UNIVERSIDAD CENFOTEC

Maestría en Ciberseguridad

Documento Final del Proyecto de Investigación Aplicada

"Diseño de una estructura de seguridad de la información de expedientes digitales especializados para centros médicos".

Sustentante

Maynor Gerardo Agüero Marín

San José, CR, mayo, 2019

Derechos de autor

Agradecimiento

Agradezco en primer lugar a Dios, que me ha guiado en todo el camino de mi vida, dándome la fuerza, la capacidad, la inteligencia y la sabiduría para evitar los obstáculos presentados y conseguir las metas propuestas.

A mis profesores y en especial a Carlos Manuel Calvo Muños, por guiarme y aportar su ideas, conceptos, experiencias e ingenio en el proceso de la confección de este trabajo tan importante.

A mi familia, por la comprensión y el apoyo brindado durante el tiempo que he dedicado al estudio y en especial en la elaboración de este trabajo.

Dedicatoria

Dedico este trabajo a mis grandes amores, las dos mujeres que han hecho de mí lo que soy y al hombrecito que me cambió la vida.

A mi madre María Julia, la mujer que me dio el regalo de la vida, la oportunidad de aprender a luchar por lo que quiero y enseñarme el camino a seguir en la vida.

A mi esposa Agnes, con quien he pasado los momentos más difíciles y los más hermosos de mi vida.

A mi hijo Sebastián quien cambio mi vida con solo el existir y darme la oportunidad de poder escuchar de su boca la palabra papá.

A los tres, gracias por ser como son, un regalo de Dios.

Tribunal examinador

Tabla de contenidos.

Resumen

Como parte de los procesos de una aplicación de seguridad en la información del historial clínico del paciente, esta investigación tiene la intención de servir de base para definir una estrategia de análisis y diseño para la creación de una estructura de seguridad de la información de expedientes digitales especializados para centros médicos.

Este estudio viene a colaborar con el fortalecimiento de la seguridad de los datos clínicos de los pacientes, ante la inminente digitalización de la totalidad de los expedientes de salud y su transformación del actual formato físico a uno completamente digital.

Con respecto al diseño de la estructura de seguridad, este propone examinar las alternativas para crear expedientes digitales confiables, en salud, desde el punto de vista de la seguridad de la información. En esta investigación se identifican los requisitos necesarios para asegurar la información de un expediente digital; se toman en cuenta las buenas prácticas de la seguridad informática y la de los archivos médicos. Se plantea la generación de una estructura de expediente digital que se complemente con los sistemas de información desarrollados actualmente y que permita la confiabilidad de la información incluida por los distintos funcionarios que interactúan con el expediente del paciente.

Con la añadidura de esta estructura de seguridad digital, los sistemas de información actuales que administran datos clínicos contarán con un verdadero expediente digital que les garantiza a los asegurados, la no modificación de los datos clínicos.

CAPÍTULO I

INTRODUCCIÓN

1 Introducción

El sector salud de Costa Rica está inmerso en una realidad tecnológica, que obliga que la información clínica sea accedida desde cualquier centro médico, en cualquier parte del país. Para poder lograr este objetivo, se han desarrollado sistemas de información, tanto en el sector privado como en el público, conocidos como expedientes digitales o expedientes electrónicos.

Esta transformación de los expedientes físicos a digitales no hace que los expedientes clínicos dejen de ser documentos de archivo. Por ello, según la norma internacional ISO 15489-1 (2001), los documentos de archivo contienen información que constituye un preciado recurso y un importante activo de la organización. La adopción de un criterio sistemático de la gestión de documentos de archivo, resulta esencial para las organizaciones y la sociedad a la hora de proteger y preservar los documentos como evidencia de sus actos. Un sistema de gestión de documentos de archivo se convierte en una fuente de información sobre las actividades de la organización, que puede servir de apoyo a posteriores actividades y toma de decisiones; se garantiza la asunción de responsabilidades frente a las partes interesadas presentes y futuras. También esta norma indica que un procedimiento de gestión de documentos debería producir documentos de archivo fidedignos que reúnan las características de autenticidad, fiabilidad, integridad y disponibilidad. (pág. 7) [8]

Por las razones citadas anteriormente, esta investigación plantea la idea, de que lo desarrollado en nuestro país, carece de confiabilidad, para convertirse en un verdadero expediente digital. Por ello, examina las características requeridas para tenerlo y plantea la estructura de seguridad, necesaria para que los datos no sean modificados y cumplan con las características de un documento de archivo y así se conviertan en un expediente digital confiable; igualmente los documentos del expediente físico que son catalogados como documentos auténticos, íntegros, fiables y disponibles, durante su ciclo de vida.

1.1 Generalidades

En general esta investigación busca evaluar las alternativas para diseñar una estructura de seguridad en un verdadero expediente digital, que le permita a los pacientes tener la confianza de que la información incluida en su expediente clínico digital sea confiable y no pueda ser modificada por ninguna persona.

1.2 Antecedentes del problema

El expediente de salud es por excelencia la herramienta utilizada por los servicios de sanidad para llevar el control de las dolencias de las personas, Este documento médico también es llamado por los profesionales en ciencias médicas como expediente clínico o historia clínica. Según De la Prieta Miralles (2002), la historia clínica nació gracias a Hipócrates en los años 460 antes de Cristo, al tener como fin el reflejo del estado de salud del paciente y sus familiares (p. 36) [1].

Desde entonces los expedientes clínicos han evolucionado de acuerdo con las herramientas tecnológicas del momento. Actualmente, con el auge de la informática y los sistemas de información, se ha querido migrar el expediente clínico a un formato digital que permita ser accedido de manera eficiente de forma remota.

En Costa Rica, el mismo gobierno de la república ha decretado una ley que consiste en establecer a nivel de la CCSS un expediente clínico digital, que, según La República de Costa Rica, en Ley 9162 (2013), en sus objetivos establece en el inciso a. Fortalecer la garantía constitucional del derecho a la vida y a la salud de los habitantes de la República, por medio del desarrollo y la creación del expediente digital único de salud en beneficio de todas las personas, al incrementar la calidad de los servicios de salud que recibe la población. También en el inciso c de la ley indica, que cada persona tenga un expediente electrónico con la información de toda la historia de atención médica, con las características de disponibilidad, integridad y confidencialidad (pág. 2) [2].

Con lo indicado en la ley 9162, el gobierno impulsa la creación de lo que ellos llaman expediente digital único en salud, más conocido como EDUS.

En el ámbito privado también se han realizado gestiones para el manejo de datos digitalmente. Por ejemplo, el Hospital Clínica Bíblica (2018), afirma en su revista *por su Salud* que, en los sistemas de información incluye el expediente electrónico que contiene todo un registro del paciente (pág. 24) [3].

El Hospital CIMA San José anuncia en artículo de Karla Barquero (2018), tener un sistema médico que involucra todas las áreas, tanto clínicas como financieras. Incluye el expediente médico electrónico y ha permitido agilizar procesos de admisión, de egresos e información a los médicos (pág. 2) [4].

Todos los antecedentes digitales mencionados anteriormente son desarrollos que hoy son una realidad, ya sea en el sector público como en lo privado; para efectos de esta investigación, no son considerados por sus características como un verdadero expediente digital.

1.3 Definición y descripción del problema

En Costa Rica se han desarrollado aplicaciones que administran la información de salud; por ejemplo, en su página oficial, la CCSS (2018), indica que, EDUS es la aplicación oficial de la Caja Costarricense de Seguro Social que le permitirá tener acceso desde su dispositivo inteligente a información relevante de su Expediente Digital Único en Salud (EDUS). (pág. 1) [5] Por lo que entendemos, que el proyecto más grande en nuestro país para diseñar un expediente digital es un software, que guarda la información de los pacientes en una o varias bases de datos. Por consiguiente y conociendo los niveles de seguridad de una base de datos bien diseñada y con sus respectivos roles de seguridad, siempre existe una persona con un nivel de DBA con los permisos para modificar información; por ello, la seguridad del expediente se encuentra sujeta a un nivel de confianza.

Debido a este nivel de confianza, surge el problema de plantear una estructura de seguridad para un expediente digital, que permita que la información clínica del paciente no se pueda modificar de ninguna forma.

1.4 Justificación

En el sector salud, tanto lo privado como lo público manejan información de los pacientes, de manera electrónica, a través de diferentes sistemas de información; pero no tiene definida una estructura de seguridad que garantice la confiabilidad de los datos clínicos de un paciente en un verdadero expediente digital. Por ello se está proponiendo el diseño de una estructura de seguridad de la información de expedientes digitales para centros médicos especializados, que le garantice a los usuarios, que los datos clínicos no podrán ser modificados por ninguna persona.

1.5 Viabilidad

1.5.1 Punto de vista técnico

Desde el punto de vista técnico, esta investigación es viable. Existen herramientas tecnológicas que pueden servir de base para la creación de la estructura por diseñar. También se está en la capacidad de realizar esta investigación y valorar las alternativas de diseño de este trabajo evaluativo. Se cuenta con conocimientos, para determinar los riegos en los que se está incurriendo. También se cuenta con la capacidad para evaluar las herramientas y tecnologías actuales, que permitan el diseño de una estructura de seguridad, para un expediente digital en el área de la salud.

1.5.2 Punto de vista operativo

Desde el punto de vista operativo, esta investigación es viable, ya que la seguridad de un expediente clínico en su versión digital es necesaria para brindar la confiabilidad a los documentos que lo conforman. Es importante poder garantizarles a los pacientes, que la información de su salud está protegida y que no podrá ser modificada de ninguna forma.

Se plantea viable, operativamente, el diseño de la estructura de seguridad de la información de expedientes digitales, especializados para centros médicos, al partir de los intereses identificados de la población que utiliza los servicios de salud y en especial los que dependen de un expediente digital, para que su atención sea rápida y oportuna. Se cuenta con el conocimiento necesario para plantear una solución adecuada y también se tiene el tiempo adecuado para dar una solución al problema planteado.

1.5.3 Punto de vista económico

Desde el punto de vista económico, esta investigación es viable, ya que se cuenta con la tecnología y las herramientas adecuadas para el diseño de la solución del problema, al tomar en cuenta que la inversión económica es nula, ya que las posibles herramientas están disponibles. Por ello, no se requiere inversión adicional en licencias o derecho de uso de software y que solo se está planteando el diseño de una estructura de seguridad de la información de expedientes digitales, especializados para centros médicos.

1.6 Objetivos

1.6.1 Objetivo general

Diseñar una estructura de seguridad de la información de expedientes digitales especializados para centros médicos.

1.6.2 Objetivos específicos

Analizar la seguridad actual de los expedientes físicos en salud para definir los controles por utilizar en el expediente digital.

Seleccionar el formato de almacenamiento más adecuado para la seguridad de los expedientes digitales.

Determinar la herramienta tecnológica apropiada para la autenticación de documentos que permita la confiabilidad de la información del expediente digital.

Establecer la base para la seguridad de la información en el almacenamiento de los documentos del expediente digital.

Formular un procedimiento de control digital para la indexación de nuevos datos al expediente digital, al mantener la confiabilidad de la información.

Definir el medio que consolide los procedimientos y herramientas que forman parte de la estructura de seguridad de la información en el expediente digital.

Describir la estructura de seguridad de la información que garantice la no modificación y confiabilidad de los datos incluidos en el expediente digital.

1.7 Alcances y limitaciones

1.7.1 Alcances

Como alcance de esta investigación se pretende el diseño de una estructura de seguridad de la información de expedientes digitales especializados para centros médicos. Este trabajo es una evaluación de la problemática en el resguardo de la información digital del paciente en bases de datos. Un sistema de información que permita se modifiquen los datos clínicos de los pacientes, no se puede considerar como expediente digital. Con esta investigación se pretende corregir los inconvenientes encontrados mediante el diseño de la estructura de un verdadero expediente digital para centros médicos.

1.7.2 Limitaciones

Como limitaciones de esta investigación, se tiene que, no se entregará ninguna solución desarrollada, sino más bien, la propuesta de diseño de la estructura de seguridad de la información de expedientes digitales especializados, para centros médicos. No se abarcarán temas relacionados con la seguridad física, lógica o de la red. Tampoco se entregará ningún desarrollo de software, ni se analizará la seguridad de ningún software, ni base de datos. También, por tratarse de una investigación que incluye varias herramientas que conforman la estructura de seguridad de la información del expediente clínico relacionado con la salud pública de nuestro país, no se entrará en el detalle o definición de normas, reglamentos y estándares que se puedan adoptar para el funcionamiento de la estructura de seguridad; el trabajo se centrará en el diseño.

1.8 Estado de la cuestión

1.8.1 Revisión sistemática

En esta revisión sistemática se localizaron los trabajos de ontologías que tratan aspectos de seguridad de la información, tecnologías, controles y estrategias en el ámbito relacionado con la estructura de seguridad que se piensa diseñar.

Teniendo en cuenta que el tema por investigar es de una estructura de seguridad de la información de expedientes digitales especializados para centros médicos. Se realizó una búsqueda exhaustiva por separado, de cada uno de los temas que conforman la posible estructura de seguridad, al conocer que la información que se busca no se encuentra en un consolidado. Esta búsqueda se realiza en dos tipos de fuentes de información: La Primera, en fuentes impresas físicamente, como libros, revistas y reglamentos de salud; en segundo lugar, fuentes digitales como libros, reglamentos, leyes, artículos racionados y otras encontradas mediante los repositorios explorados.

Repositorios utilizados

La lista de repositorios utilizados en esta investigación y sobre la cual se ejecutó la revisión sistemática de las ontologías encontradas son:
Google scholar, e-libro y SpringerLink.

Cadenas de búsqueda

Utilizando combinaciones AND sobre las palabras clave y conceptos relacionados, se establecen cadenas de búsqueda por utilizar, en la presente revisión.

- (Reglamento and expediente) and (Salud).
- (Expediente and clínico).
- (Expediente and digital) and (Salud).
- (Documentos and archivo) and (ISO).
- (Archivos and DICOM).
- (Archivos and PDF) and (Formatos).

- (Bases and datos) and (Seguridad).
- (Certificados and digitales).
- (Firma and digital).
- (Servidores and almacenamiento).
- (PACS and server).
- (Sistemas and almacenamiento).
- (Cadenas and bloques) and (Blockchain).
- (Health and information) and (Systems).
- (Estructuras and seguridad) and (Informáticas).
- (Structures and security) and (Computing).
- (Seguridad and información).
- (Security and information).
- (Arquitectura and seguridad).

Criterios para incluir y excluir fuentes de información

Después de la construcción y la revisión de los datos encontrados, se procede a la etapa de selección, en la que se identifican e incluyen los estudios primarios relevantes que a juicio de experto sean necesarios para completar el estudio y no hayan podido ser recuperados en las búsquedas realizadas.

Criterios de inclusión

En primer lugar, se identificaron los repositorios Google Scholar, e-libro y SpringerLink, que se sometieron a una fase de comprobación en cuanto a los resultados emitidos.

Segundo, se incluyen artículos emitidos entre los años del 2000 y el 2018, ya que se quiere tener un criterio real en cuanto al tema en cuestión, por lo que se definió un periodo de tiempo de 18 años para tomar en cuenta las publicaciones de un antes y un después de la digitalización de la información en salud, de nuestro país.

En tercer lugar, se incluyen leyes y reglamentos vigentes en Costa Rica, emitidos en años anteriores al 2000, que sean base esencial en el uso actual del expediente clínico.

En cuarto lugar, se incluyen artículos de fuentes de información, encontrados en buscadores de internet que sean solamente leyes, reglamentos, y trabajos de investigación importantes para la elaboración de este estudio.

En quinto lugar, se incluyen artículos en idioma inglés y español, encontrados en las búsquedas de los repositorios indicados.

Criterios de exclusión

Como primer criterio de exclusión, se descarta toda la información que no se muestre en las búsquedas de los repositorios utilizados.

En segundo lugar, se excluyen todos los artículos que, en el análisis sobre el título, las palabras claves y abstract del documento, no presenten datos importantes para esta investigación.

Tercero, no se tomarán en cuenta los artículos y obras literarias que, a criterio técnico, no muestren un aporte positivo para el desarrollo de este trabajo.

Hallazgos

Para mayor detalle de la literatura utilizada en este trabajo de investigación, en el apéndice uno se muestra los cuadros de hallazgos referentes a las obras literarias referenciadas.

CAPÍTULO II

MARCO CONCEPTUAL

2 Marco Conceptual

2.1 Expediente físico

El expediente físico, es un archivo en formato de papel que, Guerrero (2013), define archivo en formato de papel como, documentos que se guardan en soporte físico y / o material. Sigue siendo el formato más utilizado y se recomienda adaptar las normas relativas a la pertenencia y durabilidad (pág. 11) [6].

El expediente físico de salud conocido como expediente clínico nació para llevar el control de la salud de los pacientes en los centros médicos, ya sean hospitales, centros de atención primaria, consultorios médicos y otros establecimientos que llevan control de la salud de la población. Según el Reglamento del Expediente de Salud de la CCSS (1999), el expediente de salud es el conjunto de documentos derivados de la atención de una misma persona y, eventualmente, del producto de la concepción que en un establecimiento permanecen archivados bajo una misma identificación y con carácter de único. Se consideran sinónimos del término "expediente de salud": expediente médico y expediente clínico (pág. 1) [7].

El expediente clínico según la CCSS (1999), en su reglamento se justifica, al indicar que los expedientes de salud contienen la evidencia documental integrada sobre la atención brindada a los pacientes; esto le confiere un trascendental valor como instrumento de apoyo directo, en el proceso asistencial. Por ello, constituye la mejor fuente de información primaria para el análisis del estado de salud del individuo y la comunidad, para la evaluación de la calidad de la atención y para la administración de los servicios de salud (pág. 7) [7].

2.1.1 Autenticidad

Por las razones citadas, estos documentos de archivo clínico tienen controles establecidos para garantizar la autenticidad que, según ISO 15489-1 (2001), un documento auténtico es aquel del que se puede probar.

a) que es lo que afirma ser,

b) que ha sido creado o enviado por la persona que se afirma que lo ha creado o enviado; y

c) que ha sido creado o enviado en el momento que se afirma (pág. 10) [8].

2.1.2 Confiabilidad

De igual manera, se debe asegurar la fiabilidad de la información que, según ISO 15489-1 (2001). Un documento de archivo fiable es aquel cuyo contenido puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores operaciones o actividades. Los documentos de archivo deberían ser creados en el momento, o poco después, en que tiene lugar la operación o actividad que reflejan, por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones (pág. 10) [8].

2.1.3 Integridad

Otro punto importante para garantizar la seguridad del expediente clínico, es la integridad, que para la CCSS (1999), en su reglamento del expediente de salud, en su artículo 17, indica, que toda atención brindada al paciente, en cualquier área del establecimiento de salud, debe registrarse en los formularios oficiales diseñados para tal efecto e incorporarse al expediente. Los registros originados en atenciones externas al establecimiento, que por decisión del responsable de la atención, pasen a formar parte del expediente, no podrán ser excluidos (pág. 4) [7]. También, ISO 15489-1 (2001), indica que la integridad de un documento de archivo hace referencia a su carácter completo e inalterado y que es necesario que un documento esté protegido contra modificaciones no autorizadas (pág. 11) [8].

2.1.4 Trazabilidad

Otro elemento importante para el expediente físico en salud, es la trazabilidad que, según ISO 15489-1 (2001), se define para los documentos de archivo, como la creación, incorporación y conservación de información sobre el movimiento y el uso de documentos de archivo (pág. 5) [8]. Igualmente, el Reglamento del Expediente de salud de la CCSS (1999), en el artículo 48 del reglamento del expediente de salud, indica que todo expediente extraído de su anaquel, deberá ser sustituido por la correspondiente "guía de reemplazo", en la cual se indicará como mínimo: la fecha del préstamo, el responsable y su destino (pág. 10) [7].

De acuerdo con lo anterior, se pueden identificar elementos de seguridad visibles en los expedientes físicos en salud, que convierten esta herramienta clínica en un documento autentico, confiable, íntegro y trazable.

En los expedientes clínicos se encuentran elementos de seguridad que evitan que los documentos puedan ser alterados o modificados. Un control para el resguardo de la información es incluir las anotaciones y documentos de forma cronológica, anexados, sin dejar espacios vacíos, semejante a una bitácora de trabajo.

Otro instrumento utilizado para validar la confiabilidad e integridad de los datos es, que cada nota o documento es firmada en manuscrito y se adjunta el código del profesional respectivo, que avala la información indexada al expediente clínico. También, para garantizar la autenticidad de un expediente clínico en formato físico, es importante que este haya sido creado por los funcionarios de la dependencia de Registros y Estadísticas de la Salud (REDES) y que el expediente utilice los formularios establecidos para cada situación.

Para garantizar la trazabilidad se tiene que llevar un control desde su creación hasta su destrucción, que evidencie como mínimo el nombre del funcionario, la fecha y el destino físico del expediente.

2.2 Formatos de archivos para almacenamiento de datos

Actualmente, la información de salud, en archivos digitales, se basa en sistemas de información, archivos con formatos de texto e imágenes, que almacenan las anotaciones y gráficos del personal médico y las imágenes de diagnóstico médicas realizadas por los servicios con equipos digitalizados.

De acuerdo con Medrano (2012), la información procesada se organiza en archivos o ficheros, identificados mediante un nombre compuesto por ocho caracteres, un punto, y otros tres caracteres más, denominados extensión (autoexec.bat), que identifican el tipo de archivo: archivo de texto, archivo gráfico, sonido, base de datos, etc. (pág. 13) [9].

Para poder seleccionar el formato de almacenamiento más adecuado para la seguridad de los expedientes digitales, hay que analizar las alternativas de archivos que soporten el texto, los gráficos e imágenes.

2.2.1 Bases de datos

Las bases de datos relacionales son la opción más utilizada por los sistemas de información para almacenar datos, de acuerdo con Valderrey (2014). Una base de datos relacional es un conjunto de una o más tablas estructuradas en registros (líneas) y campos (columnas), que se vinculan entre sí por campos en común que poseen la misma característica en ambas tablas, como por ejemplo el nombre del campo tipo y longitud (pág. 15) [10].

Los datos sensibles en su gran mayoría están almacenados en sistemas gestores de bases de datos. Según Valderrey (2014), aactualmente, los sistemas de gestión de bases de datos (abreviado mediante SGBD o DBMS) organizan y estructuran los datos de tal modo que pueden ser recuperados y manipulados por usuarios y programas de aplicación (pág. 16) [10].

Se puede decir que la protección de las bases de datos se plantea para evitar ataques externos y no del personal que administra las bases de datos, ya que siempre existe un perfil de usuario con privilegios de administrador de base de datos (DBA) que, según Osorio (2008), el DBA es la persona que ejerce el control centralizado sobre un DBMS (pág. 20) [11].

De acuerdo con Villalobos (2018), conocer los privilegios de los usuarios es para los atacantes otra posibilidad de producir daños en el SGBD (pág. 133) [12].

2.2.2 Archivos de texto

Los archivos de texto tienen distintas exenciones, de acuerdo con las aplicaciones que se le asocian. Hoy, existen varias compañías que desarrollan procesadores de texto que guardan la información con diferente extensión; por ejemplo, el tipo de archivo punto doc, está asociado principalmente con Microsoft Office Word, que es un programa que permite crear y compartir documentos, al utilizar un conjunto de herramientas de escritura. También, en la misma compañía Microsoft han creado diferentes versiones de Word con exenciones diferentes; esto genera un problema para usuarios no expertos o que no tengan la herramienta con la que se creó el archivo de texto.

Uno de los archivos de texto más sencillos y que casi todos los procesadores de texto pueden leer, es el archivo de texto plano. Estos archivos no guardan los caracteres que dan formato al texto, solo se muestra el texto sin formato y pueden ser editados por los más simples procesadores de texto.

Los archivos de texto que guardan los formatos son documentos digitales que permiten la escritura y la inserción de imágenes, gráficos y otros elementos. Estos documentos de texto son comúnmente utilizados por el personal de salud para generar reportes médicos, transcribir información de exámenes especiales, llevar controles clínicos, entre otros usos.

Actualmente existen una gran cantidad de procesadores de texto que guardan archivos en distintos formatos con exenciones como las siguientes.

.doc. Es un formato propietario de la empresa Microsoft.

.odt. Es el formato libre escogido por ISO, que se basa en xml para que cualquier procesador de texto pueda utilizarlo.

.rtf. Es un formato desarrollado por Microsoft para ser un formato multiplataforma.

.docx. Es el sucesor del formato .doc de Microsoft para implementar una compatibilidad con el formato xml.

.html. Es el formato adecuado para documentos que se publican en internet.

.txt Es el formato básico para texto; solo permite texto sin aspecto de visualización.

2.2.3 Archivos DICOM

En el área de salud y en las especialidades de imágenes médicas se utilizan los formatos de archivos DICOM (por sus siglas en ingles Digital Imaging and Communications in Medicine). Según Álvez (2009) DICOM es un estándar en medicina para la comunicación de imágenes entre diferentes sistemas (pág. 195) [13].

Como afirma Ramos A. Hu J. y Lee K (2002)DICOM es un protocolo no propietario para el intercambio de información médica. Definen como un formato de imagen digital y una estructura de archivo para las imágenes e información asociada (pág. 63) [14].

Según Ruiz, Trujillo y García (2007) El formato DICOM específicamente describe:

i. el contenido de la información, incluyendo la estructura y codificación;
ii. servicios DICOM para la administración de la información y
iii. protocolo de mensajería (pág. 148) [15].

Según Pianykh (2009), la estructura de un archivo DICOM usa su propio lenguaje, basado en su modelo propio del mundo real. Se interpreta el mundo real como todos los datos físicos o descriptivos, como por ejemplo el nombre del paciente, el tipo de estudio, el dispositivo médico, los parámetros de la adquisición, la imagen digital, etc. que son vistos por DICOM como elementos con sus respectivos atributos y propiedades (pág. 11) [16].

Basado en estas definiciones, se puede entender que la estructura DICOM determina una clasificación entre los datos, permite una dependencia entre los grupos de elementos, que agilizan la identificación, el acceso a las variables y los parámetros de interés, dentro de un mismo archivo DICOM.

Para la utilización de datos con formatos de texto, se deben generar los datos digitales siguiendo el estándar DICOM, en cuyo caso es posible leerlos y almacenarlos como imágenes, al utilizar esta norma.

De acuerdo con Gutiérrez, Núñez, Aguirre y Delgado (2014), en el apartado 15 del estándar DICOM (PS3.15), se especifican perfiles y políticas de seguridad, así como medidas técnicas para las entidades de aplicación involucradas en el intercambio de información (p. 177) [17].

En general, de acuerdo con PS3.15, la seguridad de las imágenes DICOM siempre va a estar ligada a los sistemas de información radiología (RIS) y a los sistemas de almacenamiento y comunicación, llamados PACS (Picture Archiving and Communication System).

2.2.4 Archivos PDF

Según Adobe (2018), el formato de documento portátil (PDF) se utiliza para presentar e intercambiar documentos de forma fiable, independiente del software, el hardware o el sistema operativo. Adobe también indica que, PDF cumplen con la normativa ISO 32000 de intercambio de documentos electrónicos (pág. 1) [18].

Un elemento importante del formato PDF es que es un estándar abierto y reconocido por ISO, lo que significa que no depende de una empresa o software específico para su creación y lectura. Tanto así que Microsoft (2018), indica que, Word puede exportar el documento a un archivo PDF, que tiene el mismo aspecto en equipos Macintosh y Windows (pág. 1) [19].

La garantía que tienen estos archivos, por ser un estándar abierto, es de acuerdo con ISOtools.org (2017), que los archivos PDF son totalmente independientes e interoperables, funcionando correctamente con el software PDF de cada proveedor. Los usuarios finales deben ser capaces de obtener resultados equivalentes independientemente de la elección de software que lleven a cabo. Esta característica fundamental que los archivos PDF siempre sean visualizados y se opere con ellos de la misma forma, es la razón principal para el éxito de la tecnología (pág. 1) [20].

El formato PDF según el Banco de la República de Colombia (2013), es la herramienta pública empleada en empresas con estándares mundiales para una distribución e intercambio seguros y fiables de documentos electrónicos. Gobiernos, empresas y formadores de todo el mundo han adoptado el formato PDF de Adobe® para agilizar el intercambio de documentos, aumentar la productividad y reducir la dependencia del papel (pág. 1) [21].

Dentro de las ventajas de usar este formato se tiene que:

- El PDF puede ser abierto en cualquier dispositivo.
- El PDF ocupa muy poco espacio en tu disco duro.

- Hoy, es fácil de generar.
- Es fácil para visualizar.
- El usuario puede prohibir la impresión o la edición del documento.
- El formato permite usar formas electrónicas para determinar la autenticidad del documento.

Las desventajas que se tienen son:

- Los archivos PDF no están hechos para ser editados.
- La edición de archivos PDF no es gratuita.
- Es más fácil editar archivos en otros formatos.
- El formato PDF está orientado a la visualización.
- Es virtualmente imposible añadirle grandes bloques de texto.

Tomando en cuenta las ventajas y desventajas de estos archivos, nos da la idea de que una de las principales cualidades de los documentos PDF es la poca oportunidad que se tiene para poder modificar la información; aunado a que estos archivos soportan el uso de firma electrónica, los convierten en documentos confiables que no podrán ser alterados.

2.3 Herramientas para la autenticación

2.3.1 Criptografía

La autenticación de los documentos es esencial para dar confiabilidad a la información de un expediente digital en salud. Una alternativa importante es el uso de criptografía que, según Granados (2016), es la ciencia encargada de diseñar funciones o dispositivos. Son capaces de transformar mensajes legibles o en claro, a mensajes cifrados, de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) solamente pueden ser factibles con el conocimiento de una o más llaves (p. 6) [22].

Este método de cifrar y descifrar información mediante criptografía, genera propiedades deseables para aplicar en cualquier documento que se quiera proteger contra modificaciones. Tanto así que Escrivá, Romero y Ramada (2013), indican que, mediante técnicas criptográficas, pueden garantizarse tres propiedades vitales para la seguridad: confidencialidad, (cifrado simétrico y asimétrico), autenticación (cifrado asimétrico) e integridad (función Hash) (p. 92) [23].

Con respecto a la criptografía simétrica y asimétrica, Granados (2016), indica que, en criptografía existen deferentes documentos digitales que se usan para garantizar las propiedades de confidencialidad e integridad; estos documentos son la integración de los dos tipos de criptografía: la simétrica y la asimétrica. Al hacer esta integración se compensan las desventajas de los tipos de cifrado y se utilizan las mejores características de cada uno; se combinan rapidez del cifrado simétrico, con la facilidad de la administración de llaves del cifrado asimétrico (p. 22) [22].

2.3.2 Certificados digitales

De acuerdo con la información citada, se puede entender que estos métodos y técnicas de cifrado pueden ayudar a tener documentos inalterados, al utilizar herramientas ya existentes, como certificados digitales. Según Escrivá, Romero y Ramada (2013), el certificado digital, certificado de clave público o certificado de usuario, es un documento electrónico, identificado por un número de serie único y con un periodo de validez incluido en el propio certificado, que contiene varios datos. Está emitido por una entidad de confianza, denominada entidad de certificación y vinculada a su propietario con una clave pública (p. 96) [23].

Esta unidad de certificación es definida por Escrivá, Romero y Ramada (2013) como, una entidad a la que no más usuarios confían la creación, asignación y revocación de los certificados digitales. Su misión es asegurar que un certificado sea válido, esté vigente y corresponda a su usuario poseedor. Por tanto, permite garantizar

la autenticidad y veracidad de los datos que aparecen en los certificados digitales (p. 97) [23].

En Costa Rica estas herramientas no son desconocidas, la ley 8454 (2005), indica según el artículo primero, que se aplicará a toda clase de transacción y actos jurídicos, públicos o privados, salvo disposición legal contraria (p. 1) [24]. También se creó en ese mismo año 2005, el reglamento a la ley de certificados, firmas digitales y documentos electrónicos, con el objetivo de reglamentar y dar ejecución a la ley 8454.

Con base en la legislación vigente en materia de certificados, firmas digitales y documentos electrónicos, la firma digital es, según MICIT (2005), el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad e identificar en forma unívoca y vincular jurídicamente al autor con el documento (p. 6) [25]. De acuerdo a Escrivá, Romero y Ramada (2013), esta firma digital trata de resolver el problema de autenticidad del mensaje, es decir, que el mensaje recibido es exactamente igual al original, (integridad) y que además proviene de quien dice venir (autenticación de origen) (p. 92) [23]. A esto hay que añadir también la necesidad de garantizar el no repudio, es decir, que el emisor no pueda negar haber sido él quien generó el mensaje.

2.3.3 Firma digital

De acuerdo con lo anterior, se puede entender lo que menciona Escrivá, Romero y Ramada (2013) que, la firma digital se basa en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (p. 94) [23]. Que en el caso de nuestro país lo hace el ente certificador que, según el MICIT (2005), es la persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales (p. 4) [25]. Este certificador realiza el proceso de certificación que, de acuerdo con el MICIT (2005), es, el proceso de creación de un certificado de llave pública para un suscriptor (p. 4) [25].

Después de la creación del certificado digital y su respectiva firma digital o electrónica, se tiene la herramienta para poder autenticar los documentos digitales que,

de acuerdo con el MICIT (2005), son cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático (p. 6) [25], que tendrán un valor igual al firmado manualmente con el puño y letra. Como indica Escrivá, Romero y Ramada (2013), la firma electrónica reconocida tendrá, respecto a los datos consignados en forma electrónica, el mismo valor que la firma manuscrita, en relación con la consignación en papel (p. 95) [23].

2.4 Almacenamiento de archivos

Para establecer una base de seguridad para la información de los documentos de un expediente digital médico, hay que tomar en cuenta la estructura para almacenamiento.

2.4.1 Servidores

Según Kroenke (2003), un servidor es una computadora que forma parte de una red y provee servicios a otras computadoras denominadas clientes. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor. Algunos servicios habituales son el de archivos, que permite a los usuarios almacenar y acceder a los archivos de una computadora (p. 547) [26].

De acuerdo con Marchionni (2011), un servidor de archivo permite compartir el material y guardarlo de manera segura y ofrece una mayor capacidad de almacenamiento, que los equipos de escritorio. Puede tener varios *storage* de distinta capacidad (p. 27) [27].

Para conocer información básica referente al tema de servidores propiamente, hay que dirigirse al apéndice uno; nótese un ejemplo, de las tecnologías médicas en cuanto a servidores.

2.4.2 Servidores de imágenes médicas

En el ámbito de almacenamiento de información relacionada a datos clínicos en grandes cantidades, ya se tiene un punto de partida. En el área de imágenes

médicas existen servidores de almacenamiento llamados PACS (Sistema de archivo y comunicación de imágenes).

De acuerdo con Thomas, Banerjee y Busch (2005), el concepto de comunicación de imagen digital y radiología digital, se introdujo a finales de los años 70 y se integró cada vez más en los hospitales de todo el mundo. La visión de un departamento completamente digital, incluye, además de los dispositivos de diagnóstico totalmente digitales, una nueva y completa estructura y estándar de comunicación digital. Con el apoyo de la Sociedad Internacional de Ingeniería Óptica (SPIE), la primera conferencia y el taller sobre sistemas de archivo y comunicación de imágenes (PACS), para aplicaciones médicas, se celebró en enero de 1982; durante esa reunión, se acuñó el término PACS, que se ha convertido en una herramienta clínica de uso habitual (p. 332) [28].

De acuerdo con las tecnologías digitales médicas, se hace la siguiente pregunta: ¿Qué es PACS? De acuerdo con Dreyer, Mehta y Thrall (2002), PACS representa la integración de dispositivos de adquisición de imágenes, estaciones de trabajo con pantalla y sistemas de almacenamiento, todo conectado a través de una red informática (p. 12) [29].

La estructura de los sistemas PACS tienen diferentes módulos, uno de ellos es el PACS Server que, según Guzmán y Vega (2014), tiene como objetivo el almacenamiento y transmisión de las imágenes provenientes de los equipos de adquisición (p. 5) [30].

El almacenamiento de las imágenes médicas se realiza utilizando técnicas de compresión, de acuerdo con los estándares DICOM. Estos hacen que los sistemas PACS sean compatibles con el estándar mundial para el intercambio de imágenes médicas.

De acuerdo con Mazzoncini y Covas (2009), el servidor PACS es la pieza fundamental de esta arquitectura y puede dividirse en dos componentes principales: el controlador PACS y el servidor de archivado de imágenes. El primero consiste en equipos y programas que controlan la comunicación y todo el flujo de datos en el PACS; el segundo es responsable del almacenamiento, la seguridad y la integridad de los datos de las imágenes recibidas. En términos de hardware, el servidor de archivado de imágenes puede considerarse un "datacenter" compuesto por equipos de alto rendimiento, dispositivos de almacenamiento y conexiones de red ultra rápidas (pp. 4-5) [31].

Según Guzmán y Vega (2014), en el nivel internacional la comercialización de servidores de imágenes se encuentra fundamentalmente en manos de grandes compañías, como: General Electric, Siemens AG, Philips, Kodak, Agfa, Digital Imaging, Fujifilm y algunas otras (p. 18) [30].

De acuerdo con Rodríguez y Yero (2007), en todos los casos las soluciones se caracterizan por ser muy caras, lo que, si no está reflejado en el software, es apreciable en el hardware específico de la solución. También presentan limitaciones como la atadura a plataformas específicas (ej. Windows o UNIX) o a gestores de bases de datos relacionales determinados. Los que en los casos de servidores de elevado rendimiento utilizan gestores de bases de datos comerciales como SQL Server y Oracle, cuyas licencias son sumamente costosas. Mientras que aquellos que utilizan gestores libres se adhieren a opciones como MySQL que no resulta conveniente para manejar los inmensos niveles de información generada por los equipos en hospitales o clínicas radiológicas (p. 18) [32].

2.4.3 Administración de archivos

La administración de archivos es esencial en el almacenamiento de datos en grandes cantidades. De acuerdo con Muñoz (2017), en los sistemas informáticos modernos gestionados por sistemas operativos actuales como Windows o Linux, los

archivos siempre tienen un nombre y siempre se almacenan dentro de estructuras jerárquicas de directorios del sistema principal de archivos (p. 40) [33].

Complementando lo anterior, Medrano (2012), indica que los archivos se ubican en directorios; el nombre de un archivo, es único en ese directorio (pág. 14). [9] Para ello, Muñoz (2007), añade que, en definitiva, no pueden existir dos archivos con el mismo nombre en la misma trayectoria o ruta; se entiende por ruta el camino que hay que seguir desde la raíz de la estructura jerárquica hasta donde se encuentra el archivo (pp. 40-41) [32].

Según Medrano (2012), el nombre de un archivo y la ruta al directorio del archivo lo identifican de manera unívoca entre todos los demás archivos del sistema informático. (pág. 14) [9] Por ello, Muñoz (2017), indica que, en el mismo lugar no puede existir otro archivo con el mismo nombre (pág. 14) [33].

Medrano (2012), señala que la mayoría de los ordenadores organizan los archivos en jerarquías llamadas carpetas o directorios. Cada carpeta puede contener un número arbitrario de archivos y también puede contener otras carpetas. Las otras carpetas pueden contener más archivos y carpetas y así sucesivamente, se construye una estructura en árbol, en la que una «carpeta raíz» puede contener cualquier número de niveles de otras carpetas y archivos (pág. 14) [9].

De acuerdo con Muñoz (2017), todos los sistemas de archivos proporcionan métodos para proteger los archivos frente a daños accidentales o intencionados. Los sistemas operativos asignan a los archivos los denominados atributos o permisos. Con estos atributos o permisos, se indica qué se puede o no, hacer, sobre un archivo y su visibilidad, dentro de la estructura de archivos, qué usuarios puede hacer y qué cosas, en el archivo o incluso en el directorio (p. 41) [33].

La protección de los datos en un sistema de archivos, es imprescindible para garantizar la integridad de la información. Caballero y Clavero (2016), señalan que

la integridad de los datos es un concepto utilizado en muchos contextos, para referirse a la exactitud y fiabilidad de los datos. Es decir, la integridad garantiza que los datos están completos y sin variaciones del origen (p. 95) [34].

Por tal razón, es importante garantizar la integridad de los archivos desde su almacenamiento. De acuerdo con Muñoz (2017), los atributos que se pueden asignar a un archivo, dependerán del sistema operativo y del sistema de archivos utilizado (p. 41) [33].

Caballero y Clavero (2016), agregan que, la estructura básica de permisos en ficheros está compuesta por tres tipos de permisos:

- Lectura (r). Otorga privilegio de acceder al contenido del fichero.
- Escritura (w). Otorga el privilegio de poder modificar el contenido del fichero. (Agregar, sobrescribir o eliminar el fichero).

Ejecutar (x). Otorga el privilegio de poder indicarle al sistema operativo, que ejecute el fichero como si fuera un programa (p. 110) [34].

2.5 Control digital para la indexación de documentos.

En los expedientes médicos la indexación de nuevos documentos es un proceso continuo que se repite cada vez que el paciente es atendido o se realiza un examen especial. Por tal razón encontrar una herramienta para crear un control de transacciones digitales para la indexación de nuevos documentos al expediente digital, es de suma importancia para mantener la confiabilidad de la información.

Una opción para este control son las bitácoras digitales, que son el registro de la información importante y las acciones que se lleven a cabo en las actividades seleccionadas. Para crear el adecuado control para los requerimientos de esta investigación, se analizan las herramientas que se apeguen mejor a lo exigido por este trabajo.

2.5.1 Bitácoras en SGBD

Normalmente en los sistemas de información tradicionales se utilizan las bases de datos para generar tablas de auditoría que muestren las transacciones que se han realizado con la data resguardada. De acuerdo con Ramakrishnan y Gehrke (2007), en un SGBD, un archivo puede crearse, destruirse y se le pueden insertar y borrar registros. También soporta exploraciones; la operación de exploración permite recorrer todos los registros del archivo de uno en uno (p. 281) [35].

En el ámbito de la auditoría de datos, las bitácoras son estructuras generalmente usadas para registrar las modificaciones que se dan en la base de datos. Las bitácoras, según Chávez (2013), son herramientas que permiten registrar, analizar detectar y notificar eventos que suceden en cualquier sistema de información utilizado en las organizaciones; es la estructura más ampliamente usada para grabar las modificaciones de la BD (p. 1) [36].

De acuerdo con La Red (2014), los archivos realmente se modifican, pero antes de cambiar cualquier bloque: • Se graba un registro en la bitácora (“log”) de escritura anticipada en un espacio de almacenamiento estable: — Se indica la transacción que produce el cambio, el archivo y bloque modificados y los valores anterior y nuevo. Si la transacción tiene éxito y se hace un compromiso: • Se escribe un registro del compromiso en la bitácora. Las estructuras de datos no tienen que modificarse, puesto que ya han sido actualizadas. Si la transacción aborta: • Se puede utilizar la bitácora para respaldo del estado original: — A partir del final y hacia atrás: Se lee cada registro de la bitácora. Se deshace cada cambio descripto en él. • Esta acción se denomina retroalimentación. Por medio de la bitácora se puede: • Ir hacia adelante (realizar la transacción). Ir hacia atrás (deshacer la transacción) (p. 307) [37].

Las bitácoras también son conocidas en el ámbito informático como *logs* que, según San Martín (2014), es un término anglosajón, equivalente a bitácora en

español. Este mismo autor indica que la estructura de cada uno de los registros consta de una serie de campos para cada transacción:

- Identificador de transacción (Ti): es único para cada transacción que realiza la operación (escribir), es decir, cada transacción que va a modificar un dato.
- Identificador de elemento de datos (E): es único del elemento que se va a escribir.
- Valor nuevo (Vn): es el valor que tendrá el elemento después de escribirlo.
- Valor anterior (Va): es el valor que tiene el elemento antes de escribirlo (p. 18) [38].

2.5.2 Cadenas de bloques (Blockchain)

Según publicación de Karame (2016), el Blockchain surge como una herramienta innovadora que resulta útil en varios escenarios de aplicaciones. Una serie de grandes actores industriales, como IBM, Microsoft, Intel y NEC, están invirtiendo actualmente en la explotación de la cadena de bloques para enriquecer su cartera de productos. Varios investigadores y profesionales especulan que la tecnología Blockchain puede cambiar la forma en que hoy se ven varias aplicaciones en línea. Aunque todavía es pronto para decirlo con seguridad, se espera que el Blockchain estimule cambios considerables en una gran cantidad de productos y tenga un impacto positivo en la experiencia digital de muchas personas en todo el mundo (p. 2) [39].

De acuerdo con Tur (2018), la tecnología Blockchain constituye la base sobre la que se construyó Bitcoin y fue introducida por primera vez por su autor Satoshi Nakamoto en su white paper: *“Bitcoin: A Peer - to – Per Electronic Cash System ”,* publicado en 2008 (p. 29) [40]. Fue, varios años más tarde, cuando se comenzó a analizar la posibilidad de hacer uso de dicha tecnología para algo más. También, según Bartolomé, Bellver, Castañeda y Segura (2017), Blockchain es el nombre de una

tecnología que permite mantener registros descentralizados y distribuidos de transacciones digitales (p. 2) [41].

Tur (2018), afirma que la cadena de bloques es una base de datos apoyada en tecnología *peer to peer* y por tanto compartida por múltiples nodos, en la que se registran bloques de información (p. 25) [40]. Se entiende como una base de datos distribuida que archiva información en bloques entrelazados, para agilizar la recuperación de los datos y verificar que la información no ha sido modificada.

Según Ibáñez (2018), en Blockchain se comparte valor sin censura y se replica o distribuye la información introducida; por eso, a la cadena de bloques en ocasiones se le denomina internet del valor, al permitir un sistema de creación y conservación perenne de valor económico, donde cada activo digital sea único según sus hashes u otras características (lo que facilita su perfecta individualización registral y dotarle de la nota de infungibilidad). A tal efecto, es preciso que en la red no solamente se incorpore información, sino que además se contabilice en la base de datos (p. 61) [42].

Cada bloque de esta tecnología contiene tres elementos: La información, el hash del elemento información y el hash del bloque anterior. Por tanto, los bloques se enlazan mediante el elemento que contiene los apuntadores hash que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al bloque inicial.

De acuerdo con Ibáñez (2018), una Blockchain es concebible como libro mayor. Ciertamente, la metáfora no es afortunada, pese a que viene a reflejar las virtudes de Blockchain como espacio colector o recopilatorio de un conjunto de transacciones (p. 61) [42].

Según publicación de Anindya Ghose (2018), con respecto al funcionamiento de la tecnología de Blockchain, hay cinco principios básicos subyacentes en la tecnología.

1. Base de datos distribuida: Cada participante de la cadena de bloques tiene acceso a toda la base de datos y a su historia completa. No hay alguien que controle por sí solo los datos o la información. Cada participante puede verificar directamente los registros de sus contrapartes de transacción, sin intermediarios.

2. Transmisión de persona a persona: La comunicación ocurre directamente entre pares, en lugar de hacerlo a través de un nodo central. Cada nodo almacena y envía información a todos los demás.

3. Transparencia con seudónimo: Cada transacción y su valor asociado es visible para todos los que tengan acceso al sistema. Cada nodo, o usuario, en una cadena de bloques se identifica por medio de la dirección alfanumérica, exclusiva de más de 30 caracteres. Los usuarios pueden elegir el anonimato o brindarle pruebas de su identidad a otros. Las transacciones ocurren entre direcciones de la cadena de bloques.

4. Irreversibilidad de los registros: Una vez que una transacción entra en la base de datos y que las cuentas se actualizan, los registros no pueden alterarse, porque están vinculados con el registro de todas las transacciones previas (de ahí el término “cadena”). Se despliegan diversos algoritmos y enfoques para asegurar que los registros en la base de datos sean permanentes, ordenados en forma cronológica y disponible para todos los demás en la red.

5. Lógica computacional: La naturaleza digital del libro de registros significa que las transacciones de la cadena de bloques pueden atarse a la lógica computacional y programarse esencialmente, de forma que los usuarios pueden definir algoritmos y reglas que activan automáticamente transacciones entre nodos. (p. 22) [43]

De acuerdo con Lin y Liao (2017), la tecnología Blockchain no solo es una técnica única, sino que contiene Criptografía, Matemáticas, Algoritmo y Modelo económico. Se combinan redes de igual a igual y utilizan algoritmos de consenso distribuidos para resolver el problema tradicional de sincronización de bases de datos distribuidas; es una construcción de infraestructura integrada de campos múltiples (p. 655) [44].

En resumen, se puede asegurar que las propiedades que hacen a la cadena de bloque eficiente y segura, son: la replicación punto a punto (P2P), la descentralización (no hay un punto central), su irreversibilidad e inmutabilidad (para modificar un bloque deben ponerse de acuerdo todos los nodos), Criptografía y seguridad (información encriptado con llave pública y privada), Privacidad y transparencia (Blockchain de carácter privado), Integridad (para hacer trampa se requiere que toda la red esté de acuerdo) y Cronología (Blockchain cuenta con un registro seguro del tiempo de creación y modificación de un documento).

Tomando en cuenta la información anterior, se puede indicar que Blockchain tiene una gran capacidad para brindar seguridad a la información, dado que esta herramienta tecnológica fue creada pensando principalmente en la integridad de los datos. Por ello, podemos apoyarnos enormemente en ella, para utilizarla como resguardo de la integridad de la información, ya que para esto fue originalmente diseñada.

2.6 Sistema de información

Para utilizar como medio que consolide las herramientas y procedimientos de una estructura de seguridad, los sistemas de información encajan en el punto medular de la estructura requerida.

De acuerdo con Peralta (2009), un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio (p. 7) [45].

Los sistemas de información realizan actividades tales como entradas (datos generales), procesos (cálculos), almacenamiento (guardar información), salidas (reportes), con el fin de automatizar procesos operativos y proporcionar información para apoyar la toma de decisiones.

De acuerdo con Peralta (2009), los Sistemas de Información que logran la automatización de procesos operativos dentro de una organización, son llamados frecuentemente Sistemas Transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc. Por otra parte, los Sistemas de Información que apoyan el proceso de toma de decisiones son los Sistemas de Soporte a la Toma de Decisiones, Sistemas para la Toma de Decisión de Grupo, Sistemas Expertos de Soporte a la Toma de Decisiones y Sistema de Información para Ejecutivos. El tercer tipo de sistema, de acuerdo con su uso u objetivos que cumplen, es el de los Sistemas Estratégicos, los cuales se desarrollan en las organizaciones con el fin de lograr ventajas competitivas, a través del uso de la tecnología de información (p. 7) [45].

En el ámbito de salud, también se utilizan sistemas de información con los fines mencionados, pero dirigidos a la automatización de procesos, para brindar un mejor servicio al paciente convaleciente.

2.6.1 Sistema de información en salud

Un sistema de información en el campo de la salud se puede definir como un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de un centro médico.

Según Fernández (2017), las características de un sistema de información en salud son los criterios considerables en las etapas de diseño y control de esos sistemas. En el campo de la salud, intervienen diferentes ámbitos de acción, tanto en el

área administrativa como en la prestación de servicios; las características aprendidas deben considerarse independientemente del campo de uso (p. 24) [46].

Los sistemas de información en salud (SIS), también son conocidos como sistemas de información hospitalarios (HIS). La función de estos sistemas, según Cerritos, Fernández y Gatica (2003), es la de apoyar las actividades en los niveles operativos, tácticos y estratégicos, dentro de un Hospital. Para tal efecto se utilizan las computadoras para recabar, almacenar, procesar y comunicar información clínica y administrativa (p. 10) [47].

2.6.2 Sistemas de información radiológica

Los sistemas de información en el ámbito radiológico, son imprescindibles para llevar a cabo las actividades de gestión. Es la herramienta utilizada hoy en día en los departamentos de radiología para llevar el control de las citas y la generación de información hacia los equipos de diagnóstico y PACS.

Según citan Temes y Torres (2007), las siglas RIS son las que habitualmente se utilizan para designar la aplicación informática, capaz de dar soporte a las actividades de un departamento de Radiodiagnóstico. Estas actividades comprenden tanto las de gestión como las puramente asistenciales (p. 339) [48].

Estos mismos autores indican las cualidades que debe poseer un buen sistema:

- Debe ser completo, capaz de satisfacer todas las necesidades.
- Personalizable, capaz de adaptarse a las circunstancias de cada institución.
- Robusto, capaz de soportar todo el flujo de información.
- Intuitivo, de fácil manejo.

- Integrable con otras aplicaciones asistenciales, fundamentalmente con los sistemas de archivo y comunicación de imágenes (PACS) o el sistema de información hospitalario SIH o HIS (acrónimo inglés de Hospital Information System), y con aplicaciones clínicas, especialmente la historia clínica electrónica y el gestor de peticiones clínicas (p. 339) [48].

2.6.3 Sistemas de visualización

Un buen software para la visualización de documentos electrónicos o un software que cumpla con los requisitos necesarios, es un componente crítico para disponer de un buen sistema de gestión de documentos. Por ejemplo, de acuerdo con Angarita y Beltrán (2008), un alto porcentaje de la información médica se representa en imágenes digitales y análogas producidas en diversas modalidades como tomografía computarizada, resonancia magnética, radiografía computarizada, entre otros (p. 1) [49].

Los sistemas de visualización buscan poder representar archivos de diferentes tipos, a partir de información almacenada en un formato estándar que permitan obtener características particulares para la visualización de las imágenes requeridas. Este tipo de sistemas debe poder manipular los archivos y presentarlos de una manera clara y concisa en la pantalla de visualización. Por ejemplo, un sistema de visualización de imágenes médicas debe administrar la carga en memoria de los metadatos de una imagen almacenada en un archivo dicom; de igual manera, debe poder guardar la imagen que está en la memoria en un archivo dicom.

Según Pereira, Leibniz y Carrasco (2013), otro aspecto dentro de los sistemas de visualización, es la transmisión remota de los datos entre el servidor y los clientes (p. 5) [50]. Con respecto a esto, se puede añadir lo que cita Bengochea y Patricio (2005), que una representación visual puede comunicar algunos tipos de información, de una forma mucho más rápida y eficaz que cualquier otro método (p. 273) [51].

En la actualidad, un sistema de visualización típico es el de una biblioteca virtual, que tiene como funciones, de acuerdo con Bengochea y Patricio (2005): reunir, procesar, difundir, almacenar y usar la información documental para dar servicio a la sociedad (p. 274) [51].

De igual manera este mismo autor indica que las interfaces visuales se han hecho familiares a los usuarios en numerosas aplicaciones informáticas. Sin embargo, es todavía un área en crecimiento en el campo de la representación visual de grandes volúmenes de información textual (p. 275) [51].

Uno de los puntos altos de estos sistemas es la visualización en tiempo real. Este tipo de visualización permite la toma de decisiones en un tiempo corto, facultando el acceso continuo de la información para el bienestar del servicio brindado.

2.7 Estructura de seguridad

Una estructura de seguridad es esencial para la implementación de un expediente digital en salud, por lo que su diseño requiere la utilización de procedimientos y herramientas que le den protección a la información clínica del asegurado.

2.7.1 Seguridad de la información

Como dice en su frase célebre el experto y escritor de diversos libros de seguridad informática y criptografía, Bruce Schneier, *“la seguridad de la información es un asunto de personas, procesos y tecnología”*. Con estas palabras, se puede plantear que una estructura de seguridad de la información garantiza la confianza de las personas en un procedimiento determinado. En el caso de un expediente digital, la estructura de seguridad debe dar garantía de que la información no puede ser alterada.

De acuerdo con San Martín (2014), la seguridad de los datos conlleva crear y aplicar una serie de estrategias que cubran los procesos en donde los datos son el activo primordial. Estas estrategias deben fijar el establecimiento de políticas, controles de seguridad y procedimientos para detectar amenazas que puedan explotar

vulnerabilidades y que pongan en riesgo dichos datos; es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y gestionan (p. 131) [38].

Se puede apuntar que una estructura de seguridad es un conjunto de procesos definidos estratégicamente, para minimizar las vulnerabilidades y el riesgo de un ataque a los datos.

También Álvarez y Pérez (2014), indican que la seguridad de la información implica el diseño y aplicación de un conjunto de medidas de seguridad interrelacionado de formas muy complejas. Se suele comparar la seguridad de la información con una cadena, donde cada uno de los numerosos elementos que conforman un sistema informático se asemeja a un eslabón (p. 6) [52].

Se puede agregar que las estructuras de seguridad de la información deben ser diseñadas pensando en la seguridad de los datos y que deben aplicar las medidas adecuadas para fortalecer la confianza de la información que resguarda la estructura aplicada.

Las estructuras de seguridad, de acuerdo con Cano (2018) son: reconocimiento de los procesos fundamentales que precisan la esencia que componen la Seguridad de la Información (SI). Entre estos se encuentran: la Información (reconocida como un activo), las Estrategias del Negocio (procesos que generan valor en la organización en su operación), los Fundamentos de la SI (basados en los principios de confidencialidad, integridad y disponibilidad como características de la información) (p. 28) [53].

De acuerdo con lo citado anteriormente, la seguridad de la información es la principal meta que conlleva la creación de una estructura de seguridad. Estructura que se basa en la seguridad informática que, según define Costas (2014), es un conjunto de

técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos (p. 17) [54].

2.7.2 Arquitectura de seguridad en sistemas de información

Siguiendo con el tema de seguridad de la información SANS, es una de las instituciones más prestigiosas a nivel mundial en el ámbito de la capacitación sobre seguridad de la información, define una arquitectura de seguridad de sistemas de información basada en cinco fases. Según SANS (2004), estas cinco fases son:

1. Fase 1. Realización de Evaluaciones de la Seguridad: el fin de dicha fase es encontrar vulnerabilidades al sistema de información, independiente de que se hayan aplicado o no controles.

2. Fase 2. Formulación del Diseño de los Objetivos de la Arquitectura de Seguridad: tiene su fundamento en los resultados de la Fase 1, de tal manera que se definan con un alto nivel de acierto los objetivos de la ASI; para ello, se tiene en cuenta la definición de la arquitectura lógica y física del sistema de información.

3. Fase 3. Construcción de Políticas y Procedimientos: teniendo los resultados de las dos fases anteriores, se procede a concebir una política apropiada para el negocio a través de su conocimiento. Esta debe ser definida en su estructura, al tener en cuenta el marco de la Política Corporativa y, en esencia, debe guiar a los usuarios internos y externos sobre la forma en la cual se debe utilizar el sistema de información.

4. Fase 4. Implementación del Diseño de los Objetivos de la Arquitectura de Seguridad: habiendo seguido secuencia en el cumplimiento de las fases, se establecen los plazos, la financiación y los recursos necesarios para implementar la ASI.

5. Fase 5: Integración de las prácticas de seguridad para mantener el estado de seguridad: se propende por el mantenimiento de un entorno de trabajo seguro, basado en la aplicación exitosa de las fases del modelo. Se logra al establecer el personal idóneo y con las capacidades necesarias para la evaluación y actualización de la arquitectura de seguridad del sistema de información (p. 7) [55].

2.7.3 Seguridad de la información en el sector salud

Desde el punto de vista del sector salud, en cuanto a controles y estrategias para el resguardo de la información, en Estados Unidos existe HIPPA por sus siglas en inglés, Health Insurance Portability and Accountability Act, que es la ley de Transferencia y Responsabilidad de Seguro Médico creada en el año 1996 para proteger a los trabajadores en el padecimiento de alguna afección médica. Esta ley plantea controles importantes que se pueden tomar en cuenta para la elaboración de la estructura de seguridad de la información del expediente digital especializado en salud.

Sería importante analizar controles tales como:

- Asegurar la confidencialidad.
- Asegurar la protección de la información electrónica.
- Asegurar el Intercambio de la información digital.

De acuerdo con los autores citados anteriormente y su criterio técnico, se entiende que la seguridad de la información, en un expediente digital especializado para centros médicos, tiene que implementarse acorde a una estructura adecuada basada en la automatización de los controles utilizados en el proceso manual; se añade un reforzamiento extra para proteger la información clínica del paciente, ya que hoy, es el activo más preciado en una institución dedicada a la salud.

CAPÍTULO III

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

3 Diagnóstico de la situación actual

Respecto al expediente de salud, este es un documento legal, que en muchos países se sigue conservando en papel, aunque se tengan completamente automatizados los procesos de la información en salud. Este formato puede ser revisado por un perito para comprobar la autenticidad de este, definir el momento exacto de su creación, identificar si fue o no alterado y quien fue el médico o personal responsable de emitir el diagnóstico o realizar el procedimiento correspondiente. También un sistema de información en salud puede otorgar facilidades para procesar el texto. Por esta razón, el cambio hacia el expediente digital se ve detenido, ya que las acciones de modificación de datos restan validez legal a los datos clínicos.

En la actualidad, los datos clínicos de los asegurados se pueden encontrar en dos formatos: el tradicional expediente físico en papel, aun utilizado en todos los centros médicos de nuestro país y el formato digital que se accede por medio de un sistema de información que guarda la data en bases de datos relacionales.

3.1 Datos clínicos en formato físico

El expediente físico es la herramienta médica que conserva la evidencia documental de la atención ofrecida al asegurado. Por tal razón, hoy es el documento de archivo más utilizado en los centros de salud, sin excepción. Tanto en la CCSS, como en las clínicas y hospitales privados, continúan utilizándolo, pese al también aprovechamiento de los sistemas de información digitales, en salud.

En el caso de la CCSS, uno de los puntos importantes por lo que se sigue utilizado, es el marco regulatorio para el resguardo de los expedientes en salud. Este reglamento solo habla de documentos físicos y no se ha modificado para la utilización de sistemas de información.

De igual forma, el sector privado continúa llevando la información en un expediente físico a pesar de que la tecnología está más asentada en estos establecimientos médicos. Una de las razones de mantener el formato físico es que el

expediente clínico es un documento de archivo que debe garantizar la autenticidad, confiabilidad e integridad de la información.

En Costa Rica, el sector salud, tanto privado como público, continúa utilizando el expediente físico como la principal evidencia legal, ya que las soluciones digitales actuales no han podido satisfacer los requerimientos necesarios para su sustitución.

Una de las principales razones por las que el formato físico sigue siendo utilizado, es la seguridad de la información. El formato digital actual no llena a cabalidad las necesidades de seguridad que requiere un documento de archivo en el ámbito de la salud, le falta una estructura de seguridad acorde con la información que almacena.

Para analizar por qué el formato físico sigue siendo la principal herramienta para el personal en salud, se realizó un pequeño análisis FODA de los dos formatos utilizados conjuntamente en la actualidad.

3.1.1 Fortalezas del formato físico

El expediente clínico en formato físico tiene fortalezas importantes que han convertido este documento de archivo en un documento difícil de sustituir. Estas fortalezas se mencionan a continuación.

- Cuenta con una regulación a nivel nacional por tratarse de un documento de archivo.

- A nivel de instituciones, ya sean públicas o privadas, el expediente está regulado por reglamentos específicos.

- Cuenta con controles que garantizan la autenticidad, confiabilidad, integridad y trazabilidad.

- Es el único documento de salud con valor legal para evidenciar la historia clínica, los procedimientos realizados y la atención brindada.

3.1.2 Oportunidades del formato físico

Hoy, es difícil hablar de oportunidades si nos referimos a un documento en papel, ya que los documentos electrónicos están sustituyendo el uso del papel. Por tal razón y en el caso específico del expediente clínico en formato físico, se debe tomar en cuenta el entorno y la información que almacena.

Con base en el conocimiento adquirido, en el tema se visualizan las siguientes oportunidades del expediente físico:

- La información histórica que contiene puede ser utilizada como referencia en futuras atenciones médicas.

- El expediente físico puede ser digitalizado y convertirse en parte de un expediente digital con una estructura adecuada.

- Su estructura y controles pueden ser utilizados como base de una nueva estructura digital que garantice la autenticidad, confiabilidad, integridad y trazabilidad del expediente clínico.

- Con la estructura y herramientas adecuadas, al digitalizarse este documento, puede adquirir el mismo valor legal que el expediente físico.

3.1.3 Debilidades del formato físico

El expediente físico tiene debilidades propias de cualquier documento hecha a base de papel. En el caso de este documento de archivo médico se mencionan las siguientes debilidades:

- La ubicación del expediente después de abandonar el archivo médico no es tan trazable como se requiere.

- Este documento de archivo por estar elaborado de papel es frágil y sufre desgaste de sus tapas y documentos internos.

- Se requiere un espacio físico grande para su almacenamiento.

- No es de rápido acceso, requiere ser trasladado de su lugar de almacenamiento al departamento que lo está requiriendo.

3.1.4 Amenazas del formato físico

Las amenazas están presentes en todos los entornos, los datos clínicos no son la excepción. En el expediente físico se visualizan las siguientes amenazas.

- Por tratarse de un documento físico, puede ser sustraído si no se aplican los controles de resguardo adecuados.

- Por estar hechos de papel, están propensos a perder la información por agua o fuego.

- Pueden ser víctima de actos de vandalismos.

- Puede ser víctima de un cambio de la última hoja de anotaciones en alguna de las secciones que lo conforman.

3.2 Datos clínicos en formato digital

El formato digital utilizado actualmente para gestionar los datos clínicos en nuestro país se centra en el uso de sistemas de informática que almacenan en bases de datos relacionales. Por ejemplo, la CCSS promociona fuertemente el EDUS que es una

plataforma para la atención y asignación de citas que integra varios sistemas de información de la institución, en el nivel interno.

El sector privado también ha incursionado en el uso del formato digital para almacenar los datos clínicos de los pacientes. Los grandes hospitales privados de Costa Rica tienen sus propios sistemas de información en salud. Estos sistemas, al igual que la CCSS se utilizan para llevar el control de la atención del paciente y la asignación de citas. Por ser entes privados, estos hospitales han conseguido llevar más largo estas implementaciones, al punto de poderlas ligar con la parte financiera y manejo de los insumos utilizados en la atención de los pacientes.

Propiamente en cuanto a un expediente digital, tanto el sector público como privado, no han podido lograr una digitalización completa de los datos clínicos por motivos de seguridad y del valor legal de la información. Recordemos que el expediente clínico es un documento de archivo que tiene un valor legal para su uso en litigios judiciales.

Al igual, como se realizó con el formato físico, se procede al análisis del formato digital actual.

3.2.1 Fortalezas del formato digital actual

En la actualidad con el uso de la tecnología es difícil encontrar algo que no se encuentre en formato digital. En este caso específico, la información clínica del paciente no es la excepción. En nuestro país se han venido utilizando aplicaciones automatizadas para llevar la información al formato digital orientadas a el mejoramiento del servicio al paciente.

Dentro de las fortalezas que nos ofrece el formato digital actual (sistemas de información en salud) tenemos:

- Permiten tener la información en todo momento de forma rápida.

- Permiten la aplicación de controles de seguridad de acuerdo con lo establecido en la legislación respectiva.

- Le da una sensación de seguridad a la información mayor que el formato físico.

- La información en formato digital, tienen menos posibilidad de ser extraviada o perdida.

- Permite agilizar la búsqueda de información requerida en el momento.

- Si se aplican buenos controles en el almacenamiento de los datos se evita la pérdida de información causada por un error o intento de sabotaje externo al personal de TI.

3.2.2 Oportunidades del formato digital actual.

Las oportunidades que se tienen con la utilización del actual formato digital van de la mano con el continuo desarrollo de la tecnología; logran que la información se vuelva agradable a la hora de accederla, específica en el momento de su búsqueda, actualizable al tiempo de añadir nueva información y exacta en el uso de esta.

Los sistemas de información en salud son el formato digital actual, que proporciona oportunidades como:

- Posibilidad de obtener ventajas que se van a reflejar en una mejor atención médica.

- Aumentar la capacidad de los procesos organizacionales, debido a los controles que se pueden implementar.

- Genera la perspectiva de utilizar tecnologías de punta para el mejoramiento continuo.

- Los sistemas de información pueden ser parte de una estructura de más compleja que brinden seguridad a la información.

- La información se puede convertir en una solución rápida y eficaz a la hora de analizarla y aplicarla en un diagnóstico médico.

- Permiten la implementación de herramientas que le generan confidencialidad y autenticidad a la información.

- Pueden administrar información digitalizada en formatos de texto, imagen y otros formatos para el diagnóstico en un entorno médico automatizado.

3.2.3 Debilidades del formato digital actual

Los formatos digitales y en especial los sistemas de información utilizados en el sector salud, no son completamente seguros, en cuanto a la seguridad de la información almacenada en sus bases de datos.

Seguidamente se muestran las debilidades encontradas en el formato digital utilizado en la actualidad.

- La seguridad está basada en la confianza del personal de TI.

- La información puede ser modificada, remplazada o eliminada por un funcionario de TI con un acceso de perfil DBA de las respectivas bases de datos.

- Generalmente son sistemas centralizados que dependen del funcionamiento de la infraestructura tecnológica.

- Es difícil la consolidación de la totalidad de la información referente a un paciente para su entrega.

- Como sistema de información no tiene la validez legal que sí tiene el expediente en salud en formato físico.

- No cuentan con herramientas para autentificar los datos que garanticen la autenticidad de la información.

3.2.4 Amenazas del formato digital actual

Los sistemas de información no están exentos de amenazas; aunque se disponga de la seguridad más actualizada, no se está libre de las amenazas tecnológicas. En el sector salud y en especial el actual formato digital, utilizado para gestionar la información de los datos clínicos, puede tener las siguientes amenazas.

- No cuentan con herramientas para autentificar los datos que garanticen la autenticidad de la información.

- Puede ser víctima de un ataque tecnológico desde afuera o dentro de la organización.

- Una mala configuración puede comprometer la seguridad de la información almacenada.

- Puede ser víctima de una modificación de la información clínica.

La información digital de los datos clínicos puede perderse o ser destruida, si no se resguarda adecuadamente.

CAPÍTULO IV

ANÁLISIS DE LAS TECNOLOGÍAS ACTUALES

4 Análisis de las tecnologías actuales

Para el diseño de una estructura de seguridad de la información de expedientes digitales, especializados para centros médicos, es importante realizar un análisis, de las tecnologías de nuestro ámbito, con las que podemos contar en la actualidad.

Como ya se identificó en el capítulo anterior, los centros médicos gestionan los datos clínicos en dos formatos: el formato físico y el formato digital. Este análisis, se centra en el formato digital y en especial las tecnologías existentes, actualmente, en nuestro entorno.

4.1 Tecnologías utilizadas en datos clínicos

En las instituciones médicas de Costa Rica, se ha impulsado la digitalización de los datos clínicos. Los esfuerzos se han basado en el uso de sistemas de información. Estos sistemas, ya sea en el sector público o privado, se han orientado en el aspecto funcional y han dejado de lado la seguridad y la privacidad de los datos.

4.1.1 EDUS

Para demostrar de una mejor manera estas afirmaciones, nos centraremos en la principal herramienta desarrollada en nuestro país (EDUS). Herramienta impulsada por el gobierno de la República, mediante la Ley del expediente digital único de salud, 9162.

El EDUS es un sistema de información integrado, desarrollado por la Caja Costarricense de Seguro Social, que trata de ser la única herramienta utilizada en los hospitales de la institución benemérita de la salud en nuestro país. El EDUS se encuentra como una herramienta integrada por los siguientes sistemas:

SIAC, un sistema para la adscripción de los asegurados y otorgamiento de citas, que automatiza el servicio de registros médicos.

SIFF, el un sistema de información integrada de fichas familiares, utilizado por los funcionarios de visita domiciliar para registrar información en la atención primaria brindada por la CCSS en las distintas comunidades.

SIES, una aplicación que permite la atención médica en consulta externa, hospitalización y el servicio de urgencias. Este sistema es el que registra la información más relevante en un expediente clínico; todavía no es utilizada en todos los centros médicos.

SICI, es un sistema que registra la información diagnosticada por los médicos, con base en los exámenes de diagnóstico de citologías.

MISE, el módulo tipo single *sign on* (SSO) que permite a los funcionarios del centro médico la autenticación para acceder a los distintos sistemas que integran el EDUS.

Una vez con el conocimiento básico de los principales sistemas que integran el EDUS, podemos iniciar a realizar el análisis, para identificar, si esta herramienta cumple con lo necesario para convertirse en una estructura de seguridad de información, de un expediente digital especializado para centros médicos.

Información clínica

El EDUS es utilizado exclusivamente en los centros médicos de la CCSS, por tal razón no se incluyen los datos clínicos de las citas realizadas por asegurados en los centros privados. También es importante indicar, que, con base en los sistemas que integran el EDUS, es fácil notar que esta herramienta no almacena los datos referentes a exámenes especiales de diagnóstico, como por ejemplo exámenes radiológicos, exámenes de laboratorio y otros exámenes especiales. Los resultados de estos exámenes de diagnóstico son almacenados en el expediente físico. Estos exámenes se generan en sistemas que no tienen conexión con el EDUS, ya que son aplicativos arrendados o adquiridos por necesidad propia del centro médico. Con base en esta

situación, entendemos que a pesar del uso de EDUS en la mayoría de los centros médicos, aun se sigue utilizando el expediente físico en formato de papel.

Documento de archivo

Un expediente clínico debe cumplir como mínimo cuatro aspectos importantes, para considerarse un documento de archivo:

Ser un documento autentico, por tanto, se debe tener la confianza de ser lo que afirma ser, se debe tener la certeza de que la persona que afirma haberlo creado, realmente lo haya creado y por último tener la seguridad del momento en que ha sido creado.

Ser un documento confiable, por consiguiente, debe representar completamente todos los hechos narrados, en los datos clínicos que da testimonio.

Ser un documento íntegro, que lo obliga a garantizar que la información presente en el documento no ha tenido ninguna modificación en el transcurso del tiempo, desde su creación hasta su utilización.

Ser un documento trazable, que ofrezca eficiencia, ya que se conoce en todo momento la ubicación del archivo; igualmente proporciona seguridad de la información, se debe saber quién tiene acceso a los documentos y cuándo lo hace; se lleva un control de quién accede a la información; también se debe dar seguimiento a los procesos y conocer las actividades realizadas.

En el caso de los SIS pueden cumplir a cabalidad la trazabilidad de los datos por medio de bitácoras transaccionales, programadas para registrar las modificaciones realizadas. Pero es imposible que se garantiese la confidencialidad, integridad y autenticidad sin utilizar certificados y firma digital. Por consiguiente, se considera que el EDUS no es un expediente clínico considerado como un documento de archivo.

Seguridad de la información

EDUS utiliza el módulo MISE para la autenticación y acceso a los aplicativos que lo integran. También, por su formato de sistema de información en salud, se conoce de la utilización de bitácoras basadas en movimientos registrados en una o varias tablas de Base de Datos. Seguridad considerada insuficiente, si se toma en cuenta el tipo de datos que se manejan.

Es conocido que el EDUS no ha implementado el uso de certificados y firmas digitales, como herramienta que garantice la identidad e integridad de la información. Por esta razón y tomando en cuenta la importancia para los asegurados de su información clínica, se puede afirmar que la CCSS le ha dado prioridad a los elementos prácticos y funcionales y ha dejado de lado la seguridad y la privacidad de los datos.

Validez legal de la información

El punto más importante de este análisis es la validez legal de la información, que se almacena en las diferentes bases de datos que tiene el EDUS. Una pregunta fundamental sería:

¿El EDUS tiene la misma validez que el expediente físico en papel?

De acuerdo con la información investigada y recopilada en este trabajo, se puede responder que el EDUS no cuenta con la validez legal que sí tiene el expediente físico. Los sistemas que integran el EDUS no utilizan herramientas que garanticen realmente que la información clínica es inalterable.

También es importante recordar que el EDUS es la integración de varios SIS en una sola herramienta tecnológica. Por esta razón, entendemos que cada uno de los sistemas, almacenan la información en al menos una base de datos. Esto hace complicado recopilar la información total de un asegurado, para generar la historia clínica; se garantiza la inalterabilidad de los datos en caso de ser solicitada judicialmente.

Con respecto a la validez legal de esta información digital, al consultar el artículo 368 del Código Procesal Civil de Costa Rica, nos damos cuenta que este artículo define los documentos como: *"los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas, y en general, todo objeto mueble que tenga carácter representativo o declarativo"*; queda por fuera todo documento en formato digital.

Todo documento digital tiene valor legal en Costa Rica siempre y cuando se encuentre firmado digitalmente; esto, con base en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica, Ley N. 8454, que aplica el principio de equivalencia funcional. Por tanto, un documento digital tendrá valor legal mientras se tenga garantía de identidad e integridad de la información, mientras este acreditada por una firma electrónica que así lo garantice.

En conclusión, al cuestionamiento de la validez legal del EDUS y teniendo en cuenta que esta herramienta no utiliza aun la firma digital, se debe dejar claro que, basado en lo indicado anteriormente, EDUS no cuenta con la validez que tiene el expediente físico, ya que no puede demostrar la autenticidad de los documentos que lo conforman como expediente clínico; de igual forma, no garantiza la confiabilidad e integridad de los datos. Al ser EDUS integrado por varios SIS, que guardan la información en diferentes bases de datos, no se garantiza al ciento por ciento, que la información es la que fue incluida por el especialista en salud, en el momento indicado.

Con el análisis realizado, no se está dando a entender que EDUS es un mal desarrollo, más bien se considera una herramienta en salud funcional. Lo que se trata de explicar es que EDUS no puede ser considerado como un expediente digital, aun, ya que no cuenta con la estructura de seguridad que se requiere, para tener un valor de carácter legal y así poder sustituir el expediente físico.

4.2 Tecnológicas requeridas para la estructura de seguridad

Una estructura de seguridad para expedientes digitales debe estar basada en tecnologías que permitan garantizar la autenticidad de los datos. Esta autenticidad debe estar respaldada por cada elemento de la estructura, desde el almacenamiento, la autenticación, la administración de la estructura, los controles y la visualización de los datos clínicos.

4.2.1 Almacenamiento

En primer lugar, se requiere adoptar un formato de almacenamiento de datos que permita la no modificación. En este punto, el mercado tiene a disposición herramientas adecuadas para almacenar información y presentarlo de una manera tradicional, de fácil utilización y que impida la modificación de los datos.

4.2.2 Autenticación de datos

En segundo lugar, es importante tener una herramienta que pueda autentificar los documentos emitidos en cada cita de diagnóstico o procedimiento realizado. En este caso, se pueden seleccionar herramientas a base de mecanismos criptográficos que permiten garantizar la autoría e integridad de los documentos digitales.

4.2.3 Estructura base

En tercer lugar, se debe establecer una base tecnológica que establezca los parámetros de confianza, necesarios para administrar la estructura de seguridad. En la actualidad, podemos encontrar herramientas en el mismo ámbito médico, que se pueden adaptar o tomarlas como ejemplo para diseñar la estructura requerida.

4.2.4 Indexación de documentos

Otro punto importante es la elección de una herramienta tecnológica que permita llevar el control de la indexación de documentos digitales al expediente. Para esta labor se pueden encontrar estructuras de datos que contengan y agrupen bloques de información que controlen la indexación de documentos y mantengan la integridad y autenticidad de la data.

4.2.5 Visualización de datos clínicos

Se debe adoptar una herramienta tecnológica que permita consolidar y visualizar la información digital del historial clínico de los asegurados. En este caso es necesaria una herramienta de visualización, diseñada, de acuerdo con el formato de almacenamiento, seleccionado en el primer punto y que ayude a mantener el grado de confidencialidad, autenticidad e integridad de los datos.

Esta herramienta de visualización no es algo desconocido para el ambiente médico, ya que en el área de radiología se utiliza el RIS y PACS para imágenes médicas, de igual manera en las bibliotecas virtuales se utiliza una herramienta similar para la visualización de libros.

Esta herramienta de visualización unida a todas las anteriores, debe consolidar una estructura de seguridad de la información que permita tener un verdadero expediente digital que resguarde la integridad y autenticidad de los datos clínicos.

Para el diseño de la estructura requerida en este trabajo, en el mercado se encuentran disponibles herramientas adecuadas y sencillas. Estas tecnologías pueden trabajar conjuntamente en una estructura funcional con el objetivo de brindar la seguridad a los datos clínicos y convertirlos en un verdadero expediente digital especializado para centros médicos.

CAPÍTULO V

PROPUESTA DE LA SOLUCIÓN

5 Propuesta de la solución

La solución aquí planteada intenta resolver una inquietud en cuanto a la seguridad de los datos clínicos de los asegurados que utilizamos los servicios de salud en este país. Para reforzar esta inquietud y conocer el pensamiento de los asegurados y el personal técnico informático, en cuanto a seguridad de los expedientes digitales, se aplicaron dos cuestionarios que aportaron un panorama más real, a la problemática planteada. El apéndice tres contiene la especificación de los cuestionarios aplicados.

Según los resultados obtenidos, la información clínica de todos los usuarios en los servicios de salud debe estar protegida en una estructura de seguridad completa y formada por elementos que garanticen la integridad de los datos en todo momento. Por esta razón es que el presente trabajo busca abrir una perspectiva para el lector, en el ámbito de seguridad de la información. Se identifican los aspectos requeridos en el desarrollo de una estructura de seguridad de la información, acorde con los expedientes digitales especializados para centros médicos.

5.1 Análisis de la seguridad actual del expediente digital en salud

Como se menciona en capítulos anteriores y, de acuerdo con el enfoque de expediente digital en salud, planteado en este trabajo, en la actualidad no existe un verdadero expediente digital en salud; esto, ya que lo existente, carece de la estructura adecuada para asemejarse al expediente clínico en papel. De igual forma, no se cuenta con una estructura de seguridad que garantice la confiabilidad de la información almacenada en las bases de datos.

La seguridad de la información de los datos clínicos almacenados digitalmente por los SIS desarrollados en los diferentes centros médicos, dependen del grado de confianza hacia el personal técnico informático, ya que ellos son los encargados del resguardo de la información y tienen los privilegios para la administración de las bases de datos.

Se considera importante diseñar una estructura de seguridad que elimine la relación de confianza con el personal técnico informático y se reemplace por uno que garantice la integridad de la información y así se pueda implementar un verdadero expediente digital especializado para centros médicos.

Este trabajo propone una estructura para el mejoramiento de la seguridad de la información respecto al almacenamiento y administración de los datos clínicos; se basa en herramientas tecnológicas que, al ser unificadas, permiten mejorar los procesos de seguridad utilizados hoy, en la información clínica digitalizada.

5.2 Formato de almacenamiento y presentación

En cuanto a la información clínica, las opciones tradicionales de almacenamiento en base de datos han demostrado ser bastante ineficientes para proteger los datos confidenciales, debido a que personas ajenas a la información, (personal técnico informático) la pueden manipular. Por esta razón y pensando también en la asimilación de los especialistas en salud como usuarios finales, en este trabajo se ha elegido el formato de archivo PDF, para el almacenamiento de los datos clínicos de los pacientes, como parte de la estructura de seguridad de la información de expedientes digitales especializados para centros médicos.

El formato PDF fue creado con el objetivo del almacenamiento ligero, para compartir documentos sin importar la arquitectura, o el sistema operativo utilizado en las máquinas de los usuarios. En la actualidad es el formato más adecuado, ya que puede contener textos, mapas de bits e imágenes, por lo que debe funcionar como el remplazo perfecto para el expediente clínico en papel.

Los archivos PDF son los más utilizados para presentar información que no debe ser modificada. El formato ya posee la capacidad de bloquear y cifrar la información para solo lectura, también es importante mencionar que hoy todo dispositivo posee un programa para la lectura de archivos PDF. De igual manera, por ser un formato

de código abierto, es posible generar fácilmente documentos, con cualquier lenguaje de programación y conservarlos a lo largo del tiempo.

En cuanto a la seguridad, un archivo PDF permite levemente no ser modificado a menos que se tenga un programa especial. Pero para efectos de este trabajo se enriquece la seguridad con la utilización de herramientas criptográficas que lo vuelven más seguro e íntegro, con el fin de poder darle a la información clínica, una validez legal, igual a la del expediente físico y así contar con un verdadero expediente digital en salud.

5.3 Autenticación e integridad de los datos

Para la validación de la integridad y autenticación de los datos del expediente digital planteado en la estructura propuesta, se decidió utilizar el método criptográfico conocida como firma digital.

Este método incorpora la identidad de la persona en el documento creado, al asegurar la integridad de la información incluida en el documento. Esto por medio de la aplicación del algoritmo matemático hash al contenido del documento; posteriormente la aplicación de una clave privada mediante el algoritmo de firma, para tener como resultado la firma digital del documento. Esta firma debe ser validada por medio de un software de firma digital para garantizar la vigencia del certificado firmante, revocación del certificado y la inclusión del sello de tiempo.

En nuestro país, el uso de esta herramienta les da valor legal a los documentos digitales, ya que, de acuerdo con la ley 8454, los documentos firmados digitalmente con el certificado emitido por el gobierno de la república tienen el mismo valor que su equivalente firmado manualmente. No obstante, en la actualidad ninguno de los sistemas utilizados por los centros médicos en el país, utiliza esta herramienta para validar y certificar la información clínica de los pacientes.

En el caso específico de la estructura de seguridad de la información, propuesta para el expediente digital especializado para centros médicos, la firma digital es la herramienta que garantiza la integridad, autenticidad y confiabilidad de los datos incluidos en los documentos de expediente digital, además de brindarle la legalidad necesaria a los documentos incluidos en el expediente clínico digital.

También es importante indicar que la compatibilidad de los archivos PDF, con la firma digital, es la más adecuada, ya que, con la utilización de desarrollos a la medida, se permite la configuración y uso de la firma digital, de una forma ágil y sencilla para el usuario final.

Para mayor tranquilidad de los usuarios en los servicios de sanidad, la firma digital viene a darle a los documentos del expediente digital en salud, seguridad de que el documento fue creado por la persona indicada y que no se ha alterado en ningún momento después de su inclusión como información clínica en el expediente digital.

5.4 Almacenamiento de la información

El almacenamiento de la información es un punto importante, ya que la estructura propuesta plantea como base, guardar archivos PDF, para mantener la información clínica digitalizada. Esto conlleva a la administración de una gran cantidad de archivos, por consiguiente, gran cantidad de espacio en disco.

Para cualquier lector que no conozca las tecnologías actuales de imágenes médicas, esta propuesta de almacenamiento le parecería algo ilógico; se toma en cuenta que actualmente las tendencias se centran en guardar información en Bases de Datos, con lenguajes SQL y NO SQL.

Esta propuesta de almacenamiento de archivos PDF, está inspirada y se basa en el almacenamiento de imágenes médicas, utilizadas comúnmente en las infraestructuras de almacenamiento digital, transmisión y descarga de imágenes radiológicas (RIS - PACS).

En las infraestructuras RIS-PACS, el sistema RIS administra la información de las personas, las resguarda en una base de datos relacional y las comparte con el equipo que genera el estudio radiológico, para que los sistemas de visualización lean los datos del examen; luego el equipo guarda la información en el servidor PACS que queda registrada en la base de datos relacional, la ubicación de los archivos DICOM. Además, se crea un archivo DICOMDIR que sirve para el re-direccionamiento de las imágenes médicas y así poder ser visualizadas de manera estándar, por los especialistas que utilizan distintos visualizadores DICOM.

5.4.1 Propuesta de almacenamiento

Para efectos de la propuesta, el SIS debe administrar la información de los asegurados en su respectiva base de datos, generar los documentos PDF, procesarla, guardarla en la ubicación de almacenamiento configurada, luego debe registrar la ubicación en la base de datos y generar un archivo para el direccionamiento, que muestre la lista de la estructura del expediente de la persona.

Fundamentado en el diseño del expediente físico, se plantea la siguiente estructura, para el almacenamiento de la información en disco del expediente digital especializado para centros médicos. Basado en las experiencias de la informática médica, en cuanto a imágenes DICON y su aplicación en plataformas PACS, se presenta la siguiente propuesta de almacenamiento.

1. Un directorio raíz con nombre igual al número de identificación de la personal.
    i. Debe incluir un visualizador para uso local.
    ii. Un archivo de direccionamiento (EXPDIR) para el visualizador.
        - El archivo EXPDIR se genera cada vez que se incluye un documento.
        - Sería un archivo de texto ligero para intercambio de datos.

2. Cinco subdirectorios para guardar los tipos de documentos.
    i. Identificación de la persona.
    ii. Atención en urgencias.
    iii. Atención en hospitalización.
    iv. Atención en consulta externa.
    v. Información de exámenes médicos.

3. El subdirectorio de identificación debe tener dos subdirectorios.
    i. Información de la persona.
    ii. Información de ubicación.

4. El subdirectorio de urgencias debe tener dos subdirectorios.
    i. Notas de enfermería.
    ii. Notas de evolución médica.

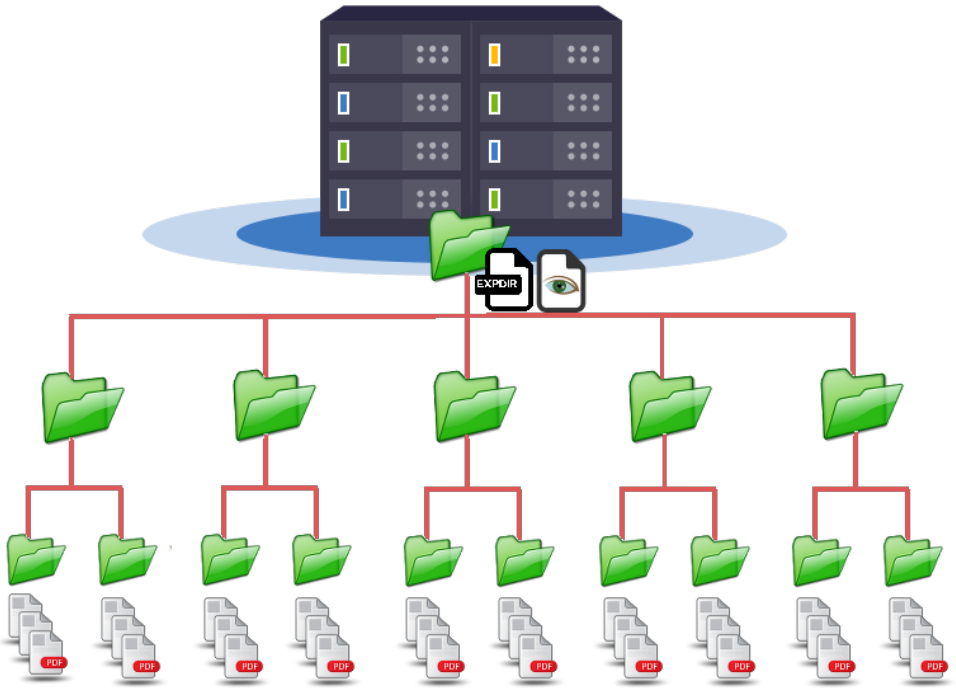
5. El subdirectorio de hospitalización debe tener dos subdirectorios.
    i. Notas de enfermería.
    ii. Notas de evolución médica.

6. El subdirectorio de consulta externa, debe tener dos subdirectorios.
    i. Notas de enfermería.
    ii. Notas de evolución médica.

7. El subdirectorio de exámenes médicos debe tener dos subdirectorios.
    i. Exámenes laboratorios.
    ii. Exámenes especiales.

8. Cada subdirectorio almacenará los documentos de la información del expediente en formato PDF.

Ilustración 1. Estructura de almacenamiento.



Esta estructura de directorios podría variar por necesidad o para facilitar la visualización de los datos; pero en términos de visualización, al utilizar el archivo EXPDIR no se tendrá ningún problema, ya que este archivo es quien da la ubicación de los documentos del expediente digital a los diversos visualizadores.

En términos sencillos, la plataforma de almacenamiento propuesta, trata de asemejarse a la utilizada en la informática médica para gestionar imágenes DICON en las plataformas PACS, con la diferencia de que los datos almacenados se convertirán en las anotaciones médicas para describir un procedimiento o diagnóstico clínico, que se indexará en el expediente digital del paciente.

5.5 Control para la indexación

Para garantizar la fiabilidad de la información clínica de la estructura propuesta, es importante tener un control digital, para la inclusión de nuevos documentos. Los expedientes clínicos no son foliados, llevan un control por fecha, firma y continuidad

en sus secciones internas. En el formato físico, este control, aunado al resguardo especial que recibe, impide la modificación de los documentos.

La propuesta para este control es incluir una bitácora digital, compuesta por una cadena de datos, creada mediante tecnología Blockchain. Con este control, lo que se busca es eliminar la intervención de las personas, ya que sería el SIS el que alimente la cadena de datos, de acuerdo con la inclusión de documentos.

Con la cadena de datos se evita la intervención de las personas en el proceso de registro de la bitácora transaccional; la tecnología Blockchain puede evitar el acceso no autorizado con sus algoritmos criptográficos seguros y su inmutabilidad que hace a los datos inviolables.

El control de los procesos de indexación de documentos se guarda en la cadena de bloques de la base de datos distribuida, que es una especie de registro de transacciones, donde la información no se almacena en un único ordenador (nodo), sino en múltiples terminales conectados entre sí. En este caso, se plantea que cada centro médico sea un nodo de la base de datos distribuida.

5.5.1 La función de Blockchain en el control de indexación

El procedimiento del control digital para registrar la información en la cadena de datos se debe realizar cada vez que se requiera ingresar un nuevo documento al expediente clínico digital. El proceso de ejecución será el siguiente:

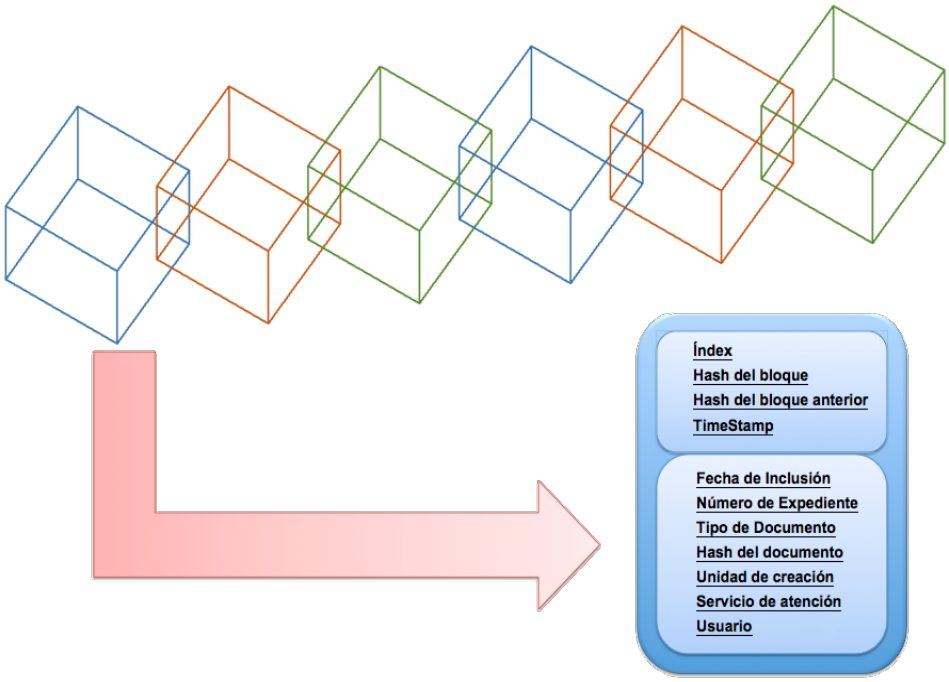
1. Se requiere ingresar un nuevo documento al expediente digital.
2. La transacción se presenta como un nuevo bloque.
3. El nuevo bloque es transmitido a todos los nodos de la red.
4. Todos los nodos de la red aprueban la validez de la transacción.
5. Con la aprobación, el nuevo bloque se añade a la cadena.
6. El documento se ingresa al expediente digital.

5.5.2 Información que se registra en los bloques

Cada bloque de la cadena lleva la información sobre la transacción realizada e indica los siguientes datos:

1. La identificación del bloque (Índex).
2. Hash del bloque anterior.
3. Hash del propio bloque.
4. Timestamp.
5. Datos de la transacción:
   a) Fecha inclusión del documento.
   b) Número del expediente.
   c) Tipo de documento incluido.
   d) Hash del documento.
   e) Unidad de creación.
   f) Servicio de Atención.
   g) Usuario de creación.

Ilustración 2. Información registrada en los bloques.



Esta estructura del bloque permite garantizar la confiabilidad de los datos incluidos en el expediente digital.

5.6 Administración de la información

En términos generales, en la actualidad los hospitales, tanto privados como gubernamental, han desarrollado sus respectivos SIS, programas similares que buscan mejorar el funcionamiento de los servicios brindados; es decir: consulta externa, hospitalización, urgencias y servicios de apoyo. De tal manera, es importante considerar que todos los servicios hospitalarios trabajan por medio de una herramienta informática que da soporte a la operación de este, sin importar el tipo de centro médico.

5.6.1 Herramienta para gestionar los datos

Los SIS han sido desarrollados para administrar la información clínica de los usuarios en los servicios de salud. Con el transcurso del tiempo se han convertido en herramientas indispensables que garantizan el adecuado registro de las acciones realizadas en los centros médicos. Algunas acciones que se pueden mencionar: contribuyen a fortalecer la calidad del registro de la información, estandarizan los criterios, incorporan nuevas formas de registro y se consolida como una fuente de información para la toma de decisiones de los profesionales en salud. Como el mejor ejemplo de un SIS, se tiene el EDUS, sistema que administra la información clínica de los asegurados de la CCSS, de una manera ágil y eficaz.

No obstante, estos sistemas de información en salud tienen como faltante, una estructura de seguridad, que les permita ser considerados un expediente digital en salud, de igual forma tener el valor legal del expediente en papel. Pero estos faltantes no los hacen inservibles o inútiles para convertirse en un engranaje más de la estructura de seguridad propuesta en este trabajo.

Como parte de la estructura de seguridad de la información, del expediente digital especializado en centros médicos, el SIS debe tener la función de administrar la información de los procedimientos o diagnósticos realizados, de la misma forma que lo

hace cualquier sistema de información. Solamente que, en la estructura propuesta, además de guardar la información, en una base de datos; debe crear un documento PDF, que sea firmado digitalmente por el especialista en salud, para garantizar la fiabilidad de los datos.

Por ejemplo, si nos centramos en el EDUS, este debería generar por diagnóstico o procedimiento realzado, un documento PDF, permitir la firma digital, registrar el movimiento en una bitácora transaccional digital y guardar el documento en una estructura adecuada para su visualización por cualquier centro médico, desde el mismo EDUS u otro SIS, adecuado a los estándares de visualización adoptados.

5.6.2 Medio de visualización

Las interfaces visuales se han hecho habituales para a los usuarios en numerosas aplicaciones informáticas. En cuanto a documentos PDF, se pueden tomar como ejemplo, las bibliotecas virtuales y los libros digitales que se pueden leer hoy. De igual forma, en el ámbito de la medicina y en especial en el área de radiología, las imágenes médicas se centran en la utilización de plataformas RIS PACS. Estos dos tipos de visualización manifiestan una forma de implementar un método, para presentar los datos clínicos en el expediente digital, planteado en este trabajo.

Tomando en cuenta las tecnologías existentes, se propone un medio de visualización, que tome como base los SIS ya existentes, Se les añade un módulo de visualización que permita estandarizar la forma de visualizar los documentos PDF que componen un expediente digital en salud. Este módulo de visualización de documentos debe tener la capacidad de interactuar con la base de datos donde se guarda la ruta de almacenamiento de los archivos y poder leer los archivos EXPDIR generados para el direccionamiento.

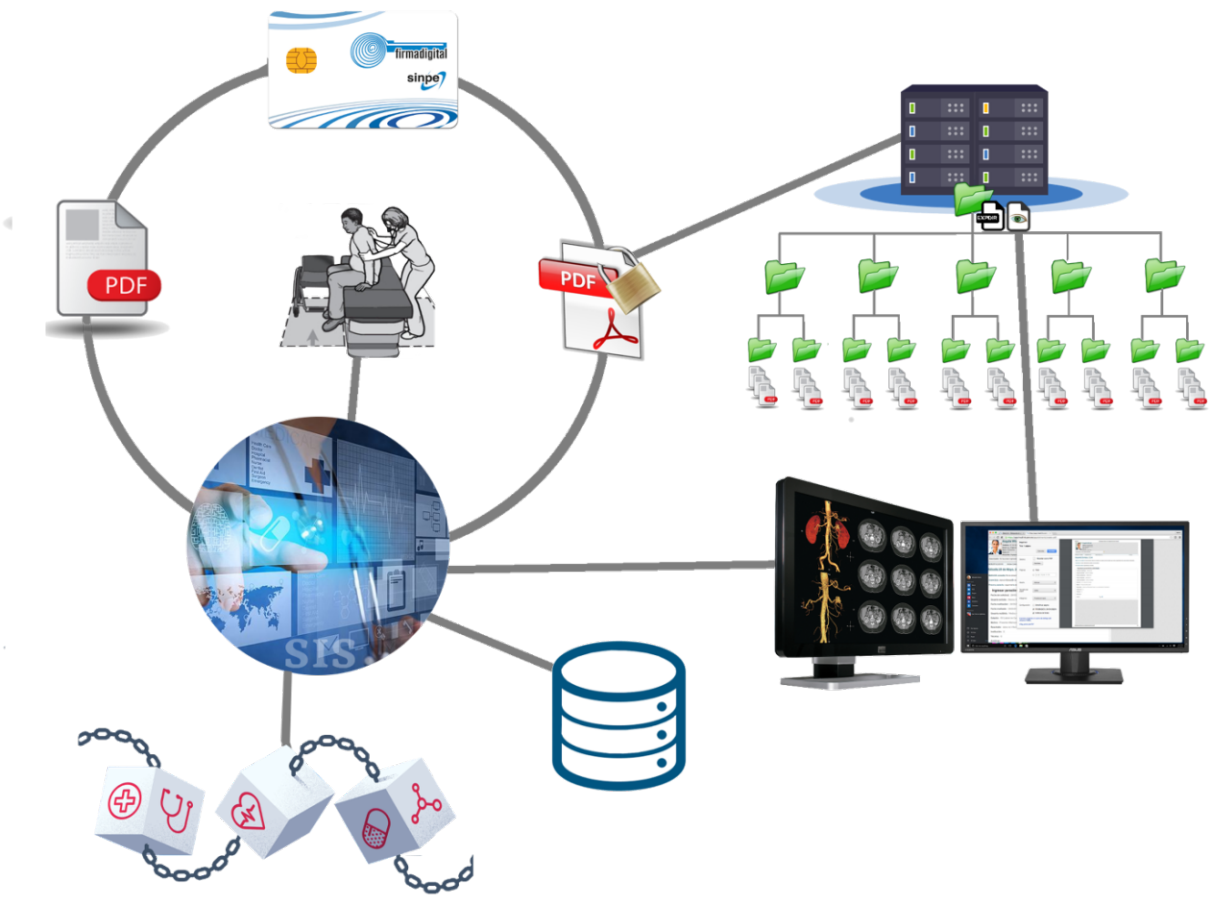
Como un aporte de esta investigación y basado en los archivos DICOMDIR se propone la implementación de un tipo de archivo EXPDIR en formato texto ligero que lea los metadatos de los documentos PDF, para indicarle al visualizador la ubicación en

disco de los archivos que conforman el expediente digital. Este tipo de archivo debe ser elaborado bajo los estándares de HL7 para facilitar el intercambio de información entre aplicativos heterogéneos.

5.7 Descripción de la estructura de seguridad

Como se muestra en la imagen, la estructura de seguridad se pone en funcionamiento con la atención del asegurado.

Ilustración 3. Estructura de seguridad



La principal herramienta tecnológica de la estructura de seguridad de la información para el expediente digital especializado para centros médicos, es el sistema de información en salud, o como se conoce en el ámbito de las tecnologías en salud, SIS.

En la estructura diseñada para garantizar la seguridad de la información clínica, el SIS es el encargado de administrar los dos procesos de la estructura: el proceso de almacenamiento de la información y el proceso de visualización del expediente digital clínico del paciente.

5.7.1 Proceso de almacenamiento de la información.

i. El SIS es el gestor de los procesos y el que pone en funcionamiento la estructura de seguridad de la información. Cuando se realiza un diagnóstico o procedimiento médico, el SIS guarda la información clínica y genera un documento PDF.

ii. Este documento PDF generado, es mostrado por el SIS para que el especialista en medicina lo firme digitalmente, con el certificado personal.

iii. Con el documento PDF de la atención médica debidamente firmado, el SIS gestiona el almacenamiento del archivo en el servidor asignado para el resguardo de los datos.

iv. Una vez guardando archivo en el servidor de almacenamiento, el SIS registra la ubicación física del documento en la base de datos correspondiente.

v. Una vez guardado el archivo y registrada la ubicación física, el SIS gestiona la creación de un nuevo bloque transaccional y lo registra en la cadena de datos del Blockchain privado.

5.7.2 Procedimiento para la visualización del expediente digital

i. Cuando el profesional en salud solicite al SIS se muestre un expediente digital, la aplicación accede a la base de datos y devuelve la ubicación en disco del expediente solicitado.

ii. Una vez conocida la ubicación en disco, el SIS se redisecciona a la raíz del directorio del expediente especifico.

iii. Ubicado en el directorio raíz, se ejecuta el archivo de visualización, para que se muestre el expediente digital.

iv. Una vez finalizada la consulta del expediente clínico, se registra lo correspondiente en la bitácora transaccional.

En general con esta estructura, se muestra de una forma ágil y diferente, una propuesta de seguridad a la información en expedientes digitales, para que los usuarios de los servicios de salud tengan la tranquilidad y la certeza de que, su información cínica en formato digital no será alterada por ninguna persona. También le garantiza que el expediente digital tendrá un valor legal en cualquier litigio judicial dentro del territorio nacional.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6 Conclusiones y recomendaciones

6.1 Conclusiones

6.1.1. En cuanto a los sistemas de información en salud, utilizados en los distintos centros médicos del país, tanto públicos como privados, se determinó que estas herramientas carecen de los elementos esenciales para ser considerados en salud, como un expediente digital.

6.1.2. Basado en el análisis realizado en este documento, se confirmó la falta de una estructura de seguridad de la información, acorde con un verdadero expediente digital, especializado para centros médicos, que permita a los usuarios de los servicios de salud, tener la confianza de que los datos no sean modificados en algún momento.

6.1.3. Se evidenció que el almacenamiento en bases de datos no garantiza la integridad de los datos, ya que, por su distribución de roles, permite que algunos usuarios técnicos puedan modificar los datos desde consolas de administración.

6.1.4. El formato de archivos PDF, se seleccionó como base de almacenamiento de la estructura de seguridad para expedientes digitales especializados para centros médicos, ya que tiene propiedades que evitan la modificación de los datos incluidos.

6.1.5. Se determinó la utilización de la firma digital como la herramienta apropiada para la autentificación de los documentos digitales y se permite que la información clínica adquiera confiabilidad y legalidad.

6.1.6. Se estableció una base para la seguridad de la información en el almacenamiento de los documentos del expediente digital, que se encargará de almacenar la información clínica, de una manera muy semejante a la utilizada en los expedientes de papel.

6.1.7. Se formuló un procedimiento de control, para la indexación de documentos basado en Blockchain, que garantiza la confiabilidad de la información y que servirá como método de verificación para determinar que la información clínica no ha sido cambiada.

6.1.8. Se definió el SIS como el medio que consolida los procedimientos y herramientas que conforman la estructura de seguridad de la información, en el expediente digital especializado para centros médicos, ya que tiene la capacidad de administrar la información clínica, transformarla en documentos no modificables, acceder al control de indexación y visualizar la información para los diagnósticos médicos.

6.1.9. Al utilizar como base los SIS existentes, se diseñó la estructura de seguridad de la información de expedientes digitales especializados para centros médicos, que permite ser implementado en cualquier institución de sanidad, sea pública o privada.

6.1.10. Con la utilización de la estructura de seguridad de la información diseñada, el usuario de los servicios de salud tendrá la certeza de que su información clínica no podrá ser modificada en ningún momento, ya que los controles implementados evidenciarían cualquier alteración.

6.2 Recomendaciones

6.2.1. Para los sistemas de información utilizados actualmente en los servicios de salud, se recomienda la implementación de los elementos necesarios para cumplir con los requerimientos obligatorios para ser considerados un documento de archivo digital.

6.2.2. Para demostrar confianza a los usuarios de los servicios de sanidad, en cuanto a expedientes digitales en salud, se recomienda aplicar controles que den seguridad a la información clínica y que garanticen la integridad de los datos.

6.2.3. Para la protección de los datos clínicos, se recomienda el almacenamiento de la información de los usuarios, en formatos no modificables, debidamente autentificados y firmados digitalmente, para evitar la modificación de la data después de haberse incluido en el expediente digital.

6.2.4. Como formato de almacenamiento de los datos clínicos, se recomienda la utilización de documentos PDF, ya que tienen propiedades que los hacen difícil de modificar y son el tipo de archivos que se asemejan mejor a un papel digital.

6.2.5. Para garantizar la autenticidad de la información clínica, así como la confiabilidad de esta, se recomienda la utilización de los certificados digitales emitidos por el gobierno de la República, para firmar los documentos digitales del expediente clínico.

6.2.6. En cuanto al almacenamiento de los archivos, se recomienda la utilización de una estructura diseñada, acorde con las necesidades del expediente clínico, con la implementación de las medidas de seguridad, física, lógica y para el traslado de información.

6.2.7. Como medida de control digital, o bitácora transaccional, que impida la alteración de las anotaciones, se recomienda la utilización de una cadena de datos privada de Blockchain, que garantice la integridad de la información en los documentos del expediente digital en salud.

6.2.8. Tomando como base los desarrollos en las instituciones de salud, se recomienda la utilización de los S.I.S actuales, como la plataforma principal de la estructura de seguridad, planteada en este trabajo.

6.2.9. Para la utilización de un expediente digital en salud, se recomienda la implementación de la estructura de seguridad planteada en este trabajo; ya que su principal característica es impedir la modificación de los datos clínicos de los usuarios.

CAPÍTULO VII

REFLEXIONES FINALES

7 Reflexiones finales

En este trabajo se busca entregar una solución diferente al problema que tienen los datos clínicos, a la hora de ser digitalizados.

En primer lugar, se definió lo que es un expediente clínico, para así poder entender lo que sería un expediente digital clínico. Se analizaron las diferencias entre un sistema de información en salud y un expediente digital especializado para centros médicos.

Como segundo punto, se propuso cambiar la forma tradicional de guardar la información digital de los asegurados (información que será considerada como historia clínica). Se planteó el uso de formatos de almacenamiento y herramientas que convirtieran los datos clínicos en información confiable, auténtica y no repudiable.

En tercer lugar, se expone la necesidad de utilizar herramientas tecnológicas actualizadas, como la firma digital y cadenas de datos Blockchain, que aporten seguridad a la información clínica almacenada en medios digitales.

Se diseñó una estructura de seguridad de la información de expedientes digitales especializados en centros médicos, para garantizarles a los usuarios de los servicios de sanidad, que los datos clínicos, almacenados en formato digital, no serán modificados por ninguna persona y con ello garantizar la integridad, autenticidad y confiabilidad de la información y poder contar con un verdadero expediente digital en salud, con la misma validez legal que el expediente físico utilizado en la actualidad.

CAPÍTULO VIII

TRABAJOS A FUTURO

8 Trabajos a futuro

Por una cuestión de tiempo y recursos, la presente investigación comprende solo el diseño de la estructura de seguridad de la información de expedientes digitales especializados para centros médicos; por ello se considera sumamente importante el desarrollo e implementación de la estructura de seguridad. Esta estructura vendría a beneficiar a los usuarios de los servicios de salud, ya que se tendría la certeza de que la información clínica digital no se modifica en ningún momento y les permitirá a los datos clínicos digitales tener un valor legal en caso de un litigio judicial.

Otro trabajo a futuro, basado en la estructura diseñada, sería la aplicación de estándares internacionales especializados en el ámbito de la salud. Estándares que apliquen controles en cuanto a la protección de la privacidad, el traslado y el acceso de los datos por parte de los profesionales en ciencias médicas, con el fin de asegurar la información de salud almacenada en el expediente clínico. La aplicación de las medidas de control vendría a garantizarles a los usuarios de los servicios de sanidad, la seguridad de la información clínica, incluida en el expediente digital especializado, para centros médicos.

Adicionalmente, un trabajo a futuro sugerido sería la aplicación de seguridad física, lógica y de red, para la plataforma de almacenamiento y visualización del expediente digital especializado para centros médicos. Ya que, según lo estricto de las medidas de control que se definan en cuanto a los archivos digitales y en especial los que contienen información clínica, así de estricto debería ser la seguridad aplicada para el resguardo de la información clínica.

Glosario.

CCSS: Caja Costarricense del Seguro Social.

CGI: Centro de Gestión Informática.

EDUS: Expediente Digital Único en Salud.

MISE: Módulo Integrado de Seguridad.

SIAC: Sistema Integrado de Agendas y Citas.

SIES: Sistema Integrado de Expediente de Salud.

TIC: Tecnologías de Información y Comunicaciones.

SSO: Procedimiento single sign on para la autenticación y habilitación del usuario, para acceder a varios sistemas con una sola instancia de identificación.

SIS: Sistema de información en salud.

HIS: Sistemas de información hospitalaria o sistemas de información en salud, por sus siglas en ingles. (Health Information Systems).

RIS: Sistema de Información Radiológico, por sus siglas en ingles. (Radiological Information System).

PACS: Sistema computarizado para el archivo digital de Imágenes médicas, por sus siglas en ingles (Picture Archiving and Communication System).

DICOM: Es el estándar reconocido mundialmente para el intercambio de imágenes médicas. por sus siglas en ingles (Digital Imaging and Communication in Medicine).

MICID: Es el Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica.

EXPEDIR: Nombre del archivo propuesto para el uso del expediente digital exportado a un equipo, disco o unidad extraíble. Es un archivo en formato de texto ligero para la ubicación de documentos.

Paciente: Persona que recibe atención en un servicio de salud, en la CCSS se conoce como asegurado y en el área privada como cliente.

Expediente clínico: Es el conjunto de documentos con los datos personales e información médica de un paciente.

Expediente digital: Es el conjunto de documentos digitales que se encuentran en el expediente clínico del paciente.

Datos clínicos: Son todos los datos referentes a la salud de un paciente.

Hash: Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos (ya sea un texto, una contraseña o un archivo) en una nueva serie de caracteres con una longitud fija que representa un resumen de todo el bloque arbitrario de datos.

HL7: Es un estándar para facilitar el intercambio electrónico de información clínica.

XML: Es un lenguaje de marcado para representar información estructurada.

Referencias

[01] De la Prieta Miralles, V. (2002). La historia clínica: aspectos lingüísticos y jurídicos. Panacea.

[02] Gobierno de la República de Costa Rica. (13 de 09 de 2013). Ley Expediente digital único de salud, Num 9162,. Diario Oficial La Gaceta .

[03] Hospital Clínica Bíblica. (2018). Revista por su salud, edición especial, Año II • XV Edición. , 24.

[04] Barquero, K. (16 de 03 de 2018). Hospital CIMA San José alcanza mayoría de edad con ampliación y nuevos servicios.

[05] Caja Costarricense de Seguro Social. (16 de 09 de 2018). Página oficial. Recuperado el 16 de 09 de 2018, de http://www.ccss.sa.cr/appedus/

[06] Guerrero Logroño, Rosa María. (2013). Sistema de archivo y clasificación de documentos, ADGG0308. (E. IC, Ed.)

[07] Gobierno de la República de Costa Rica. (29 de 09 de 1999). Reglamento del Expediente de Salud de la CCSS. Diario Oficial La Gaceta No. 189. Diario Oficial La Gaceta , pág. 1.

[08] Norma internacional ISO 15489-1. (2001). Información y documentación – Gestión de documentos– Primera edición.

[09] De Medrano, Lucía. (2012). Instalación y Manejo de Sistemas Operativos.

[10] Valderrey Sanz, P. (2014). Gestión de Bases de Datos. Editorial RA-MA.

[11] Osorio Rivera , F. (2008). Bases de datos Relacionales Teoría y Practica. Editorial ITMJohnny.

[12] Villalobos Murillo, J. (2018). Vulnerabilidad de Sistemas Gestores de Bases de Datos. Uniciencia , 22 (1011-0275), 133.

[13] Alvez,, C. (2009). Experiencias en la gestión de imágenes por contenido en bases de datos objeto-relacionales. Universidad Nacional de Entre Ríos.

[14] Tirado Ramos Alfredo, Hu Jingkun and Lee K. P. (2002). Information object definitions-based UML representation of DICOM structured reporting: a case study on transcoding DICOM to XML. J Am Med Inform Assoc. JAMIA , 9 (11751804), 63.

[15] Ruiz Carlos, T. A. (2007). Aproximación a la representación en XML de objetos DICOM para fotografiá médica digital. EIA , 8 (1794-1237), 148.

[16] Pianykh, O. (2009). Digital Imaging and Communications in Medicine (DICOM) A Practical Introduction and survival Guide. Springer.

[17] Gutiérrez Martínez, J., Núñez Gaona, M., Aguirre Meneses, H., & Delgado Esquerra, R. (2014). Implementación de la seguridad en el manejo de las imágenes médicas. Medigraphic , 3, 177.

[18] Adobe. (2018). PDF: tres letras que cambiaron el mundo. Recuperado el 3 de 10 de 2018, de Pagina Oficial de Adobe: https://acrobat.adobe.com/la/es/acrobat/about-adobe-pdf.html

[19] Microsoft. (2018). Formatos de archivo para guardar documentos. Recuperado el 3 de 10 de 2018, de Pagina Oficial de Microsoft: https://support.office.com/es-es/article/formatos-de-archivo-para-guardar-documentos-88de3863-c9e5-4f89-be60-906f9065e43c

[20] ISO. (14 de 8 de 2017). ISO 32000: Evolución del estándar mundial para documentos electrónicos Recuperado de . Recuperado el 3 de 10 de 2018, de ISOTools: https://www.isotools.org/ 2017/08/14/iso-32000-evolucion-estandar-mundial-documentos-electronicos/

[21] Banco de la República I Colombia. (2013). ¿Qué es el formato PDF de Adobe? Recuperado el 9 de 11 de 2018, de http://www.banrep.gov.co/es/contenidos/page/qu-formato-pdf-adobe

[22] Granados Paredes, G. (2016). Introducción a la Criptografía. Revista Digital Universitaria , 7 (7), 6.

[23] Escrivá Gascó Gema, R. S. (2013). Seguridad informática. Macmillan Iberia, S.A.

[24] Gobierno de la República, C. R. (13 de 10 de 2005). Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Diario Oficial la Gaceta (197), pág. 1.

[25] Ministerio de Ciencia y Tecnología, C. R. (2005). Reglamento a la ley de certificados, firmas digitales y documentos electrónicos.

[26] Kroenke, D. M. (2003). Procesamiento de Base de Datos. Fundamentos, diseño e implementación. México, D.F: Pearson Prentice Hall.

[27] Marchionn, E. A. (2011). Administrador de servidores, primera edición. USERSHOP.

[28] Adrian M.K. Thomas Arpan K., B. U. (2005). Classic Papers in Modern Diagnostic Radiology. Springer-Verlag Berlin Heidelberg.

[29] Dreyer, K. J., Hirschorn, D. S., & Thrall, J. H. (2002). PACS A Guide to the Digital Revolution.

[30] Guzmán Díaz Carlos, B. V. (2014). Sistema para el almacenamiento y transmisión de imágenes médicas. Revista Cubana de Informática Médica .

[31] Mazzoncini de Azevedo, M. P., & Covas Salomão, S. (2009). PACS: Sistemas de Arquivamento e Distribuição de Imagens. Revista Brasileira de Física Médica. , 4-5.

[32] González Rodríguez, L., & Durañona Yero, Y. (2007). Servidor de Imágenes Médicas (Cassandra Server). Cuba.

[33] Muñoz Lopez, F. J. (2017). Instalación y Actualización de Sistemas Operativos. Madrid, España: Paraninfo.

[34] Caballero González, C., & Clavero García, J. A. (2016). Sistemas de Almacenamiento. Paraninfo.

[35] Ramakrishnan Raghu, G. J. (2007). Sistemas de gestión de bases de datos (3a. ed.),. Madrid, España.: McGraw-Hill.

[36] Chavez, O. (22 de 05 de 2013). Administracion De Base De Datos. Recuperado el 21 de 11 de 2018, de blogger: http://chavez-atienzo-2013.blogspot.com/

[37] La Red Martínez, D. L. (2014). Sistemas operativos, El Cid Editor.

[38] San Martín González, E. (2014). Salvaguarda y seguridad de los datos: administración de bases de datos. Málaga, España: IC Editoria.

[39] Karame, G. (2016). On the Security and Scalability of Bitcoin's Blockchain. Conference on Computer and Communications Security. Vienna, Austria.

[40] Tur Faúndez, C. (2018). Derecho de las nuevas tecnologías. Madrid, España: Editorial Reus.

[41] Bartolomé Pina, A. R., Carles, B. T., Castañeda Quintero, L., & Adell Segura, J. (2017). Blockchain en Educación: introducción y crítica al estado de la cuestión. Revista electrónica de Tecnología Educativa (61).

[42] Ibáñez Jiménez, J. W. (2018). Blockchain: primeras cuestiones en el ordenamiento español. Madrid: Dykinson.

[43] Ghose, A. (11 de 8 de 2018). El ‘Blockchain’ cambiará el mercadeo y la publicidad digital. El Financiero.

[44] Iuon-Chang, L., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges, International. Journal of Network Security , 19 (5), 653-659.

[45] Peralta, M. (2009). Sistema de Información. El Cid Edito.

[46] Fernández Rodríguez, J. (2017). Sistemas de información en salud. UNED. Recuperado el 05 de 12 de 2018, de Repositorio UNED: Recuperado de http://repositorio.uned.ac.cr/reuned/bitstream/120809/ 444/1/ GE316%20 Sistemas%20de%20informaci%C3%B3n%20en%20salud%20-%202011%20-%20Salud.pdf

[47] Cerritos Antonio, F. P. (2003). Sistema de Información Hospitalaria. Recuperado el 9 de 12 de 2018, de UNAM- Facultad de Medicina: http://sukuun.com.mx/contenido/MAOS/Tareas/Tarea3Sistemasdeinformacionhospitalaria.pdf

[48] Temes Montes, J. L., & Torres Mercedes, M. (2007). Gestión hospitalaria (4a. ed.). Madrid, España: McGraw-Hill.

[49] Angarita Sanguino, C. R., & Beltrán Galvis, N. (12 de 2008). Aplicación Web para la visualización de imágenes médicas MEDICOMWEB, ISSN 0122-820X, recuperado de. Recuperado el 15 de 12 de 2018, de https://www.researchgate.net/publication/304869020_ Aplicacion_Web_para_la_visualizacion_de_imagenes_medicas_MEDICOMWEB

[50] Ing. Pereira Bárzaga, O., Ing. Pérez Buján, L., & Ramón, I. C. (2013). Sistema de visualización remota para la representación interactiva de volúmenes de datos médicos. Revista Cubana de Informática Médica , Vol.5 (No.2).

[51] Bengochea, L., & Patricio Miguel Ángel. (2005). Sistemas de visualización para bibliotecas digitales. Revista española de Documentación Científica , v28.i3. (170), pp 273, 276.

[52] Álvarez Marañón, G., & Pérez García, P. P. (2014). Seguridad informática para empresas y particulares. Madrid, España: McGraw-Hill.

[53] Cano, J. (2018). Arquitecturas de Seguridad Informática: Entre la administración y el gobierno de la Seguridad de la Información. Seminario de Actualización en seguridad informática. Documento Módulo I .

[54] Costas Santos, J. (2014). Mantenimiento de la seguridad en sistemas informáticos. Madrid, España: Editorial RA-MA.

[55] Institute SANS. (2004). SysAdmin Audit, Networking and Security Institute. Information Systems Security Architecture: A Novel Approach to Layered Protection. E

APÉNDICES

Apéndice No 1. Publicaciones utilizadas

A las publicaciones encontradas con los criterios de búsqueda indicadas en el estado de la cuestión, se analizaron alrededor de ciento veinte publicaciones de las cuales se determinaron como importantes para esta investigación cincuenta y cinco de ellas, las cuales tratan los temas relacionados a la seguridad de la información en cuanto a las partes que componen la estructura de seguridad a diseñar. De igual manera se tomaron en cuenta temas relacionados propiamente a la seguridad informática, la gestión de la información en sistemas de salud y asuntos requeridos para el desarrollo de este trabajo.

A continuación, se muestra los cuadros de resumen de los hallazgos.

Identificación	
Título	La historia clínica: aspectos lingüísticos y jurídicos.
Publicación:	2002
Autores:	De la Prieta Miralles V.
Referencia:	[1]
Descripción	
Área:	Sanidad y Bienestar Social.
Resumen:	Esta publicación aborda la historia de la historia clínica.
Aspectos por destacar	
La historia clínica es la narración escrita, en soporte de papel o informático, clara, precisa, detallada y ordenada de todos los datos y conocimientos, tanto personales como familiares, que se refieren a un paciente y que sirven de base para el juicio definitivo de su enfermedad actual o de su estado de salud. Resume la herencia y hábitos de un ser humano; su constitución, fisiología y psicología, su ambiente y, siempre que sea posible, la etiología y evolución de la enfermedad.	

Identificación	
Título	Ley Expediente digital único de salud
Publicación:	23 de setiembre del 2013
Autores:	Gobierno de Costa Rica
Referencia:	[2]
Descripción	
Área:	Salud
Resumen:	Esta ley se refiere al expediente único en salud de la CCSS
Aspectos por destacar	
La finalidad de esta ley consiste en establecer el ámbito y los mecanismos de acción necesarios para el desarrollo del proceso de planeamiento, financiamiento, provisión de insumos y recursos e implementación del expediente digital único de salud, desde una perspectiva país.	

Identificación	
Título	Beneficios a nivel interno
Publicación:	2018
Autores:	Hospital Clínica Bíblica Revista por su salud, edición especial, XV.
Referencia:	[3]
Descripción	
Área:	Salud
Resumen:	Este articulo aborda los beneficios brindados en la atención
Aspectos por destacar	
A través del manejo de la comunicación y la información, se toman las decisiones basándose en los datos. En los sistemas de información se incluye el expediente	

electrónico que contiene todo un registro del paciente, y esta in- formación es vital para que se busque en la red de datos una comunicación efectiva entre los personeros.

Identificación	
Título	Hospital CIMA San José alcanza mayoría de edad con ampliación y nuevos servicios.
Publicación:	16 marzo de 2018
Autores:	Karla Barquero.
Referencia:	[4]
Descripción	
Área:	Salud
Resumen:	Este artículo cita la utilización de un expediente electrónico.
Aspectos por destacar	
En ese aspecto de modernización, el centro médico destaca por emplear un sistema hospitalario único llamado All Script, que es utilizado en los mejores hospitales de Estados Unidos.	

Identificación	
Título	EDUS
Publicación:	2018
Autores:	Caja Costarricense de Seguro Social.
Referencia:	[5]
Descripción	
Área:	Salud.
Resumen:	Publicación habla del expediente en salud.

Aspectos por destacar
EDUS es la aplicación oficial de la Caja Costarricense de Seguro Social que le permitirá tener acceso desde su dispositivo inteligente a información relevante de su Expediente Digital Único en Salud (EDUS.

Identificación	
Título	Sistema de archivo y clasificación de documentos.
Publicación:	2013
Autores:	Rosa María Guerrero Logroño.
Referencia:	[6]
Descripción	
Área:	Documentos de Archivo
Resumen:	Este libro habla de la clasificación de documentos de archivo.
Aspectos por destacar	
Aplicar las técnicas de archivo convencional e informático, utilizando los sistemas de clasificación, codificación y almacenamiento apropiados a la información y documentación que se gestiona.	

Identificación	
Título	Reglamento del Expediente de Salud de la CCSS.
Publicación:	1999
Autores:	Gobierno de la República de Costa Rica.
Referencia:	[7]
Descripción	
Área:	Reglamento.

Resumen:	Este reglamento norma la utilización del expediente físico.
Aspectos por destacar	
Este reglamento contiene las regulaciones mínimas que deben aplicarse en todos los establecimientos de la Caja Costarricense de Seguro Social.	

Identificación	
Título	Información y documentación.
Publicación:	2001
Autores:	Norma internacional ISO 15489-1.
Referencia:	[8]
Descripción	
Área:	Gestión de documentos.
Resumen:	Esta norma abarca aspectos relacionados a la gestión de documentos físicos y digitales.
Aspectos por destacar	
La normalización de las políticas y los procedimientos de la gestión de documentos de archivo asegura la adecuada atención y protección de estos, y permite que la evidencia y la información que contienen puedan ser recuperadas más eficiente y eficazmente usando practicas y procedimientos normalizados.	

Identificación	
Título	Instalación y Manejo de Sistemas Operativos.
Publicación:	2012
Autores:	Lucía de Medrano.
Referencia:	[9]

Descripción	
Área:	Sistemas operativos
Resumen:	Esta publicación se refiere a la instalación y manejo de los sistemas operativos
Aspectos por destacar	
Se habla de que información procesada se organiza en estructuras como archivos, los cuales son identificados por un nombre más la extensión, que identifican el tipo de archivo.	

Identificación	
Título	Gestión de bases de datos.
Publicación:	2014
Autores:	Pablo Valderrey Sanz.
Referencia:	[10].
Descripción	
Área:	Bases de Datos.
Resumen:	Este libro se refiere a conceptos en cuanto a base de datos.
Aspectos por destacar	
Se destacan conceptos de bases de datos, tales como BD relacional, modelo de datos, tablas, vistas, entre otros.	

Identificación	
Título	Bases de Datos Relacionales Teoría y Práctica.
Publicación:	2018
Autores:	Fray León Osorio Rivera.

Referencia:	[11]
Descripción	
Área:	Bases de Datos
Resumen:	Este libro muestra teoría y práctica referente a las Bases de Datos
Aspectos por destacar	
Como aspecto por destacar en esta publicación define lo que es un DBA, lo que realiza y sus funciones y obligaciones en una Base de Datos	

Identificación	
Título	Vulnerabilidad de Sistemas Gestores de Bases de Datos.
Publicación:	2008
Autores:	Johnny Villalobos Murillo (2008).
Referencia:	[12]
Descripción	
Área:	Bases de datos.
Resumen:	Este trabajo habla de las vulnerabilidades de las Bass de Datos.
Aspectos a destacar	
En este trabajo se destaca la constante preocupación por la seguridad de las bases de datos. En esta publicación se estudia cómo se configuran las conexiones hacia una base de datos, explicando los posibles errores.	

Identificación	
Título	Experiencias en la gestión de imágenes por contenido en bases de datos objeto relacionales.
Publicación:	2009

Autores:	Carlos E. Álvez.
Referencia:	[13]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este libro hace un análisis sintético de los objetos de Oracle para el almacenamiento de imágenes DICOM y sus metadatos.
Aspectos por destacar	
En este artículo se analizan diversos mecanismos que brinda la tecnología Objeto-Relacional (OR) para el almacenamiento de imágenes en una Base de Datos.	

Identificación	
Título	Information object definitions-based UML representation of DICOM structured reporting: a case study on transcoding DICOM to XML.
Publicación:	2002
Autores:	Tirado-Ramos A., Hu J. and Lee K. P (2002).
Referencia:	[14]
Descripción	
Área:	Tecnologías médicas.
Resumen:	Este Libro se refiere a la estructura del formato DICOM.
Aspectos por destacar	
Define conceptos y explica la estructura de las imágenes DICOM. Los autores afirman que las representaciones del estándar DICOM Structured Reporting, utilizan lenguajes de modelado orientados a objetos como el Lenguaje de modelado unificado, pueden proporcionar una vista de referencia de alto nivel del marco semánticamente de DICOM y sus estructuras complejas.	

Identificación	
Título	Aproximación a la representación en XML de objetos DICOM para fotografía médica digital.
Publicación:	2007
Autores:	Carlos Ruiz, Andrés Trujillo, Albín García.
Referencia:	[15]
Descripción	
Área:	Tecnologías médicas
Resumen:	El Artículo se refiere al estándar DICOM
Aspectos por destacar	
El estándar DICOM es un protocolo no propietario para el intercambio de información médica.	

Identificación	
Título	Digital Imaging and Communications in Medicine (DICOM) A Practical Introduction and survival Guide
Publicación:	2009
Autores:	Oleg S. Pianykh.
Referencia:	[16]
Descripción	
Área:	Tecnologías médicas.
Resumen:	Esta guía trata de las reglas del Estándar DICOM.
Aspectos por destacar	
Esta guía presenta las reglas para el estándar DICOM.	

Identificación	
Título	Implementación de la seguridad en el manejo de las imágenes médicas
Publicación:	2014
Autores:	Gutiérrez Martínez J, Núñez Gaona MA, Aguirre Meneses H, Delgado Esquerra RE.
Referencia:	[17]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este trabajo de investigación aborda la seguridad de la información en instituciones hospitalarias.
Aspectos por destacar	
La seguridad en los sistemas de información (SI) que administran las imágenes médicas generadas en una institución hospitalaria, es un proceso continuo que tiene como fin conservar la confidencialidad, integridad, disponibilidad de las imágenes y protección de la identidad del paciente en los sistemas de almacenamiento y comunicación denominados PACS.	

Identificación	
Título	PDF: tres letras que cambiaron el mundo.
Publicación:	3 de octubre del 2018
Autores:	Adobe.
Referencia:	[18]
Descripción	
Área:	Tipos de archivos.

Resumen:	Esta publicación trata de explicar que es el formato PDF.
Aspectos por destacar	
La publicación indica que el formato de documento portátil (PDF) se utiliza para presentar e intercambiar documentos de forma fiable, independiente del software, el hardware o el sistema operativo.	

Identificación	
Título	Formatos de archivo para guardar documentos.
Publicación:	3 de octubre del 2018
Autores:	Microsoft.
Referencia:	[19]
Descripción	
Área:	Tipos de Archivos.
Resumen:	Esta publicación muestra los formatos con los cuales es compatible el programa Microsoft Word.
Aspectos por destacar	
El programa Microsoft Word puede exportar su información a archivos PDF.	

Identificación	
Título	ISO 32000: Evolución del estándar mundial para documentos electrónicos.
Publicación:	14 agosto del 2017
Autores:	ISOTools.
Referencia:	[20]

Descripción	
Área:	Tipos de archivos.
Resumen:	Esta publicación se refiere a la evolución del estándar pdf.
Aspectos por destacar	
De acuerdo con la publicación los archivos PDF son totalmente independientes e interoperables, funcionando correctamente con el software PDF de cada proveedor.	

Identificación	
Título	¿Qué es el formato PDF de Adobe?
Publicación:	2013
Autores:	Banco de la República I Colombia.
Referencia:	[21]
Descripción	
Área:	Tipos de archivos
Resumen:	Esta publicación explica que es el formato PDF de Adobe
Aspectos por destacar	
De acuerdo con la publicación PDF es la herramienta pública empleada en empresas con estándares mundiales para la distribución e intercambio seguro y fiable de documentos electrónicos.	

Identificación	
Título	Introducción a la Criptografía
Publicación:	2016
Autores:	Gibrán Granados Paredes.
Referencia:	[22]

Descripción	
Área:	Seguridad informática
Resumen:	Esta Revista nos introduce en el tema criptografía, explica la necesidad de la Seguridad de la Información en una organización. También indica la necesidad de proteger la información y los sistemas que administramos.
Aspectos por destacar	
Esta revista destaca que con la criptografía se puede garantizar las propiedades de integridad y confidencialidad, pero hay que saber cómo utilizarla; para ello es importante tener claros los conceptos básicos que están detrás de los sistemas criptográficos modernos.	

Identificación	
Título	Seguridad informática
Publicación:	2013
Autores:	Gema Escrivá Gascó, Rosa María Romero Serrano y David Jorge Ramada.
Referencia:	[23]
Descripción	
Área:	Seguridad informática
Resumen:	Este libro aborda los temas relacionados con seguridad de la información.
Aspectos por destacar	
En este libro se destaca que, mediante técnicas criptográficas, se pueden garantizar tres propiedades vitales para la seguridad: confidencialidad, autenticación e integridad.	

Identificación	
Título	Ley de certificados, firmas digitales y documentos electrónicos
Publicación:	2005
Autores:	República de Costa Rica
Referencia:	[24]
Descripción	
Área:	Leyes
Resumen:	Esta Ley regula lo referente a firmas digitales y documentos electrónicos.
Aspectos por destacar	
En esta ley destacamos que los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito.	

Identificación	
Título	Reglamento a la ley de certificados, firmas digitales y documentos electrónicos.
Publicación:	2005
Autores:	MICID.
Referencia:	[25]
Descripción	
Área:	Leyes y reglamentos
Resumen:	Este reglamento regula todo lo referente a la ley de certificados y firmas digitales.

Aspectos por destacar
En esta ley se destaca la definición de Firma Digital como un conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

Identificación	
Título	Procesamiento de Base de Datos. Fundamentos, diseño e implementación.
Publicación:	2003
Autores:	David M. Kroenke.
Referencia:	[26]
Descripción	
Área:	Bases de datos
Resumen:	Este libro se refiere a los fundamentos de bases de datos.
Aspectos por destacar	
En este libro se destaca la definición de un servidor como una computadora que forma parte de una red, provee servicios a otras computadoras denominadas clientes, es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor. Algunos servicios habituales son el de archivos, el cual permite a los usuarios almacenar y acceder a los archivos de una computadora.	

Identificación	
Título	Administrador de servidores
Publicación:	2011
Autores:	Enzo Augusto Marchionni.
Referencia:	[27]

Descripción	
Área:	Servidores
Resumen:	Este libro aborda información referente a la administración de servidores.
Aspectos por destacar	
En este libro se destaca la información encontrada referente a las características de un servidor y sus funcionamientos dentro de una organización o empresa.	

Identificación	
Título	Classic Papers in Modern Diagnostic Radiology.
Publicación:	2005
Autores:	Adrián M.K. Thomas Arpan K. Banerjee Uwe Busch.
Referencia:	[28]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este libro se refiere a los avances técnicos en la radiología de diagnóstico en las últimas décadas.
Aspectos por destacar	
Se destaca que el tema de la radiología de diagnóstico ahora es muy grande y los departamentos de radiología están involucrados en todas las áreas de la atención.	

Identificación	
Título	PACS A Guide to the Digital Revolution
Publicación:	2002
Autores:	Keith J. Dreyer Amit Mehta James H. Thrall.

Referencia:	[29]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este libro proporciona una visión general de la tecnología PACS
Aspectos por destacar	
La informática de imágenes médicas, los Sistemas de archivo de imágenes y comunicaciones (PACS) se han convertido en una parte fundamental de la infraestructura tecnológica que respalda la práctica de la radiología.	

Identificación	
Título	Sistema para el almacenamiento y transmisión de imágenes médicas
Publicación:	2014
Autores:	Carlos Guzmán Díaz y Denys Bárbaro Vega Aguilar.
Referencia:	[30]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este artículo tiene como objetivo el desarrollo de un servidor de almacenamiento y transmisión de imágenes médicas.
Aspectos por destacar	
Se destaca el desarrollo de un sistema PACS desde cero explicando detalladamente la estructura utilizada. Esto debido a lo costoso de adquirir un sistema PACS de una marca comercial.	

Identificación	
Título	PACS: Sistemas de Arquivamento e Distribuição de Imagens

Publicación:	2009
Autores:	Paulo Mazzoncini de Azevedo-Marques, Samuel Covas Salomão.
Referencia:	[31]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este artículo de revista trata del almacenamiento y distribución de las imágenes médicas.
Aspectos por destacar	
Se destaca de este artículo de revista brasileña que, la mejor solución para administrar estas imágenes digitales está en la adopción de un Sistema de Archivado y Distribución de Imágenes (PACS, del inglés Picture Archiving and Communication System).	

Identificación	
Título	Servidor de Imágenes Médicas.
Publicación:	2007
Autores:	González Rodríguez L, Durañona Yero Y.
Referencia:	[32]
Descripción	
Área:	Tecnologías médicas
Resumen:	Este artículo tiene como objetivo el desarrollo de un servidor de almacenamiento y transmisión de imágenes médicas.
Aspectos por destacar	
Se destaca que es un sistema orientado al área de radiología de una clínica hospitalaria, con el fin de almacenar y transmitir las imágenes generadas por los equipos de adquisición.	

Identificación	
Título	Instalación y actualización de sistemas operativos
Publicación:	2017
Autores:	Javier Muñoz López (2017).
Referencia:	[33]
Descripción	
Área:	Sistemas operativos
Resumen:	Este libro se refiere a la actualización e instalación de sistemas operativos.
Aspectos por destacar	
Se destaca que los sistemas informáticos modernos son gestionados por sistemas operativos actuales como Windows o Linux.	

Identificación	
Título	Sistemas de Almacenamiento.
Publicación:	2016
Autores:	Carlos Caballero González y Juan Antonio Clavero García.
Referencia:	[34]
Descripción	
Área:	Sistemas de almacenamiento
Resumen:	Este libro se refiere al almacenamiento de información.
Aspectos por destacar	
Se destaca la introducción con la que se muestra este libro. La información se ha utilizado y tratado a lo largo de la historia a través de libros, periódicos, revistas… En	

definitiva, en soporte papel. Es a partir del nacimiento de los computadores cuando se comienza a manejar utilizando máquinas electrónicas y la lógica.

Identificación	
Título	Sistemas de gestión de bases de datos.
Publicación:	2007
Autores:	Raghu Ramakrishnan y Johannes Gehrke.
Referencia:	[35]
Descripción	
Área:	Bases de datos
Resumen:	Este libro se refiere a los sistemas de gestión de bases de datos
Aspectos por destacar	
Se destaca en este libro el trato de los principios de los sistemas de bases de datos y la forma en que se pone énfasis en la manera en que se utilizan para el desarrollo de aplicaciones que hacen un empleo intensivo de los datos.	

Identificación	
Título	Administración de base de datos.
Publicación:	2013
Autores:	Omar Chávez
Referencia:	[36]
Descripción	
Área:	Bases de datos
Resumen:	El artículo se trata sobre la administración de las bases de datos.

Aspectos por destacar
Esta publicación destaca que las bitácoras son herramienta que permite registrar, analizar detectar y notificar eventos que suceden en cualquier sistema de información utilizado en las organizaciones.

Identificación	
Título	Sistemas operativos
Publicación:	2014
Autores:	David Luis La Red Martínez
Referencia:	[37]
Descripción	
Área:	Sistemas Operativos
Resumen:	Este libro trata aspectos fundamentales de los sistemas operativos.
Aspectos por destacar	
En esta publicación se destaca para este trabajo la explicación de los archivos como parte del sistema operativo.	

Identificación	
Título	Salvaguarda y seguridad de los datos: administración de bases de datos
Publicación:	2014
Autores:	Enrique San Martín González (2014)
Referencia:	[38]
Descripción	
Área:	Seguridad informática

Resumen:	Este libro trata del resguardo de los datos en la administración de las bases de datos.
Aspectos por destacar	
En este libro se destaca el concepto de salvaguarda de datos que corresponden al hecho de tener los datos sin posibilidad de perderlos, tenerlos siempre a salvo y con posibilidad de recuperarlos, en caso de cualquier tipo de incidente.	

Identificación	
Título	On the Security and Scalability of Bitcoin's Blockchain.
Publicación:	2016
Autores:	Ghassan Karame.
Referencia:	[39]
Descripción	
Área:	Seguridad Informática
Resumen:	Este documento se refiere a la tecnología cadenas de bloques
Aspectos por destacar	
El documento destaca que el Blockchain surge como una herramienta innovadora que resulta útil en varios escenarios de aplicaciones.	

Identificación	
Título	Derecho de las nuevas tecnologías.
Publicación:	2008
Autores:	Carlos Tur Faúndez.
Referencia:	[40]

Descripción	
Área:	Seguridad Informática. Blockchain
Resumen:	Esta publicación se refiere al Blockchain como una nueva tecnología.
Aspectos por destacar	
En esta publicación se destaca que la cadena de bloques es una base de datos apoyada en tecnología peer to peer.	

Identificación	
Título	Blockchain en Educación: introducción y crítica al estado de la cuestión.
Publicación:	2017
Autores:	Antonio Ramón Bartolomé Pina, Carles Bellver Torlà, Linda Castañeda Quintero, Jordi Adell Segura.
Referencia:	[41]
Descripción	
Área:	Seguridad Informática. Blockchain
Resumen:	Este artículo de revista electrónica se refiere al Blockchain
Aspectos por destacar	
En este artículo se destaca que la tecnología de Blockchain está abandonando el terreno de la moneda digital para incursionar otros campos. Pero las expectativas que están levantando llevan a plantearse preguntas de cómo podría aprovecharse las oportunidades de esta nueva tecnología.	

Identificación	
Título	Blockchain: primeras cuestiones en el ordenamiento español
Publicación:	2018
Autores:	Javier Wenceslao Ibáñez Jiménez.
Referencia:	[42]
Descripción	
Área:	Blockchain
Resumen:	Este libro orienta hacia la reflexión acerca de las cuestiones esenciales que presentan los registros distribuidos.
Aspectos por destacar	
Se destaca en este libro que en Blockchain se comparte valor sin censura, pero además se replica o distribuye la información introducida, y por eso a la cadena de bloques en ocasiones se le denomina internet del valor.	

Identificación	
Título	El ‘Blockchain’ cambiará el mercadeo y la publicidad digital
Publicación:	11 agosto de 2018
Autores:	Anindya Ghose.
Referencia:	[43]
Descripción	
Área:	Nuevas tecnologías
Resumen:	Este artículo trata del uso del Blockchain en el mercado de la publicidad

Aspectos por destacar
En este artículo se destacan los cinco principios básicos subyacentes en la tecnología de cadenas de bloques.

Identificación	
Título	A Survey of Blockchain Security Issues and Challenges, International Journal of Network Security.
Publicación:	2007
Autores:	Luon-Chang Lin y Tzu-Chun Liao.
Referencia:	[44]
Descripción	
Área:	Seguridad de la Información
Resumen:	Este artículo habla de la tecnología Blockchain y lo que la convierte en una herramienta única y robusta.
Aspectos por destacar	
En este artículo se destaca que la tecnología Blockchain no solo es una técnica única, sino que contiene Criptografía, Matemáticas, Algoritmo y Modelo económico.	

Identificación	
Título	Sistema de Información, El Cid Editor.
Publicación:	2009
Autores:	Manuel Peralta.
Referencia:	[45]
Descripción	
Área:	Sistemas de Información

Resumen:	Este libro se refiere a los conceptos que rodean los sistemas de información.
Aspectos por destacar	
En este libro se destaca que los Sistemas de Información automatizan procesos operativos dentro de una organización, y por eso son llamados Sistemas Transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc.	

Identificación	
Título	Sistemas de información en salud.
Publicación:	2011
Autores:	Jessica Fernández Rodríguez
Referencia:	[46]
Descripción	
Área:	Sistemas de Información
Resumen:	Este trabajo abarca, en forma general, la materia de los sistemas de información, aplicable a diversos ámbitos.
Aspectos por destacar	
Esta publicación se destaca la comprensión de los temas que se profundizarán en las características de un sistema de información en salud.	

Identificación	
Título	Sistema de Información Hospitalaria
Publicación:	2003
Autores:	Antonio Cerritos, Francisco J. Fernández Puerto y Florina Gatica Lara.

Referencia:	[47]
Descripción	
Área:	Sistemas de información
Resumen:	Este documento de la informática medica se refiere a los sistemas de información en salud (HIS)
Aspectos por destacar	
En este documento se destaca la definición de un Sistema de Información Hospitalaria, definido como: un sistema de información orientado a satisfacer las necesidades de generación de información.	

Identificación	
Título	Gestión Hospitalaria.
Publicación:	2007
Autores:	José Luis Temes Montes y Mengíbar Torres Mercedes.
Referencia:	[48]
Descripción	
Área:	Medicina
Resumen:	Este libro trata la gestión hospitalaria desde diversos puntos
Aspectos por destacar	
En este libro se destaca la utilización de las siglas RIS para designar la aplicación informática capaz de dar soporte a las actividades de un departamento de Radiodiagnóstico.	

Identificación	
Título	Aplicación Web para la visualización de imágenes médicas
Publicación:	2018
Autores:	Carlos René Angarita Sanguino, Nelson Beltrán Galvis.
Referencia:	[49]
Descripción	
Área:	Sistemas de información y Medicina.
Resumen:	Este artículo muestra el proceso de desarrollo de una solución para especialistas en medicina, que visualiza exámenes médicos donde se incluyen imágenes DICOM.
Aspectos por destacar	
En este artículo se destaca que los diagnósticos por imágenes se han convertido en uno de los elementos más importantes en la práctica de la medicina moderna.	

Identificación	
Título	Sistema de visualización remota para la representación interactiva de volúmenes de datos médicos.
Publicación:	2013
Autores:	Ing. Osvaldo Pereira Bárzaga, Ing. Leitniz Pérez Buján, Ing. Ramón Carrasco Velar.
Referencia:	[50]
Descripción	
Área:	Tecnologías Médicas
Resumen:	Este artículo de revista aborda el tema de los sistemas de visualización de imágenes DICOM

Aspectos por destacar
Este artículo destaca que las aplicaciones de visualización médica han adquirido un elevado auge en la medicina a nivel mundial.

Identificación	
Título	Sistemas de visualización para bibliotecas digitales.
Publicación:	2005
Autores:	Luis Bengochea, Miguel Ángel Patricio.
Referencia:	[51]
Descripción	
Área:	Sistemas de visualización.
Resumen:	Este artículo se aborda temas relacionados a los sistemas de visualización para bibliotecas digitales.
Aspectos por destacar	
En este artículo se destaca que una representación visual puede comunicar algunos tipos de información, de una forma más rápida y eficaz que cualquier otro método.	

Identificación	
Título	Seguridad informática para empresas y particulares.
Publicación:	2004
Autores:	Gonzalo Álvarez Marañón y Pedro Pablo Pérez García.
Referencia:	[52]
Descripción	
Área:	Seguridad Informática
Resumen:	Este libro trata el tema la seguridad informática

Aspectos por destacar
Se destaca en este libro que la seguridad no es una disciplina de todo o nada, que no existen sistemas 100% seguros y que la seguridad es el resultado de operaciones realizadas por personas y soportadas por la tecnología.

Identificación	
Título	Arquitecturas de Seguridad Informática: Entre la administración y el gobierno de la Seguridad de la Información.
Publicación:	2008
Autores:	Jeimy Cano (2008).
Referencia:	[53]
Descripción	
Área:	Seguridad informática
Resumen:	Esta publicación aborda lo referente a la arquitectura de seguridad informática

Aspectos por destacar
En este documento destaca y detalla el modelo de arquitectura de seguridad de la información el cual se encuentra enmarcado en la descripción de los elementos que lo conforman.

Identificación	
Título	Mantenimiento de la seguridad en sistemas informáticos.
Publicación:	2014
Autores:	Jesús Costas Santos.
Referencia:	[54]

Descripción	
Área:	Seguridad Informática
Resumen:	Este libro trata de acercar al lector a los aspectos más importantes de la seguridad informática
Aspectos por destacar	
Este libro analiza la seguridad informática desde distintas perspectivas y define una estructura de seguridad como un grupo de técnicas encaminadas a obtener altos niveles de seguridad.	

Identificación	
Título	Information Systems Security Architecture: A Novel Approach to Layered Protection.
Publicación:	2004
Autores:	SANS. (SysAdmin Audit, Networking and Security Institute).
Referencia:	[55]
Descripción	
Área:	Seguridad de la Información
Resumen:	Esta publicación se refiere a la arquitectura de seguridad en la información.
Aspectos por destacar	
Se destaca en la publicación las fases en las que dividen una arquitectura de seguridad.	

Apéndice No. 2. Servidores

Con respecto servidores y el procesamiento de datos, los servidores según indica Marchionni (2011), pueden tener varios procesadores con varios núcleos cada uno; incluye grandes cantidades de memoria RAM. En cuanto a almacenamiento de información este mismo autor menciona que, el espacio ya no se limita a un disco duro, sino que puede haber varios de ellos, con capacidad del orden de TB. [27]

También los servidores hoy vienen con herramientas que los hacen más eficientes. De acuerdo con Marchionni (2011). Una muy importante es la de la configuración del array, o el conjunto de discos del cual se dispone. Ellos pueden estar en el servidor o conectados a él en una unidad storage. El array se organiza en niveles de RAID (del inglés Redundant Array of Independent Disks, o conjunto redundante de discos independientes.) Las ventajas que esto representa, en vez de tener toda la información en un solo disco, son mayor integridad, rendimiento, tolerancia a fallos y capacidad. [27]

La tecnología RAID según Vásquez (2012), nos permite, mediante hardware o software, combinar dos o más discos de forma que sean vistos como una única unidad lógica. La información se almacena en ellos de forma redundante proporcionando distintos niveles de tolerancia a fallos.

De acuerdo con lo citado sobre los esquemas RAID existentes y sus principales características, Vázquez (2012) nos define las siguientes:

RAID 0. De todos los esquemas RAID, éste es el único que no proporciona tolerancia a fallos. Se utiliza exclusivamente cuando necesitamos altos rendimientos, la cantidad de espacio disponible es crítica y la disponibilidad nos la deben de proporcionan otros esquemas. Permite que múltiples discos sean vistos como una única unidad lógica mediante una técnica denominada drive spanning, de forma que la capacidad de la unidad lógica es igual a la suma de las capacidades de todas las unidades físicas. Se puede usar con cualquier número de discos físicos (de dos en adelante) limitados sólo por la capacidad de nuestra controladora. Para distribuir los datos entre los diferentes

discos físicos se usa otra técnica denominada drive striping que maximiza el rendimiento de las operaciones de entrada/salida. Para ello, se divide el disco lógico en bloques de datos denominados bandas (stripes), las cuales se distribuyen entre los discos físicos. Durante las operaciones de lectura y escritura los discos operan simultáneamente.

RAID 1. Emplea la técnica denominada drive mirroring, mediante la cual creamos un único disco lógico usando para ello dos (y sólo dos) discos físicos. Todos los datos que escribimos en el disco lógico son escritos en ambos discos físicos, de forma que ambos son, en todo momento, gemelos. El espacio real disponible se reduce, pues, al 50%. El rendimiento en la lectura de datos se incrementa, pero empeora en la escritura. RAID 1 nos proporciona un buen nivel de tolerancia a fallos y de rendimiento, pero la peor eficiencia en cuanto al espacio de almacenamiento disponible. Cuando usamos RAID 1 con dos controladoras de disco independientes, la técnica resultante se denomina drive duplexing y nos proporciona uno de los máximos niveles de tolerancia a fallos que podemos lograr en este aspecto.

RAID 1E o RAID 6. El RAID 1E (enhaced) combina las técnicas de mirroring y striping de forma que nuestro disco lógico es igualmente dividido en bandas, de forma que cada una de ellas está escrita en dos discos distintos. De esta forma podemos permitir cualquier número de discos físicos y no sólo dos como en el RAID 1. El espacio útil sigue reducido al 50% de la capacidad total y todo lo dicho en cuanto al rendimiento de lecturas y escrituras del RAID 1 es válido también para este esquema.

RAID 10 o RAID 1+0. Combina también, aunque de distinta forma, las técnicas de mirroring y striping. Es el resultado de realizar un mirroring de dos volúmenes de disco con RAID 0. El número de discos usados ha de ser par, la capacidad de espacio útil es del 50% y tenemos rendimientos de lectura y escritura similares a los proporcionados por RAID 0.

RAID 3. RAID 3 requiere al menos tres discos físicos. Uno de ellos está dedicado exclusivamente a almacenar la paridad de los datos de todos los demás. Los

datos se encuentran, al igual que en esquemas anteriores, divididos en bandas. Usando paridad en lugar de mirroring estamos reduciendo considerablemente el espacio necesario para la redundancia de datos. Proporciona un alto rendimiento en operaciones de lecturas de grandes bloques y, como contrapartida, ocasiona un cuello de botella en las operaciones de escritura. RAID 3 está recomendado exclusivamente en las aplicaciones que requieran uso intensivo de lectura de datos y escasas escrituras. Este esquema y el siguiente (RAID 4) prácticamente no se usan en la actualidad, habiendo sido desplazados por RAID 5.

RAID 4. Es similar a RAID 3 con la única diferencia de que utiliza bandas más grandes para mejorar algo el rendimiento en las operaciones de escritura.

RAID 5. Este esquema usa bandas para almacenar los datos y paridad para proporcionar tolerancia a fallos. La principal diferencia respecto a RAID 3 y RAID 4 es que no dedica un disco en exclusiva para la paridad, sino que almacena ésta en bandas intercaladas entre los datos de todos los discos. Requiere un mínimo de tres discos y su eficacia en cuanto a espacio de almacenamiento es idéntica a la proporcionada por los dos RAID's anteriores. La distribución de las bandas de paridad entre todos los discos elimina el cuello de botella existente en las escrituras.

En cuanto al tamaño físico de los Servidores, Marchionni (2011) indica que estos, por sus diferencias físicas, de tamaño y de diseño, también se dividen en rackeables, tipo tower y blades. Los rackeables son aquellos que se pueden colocar dentro de un armario con correderas (rack); suelen ser delgados como una laptop de grandes dimensiones. Los servidores tower son los más típicos, parecidos a una computadora personal (Personal Computer – PC) físicamente, pero más potente. Por último, los blades son equipos grandes que permiten cambiar o agregar hardware mientras el servidor está activo. [27]

Apéndice No. 3. Cuestionarios aplicados

Preguntas aplicadas a personas usuarias de los servicios en salud

1. ¿Sabía que la información de su salud, después de ingresada al expediente clínico, no debe ser modificada?

   ☐ Sí. ☐ No.

2. ¿Ha escuchado hablar del expediente digital en salud?

   ☐ Sí. ☐ No.

3. ¿Qué entiende por expediente digital en salud?

   ☐ Algo como un libro digital.

   ☐ El expediente de papel digitalizado.

   ☐ Un grupo de documentos PDF que no se pueden modificar

   ☐ Un app que puedo ver en mi teléfono.

   ☐ Un sistema computacional creado por un centro médico

   ☐ Otro. _____

4. ¿Conoce si los expedientes digitales en salud tienen valor legal?

   ☐ Sí. ☐ No.

   R/ Si, deben tenerlo.

5. ¿Conoce donde se guarda la información de un expediente digital en salud?

   ☐ Sí. ¿Dónde? _____ ☐ No.

6. ¿Considera seguro el uso del expediente digital para almacenar la información de la salud de la población nacional?

   ☐ Sí. ☐ No.

7. ¿Considera correcto que un funcionario **no médico** vea y modifique la información de su expediente digital en salud?

   ☐ Sí. ☐ No.

8. ¿Conoces lo que es firma digital?

   ☐ Sí. ☐ No.

9. ¿Sabía que la Firma digital es una herramienta creada por el Banco Central que le da valor legal a los documentos digitales? Haciéndolos legalmente iguales que los firmados manualmente.

   ☐ Sí. ☐ No.

10. De acuerdo con la definición de firmas y Digital. ¿Considera importante utilizarla en el expediente digital?

    ☐ Sí. ☐ No.

    ¿Por qué? _____

11. ¿Qué características de seguridad considera debe tener un expediente digital en salud?

    ☐ Una bitácora que indique quién vio o abrió y modifico el expediente digital

    ☐ Uso de firma digital.

    ☐ Que solamente los médicos lo puedan modificar anotaciones ya guardadas

    ☐ Que solamente el informático que lo creó lo pueda modificar a información incluida.

    ☐ Que nadie lo pueda modificar.

    ☐ Que tenga un control del almacenamiento de la información.

    ☐ Que la información solo pueda ser vista por especialistas médicos.

    ☐ Que tenga valor legal en caso de una mala atención médica.

    ☐ Otro. _____

12. ¿Conoce los documentos PDF?

☐ Sí. ☐ No.

13. ¿Sabía que un documento PDF es difícil de modificar? ¿Y si es firmado con la firma digital no puede ser modificado, sin que la firma se invalide?

☐ Sí. ☐ No.

14. ¿Aceptaría que los documentos de su expediente digital estuviesen en un formato PDF firmados digitalmente y con un control digital que controla la indexación de los nuevos documentos?

☐ Sí. ☐ No.

Preguntas aplicadas a personal técnico informático

1. ¿Qué tipo de formatos de almacenamiento de datos clínicos conoce?

☐ Bases de dados SQL ☐ Documento PDF

☐ Bases de datos NO SQL ☐ Imágenes DICOM

☐ Archivos de texto ☐ Otro _____

2. ¿Qué tipos de perfiles de usuarios conoce, en las BD de los Sistemas de Información?

☐ DBA. ☐ Usuarios superiores

☐ Administrador de BD. ☐ Usuarios generales

☐ Administrador de Aplicaciones. ☐ Otro _____

3. Según su conocimiento técnico, en una BD de un sistema de información en general, deben existir usuarios con permiso para:

   ☐ El control total de la BD. ☐ Solo para consultar datos.

   ☐ Modificar cualquier dato. ☐ Solo para modificar ciertos datos.

   ☐ Solo ingresar Datos. ☐ Otro _____

4. De acuerdo con su conocimiento técnico, un usuario DBA puede:

   ☐ Modificar cualquier información ☐ Consultar datos incluidos.

   ☐ Dar mantenimiento a la BD ☐ Tener acceso total a los datos.

   ☐ Ingresar datos. ☐ Otro _____

5. ¿Qué grado de confiabilidad para la información, considera que tiene una base de datos bien configurada?

   ☐ Es 100% confiable. ☐ Es de 50% a 69% confiable.

   ☐ Es de 90% a 99% confiable. ☐ Es de 1% a 49% confiable.

   ☐ Es de 70% a 89% confiable. ☐ Es de 0% confiable.

6. ¿Conoce algún sistema de información que guarde datos en archivos de texto?

   ☐ Sí ☐ NO

7. ¿Considera confiable el almacenamiento en archivos de texto?

   ☐ Sí, completamente. ☐ No, nada confiable ☐ Poca confiabilidad

8. ¿Qué grado de seguridad para el resguardo de la información considera que tienen los archivos de texto?

   ☐ Es 100% seguro. ☐ Es de 50% a 69% seguro.

   ☐ Es de 90% a 99% seguro. ☐ Es de 1% a 49% seguro.

   ☐ Es de 70% a 89% seguro. ☐ Es 0% seguro.

9. ¿Conoce algún sistema de información que guarde datos en archivos PDF?

☐ Sí ☐ NO

10. ¿Considera confiable el almacenamiento de información en archivos PDF?

☐ Sí completamente. ☐ No, nada confiable ☐ Poca confianza

11. ¿Qué grado de seguridad para la información considera que tienen los archivos PDF?

☐ Es 100% seguro. ☐ Es de 50% a 69% seguro.

☐ Es de 90% a 99% seguro. ☐ Es de 1% a 49% seguro.

☐ Es de 70% a 89% seguro. ☐ Es 0% seguro.

12. ¿Conoce algún sistema de información que guarde datos en archivos DICOM?

☐ Sí ☐ No

13. ¿Considera seguro el almacenamiento en archivos DICOM?

☐ Sí completamente. ☐ No, nada seguro ☐ Poca seguridad

14. ¿Qué grado de seguridad para la información considera que tienen los archivos DICOM?

☐ Es 100% seguro. ☐ Es de 50% a 69% seguro.

☐ Es de 90% a 99% seguro. ☐ Es de 1% a 49% seguro.

☐ Es de 70% a 89% seguro. ☐ Es de 0% seguro.

15. ¿Conoce la herramienta de firma digital de Costa Rica?

☐ Si ☐ No

16. ¿Ha utilizado, o ha observado información firmada digitalmente?

☐ Sí ☐ No

17. ¿En qué formato ha utilizado o ha observado el uso de la firma digital?

☐ Bases de datos SQL ☐ Documento PDF

☐ Bases de datos NO SQL ☐ Imágenes DICOM

☐ Archivos de texto ☐ Otro _____

☐ Ninguno.

18. Según su conocimiento técnico, ¿qué características de seguridad, adquieren los datos firmados digitalmente con el certificado de firma digital emitido en Costa Rica?

☐ Confiabilidad. ☐ Certeza de quien lo firmó.

☐ Legalidad. ☐ Evidencia de que nadie lo modificó.

☐ Inmodificables. ☐ Otro _____

19. ¿Conoce algún sistema de información en salud (SIS) que utilice la firma digital para la seguridad de la información?

☐ Sí ¿Cuál? _____ ☐ No

20. ¿Conoce o ha observado documentos PDF firmados digitalmente?

☐ Sí ☐ NO

21. ¿Considera confiable el almacenamiento de la información en archivos PDF firmados digitalmente?

☐ Sí completamente. ☐ No, nada confiable ☐ Poca confianza

22. ¿Qué grado de confiabilidad considera que tiene la información almacenada en archivos PDF firmados digitalmente?

- ☐ Es 100% confiable.
- ☐ Es de 90% a 99% confiable.
- ☐ Es de 70% a 89% confiable.
- ☐ Es de 50% a 69% confiable.
- ☐ Es de 1% a 49% confiable.
- ☐ Es de 0% confiable.

23. Tomando en cuenta la importancia de la información clínica, y que esta, no debe ser modificada, ¿cuál tipo de formato digital considera más adecuado para guardar la historia clínica de una persona?

- ☐ Bases de datos SQL
- ☐ Bases de datos NO SQL.
- ☐ Archivos de texto.
- ☐ Documento PDF + Firma Digital
- ☐ Imágenes DICOM
- ☐ Otro _____

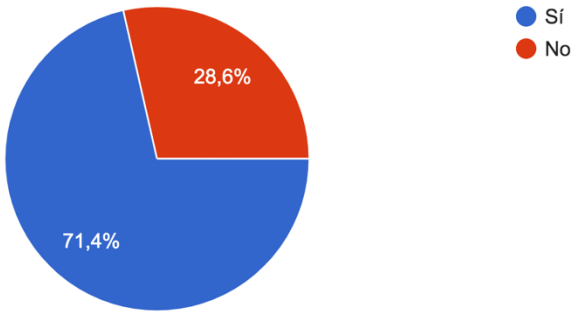
24. ¿Qué herramientas considera importantes de incluir, como parte de una estructura de seguridad para expedientes digitales?

- ☐ Sistema de información.
- ☐ Bases de datos.
- ☐ Blockchain.
- ☐ Almacenamiento en archivos PDF
- ☐ Firma Digital.
- ☐ Sistemas de visualización.
- ☐ Otro _____

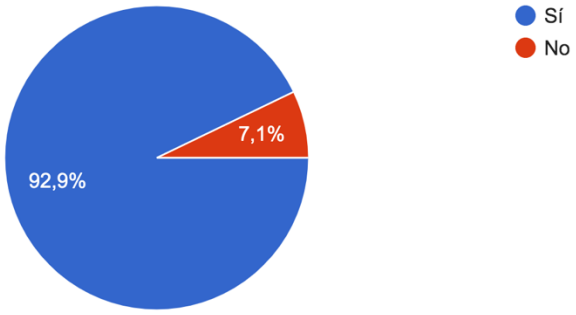
Respuestas de las personas usuarias del servicio de salud.

Tamaño de la poblacion	*75 000*
Nivel de confianza	*95%*
Margen de error	*10%*
Tamaño de la muestra	*96*

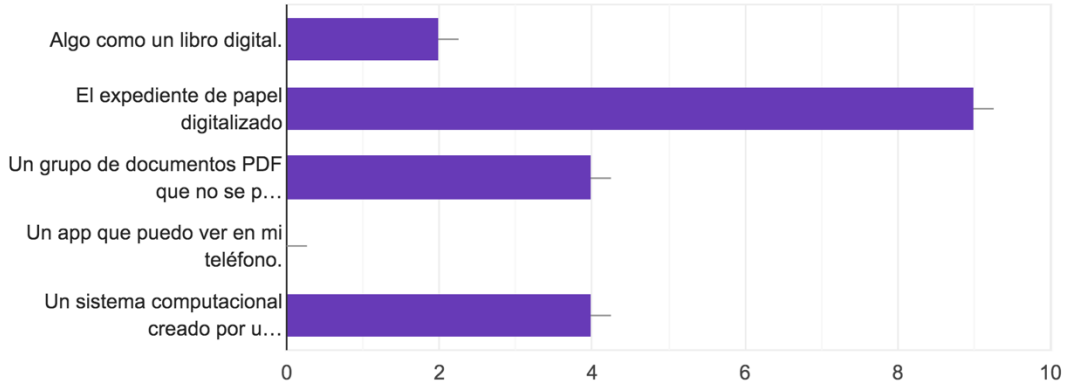
1. ¿Sabia que la información de su salud, después de ingresada al expediente clínico, no debe ser modificada?



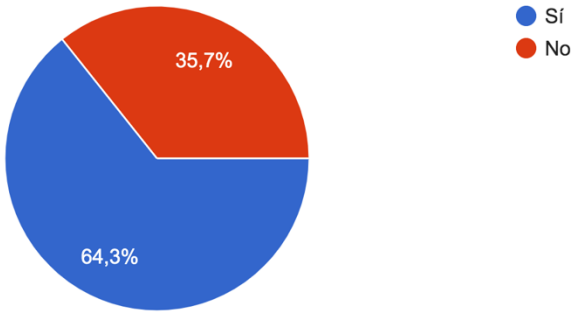
2. ¿Ha escuchado hablar del expediente digital en salud?



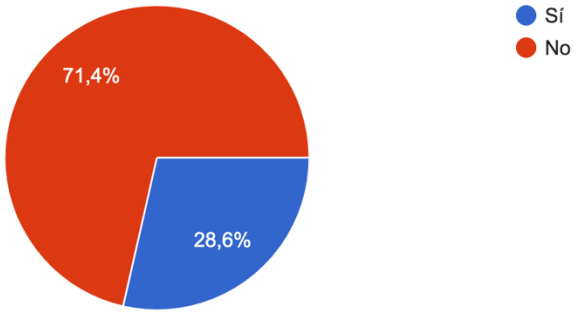
3. ¿Que entiende por expediente digital en salud?



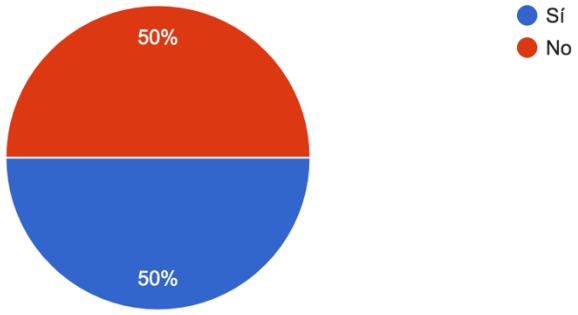
4. ¿Conoce si los expedientes digitales en salud tienen valor legal?



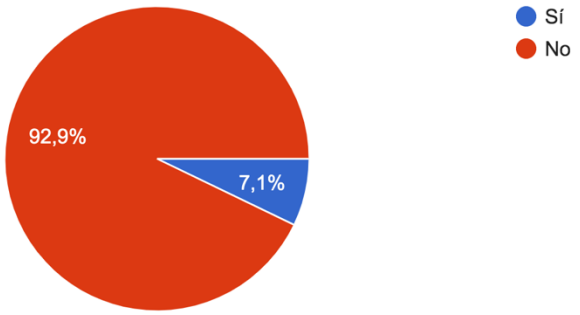
5. ¿Conoce donde se guarda la información de un expediente digital en salud?



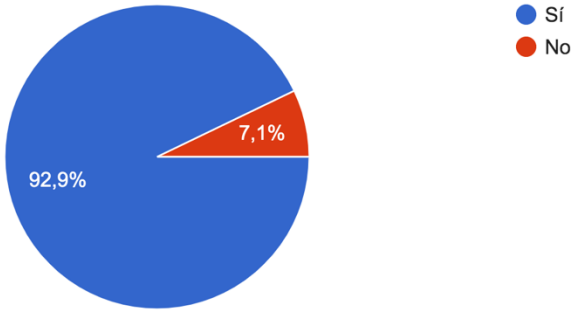
6. ¿Considera seguro el uso del expediente digital para almacenar la información de la salud de la población nacional?



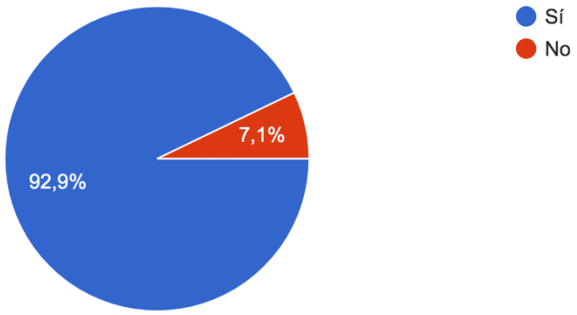
7. ¿Considera correcto que un funcionario no médico vea y modifique la información de su expediente digital en salud?



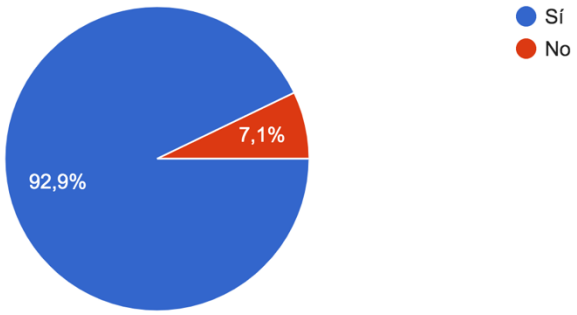
8. ¿Conoces lo que es firma digital?



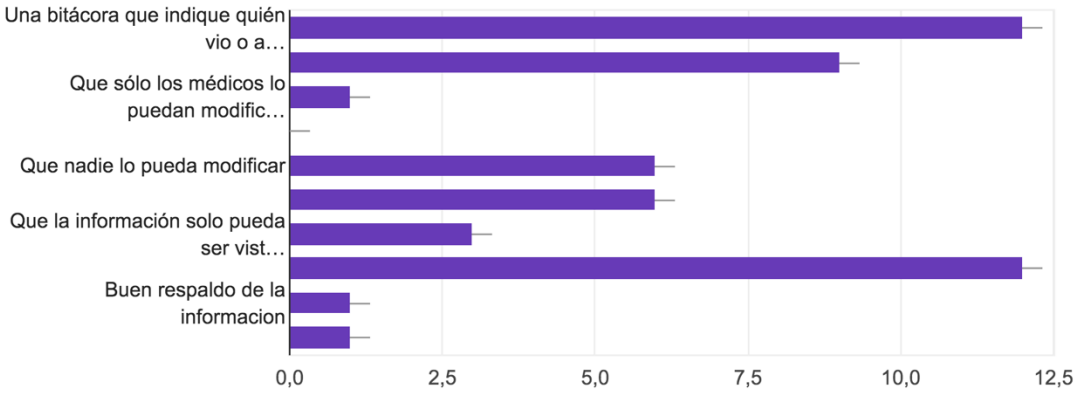
9. ¿Sabia que la Firma digital es una herramienta creada por el Banco Central que le da valor legal a los documentos digitales? Haciéndolos legalmente iguales que los firmados manualmente.



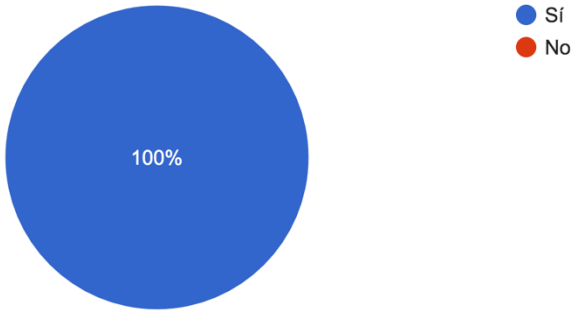
10. De acuerdo a la definición de firmas y Digital. ¿Considera importante utilizarla en el expediente digital?



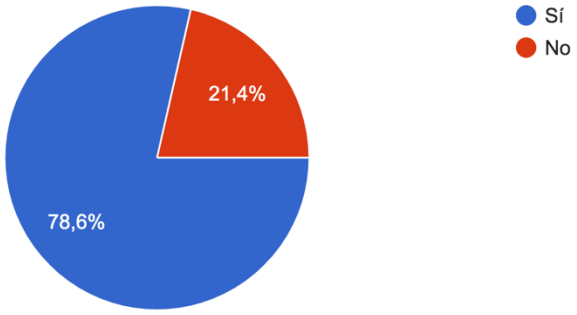
11. ¿Que características de seguridad considera debe tener un expediente digital en salud?



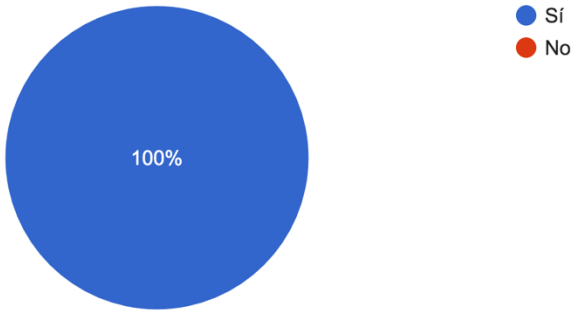
12. ¿Conoce los documentos PDF?



13. ¿Sabia que un documento PDF es difícil de modificar? ¿Y si es firmado con la firma digital no puede ser modificado, sin que la firma se invalide?



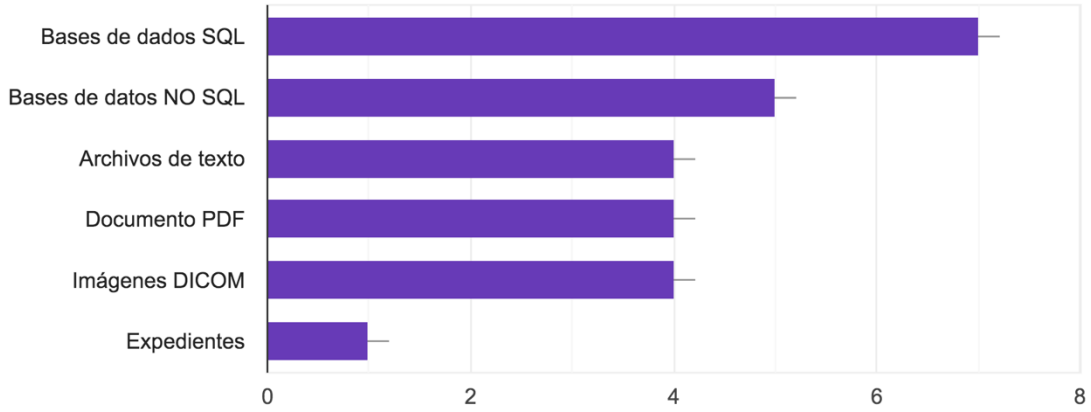
14. ¿Aceptaría que los documentos de su expediente digital estuviesen almacenados en archivos PDF firmados digitalmente y con un control digital que controle el ingreso de los nuevos documentos?



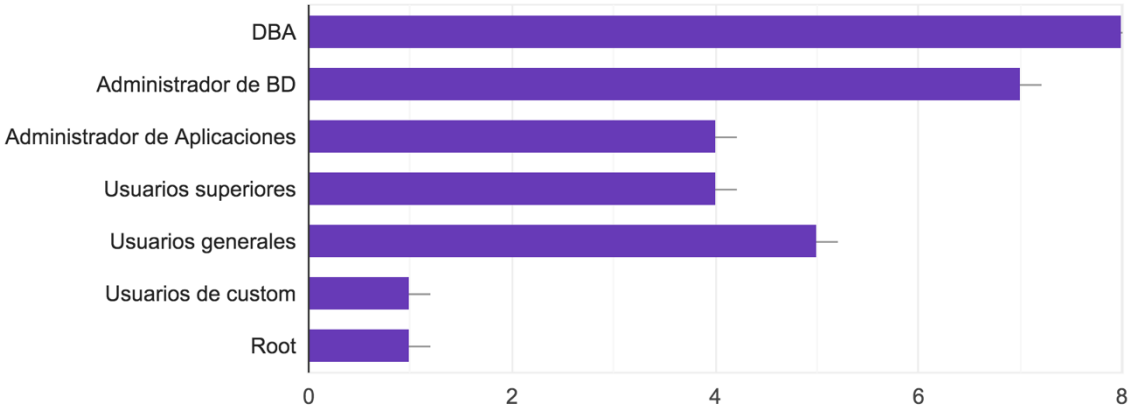
Respuestas del personal Técnico Informático.

Tamaño de la poblacion	*50*
Nivel de confianza	*95%*
Margen de error	*10%*
Tamaño de la muestra	*34*

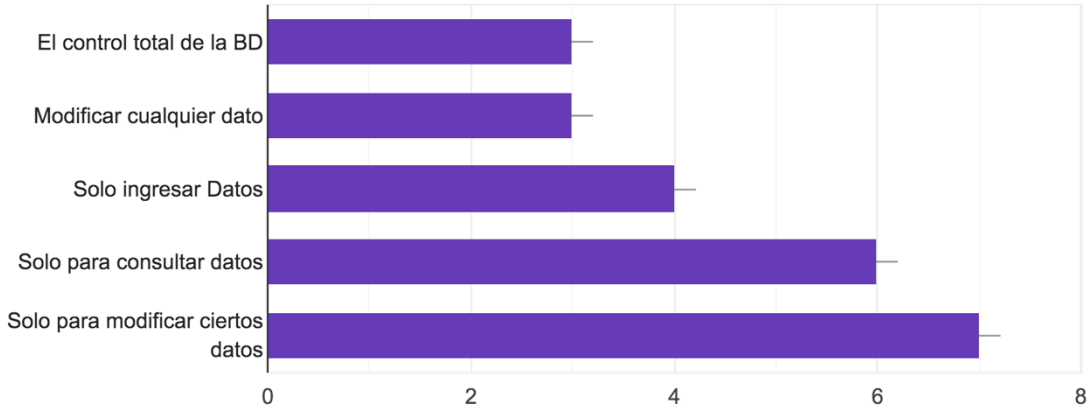
1. ¿Que tipo de formatos de almacenamiento de datos clínicos conoce?



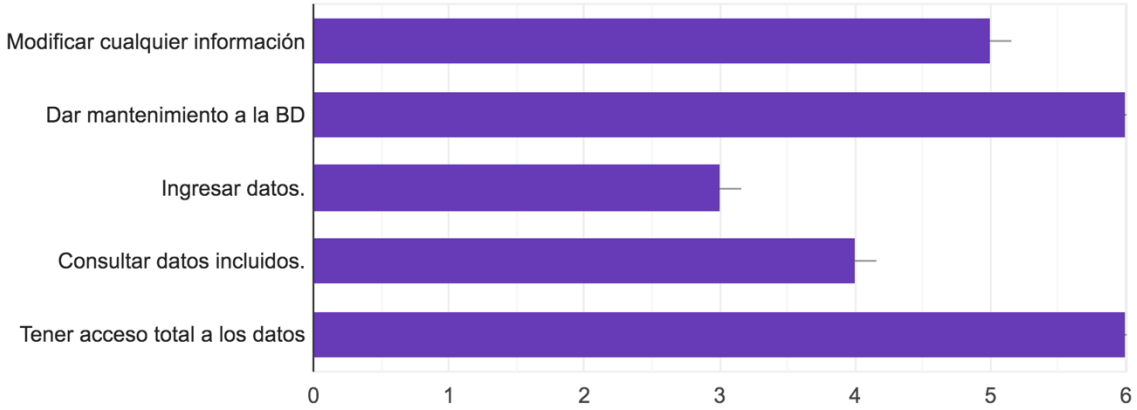
2. ¿Que tipos de perfiles de usuarios conoce, en las BD de los Sistemas de Información?



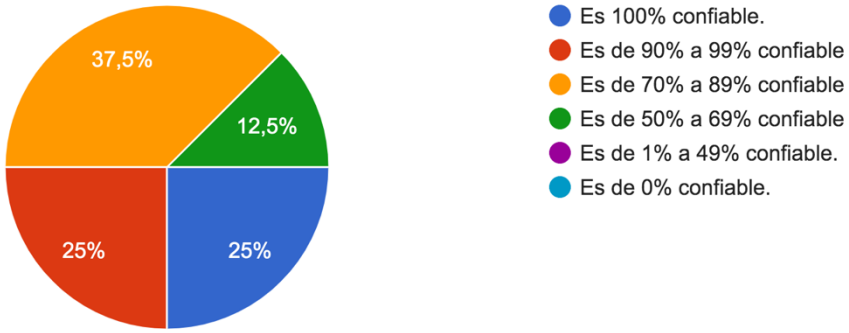
3. Según su conocimiento técnico, en una BD de un sistema de información en general, deben existir usuarios con permiso para:



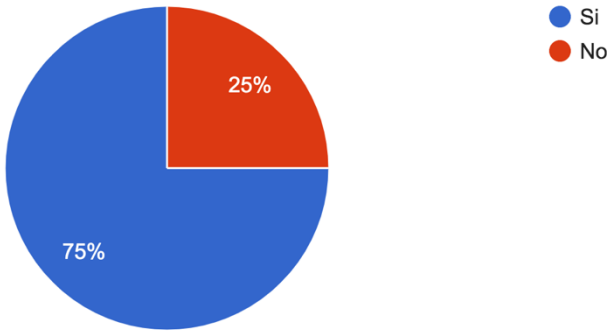
4. De acuerdo a su conocimiento técnico, un usuario DBA puede:



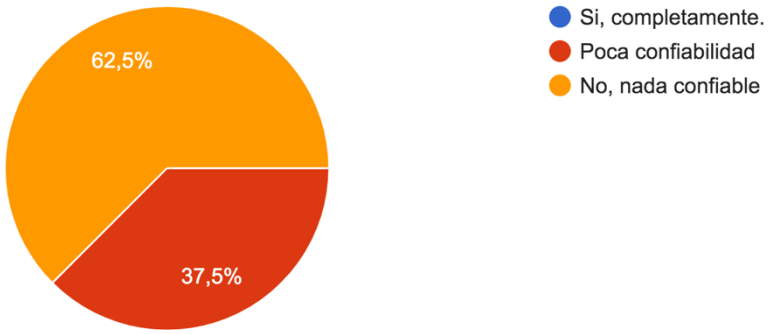
5. ¿Que grado de confiabilidad para la información, considera que tiene una base de datos bien configurada?



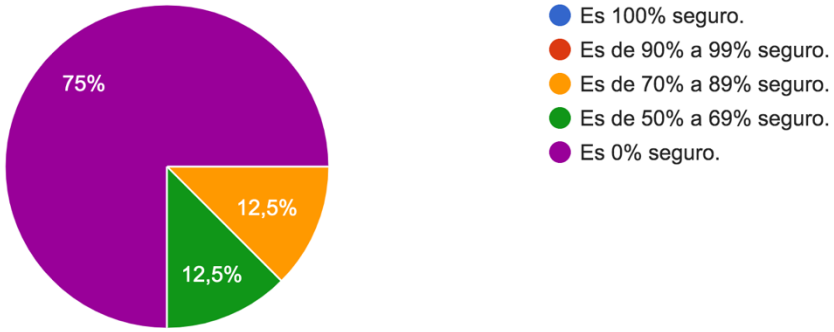
6. ¿Conoce algún sistema de información que guarde datos en archivos de texto?



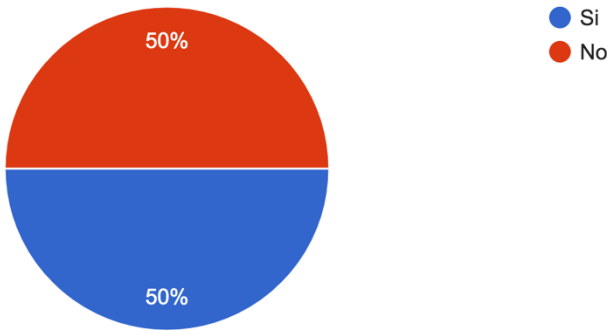
7. ¿Considera confiable el almacenamiento en archivos de texto?



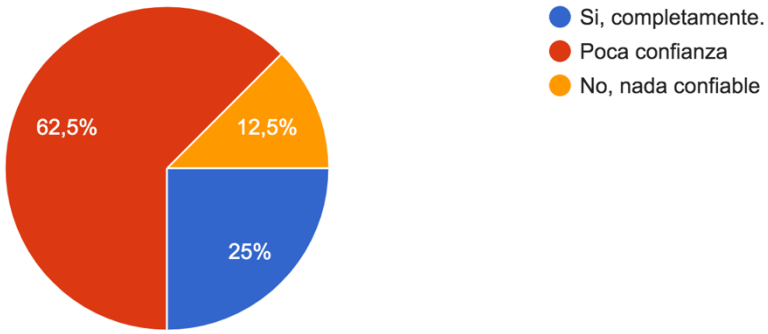
8. ¿Que grado de seguridad para el resguardo de la información considera que tienen los archivos de texto?



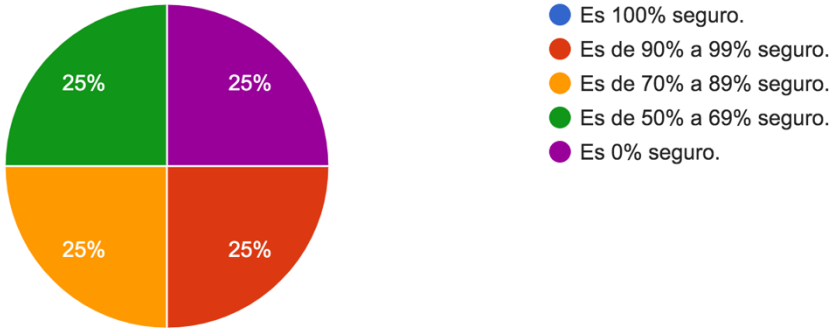
9. ¿Conoce algún sistema de información que guarde datos en archivos PDF?



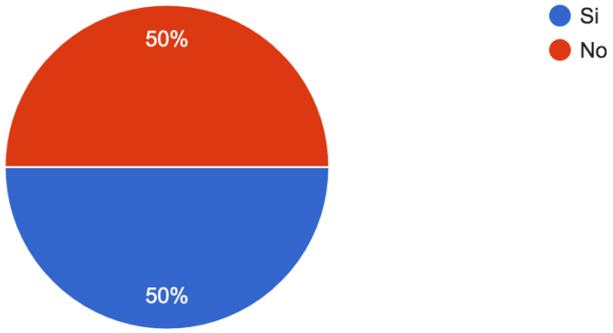
10. ¿Considera confiable el almacenamiento de información en archivos PDF?



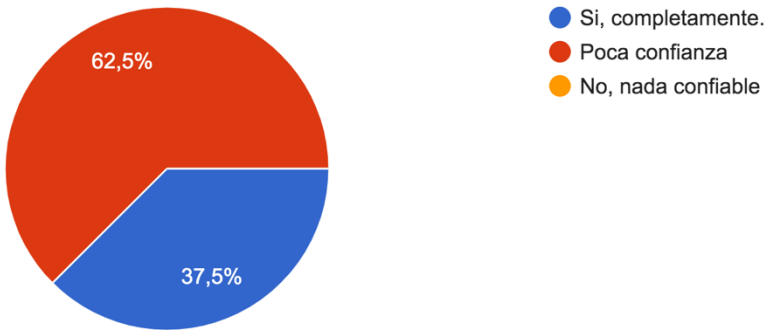
11. ¿Que grado de seguridad para la información considera que tienen los archivos PDF?



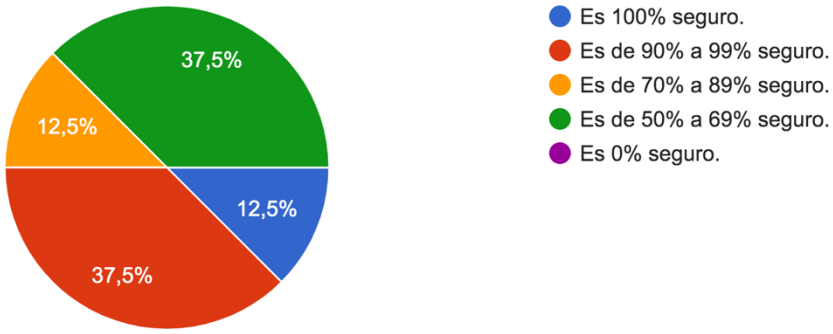
12. ¿Conoce algún sistema de información que guarde datos en archivos DICOM?



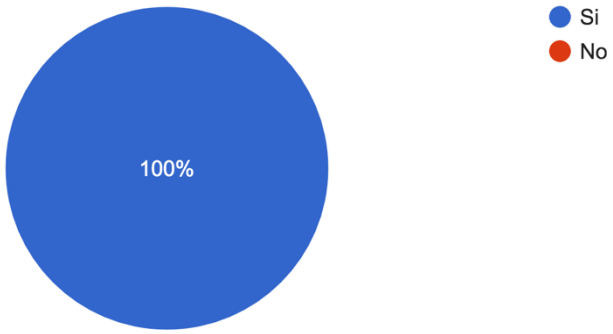
13. ¿Considera seguro el almacenamiento en archivos DICOM?



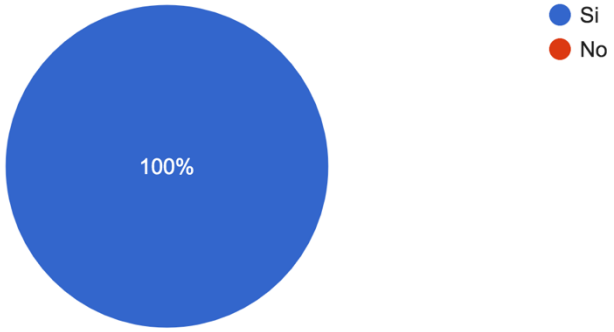
14. ¿Que grado de seguridad para la información considera que tienen los archivos DICOM?



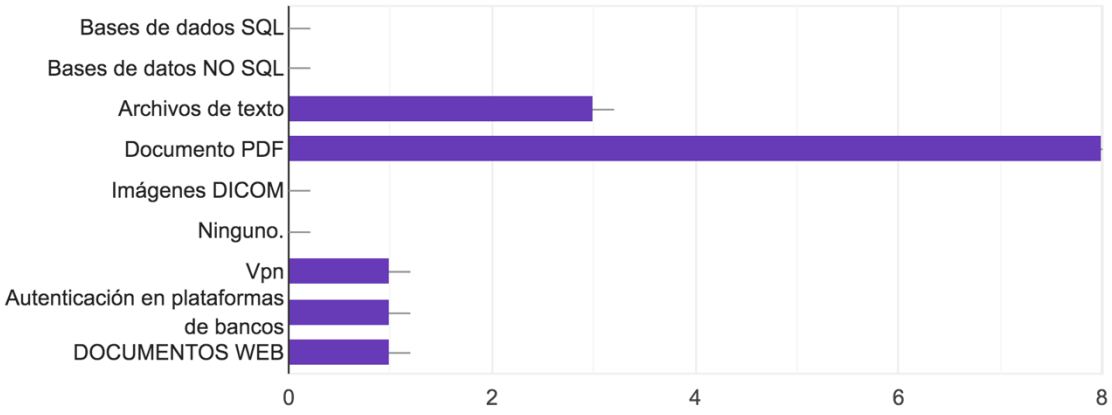
15. ¿Conoce la herramienta de firma digital de Costa Rica?



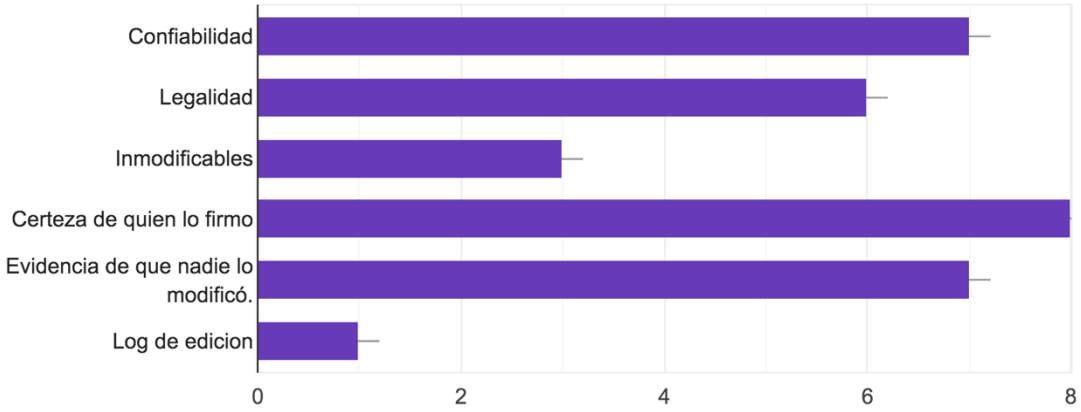
16. ¿Ha utilizado, o ha observado información firmada digitalmente?



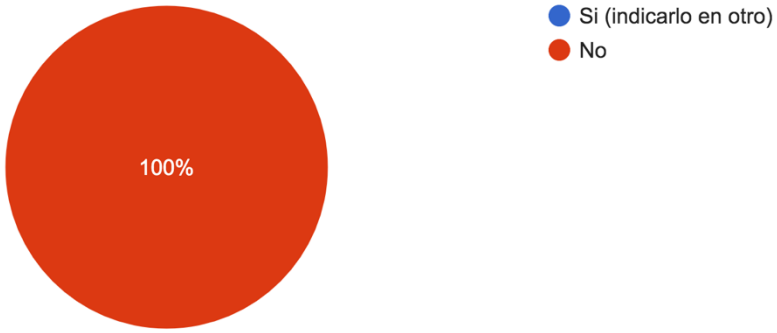
17. ¿En que formato ha utilizado o ha observado el uso de la firma digital?



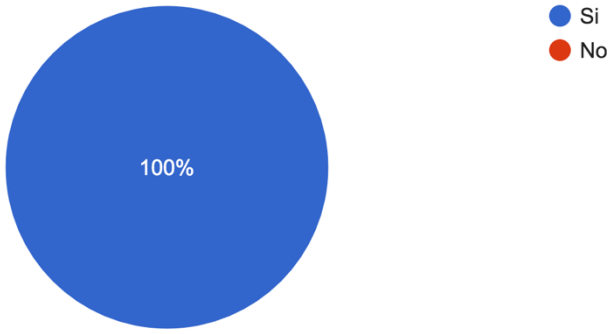
18. Según su conocimiento técnico. ¿Que características de seguridad, adquieren los datos firmados digitalmente con el certificado de firma digital emitido en Costa Rica?



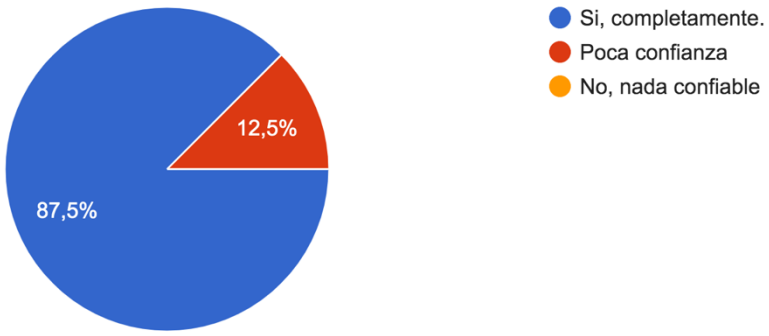
19. ¿Conoce algún sistema de información en salud (SIS) que utilice la firma digital para la seguridad de la información?



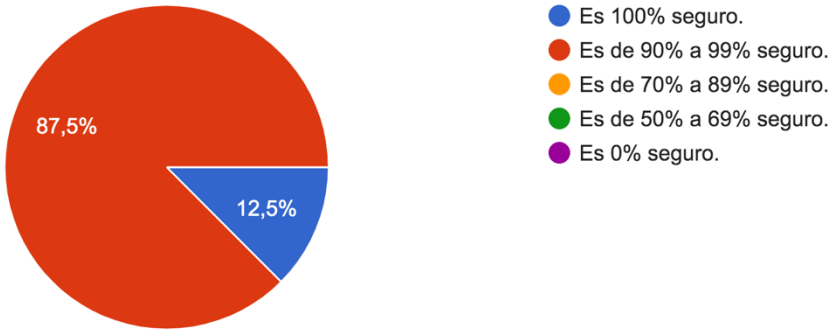
20. ¿Conoce o ha observado documentos PDF firmados digitalmente?



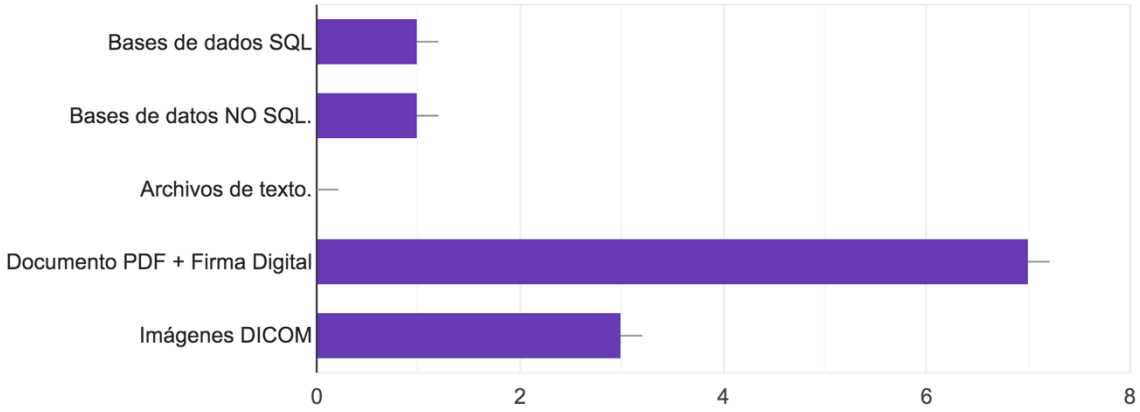
21. ¿Considera confiable el almacenamiento de la información en archivos PDF firmados digitalmente?



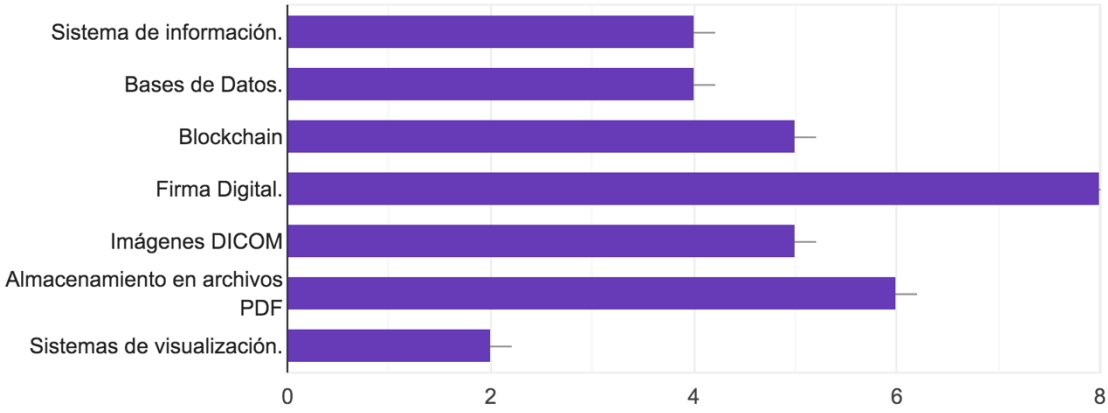
22. ¿Qué grado de confiabilidad considera que tiene la información almacenada en archivos PDF firmados digitalmente?



23. Tomando en cuenta la importancia de la información clínica, y que esta, no debe ser modificada. ¿Cuál tipo de formato digital considera más adecuado para guardar la historia clínica de una persona?



24. ¿Qué herramientas considera importantes de incluir, como parte de una estructura de seguridad para expedientes digitales?



Apéndice No. 4. Controles y cumplimiento de HIPAA

Más allá del diseño de la estructura de seguridad de la información de expedientes digitales especializados para centros médicos, como se propone en este trabajo, y conociendo que los sistemas de información no se dejarán de utilizar, más bien, se convertirán en el elemento central de las estructuras de seguridad de la información. Se debe tomar en cuenta el cumplimiento de controles claves para la privacidad, protección y seguridad de la información de los datos clínicos. En este punto, los controles, las reglas y cumplimiento de estas, son importante para el acatamiento de estándares informáticos en el sector sanitario, como lo son HIPAA y HL7.

HIPAA es una es la ley aplicada en Estados Unidos que comprende la Transferencia y Responsabilidad de la información clínica de los pacientes. Su objetivo es asegurar la información personal del paciente y asegurar la protección de la información clínica, tanto física como digital.

Reglas de Privacidad para la confidencialidad del paciente

En HIPAA se establece que todas las organizaciones de atención médica deben cumplir con pautas concretas destinadas a salvaguardar la confidencialidad e integridad de los datos clínicos. Por consiguiente, un punto clave para cumplimiento de HIPAA, y que se debe aplicar al diseño de la estructura planteada en este trabajo, es la privacidad de la información, esto consiste en el aseguramiento de la información clínica. Para tales efectos se considera importante la elaboración de contratos que impongan medidas de seguridad específicas que eviten hacer de conocimiento público la información digital en salud, y en especial sin el consentimiento de la persona usuaria, del servicio de sanidad. Estos contratos deben ser elaborados entre las instituciones que brindan el servicio de salud, ya sean instituciones públicas o privadas, con los trabajadores que manipulan la información de los pacientes y las empresas que les venden servicios especializados a estas instituciones de salud.

Con la definición de un buen reglamento de privacidad, el personal de salud y las empresas contratadas, tiene las reglas claras del uso que se le debe dar a la información de los pacientes, así como las restricciones que se tienen.

En este punto algunas medidas para proteger la privacidad de la información digital clínica son:

1. La implementación de políticas de confidencialidad de la información clínica.

2. Protección de los datos de identificación de las personas usuarias del servicio de salud.

3. Elaboración de contratos de privacidad con las empresas proveedoras de servicios.

4. Inclusión en los contratos laborales de los funcionarios de salud, de cláusulas privacidad y confidencialidad de la información que se maneja de los asegurados.

5. Tener un grupo personal capacitados para dar declaraciones acerca se situaciones especiales respecto a temas de salud o que afecten la privacidad de la información del paciente.

6. En caso del uso de información clínica con fines educativos o para obtener estadísticas, se deben anonimizar los datos clínicos, para proteger la identidad de los pacientes.

7. Para los casos en que los datos no se puedan disociarse y sea necesario mantener la identidad de la persona, se deberá recabar el consentimiento expreso y por escrito de los pacientes.

8. Realizar capacitaciones constantes al personal, para la instrucción y el recordatorio de los procedimientos de privacidad de la información que tiene la institución.

9. En cuanto a los sistemas de información en salud, es importante que estos cumplan con los requisitos del resguardo de la información privada de los pacientes. Teniendo las herramientas para anonimizar la información a las personas que no requieren conocerla.

10. También en cuanto a bases de datos, es necesario el enmascaramiento de la información del paciente, para que el menor número de personal técnico pueda ver la información personal y asociarla con los diagnósticos o procedimientos médicos.

Reglas de seguridad para la información

HIPPA establece un conjunto de procesos o reglas de seguridad para proteger el acceso a la información. También establece requisitos técnicos para las empresas proveedoras de servicios médicos. Estas medidas de seguridad permiten el resguardo y el traslado de la información de una manera segura.

La seguridad que plantea HIPAA en esta regla de seguridad se refiere a la protección de la información, incluidas las medidas: físicas que se centran en procesos para protegen el equipo físico y los edificios relacionados, estas disposiciones tratan de prevenir los peligros naturales y los del medio ambientales, así como los de las intrusiones físicas. Las medidas tecnológicas que se refieren a los mecanismos técnicos y procesos diseñados para proteger, controlar y monitorear el acceso a la información. Y las medidas administrativas que son las prácticas diseñadas para controlar las medidas de seguridad y la conducta del personal que acceden, ven, procesan y distribuyen electrónicamente información médica protegida.

Dentro de los puntos clave que plantea HIPAA para su cumplimiento en la regla de seguridad, tenemos que se deben cumplir medidas como:

1. El cifrado de la información, para proteger los datos clínicos de los pacientes.
    a. Protección de la información clínica en tránsito.

    b. Protección de la información clínica en uso.

    c. Protección de la información clínica en respaldos y en pasivo.

2. Administración de la información médica de manera escalable y flexible con diversos niveles de acceso.

3. Implementación de la autentificación de factor múltiple, que garantice el acceso autorizado a los datos críticos

4. Utilización de aplicaciones que garanticen la protección de la información clínica.
    a. Utilización de aplicaciones certificadas en el uso de procedimientos de privacidad del paciente.

    b. Las aplicaciones deben protegerse en los niveles físico, lógico, humano y logístico.

    c. Utilización de procedimientos que garanticen la autorización, autentificación, disponibilidad, confidencialidad, integridad de los datos y el no repudio de los archivos médicos.

5. Utilización de VPN para el acceso remoto de la información desde lugares externos a las redes de la institución.

6. Utilización de capas de conexión seguras (SSL, HTTPS)
7. Utilización de equipos duplicados para e resguardo de la información de forma segura en caso de un siniestro.

8. Utilización de sistemas de potencia en los equipos que resguardan la información clica de los asegurados.

9. Utilización de dispositivos de control de acceso para el resguardo de los dispositivos que resguardan la información clínica.

10. Tener prevenciones para desastres por medio de un plan en caso de desastres.

También dentro de las medidas por utilizar para cumplir con HIPPA, se tienen las relacionadas al intercambio de información entre aplicativos médicos. Por lo que la utilización del estándar HL7 es imprescindibles, siendo este diseñado exclusivamente para ser utilizado en las tecnologías médicas.

HL7 es un estándar importante para la aplicación y que va de la mano con HIPAA, este estándar facilita el intercambio de la información clínica en formato digital, utilizando los lenguajes UML y XML para que la información compartida sea analizada en las diferentes áreas, sin importar la tecnología y dispositivos utilizados.

Las especificaciones del modelo HL7 son las más utilizadas en mensajería, ya que son un estándar que permite a las aplicaciones heterogéneas de salud intercambien datos clínicos, sin importar las marcas comerciales de los aplicativos. En resume HL7 define:

1. Un modelo información de referencia genérico en el cual se basan los demás estándares.

2. Apunta a resolver la comunicación entre sistemas mediante mensajería XML.

3. Permite interoperabilidad entre sistemas heterogéneos de salud.

Por tanto y conociendo que el expediente digital es la recopilación de toda la información clínica de una determinada persona, que se genera en muchos aplicativos diferentes, tales como laboratorios, sistemas de registros médicos, sistemas de información médica, sistemas radiológicos y de imágenes digitales, entre otros. Es importante tener un canal de comunicación para el intercambio de información.

Este medio de comunicación para el entendimiento entre aplicativos tecnológicos, se simplifica con la utilización del estándar HL7, que, de acuerdo con las reglas de privacidad y seguridad vistas en los puntos anteriores, este estándar se puede incluir a la perfección, dentro de las medidas necesarias para el cumplimiento de HIPAA. Por consiguiente, la utilización de HL7 en los competentes de la estructura de seguridad de la información de expedientes digitales especializados para centros médicos, es importante a la hora de la implementación.