionado, uso de mecanismos incluidos en el BUS o la suite de productos adquirida, el uso de WS-Guardian o de otros productos de seguridad complementarios. Al momento de escritura de este documento no se encuentra seleccionado un BUS por lo que no es posible hacer una definición única en este momento.

7.5. INTEGRIDAD Y NO REPUDIO DE SERVICIOS

La integridad y el no repUdio se consiguen mediante el empleo de firmas digitales las cuales a su vez hacen uso de cifrado y hashing, que en la seguridad de servicios web se basa en el uso del estándar XML Signature.

Las especificaciones técnicas recomendadas a nivel técnico para hacer utilización de Firma Digital son:

- Uso de algoritmos que a la fecha de uso se consideren seguros y sean estándar. Al día de hoy estos algoritmos pueden ser SHA-256 o SHA-512.
- Uso de certificados emitidos por una autoridad certificadora válida en Ecuador.

7.6. CONFIDENCIALIDAD DE LOS SERVICIOS

La confidencialidad se garantiza mediante la implementación de cifrado en los campos sensibles del mensaje, o el cifrado completo del mensaje. Por facilidad y con el fin de evitar posibles brechas de seguridad por una identificación no adecuada, se debe cifrar el contenido completo del mensaje cuando se intercambia con terceros y al menos este mensaje contiene un campo clasificado como confidencial. Debe estar regido por XML encryption. Existen varios algoritmos válidos al día de hoy, pero se recomienda que siempre los mismos sean usados bajo llaves de al menos 256 bytes.

7.7. AUDITORÍA DE LOS SERVICIOS

Como condiciones de trazabilidad se debe tener en cuenta que el flujo de la información entre el servicio expuesto y el cliente que lo invoca debe dejar rastro de auditoría en el momento en que es realizado el consumo del servicio y en el momento que se da respuesta a la petición. Es decir, no es válido almacenar únicamente las peticiones que pudieron ser procesadas sino en cambio todos los mensajes que fueron recibidos y todos los mensajes que fueron enviados.

Para lograr esta recopilación de información a nivel de petición concreta a un servicio determinado se debe utilizar una tecnología que permita actuar como un filtro en la invocación de los servicios, permitiendo configurar y escoger la información que se considera relevante para realizar el proceso de rastreo de las peticiones realizadas y de la información que ha viajado como resultado del consumo de los servicios.

La forma recomendada para realizar las tareas de recolección de información de auditoría y trazabilidad sobre una o muchas capas de servicios es la utilización de fachadas de servicios del tipo "interceptor", las cuales se comportan como un "sniffer" sobre las peticiones que son enviadas a los servicios, esta tecnología es normalmente ofrecida por las plataformas de BUS de interoperabildiad los cuales de manera normalmente parametrizable ofrecen la funcionalidad de acceder a la información que viaja en las peticiones y respuestas sin hacer manipulación ni cambio de datos, esto permite que se puedan hacer tareas de registro de datos de auditoría sin tener que hacer modificaciones en los servicios fuentes ya existentes.

8. ESQUEMA DE SEGURIDAD PARA TERCEROS

Se autentica la entidad, no el usuario que está usando el sistema informático del tercero. En este orden de ideas, cada entidad o cada convenio diferente con una entidad particular debe tener su certificado propio el cual está relacionado con el convenio que especifica ,que operaciones de qué servicios tiene derecho a invocar.

Para garantizar el no repudio de la información que ha sido intercambiada entre la RPIS y otras entidades externas se debe hacer uso de las características de seguridad a nivel de mensaje.

Dentro de estas características de seguridad a nivel de mensaje tenemos la utilización de Firmas Digitales, proceso en el cual cada una de las partes que intervienen en la comunicación (Servicio y cliente consumidor) hace uso cada uno de una llave que tiene un respaldo válido ante una autoridad certificadora. Esta llave es usada para Firmar la información que es entregada en las peticiones realizadas a los servicios, de esta forma se garantiza que la información recibida en el servicio está siendo emitida por una entidad (tercero) en la cual confiamos y con la cual establecemos acuerdos de intercambio de información previamente; como valor adicional el cliente o consumidor del servicio también tiene la potestad de verificar si la información que recibe en la respuesta del servicio consumido es emitida por la RPIS.

Los siguientes pasos son los necesarios para establecer un intercambio con un tercero:

(1) Determinar las opciones de seguridad que aplican para el tercero de acuerdo con las operaciones sobre las cuales va a hacer uso. Lo anterior basado en las consideraciones incluidas en este documento y el estudio del caso particular.
(2) El uso de los mecanismos de autenticación es obligatorio para todos los servicios web de la RPIS. Debe pues entonces configurarse esta verificación para el servicio. Lo anterior de acuerdo con el apartado de autenticación y autorización de servicios de este documento.
(3) En orden de cumplir el anterior numeral, debe importarse la llave pública del tercero asociada a esta relación. Puede ser una ya usada para el consumo de otro servicio, pero debe garantizarse que dicha llave es usada solo por una aplicación del tercero o un área del tercero.
(4) Debe configurarse, al menos hasta que el mensaje llegue a la red interna de la RPIS, seguridad por canal lo que en términos prácticos se implementa como comunicación a través de HTTPS.
(5) Debe limitarse el tráfico hacia el BUS de interoperabiliad de forma que solo pueda ser alcanzado por el elemento de red que permite la comunicación con los terceros.
(6) Debe configurarse la autorización, al nivel permitido por la herramienta de gestión de seguridad para los servicios web de forma que el tercero solo tenga acceso explícito al servicio web que requiere y a las operaciones específicas necesarias.
(7) Debe configurarse la exigibilidad de la firma de los mensajes por parte del cliente y el firmado de los mensajes salientes de la RPIS. Lo anterior de acuerdo con el apartado de integridad y no repudio de servicios de este documento.
(8) Debe configurarse un mecanismo de marcas de tiempo, **timestamp**, para evitar ataques de repetición o bien para toda la interacción o bien para las operaciones que afectan la información, es decir, aquellas que no pueden ser clasificadas como de "lectura".

(9) Si alguno de los mensajes intercambiados por el tercero en una operación específica contiene al menos un campo que de acuerdo con el Gobierno de datos esté clasificado como confidencial, debe cifrarse la totalidad del mensaje.
(10) Debe configurarse la trazabilidad, auditoría de los mensajes. Lo anterior de acuerdo con el apartado de auditoria de servicios de este documento.
(11) Revisar, auditar, que las opciones de seguridad definidas en el numeral 1 de este listado hayan sido aplicadas correctamente en el ambiente productivo.

9. P&S-ARQUITECTURA CONCEPTUAL

Esta sección proporciona una descripción general de la arquitectura conceptual e introduce diez servicios P&S que en conjunto satisfarán todos los requisitos P&S discutidos en la sección anterior. La arquitectura se basa en una visión de un estado futuro deseado de cómo debería funcionar la Historia Clínica Electrónica Interoperable en Ecuador, en los próximos años. Este estado futuro tiene ciertas características clave que se describen brevemente y también viene con un conjunto de supuestos que primero deben cumplirse.

9.1. VISIÓN

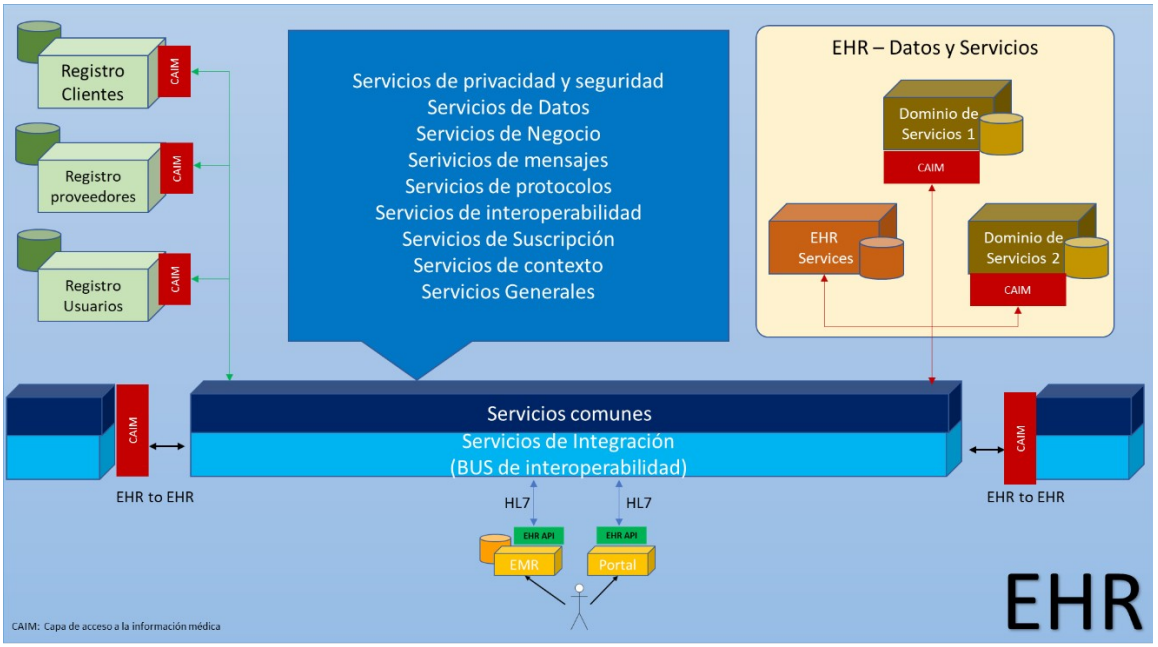
Definimos para la interoperabilidad entre la RPIS y el operador logístico una arquitectura basada en mensajes que permite a los usuarios acceder a los datos en un repositorio de datos EHR, así como a uno o más repositorios de dominio (por ejemplo: un repositorio prescripciones, un repositorio de consejos farmacéuticos, un repositorio de dispensaciones). Los usuarios acceden a estos datos interactuando con un sistema POS (el Sistema usado en el Punto de Servicio) conectado al EHR o con un portal clínico cuyo back-end está conectado al EHR. En todos los casos, la interacción del usuario hace que se construya un mensaje **HL7** (por el sistema POS, por el middleware conectado al sistema POS o por el sistema del portal clínico) y luego enviado a los servicios comunes de EHR.

Conceptualmente, la capa de acceso a la información médica (CAIM) actúa como un filtro para garantizar que la PHI confidencial nunca se recopile, use o divulgue de manera inapropiada. Los diez servicios P&S que se muestran en el diagrama, que forman parte de un conjunto más grande de servicios comunes integrados en el BUS de interoperabilidad, trabajan juntos para crear la malla en ese filtro:

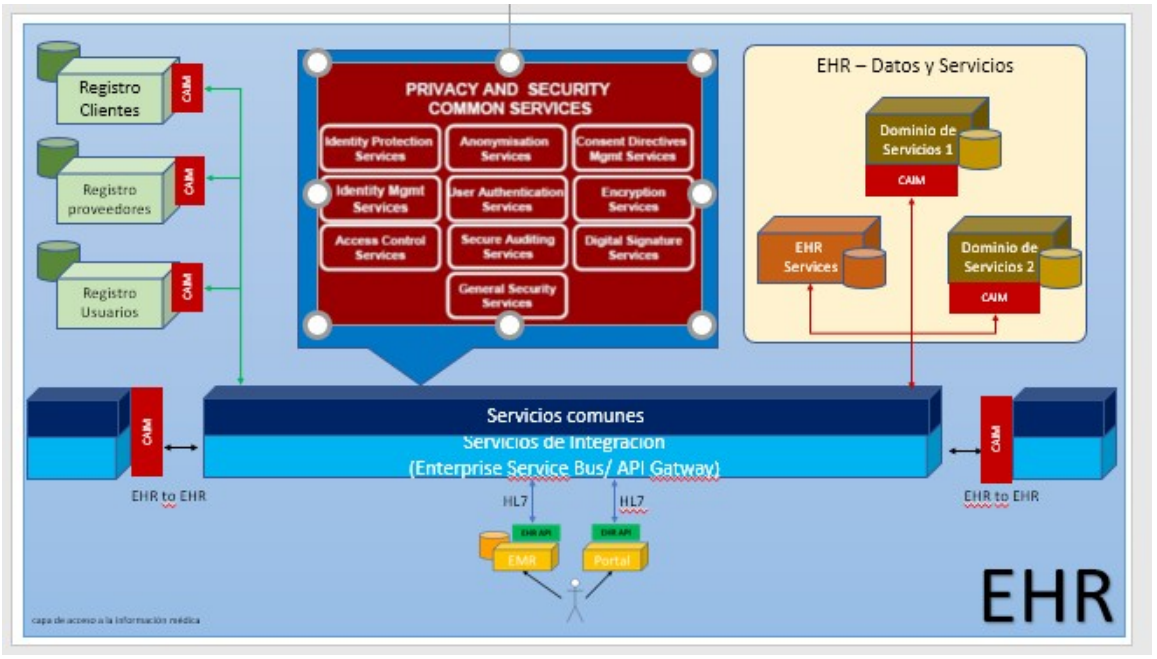
El EHR también se basa en varios repositorios de información adicional:

- un registro de clientes que contenga una entrada para todos (o la mayoría) de los pacientes / personas residentes en la jurisdicción;
- un registro de proveedores que contenga una entrada para cada proveedor de atención médica regulado que ejerza en la jurisdicción;
- y un registro de usuarios que contiene una entrada para cada usuario de EHR que está registrado bajo el modelo de gestión de usuarios de confianza.

Además de estos repositorios de datos, el EHR también proporciona sistemas de acceso con servicios comunes que facilitan el acceso y la actualización de los repositorios. Los servicios P&S se encuentran entre los muchos servicios comunes que proporcionará el EHR. La siguiente figura enumera todos los servicios comunes de EHR, incluidos los servicios P&S.



La siguiente figura presenta los diez servicios P&S:



9.2. DESCRIPCIÓN GENERAL DE LOS SERVICIOS P&S

Este documento identifica diez servicios P&S que son críticos para la protección de la PHI en los entornos de información de salud compartida. Estos servicios son parte de un conjunto más amplio de herramientas de protección de datos que todos los usuarios de PHI en un entorno de interoperabilidad de datos clínicos deben adoptar, incluidas varias políticas y procedimientos de protección de datos, capacitación en privacidad y seguridad para los usuarios , así como la posible acreditación de los usuarios de la interoperabilidad y las organizaciones que representan para asegurarse de que han cumplido con sus responsabilidades de proteger la PHI en el entorno de salud compartida. La protección exitosa de la PHI depende de una combinación óptima de ambas: políticas e instrumentos tecnológicos.

Los diez servicios P&S descritos aquí se clasificarían como instrumentos de "tecnología", en lugar de "políticas", para proteger la PHI. Porque en este documento definiremos una arquitectura conceptual de P&S, estos servicios no prescriben tecnologías, productos de proveedores o entornos de sistemas operativos específicos; sin embargo, reconocemos que los usuarios de la Plataforma de interoperabilidad de la RPIS eventualmente adoptarán tecnologías específicas de privacidad y seguridad para respaldar la implementación de los servicios P&S identificados en este documento.

La siguiente lista resume los diez servicios P&S que proporcionarán la mayor parte de la funcionalidad P&S dentro del entorno de datos de salud compartidos, así como un grupo de servicios comunes con implicaciones P&S:

(1) Un **Servicio de gestión de identidad de usuario** que incluye componentes de servicio para abordar la necesidad de Identificar con precisión a los usuarios del sistema. Maneja tareas como registrar usuarios, asignar roles que definen sus privilegios de acceso (por ejemplo, un cardiólogo no podría acceder a los datos de salud mental) y administrar los cambios en el estado del usuario.

(2) Un **Servicio de autenticación de usuarios** - un servicio transaccional que se basa en la gestión de la identidad para establecer la validez de la identidad reclamada de un usuario que inicia sesión en el sistema y, por lo tanto, proporciona protección contra transacciones fraudulentas. Para racionalizar la gestión de las sesiones en las que los usuarios tienen acceso a información confidencial, se generan tokens de autenticación con caracteres protectores como ID de usuario y time-out.

(3) Un **Servicio de control de acceso** que proporciona metodologías de control de acceso como parte de un servicio de administración de privilegios unificado para usuarios de la plataforma de interoperabilidad. Este servicio es fundamental para

garantizar la confidencialidad e integridad de la PHI. Se pueden seguir tres modelos:

a. control de acceso basado en roles, donde el acceso a tipos específicos de PHI se basa en el rol desempeñado por el usuario según lo determinado (por ejemplo) por su acreditación profesional),

b. acceso basado en grupos de trabajo control, que basa el acceso a la HCE de un paciente / persona determinada en la membresía del usuario en uno o más grupos de trabajo (como equipos clínicos o personal de una práctica familiar), y

c. control de acceso discrecional, que permite a los usuarios con un acceso legítimo al EHR de un paciente / persona (por ejemplo, un médico de familia) para otorgar acceso a otros usuarios que no tienen una relación previamente establecida con el EHR de ese paciente / persona (por ejemplo, un especialista). Los subcomponentes del servicio de control de acceso incluyen la administración de reglas comerciales para el control de acceso (traduciendo la política de control de acceso en reglas comerciales automatizadas que se pueden aplicar en tiempo real); asignación de roles a usuarios; asociar usuarios individuales con grupos de usuarios (por ejemplo: equipos de atención y personal de la clínica); gestionar la asociación entre los usuarios y los pacientes / personas en cuya atención participarán; suspensión rápida de los privilegios de acceso de los usuarios; y autorizar a los usuarios.

(4) Un **Servicio de gestión de directivas de consentimiento** que traduce los requisitos de privacidad que surgen de fuentes como la legislación, las políticas y las directivas de consentimiento específicas de las personas, y aplica estos requisitos en un entorno de EHR. El servicio se basa en un vocabulario común de privacidad basado en los estatutos ecuatorianos de protección de datos de salud y otras leyes de privacidad.

Un servicio componente gestiona las reglas comerciales relacionadas con el consentimiento, por ejemplo, procedimientos para registrar las directivas de consentimiento del paciente, validar el consentimiento o invalidar las directivas de consentimiento. Otro componente permite a las personas otorgar, retener o retirar su consentimiento para la recopilación, uso o divulgación de su PHI de acuerdo con la legislación y las políticas de privacidad aplicables. También permite información como la identificación de un tomador de decisiones sustituto autorizado (cuando corresponda) y las estipulaciones del paciente / persona involucrada sobre qué usuarios del sistema de información de EHR tienen acceso a su PHI.

Los componentes transaccionales sirven para validar el consentimiento, para mapear directivas de consentimiento entre jurisdicciones y, cuando sea necesario, para invalidar el consentimiento. Un servicio de control de acceso de pacientes permite a los pacientes restringir el acceso a componentes específicos de su HCE, por ejemplo, su perfil de medicamentos recetados.

(5) Un **Servicio de protección de identidad** que facilitará el almacenamiento por separado de información personal que identifica de forma única a las personas (por ejemplo, nombre, dirección, número de identificación, etc.) de la información de salud relacionada con su atención y tratamiento, diagnóstico, etc. Este servicio proporcionaría a los usuarios autorizados un acceso sin problemas a PHI mediante el uso de una tabla de enlace o servicio que conecta el identificador público (PID) de un individuo con su información médica personal (PHI) sin que los dos conjuntos de datos residan en la misma ubicación física.

(6) Un **Servicio de anonimización** que toma PHI que representa a un individuo identificable y luego elimina todos los identificadores personales. El objetivo es hacer que la información sea accesible para los usuarios secundarios de los datos sanitarios (investigadores y administradores sanitarios) sin infringir la privacidad del paciente. En algunos casos, se puede preferir la **seudonimización** (uso de una designación de código única en lugar de material que revele la identidad) a la anonimización completa. Tanto la anonimización como la seudonimización son técnicamente complejas, y el servicio debe evitar todos los medios para inferir identidades, especialmente cuando los interesados son personas con atributos o situaciones raros o distintivos.

(7) Un **Servicio de cifrado** que mantiene la confidencialidad de los datos mediante criptografía. Los servicios de componentes incluyen administración de claves (creación, renovación y revocación de claves de cifrado); cifrado de datos EHR dentro de bases de datos; cifrado de datos almacenados, como archivos de respaldo y archivo; y cifrado de datos (como mensajes) durante la transmisión. Varios otros servicios de esta lista dependerán del servicio de cifrado.

(8) Un **Servicio de firma digital** que permite a un profesional de la salud firmar un documento digital (correo electrónico, historia clínica electrónica, prescripción, etc.) de la misma manera que aplicaría una firma al papel, y con la seguridad de que la firma no se puede falsificar ni ni el documento ni la firma pueden modificarse sin invalidar la firma. Los servicios de componentes incluyen generar pares de claves de firma digital, garantizar que las claves de firma digital privadas permanezcan protegidas y publicar la clave de verificación de identificación y firma de cada participante en un documento llamado "certificado digital". Otros servicios de componentes incluyen la aplicación de firmas digitales a datos; verificación de firma digital;

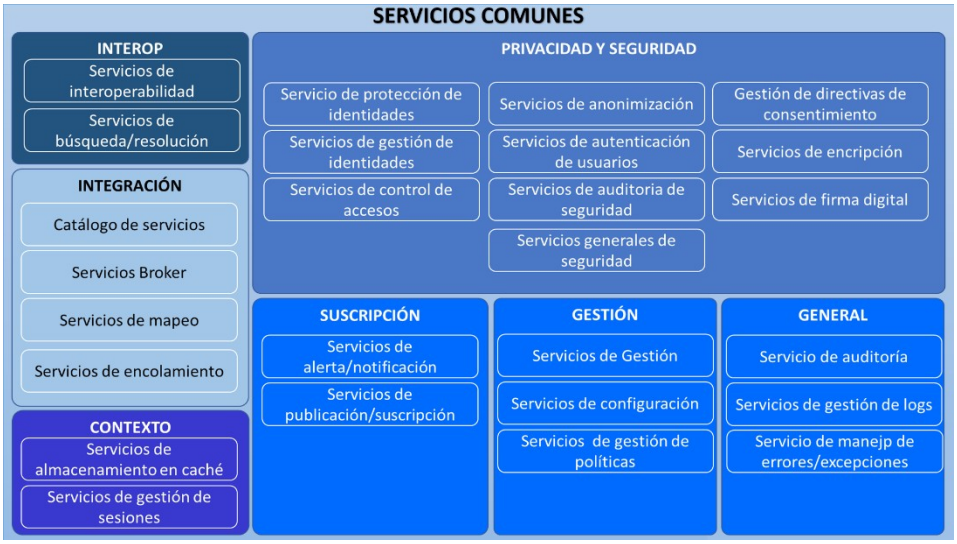
(9) Un **Servicio de auditoría** seguro para registrar eventos importantes relacionados con la privacidad y la seguridad en un registro de eventos. Los servicios de componentes incluyen registro de eventos y análisis de registros.

(10) **Servicios generales de seguridad** como escaneo en busca de virus, respaldo seguro y restauración de datos, archivo seguro de datos y destrucción segura de datos

Otros servicios comunes que tienen implicaciones de P&S, como:

a. Un **servicio de gestión de políticas** que funciona como una forma uniforme de acceder, modificar y coordinar las reglas comerciales relacionadas con la privacidad que los servicios P&S (entre otros) ponen en funcionamiento. Algunos ejemplos de servicios que se basan en estas reglas relacionadas con la privacidad incluyen los Servicios de control de acceso, los Servicios de administración de identidad del usuario, los Servicios de protección de identidad y los Servicios de administración de directivas de consentimiento.
b. **Gestión de sesiones (**abrir, cerrar, y finalizar sesiones de usuarios)
c. **Registro de clientes** (en la medida en que pueda utilizarse para señalar a pacientes / personas cuya privacidad y seguridad corren un riesgo elevado),
d. **Registro de proveedores y registro de usuarios** (resolución de identificadores de proveedores)
e. **Notificación** (notificar a un oficial de privacidad de un usuario que anula las directivas de consentimiento o acceder a datos bloqueados, o notificar a un oficial de seguridad de un evento relacionado con la seguridad o una posible violación de seguridad),
f. **Mensajería y**
g. **Gestión de accesos** de pacientes/personas a su HCE

Cada uno de los servicios de privacidad y seguridad se muestra en el siguiente diagrama, junto con los demás servicios de la Plataforma de interoperabilidad (servicios de datos, servicios comerciales, servicios de mensajería, servicios de protocolo, servicios de gestión de suscripciones, servicios de contexto y servicios generales).

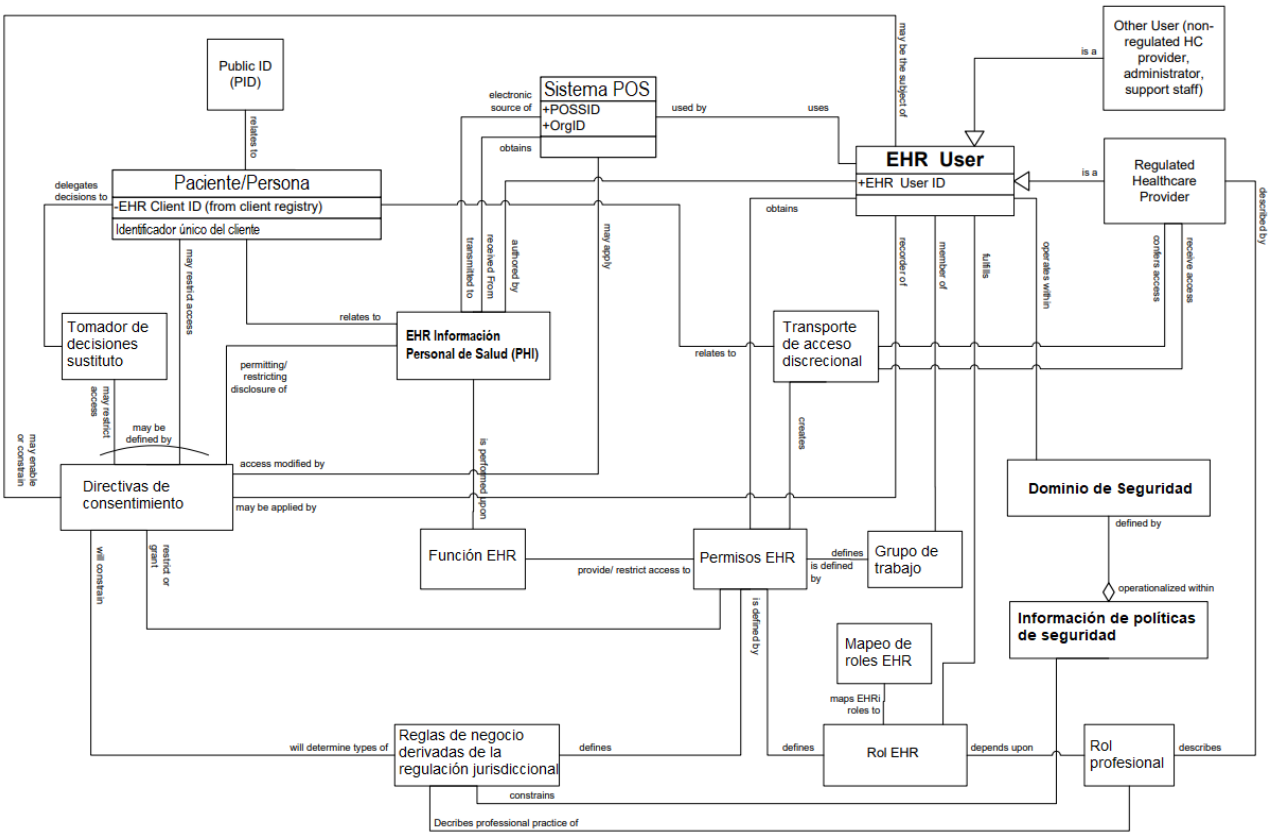


9.3. MODELO DE DATOS CONCEPTUAL PARA LOS SERVICIOS P&S

A continuación un modelo de datos (UML) conceptual para todos los componentes de datos principales de la arquitectura EHR P&S.

Las dos figuras a continuación muestran varias clases de datos

- Paciente / persona, incluidos atributos como un identificador único de cliente,
- Identificador público (PID), como tipo y número de documento de identidad, números de tarjetas de salud, etc., asignado a pacientes / personas (donde cada paciente / persona tiene cero o más PID.
- Usuario de EHR/PIS, incluidos atributos (entre muchos otros no especificados) como ID de usuario de EHR,
- Proveedor de atención médica regulado, una especialización de usuarios de HER/PIS, cada uno de los cuales tiene una función professional (RPIS)
- ID de instancia del sistema OS,
- ID de organización,
- Rol profesional; una clase de posibles roles que se pueden asignar a los usuarios de HER/PIS con fines de control de acceso,
- Rol de HER/PIS; una clase de posibles roles que se pueden asignar a los usuarios de HER/PIS con el fin de controlar el acceso (los ejemplos incluyen médico, odontólogo, farmacéutico, paciente / persona, dispensador, investigador, etc.),
- Mapeo de roles de EHR/PSI: mediante el cual un conjunto de roles del sistema de información de los puntos de servicio (POS) se asigna a un conjunto de roles de HER/PSI o donde un conjunto de roles en una implementación de EHR jurisdiccional se asigna a los de otra jurisdicción,
- Transporte de acceso discrecional; es decir, cuando un proveedor de atención médica confiere acceso a la HCE de un paciente / persona específico a otro proveedor de atención médica
- Política de seguridad de la información y
- Dominio de seguridad de la información.



10. GOBIERNO DEL EHR

18.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

¿Por qué un EHR requiere gobernanza? La gobernanza es necesaria porque los custodios de la atención médica no utilizarán un EHR a menos que tengan la seguridad de que sus responsabilidades de custodia no se verán comprometidas en el proceso. Sin esa garantía, los usuarios no confiarán en el sistema. Sin esa confianza, el usuario no hará un uso generalizado y eficaz del EHR.

La gobernanza eficaz de una HCE interoperable se basa en varios componentes centrales:

- articulación clara de confianza y responsabilidad,
- establecimiento de estándares mínimos,
- criterios de cumplimiento y medición del cumplimiento, y
- marcos y políticas y procedimientos detallados

Como se discutió en la mesa de arquitectura, el **MSP** es muy conciente de que no tiene mandato para participar en la gobernanza de las operaciones de EHR o para desarrollar políticas operativas o para evaluar el cumplimiento.

Este documento continúa evolucionando dentro de un marco colaborativo de consultas con expertos del BID en informática de la salud y se espera que se logre un amplio consenso sobre la arquitectura conceptual de P&S. Sin embargo, la cuestión de cómo exactamente el diseño seguro y protector de la privacidad, la implementación y operación continua de la EHR es, en última instancia, una cuestión que debe resolverse mediante cualquier estructura de gobernanza de la información que se establezca para guiar el despliegue de la EHR en Ecuador y el futuro flujo de información interjurisdiccional que facilitará la EHR.

Muchos problemas de gobernanza de EHR están sin resolver al momento de escribir este documento. Al afirmar que la resolución de problemas de gobernabilidad está fuera del alcance de este documento, los autores de ninguna manera desean disminuir la importante tarea de resolver estos importantes problemas.

Hacemos énfasis sobre dos cuestiones de gobernanza que pertenecen al contenido de este documento:

(1) Uno de los supuestos hechos en este documento tiene implicaciones significativas para la gobernanza; es decir, Supuesto: "*Cada implementación de la EHR almacenará la información médica personal (PHI) bajo el gobierno de la jurisdicción de implementación.*" Esto tiene implicaciones no solo para las transferencias de información entre jurisdicciones, sino también para el mantenimiento de la soberanía sobre la información mantenida bajo custodia.

(2) Si bien el énfasis en este documento está en proteger la privacidad de los pacientes / personas, la privacidad de los proveedores de atención médica no es menos importante. Como se indica en este documento, la información confidencial obtenida durante el proceso de registro incluye información personal y debe protegerse como tal. De manera más general, los proveedores de atención médica deben estar seguros de que la información recopilada con fines de tratamiento y atención no se utilizará de manera secundaria para controlar los hábitos de práctica de los proveedores de atención médica individuales (identificables) sin su consentimiento expreso. Hacer lo contrario invita a dejar de utilizar el EHR por parte de los proveedores de atención médica.

18.2. DESARROLLO DE MODELOS Y MARCOS DE GOBIERNO

Es necesario abordar los problemas relacionados con la transferencia de PHI a través de sistemas interoperables. Incluso dentro de una jurisdicción, sería necesario

establecer modelos de gobernanza para abordar las transferencias intrajurisdiccionales de PHI de una institución a otra. Quedan muchas preguntas pendientes. ¿Cuáles son las funciones del intercambio de datos entre organizaciones? Cuales son los criterios mínimos para acuerdos efectivos de intercambio de datos? ¿Cómo se aborda la custodia y se mantienen las responsabilidades del custodio cuando los datos fluyen de una jurisdicción a otra o de una organización a un EHR?

Tales preguntas requieren mucha discusión y resolución de políticas. Durante los talleres de la mesa de arquitectura, los participantes expresaron claramente la necesidad de desarrollar un consenso sobre qué modelos de gobernanza serían más efectivos. También querían un marco claro dentro del cual se pudieran responder las preguntas sobre gobernanza y políticas. Este marco y estos modelos de gobernanza serán necesarios para respaldar el despliegue de la arquitectura técnica.

Existe una incertidumbre considerable entre los representantes de la RPIS en cuanto a las responsabilidades de custodia de información generada en la atención médica, especialmente en lo que se refiere a las divulgaciones entre instituciones de la PHI, la claridad es esencial si los custodios de la atención médica van a utilizar el EHR con confianza y seguridad de que sus responsabilidades de custodia no se verán comprometidas en el proceso.

Si bien estos problemas de gobernanza están mucho más allá del alcance de un documento de arquitectura, el desarrollo y la implementación de la EHR dependen fundamentalmente de que estos problemas de gobernanza se aborden de manera adecuada; sin embargo, los problemas de gobernanza pueden resolverse en el futuro, los representantes de la RPIS han indicado claramente que una gobernanza eficaz es fundamental para garantizar la confianza de los proveedores de atención médica y del público en general en la seguridad, integridad y confiabilidad de los registros de salud electrónicos.

18.3. DESARROLLO DE POLÍTICAS Y PROCEDIMIENTOS

La operación efectiva de la arquitectura conceptual P&S no será posible como se describe en este documento sin el desarrollo de las siguientes políticas y procedimientos (la siguiente no es una lista exhaustiva):

(1) Una política de control de acceso que determina, para cada rol de usuario y en cada jurisdicción, los servicios de EHR que el usuario puede utilizar y los campos de datos de EHR a los que el usuario puede acceder o actualizar;
(2) Un mapeo, cuando corresponda, de los roles de los usuarios organizacionales con los roles de los usuarios de EHR. Esto respaldará la implementación de una jurisdicción de gestión de usuarios organizacionales confiables;

(3) Un mapeo de roles y privilegios de acceso del EHR de una jurisdicción a otra para todas las jurisdicciones que permitan solicitudes de acceso (bajo circunstancias estrictamente controladas) de usuarios en otra jurisdicción
(4) Una política para la denegación o revocación del consentimiento, incluida una descripción definitiva de las directivas de consentimiento permisibles y las circunstancias bajo las cuales pueden aplicarse o anularse;
(5) Una política sobre el mapeo de la Identificación única del paciente/persona entre jurisdicciones.
(6) Una política sobre lo que constituye niveles adecuados de autenticación y una evaluación de amenazas y riesgos de las combinaciones de factores de autenticación que proporcionarán formas equivalentes de lograr este nivel de autenticación
(7) Un esquema de mensajes de consentimiento adoptado a nivel nacional y con apoyo y aplicación jurisdiccional.

11. ESTÁNDARES DE PRIVACIDAD Y SEGURIDAD

Los estándares correctos adoptados en el momento adecuado pueden hacer una contribución importante al desarrollo del EHR y a su eficiente funcionamiento continuo. Lo harán aplicando restricciones de diseño críticas: los estándares elegidos apropiadamente conservan el tiempo y el esfuerzo de los diseñadores al proporcionar una base estable de capacidades y procesos predefinidos que no necesitan ser reinventados.

En este documento se consideran tres tipos de estándares:

(1) Estándares de mejores prácticas que especifican en detalle cómo se debe llevar a cabo una actividad;
(2) Estándares de evaluación que especifican un nivel mínimo por debajo del cual el desempeño se considera inaceptable, o un nivel deseado en el que el desempeño se considera efectivo o merece la certificación; y
(3) Normas técnicas que especifican en detalle cómo funcionan los protocolos de tecnología de la información

Algunos de estos estándares son:

(1) Lenguaje de marcado de control de acceso extensible (XACML),
(2) Lenguaje de marcado de afirmaciones de seguridad (SAML),
(3) El estándar de cifrado de lenguaje de marcado extensible (XMLEnc), y
(4) El estándar de firma digital del lenguaje de marcado extensible (XMLDSig).

12. IMPLICACIONES PARA LOS PROVEEDORES DE LOS SISTEMAS DE INFORMACIÓN DE LA RPIS

Sin la cooperación de los proveedores para modificar e implementar sistemas EMR/HIS (o como los denominamos de manera general en este documento, “sistemas de los puntos de servicio – POS) para interactuar con el EHR, el EHR no llegará ni cerca de alcanzar su potencial. Es así como las entidades deben compromete a trabajar en estrecha colaboración con los proveedores o con sus desarrolladores (si sus sistemas fueron desarrollado in-house) para garantizar que esta arquitectura conceptual sea completa y pueda implementarse de manera efectiva.

Esperamos que las jurisdicciones hagan referencia a esta arquitectura al planificar y diseñar EHR interoperables y, por lo tanto, los proveedores deben esperar que los aspectos de esta arquitectura se mencionen en los RFP. Por lo tanto, la comprensión de esta arquitectura para los proveedores de soluciones en el mercado de la salud ecuatoriano es esencial.