Vulnerabilidades de las historias clínicas digitales ocasionadas por los Trabajadores de Salud

Presentado por:
Nelly Angélica Achury Peñaloza 35251713

Universidad Abierta y a Distancia UNAD
Programa Ingeniería de Sistemas
Girardot – Cundinamarca
2018

Vulnerabilidades de las historias clínicas digitales ocasionadas por los Trabajadores de Salud

Presentado por:
Nelly Angélica Achury Peñaloza 35251713

Trabajo De Grado Presentado Como Requisito Para Optar Al Título De
Ingeniería de Sistemas

Director/Asesor:
Ingeniera Vanessa Carolina Gutiérrez Mendoza

Director/Asesor:
Ingeniera Vanessa Carolina Gutiérrez Mendoza

Universidad Abierta y a Distancia UNAD
Programa Ingeniería de Sistemas
Girardot – Cundinamarca
2018

Página de aceptación

_____

_____

_____

_____

_____

_____

Dedicatoria

A mi compañero, amigo y esposo Felipe Camacho, quien siempre ha creído en mí, quien me apoyo y tuvo toda la paciencia en cada paso durante estos años; a mi padre y madre quienes me enseñaron constancia y disciplina; a mi hermano Oswaldo quien con admiración observo y es ejemplo a seguir; a mi hermosa hija que llego este año como bendición a mi hogar y a mi vida.

Agradecimientos

Agradezco a Dios principalmente quien puso a cada persona en mi camino como apoyo y motivante para llevar a feliz término mi carrera.

Índice

Resumen 12

Abstract 13

Introducción 14

Justificación 18

Objetivos 19

Objetivo General 19

Objetivos Específicos 19

Contenido 20

1. Hipótesis 20

2. Resultados esperados 20

3. Marco Referencial 20

3.1. Marco Conceptual 20

3.2. Metodología 26

3.3. Marco Jurídico 27

4. Tipo de Investigación 29

Capítulo 1: Factores de la Historia Clínica Digital 31

Capítulo 2: Importancia sobre la seguridad de las contraseñas en el ámbito laboral 34

Capítulo 3: Legislación aplicada en seguridad informática para el sistema de salud 38

Capítulo 4: Proposición de Encuesta a los Trabajadores de Salud 39

Capítulo 5: Presentación de Resultados de Encuesta 40

Capítulo 6: Análisis de Resultados 51

Capítulo 7: Perspectiva de Ingeniería de Sistemas en la problemática 54

7.1 Antecedentes de ataques cibernéticos 56

Conclusiones 58

Referencias y Enlaces 63

Anexos 67

Anexo 1. Encuesta virtual Trabajadores en Salud 67

Anexo 2. Resolución 1995 de 1999 71

Anexo 3. Legislación vigente para historias clínicas digitales en Colombia 79

Índice Ilustraciones

Ilustración 1 Resolución 1995 de 1999..... 28

Ilustración 2 Características de la muestra y porcentaje de participantes con buenas prácticas de seguridad según las variables sociodemográficas. 36

Ilustración 3 Legislación Vigente Historias Clínicas Digitares Colombia 38

Ilustración 4 IPS aplicadas con la encuesta virtual..... 40

Ilustración 5 Clase de IPS 41

Ilustración 6 Rango de edad..... 41

Ilustración 7 Cargo desempeñado dentro de la IPS 42

Ilustración 8 Importancia de la seguridad informática..... 42

Ilustración 9 Tipo de Sistema de Información que maneja la IPS..... 43

Ilustración 10 Experiencia medida en años en el cargo actual 43

Ilustración 11 Perspectiva de Seguridad frente al Software empleado..... 44

Ilustración 12 Ingreso al sistema con usuario y contraseña 45

Ilustración 13 Seguridad de contraseña 45

Ilustración 14 Seguridad de Contraseña 46

Ilustración 15 Seguridad en el proceso de información en el equipo de Computo 47

Ilustración 16 Uso personal de usuario y contraseña 47

Ilustración 17 Percepción de seguridad en uso de contraseña 48

Ilustración 18 Percepción de capacitación sobre seguridad de la Información 49

Ilustración 19 Empleo de Software como sistema de ingreso de Historias Clínicas..... 49

Ilustración 20 Conoce el Protocolo de seguridad de información de la IPS 50

Índice Tablas

Tabla 1 Clasificación de las amenazas que pueden producir un problema de seguridad en la organización 23

Tabla 2 Características de la muestra y porcentaje de participantes con buenas prácticas de seguridad según las variables sociodemográficas. 36

Resumen

Cuando nos referimos a las instituciones de salud, las cuales avanzan a pasos agigantados en materia de sistemas de información que les facilite llevar a cabo los procesos diarios, es imposible pensar en vulnerabilidades de seguridad y la exposición de la información a terceros con intereses de por medio y más teniendo en cuenta los diferentes casos que se han presentado durante los últimos años con referente a hackers. La atención a estos sucesos solo se ve cuando los eventos infortunados son dados a conocer a la opinión pública, es de aclarar que de un 100% de los casos que suceden a nivel nacional y mundial el 3% de ellos son dados a conocer, dependiendo la severidad del mismo; de acuerdo con lo anterior este tema en específico es preocupante si se tiene presente que la legislación mundial considera que la información médica de los pacientes es estrictamente confidencial. Partamos de un principio: absolutamente, y sin excepción, toda la información médica registrada en la historia clínica del paciente y alojada en computadores o servidores de las instituciones de salud está solo en custodia de estas últimas, los dueños de la información son los pacientes y de acuerdo artículo 34 de la ley 23 de 1981 la historia clínica es un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previsto por la ley[1].

[1] Tomado de Derechos y Obligaciones en la relación Médico-Paciente Dr. Ricardo Barona Betancuort Pag 5.

Abstract

When we refer to health institutions, which have great advancing in terms of information systems that make it easier for them to carry out daily processes, it is impossible to think of security vulnerabilities and the exposure of information to third persons with other interests and more taking into account the different cases that have been presented during the last years with reference to hackers. The attention to these events is only seen when unfortunate events are made known to the public, is to clarify that 100% of the cases that occur nationally and globally 3% of them are made known, depending the severity of it; according to about, this specific issue is worrisome if it is kept in mind that the world legislation considers that the medical information of patients is strictly confidential. Let's start from the beginning: absolutely, and without exception, all the medical information registered in the patient's medical record and hosted on computers or servers of health institutions is only in the custody of these, the owners of the information are the patients and according to article 34 of Law 23 of 1981, the clinical record is a private document submitted to a reservation that can only be known by third parties with the patient's authorization or in the cases provided for by law.

Introducción

La historia clínica y los registros médicos, son documentos de alto valor administrativo, educativo, gerencial y personal, por tanto la integridad de la información contribuye a mejorar la calidad de atención de los pacientes ya que esta información será única y exclusiva de cada uno de ellos; por tal motivo es importante tener un sistema de información que nos permita administrar y gestionar los datos consolidados a través del tiempo de los pacientes que acceden al servicio de salud así fue creada la historia médica clínica.

La medicina, la cual dicta un camino a seguir cuando de asistir, en general, a un enfermo se trata, es el saber que se ocupa de solucionar una problemática, orientada en la restauración de la salud cuando está se encuentra alterada en un semejante; durante el transcurrir de la historia y evolución de la humanidad hemos tenido la necesidad de plasmar todos los hallazgos mediante escritos, en el caso de la medicina no fue diferente y por medio del análisis, suposiciones, y métodos científicos, se establecieron diagnósticos, procedimientos y tratamientos que datan su origen desde la antigua Grecia; quienes mediante escritos mitológicos y los Egipcios mediante papiros detallaban en escritos con precisión la descripción de la enfermedad y los tratamientos o prescripciones generadas; de esta manera evolucionamos a la edad media donde se encuentran los primeros estudios de medicina y en donde se da inicio a la organización estructural de la historia clínica; esta evolución trae consigo avances tecnológicos para el siglo XIX, por medio del cual surgen nuevos inventos, que permiten a los médicos generar diagnósticos y tratamientos asertivos; de esta manera pudimos llegar a cuantificar, medir signos y síntomas, enriqueciendo de manera permanente la historia clínica del paciente en cada consulta con descripción, precisión y coherencia.

Teniendo en cuenta que para la segunda mitad del siglo XX se inicia la creación de los servicios nacionales de salud y con ello la creación de los hospitales, este crecimiento causa que las historias clínicas pierden su propiedad particular por parte de un médico a

convertirse en propiedad institucional, de esta manera y buscando una organización y fácil seguimiento de las historias clínicas, son ordenadas en forma cronológica y de acuerdo a cada episodio o consulta del paciente al sistema de salud.

Para finales del siglo XX e influenciados por el concepto de sanidad privada y los conceptos legales y la participación del paciente en el manejo de la información surge una perspectiva jurídica de la historia clínica, que incluye el soporte de documentos como consentimiento informado y testamento vital; teniendo en cuenta que la Historia Clínica contiene información privada del paciente, antecedentes personales y familiares, sus hábitos y todo aquello vinculado con su salud biopsicosocial, se debe garantizar la privacidad de información, de acuerdo a la ley de protección de datos y a la ética profesional de cada persona; es importante tener presente que la historia clínica debe ser elaborada para proteger, resguardar y preservar la salud del paciente; esta no se limita a ser una narración o exposición de hechos simplemente, sino que incluye en una sección de apartes de los juicios, documentos, procedimientos, informaciones y consentimiento informado. Es importante tener en cuenta que la historia clinica puede ser utilizada para la investigación y la docencia, como indicador de estadísticas y comportamientos generales.

De esta manera nace la historia clínica el cual es un documento privado, de tipo técnico, clínico, legal obligatorio y sometido a reserva, y en el que se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en la atención del paciente.

Para inicios del siglo XXI y con los avances tecnológicos nos han permitido acceder a una mayor cantidad de servicios a nivel nacional e internacional, permitiendo compartir experiencias e investigaciones de nuevos avances en la medicina, disminuyendo las fronteras de acceso a tratamientos para los pacientes. Hoy en día la tecnología aporta grandes soluciones a la vida cotidiana, es por esto que apoyado en un sistema de información se pueden mejorar gran parte de los problemas administrativos, legales o de satisfacción en la atención.

Debido al volumen de información que se generan en las IPS se constituyó la Historia Clínica Digital o en Formato Electrónico, con esto el Sistema de Salud debe garantizar de igual manera la integralidad, confidencialidad, autenticidad de la información de los pacientes, los cuales son los pilares del Sistema General de Salud Colombiano; sin embargo con el crecimiento y avances de la tecnología es difícil medir o cuantificar los problemas de vulnerabilidad que pueden afectar a los Sistemas de Información, adicional a lo dicho anteriormente, el factor humano juega un papel importante en los riesgos del manejo de la información confidencial de los usuarios.

Es importante resaltar que el 90% de la operación médica es tercerizada, esto provoca que los ciber delincuentes vean un factible hueco para ingresar y de esta manera estafas a esos terceros con información falsa.

Los ciber delincuentes pueden crear una identidad falsa completa y operar con ella o estafar a las aseguradoras gracias a esos datos. Por ejemplo, pueden aprovechar esa identidad para adquirir medicamentos y venderlos posteriormente en la 'deep web'[2]. Por otra parte, hay que tener en cuenta la gravedad de que se sustraigan datos especialmente sensibles para los pacientes, como por ejemplo: conocer información irreevante no es tan problemático como conocer el tipo de sangre o algunos inconvenientes de salud saber dónde vive no es lo mismo que conocer el grupo sanguíneo o alergias de una persona.[3]

Con esta monografía se busca presentar una investigación sobre la vulnerabilidades que se pueden generar en el manejo de la información a través de las historias clínicas digitales; teniendo en cuenta que estos problemas de vulnerabilidades pueden

[2] Deep web o Web profunda es el contenido de internet que no está indexado y donde los buscadores no pueden acceder es básicamente la parte de internet a la que solo accedes si conoces donde se encuentra ubicada la información esta es empleada entre otros para transacciones ilegales u ocultar información. Tomado de vhttps://blogthinkbig.com/que-es-la-deep-web

[3] Tomado de http://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-seguridad_informatica-ciberataques-datos-privacidad_0_427657312.html

presentarse en su gran mayoría por parte de los funcionarios y de esta manera la incidencia en los descuidos de estos, permitiendo así el acceso a la información por parte de terceros con propósitos maliciosos; es por eso que se dará a conocer una investigación legislativa previa que permita tener claridad de los procesos de acuerdo a la ley a nivel nacional e internacional; por otro lado se realizaran acercamientos a los usuarios finales por medio de métodos de investigación que nos permitan conocer la percepción de las personas implicadas en el proceso, aplicando una metodología ambiciosa de encuesta por internet, se espera abarcar un gran número de trabajadores de salud de diversas ciudades ubicadas en los departamentos de Cundinamarca, Bolivar, Tolima, Atlantico, Boyaca y Bogotá, con el resultado de este muestreo esperamos obtener resultados objetivos de percepción y actitudes por parte de los funcionarios al igual que información sobre las herramientas informáticas o aplicativos con los cuales se protege la información de las historias clínicas.

Justificación

Con los avances tecnológicos que han llevado a sistematizar los diferentes sectores financieros, gubernamentales, bancarios, etc. a nivel internacional y por ende nacional, nuestro país debe entrar en el marco de sistematizar la información del Sistema de Salud, un tema de por si complejo por los actores involucrados IPS, EPS, Entes Territoriales, Entidades Públicas y Privadas, Registraduría, Ministerio de Hacienda, entre otros.

Sin embargo, uno de los actores implicados en este sistema es, el personal de Salud, quien son al final los que acceden, modifican, y consultan la información de las historias clínicas de los pacientes de las EPS, por tanto, su conocimiento sobre la vulnerabilidad del sistema de información, la responsabilidad del manejo de la información, la custodia y calidad de la información ingresada, etc. son aspectos que se deben tener en cuenta para identificar el grado de conocimiento del personal de Salud en dicha problemática, por tanto en el desarrollo de esta monografía se espera observar los aspectos jurídicos que apoyan esta práctica, a la vez que mediante la aplicación de una encuesta al personal de salud de diversas Clínicas y Hospitales lograr cuantificar y calificar la perspectiva de ellos como los partícipes de este sistema.

Objetivos

Objetivo General

Analizar, de acuerdo a la investigación realizada el factor de riesgo que generan los trabajadores de salud en la vulnerabilidad de las historias clínicas digitales.

Objetivos Específicos

- Investigar sobre los componentes jurídicos que intervienen en la protección de las historias clínicas.

- Analizar los estudios realizados sobre vulnerabilidad de historias clínicas y su aplicabilidad en nuestro sistema de salud.

- Plantear la necesidad de crear un protocolo de seguridad de historias clínicas digitales con base a los estudios realizados a nivel internacional.

Contenido

1. Hipótesis

La vulnerabilidad de las historias clínicas digitales se ve incrementada por diversos factores de riesgo, entre los más distinguibles se encuentra el generado por descuidos de los funcionarios del sistema de salud sean estos intencionales o no intencionales.

2. Resultados esperados

Investigar los avances jurídicos que existen en nuestro país que protegen la información de los pacientes en la inclusión de historias clínicas digitales.

Aplicar una encuesta digital para concretar la perspectiva de los trabajadores del sector salud frente a la responsabilidad como actores del sistema frente a la vulnerabilidad de las historias clínicas digitales.

3. Marco Referencial

La historia clínica es un documento con reserva, que para efectos legales, debe existir con los hechos de confiabilidad, respeto, idoneidad y ética, por parte de todos los actores quienes participan en la elaboración de esta, desde el paciente hasta el personal administrativo de las IPS, y resaltar que sirve como un hecho probatorio, para cualquier requerimiento legal y de prestación

3.1. Marco Conceptual

Concepto	**Definición**

Seguridad de la Información	La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma, consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización. El Sistema de Gestión de Seguridad de la Información ISO 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada. Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.[4]
Sistema de Salud	Un sistema de salud es la suma de todas las organizaciones, instituciones y recursos cuyo objetivo principal consiste en mejorar la salud. Un

[4] Tomado de (Rondon & Eslava, 2014)

<table>
<tr><td></td><td>sistema de salud necesita personal, financiación, información, suministros, transportes y comunicaciones, así como una orientación y una dirección generales. Además tiene que proporcionar buenos tratamientos y servicios que respondan a las necesidades de la población y sean justos desde el punto de vista financiero.</td></tr>
<tr><td>Tipos de Vulnerabilidad Informática</td><td>De acuerdo a la Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria, existen 5 tipos de clases de amenazas para la seguridad:
Divulgación accidental
Empleado curioso
Violación de la privacidad de los datos por un trabajador
Violación de la privacidad de datos por un externo con intrusión fisica
Intrusión no autorizada en la red del sistema
<table><tr><td>Nivel</td><td>Clasificación de amenazas</td></tr><tr><td>1</td><td>Divulgación accidental (accidental disclousure). El trabajador sanitario, sin querer, revela información del paciente a otros. Por ejemplo, mensaje de correo electrónico enviado a la dirección incorrecta.</td></tr><tr><td>2</td><td>Empleado curioso. Un trabajador con privilegios de acceso a los datos de un paciente accede a ellos por curiosidad o ara sus propios fines.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>Por ejemplo, un profesional sanitario que accede a la información de salud de un compañero de trabajo</td></tr>
<tr><td>3</td><td>Violación de la privacidad de los datos por un trabajador. Miembro del personal que tiene acceso a la información de un paciente la transmite al exterior con ánimo de lucro o por algún tipio de animadversión hacia un paciente</td></tr>
<tr><td>4</td><td>Violación de la privacidad de datos por un externo con intrusión física. Un externo que entra en la instalación física y de manera forzada accede al sistema</td></tr>
<tr><td>5</td><td>Intrusión no autorizada en la red del sistema. Un externo, ex empleado, paciente o hacker que se introduce en la red del sistema de la organización desde el exterior y accede a la información del paciente o hace que el sistema deje de funcionar (ataque a la disponibilidad)</td></tr>
</table>
Tabla 1 Clasificación de las amenazas que pueden producir un problema de seguridad en la organización[5]
</td></tr>
<tr><td>Consecuencias de Amenazas de Seguridad</td><td>Las amenazas son acontecimientos que pueden desencadenar un incidente en el centro de AP, produciendo impactos materiales o inmateriales en</td></tr>
</table>

[5] Tomado de (Nacional, Seguridad, De Términos, & Abreviaturas, 2011)

	los recursos del sistema de información o relacionados con este, necesarios para que el centro funcione correctamente.[6] Determina estas amenazas en Daños de Imagen: Los usuarios pierden credibilidad sobre la entidad de Salud Consecuencias legales: Sanciones Económicas y legales contra el establecimiento de salud y el personal de salud. Otras consecuencias: Las afectaciones de la pérdida de información confidencial sobre el paciente.
Confidencialidad:	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.[7]
Gestión de incidentes	Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas
Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

[6] Tomado de (MinisterioSalud, 1999)

[7] Tomado de (MinisterioSalud, 1999)

Incidente de seguridad	Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
Medidas de Seguridad	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación
Política de Seguridad	Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que se consideran críticos.
Proceso	Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado
Seguridad de la información	Es la protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de proporcionar confidencialidad, integridad y disponibilidad.
Servicio	Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades del paciente.
Sistema de Gestión de la Seguridad de la Información	Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y

	mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
Historia clínica	Según el artículo 1 de la resolución 1995 de 1999 la Historia Clínica "es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley[8].
EHR	Electronic Health Record o registro electrónico de salud, estos sistemas están diseñados para almacenar datos con precisión y registrar la información del paciente a través del tiempo.

3.2. Metodología

Hasta el momento las investigaciones teóricas sobre el problema planteado permiten vislumbrar los avances legislativos en nuestro país frente al tema de vulnerabilidad de historias clínicas sin embargo no existen investigaciones que trabajen sobre estas vulnerabilidades directa o parcialmente al igual que la negligencia en la protección de la información por parte del personal en salud, por ese motivo se presentara un análisis de los efectos de vulnerabilidad causados por el personal del sistema de salud.

[8] Tomado de Resolución 1995 (MinisterioSalud, 1999)

3.3. Marco Jurídico

La Resolución 1999 del 8 de julio de 1995, por la cual se establecen las normas básicas para el manejo de la historia clínica en su artículo tercero, nos refiere las siguientes características:

- Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionado con sus dimensiones personal, familiar y comunitaria.
- Secuencialidad: Los registros de la prestación de los servicios en salud deben consignarse en la secuencia cronológica en que ocurrió la atención. Desde el punto de vista archivístico la historia clínica es un expediente que de manera cronológica debe acumular documentos relativos a la prestación de servicios de salud brindados al usuario.
- Racionalidad científica: Para los efectos de la presente resolución, es la aplicación de criterios científicos en el diligenciamiento y registro de las acciones en salud brindadas a un usuario, de modo que evidencie en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo.
- Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.
- Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.[9]

[9] Tomado de Resolución 1995 (DocSlide, n.d.)

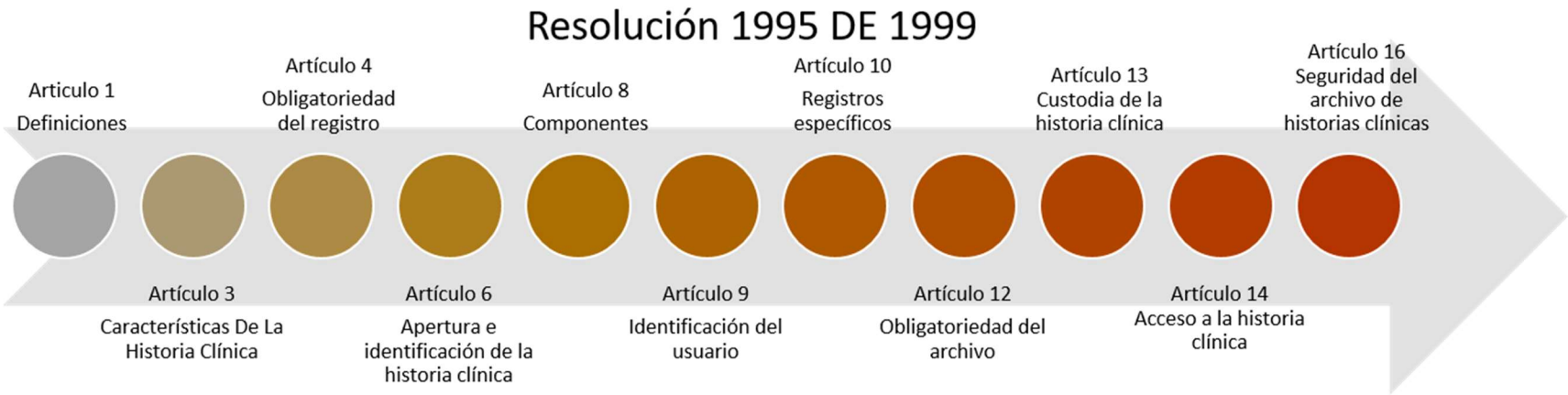

Ilustración 1 Resolución 1995 de 1999

Ver anexo 2 Resolución 1995 de 1999

4. Tipo de Investigación

Al realizar una verificación en diversas fuentes biográficas acerca de los diferentes tipos de investigación, como son la investigación Exploratoria, Descriptiva, Correlacional y Explicativa; teniendo en cuenta factores como la complejidad del tema elegido, los objetivos propuestos y la hipótesis planteada para esta monografía, el tipo de investigación que he seleccionado es *la investigación Cualitativa* ya que brindará las herramientas necesarias para poder dar respuesta a la hipótesis. *La vulnerabilidad de las historias clínicas digitales incrementa por factores de riesgo generados por descuidos intencionales o no intencionales de los trabajadores del sistema de salud*; ya que por sus características este tipo de investigación van más allá que otro tipo de investigaciones como lo son la descriptiva y correlacional, la investigación cualitativa es eminentemente inductiva y el análisis de datos surge principalmente del análisis de diarios personales, observaciones, estudio de transcripciones de revistas, lecturas informativas y criterios personales.

Una vez definidos cuales son los resultados que se esperan obtener de este proyecto investigativo, la herramienta que nos brinda mayor validez y confiabilidad a la hora de recoger la información requerida es el cuestionario, elaborado con base en toda la información previamente recolectada sobre la problemática seleccionada, el cual incluirá preguntas cerradas y abiertas, los cuales son fáciles de contestar, brindando un ítem evaluador, con preguntas neutrales, no directas, estableciendo el orden adecuado de las mismas dentro del cuestionario, y a su vez permiten recoger la información necesaria para poder medir cuantitativamente los resultados y así alcanzar los objetivos propuestos.

Recolección y organización de datos (Aplicación de encuestas)

Se realiza un proceso de encuestas aleatorias, para medir cuantitativamente la percepción del tema abordado durante esta investigación por el personal de salud y validar con esta información la apreciación del tema en los involucrados; aprovechando

la herramienta de internet se compartirá el enlace con diferentes personas a nivel nacional, cuyo requisito indispensable es ser actores-trabajadores en el sistema de salud, se proyecta realizar la encuesta alrededor de 200 personas de diferentes ciudades y diferentes participaciones en el sistema.

La elaboración del proyecto educativo “Vulnerabilidad de seguridad informática en las historias clínicas de los pacientes del servicio de salud” va a permitir favorecer la adquisición de conocimientos habilidades y valores en el proceso de aprendizaje para la protección de datos clínicos y favorecer por ley el derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada; esta información de tipo sensible.

Capítulo 1: Factores de la Historia Clínica Digital

En la actualidad y con los avances tecnológicos se hace necesaria una globalización de la información médica de los pacientes, lo que permitirá a un futuro una mejor disponibilidad de la información ofreciendo al paciente, un nuevo enfoque para su atención; esto implica que la historia clínica debe dejar de ser una relación médico-paciente para convertirse en un sistema virtual de información clínica, y que mejor herramienta para el desarrollo de las historias clínicas digitales que la Tecnologías de la Información y la Comunicación (TIC).

De acuerdo a una encuesta aplicada por la empresa DriCloud en el año 2015 todavía aproximadamente el 45% de las clínicas en España y Latinoamérica continúan utilizando el papel; el otro 50% utilizan una historia clínica electrónica anticuada o almacenan la información en programas como el Excel o Word que no cumplen con la legislación y solo el 5% trabaja desde la Nube, con sistemas protegidos de virus, borrado o pérdida de datos médicos de forma accidental[10].

Colombia ha ido mejorando su legislación y la unificación de procesos de información, teniendo en cuenta la necesidad de los avances tecnológicos en el año 2007 mediante el Decreto 4747 y la Resolución 3047 de 2008 emanada por el Ministerio de Protección Social, se definieron los formatos, mecanismos de envío, procedimientos y términos a ser implementados en las relaciones entre prestadores de servicios de salud y entidades responsables del pago de servicios de salud, mediante estos anexos técnicos los diferentes actores del sistema (EPS, IPS, Entes Territoriales, y los diversos Régimes) realizaran los reportes de los servicios en salud requeridos por los usuarios, esto obligo a todos los actores a hablar el mismo idioma y aunque no trabajan con el mismo sistema

[10] Tomado de https://dricloud.com/historia-clinica-digital/# 22 de Enero de 2018

de información, el formato de reporte es único para cada evento o proceso dentro del sistema.

De igual manera se avanzó exponencialmente al unificar las bases de datos de los Regímenes Contributivo, Subsidiado, de Excepción y Especial, esto mediante la plataforma de Fosyga donde se encuentra centralizado el flujo de dineros de la nación para la atención en salud de la población Colombiana; esto teniendo en cuenta que anteriormente al año 2012 las bases de datos se manejaban de manera individual y localmente entre municipio y departamentos, sin ninguna clase de verificación lo que provocaba duplicidades y mala identificación de los afiliados, y aunque este contexto se sale del tema de las historias clínicas digitales, permite brindar una conceptualización frente a los avances que enfrenta y realiza Colombia frente a la seguridad de la información en salud.

Por tanto es importante aclarar que la seguridad de la información en el ámbito de la salud es el conjunto de diferentes medidas tanto administrativas, organizativas, físicas, técnicas, legales y educativas encaminadas a proteger la información, al paciente y al personal de salud esto frente a las diversas situaciones que se pueden presentar de acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas; lo anterior con el fin de proporcionar y garantizar la ejecución de los 3 pilares básicos de los sistemas de salud y establecidos en nuestra Constitución los cuales son Confidencialidad, Integridad y Disponibilidad De La Misma.[11]

La confidencialidad; según el diccionario de la Real Academia Española lo define como “Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas”[12] en el caso de las Historias Clínicas y el Sector Salud hace referencia al proceso que asegura la privacidad de la información, para que sea accesible solo por los

[11] Tomado de Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria

[12] Tomado de http://www.rae.es/ 25 de Enero de 2018.

actores del sistema de acuerdo a lo establecido en la normatividad vigente y dicha información solo se puede emplear para el destino o solicitud requerido; es importante destacar que esto se encuentra inmerso dentro del Juramento de Hipócrates y el Código de Ética que presenta el personal de Salud a nivel Nacional.

La integridad, El diccionario de la Real Academia Española de la lengua lo define como “Cualidad de Integro”, para nuestro caso refiere a la obligación de garantizar la exactitud de la información y la protección de la misma, evitando que sea modificada o alterada por cualquier otra persona, esto brinda a los pacientes tranquilidad al garantizarles que la información médica no ha sido modificada y por tanto no existe riesgo de errores médicos o perdida de información.

En cuanto a la disponibilidad, El diccionario de la Real Academia Española de la lengua lo define como “La cualidad o condición de Integro” frente a las Historias Clínicas hace referencia o aplicabilidad en la garantía de proporcionar la información solo al personal autorizado, esto cae en responsabilidad en nuestro país sobre las IPS quienes son las encargadas de velar por la seguridad de la información registrada en sus bases de datos, la cual debe ser posible acceder en momentos críticos o de atención médica.

Al garantizar la ejecución de estas actividades Colombia seguirá haciendo grandes avances frente al movimiento de historias clínicas digitales tal como lo han realizado los países de Estados Unidos, España, México y Uruguay, por citar algunos ejemplos.

Capítulo 2: Importancia sobre la seguridad de las contraseñas en el ámbito laboral

La idea de contraseña fue introducida a la informática modera por el Ingeniero Fernando Corbató [13]quien trabajaba en MIT en el año 1960 y vio la necesidad de limitar el acceso a la información dentro de una misma computadora que compartía con otros investigadores, esto les permitiría proteger la información registrada permitiendo el acceso solo a sus propios archivos.

En la actualidad necesitamos contraseña para prácticamente todo, con el fin de garantizar la seguridad de nuestra información, estas contraseñas las empleamos en la actualidad para proteger diversos accesos como por ejemplo el inicio de sesión de Windows de nuestro pc en el hogar y en el trabajo, cuentas de correo electrónico y de Facebook, Twitter, Skype, Spotify, Netflix y otras redes, Sistemas Operativos, cuentas de televisión por cable, compras online, acceso a dispositivos móviles, y sus aplicaciones, software y aplicativos, por mencionar algunas.

Con tanta información virtual que debemos manejar y proteger día tras día, es casi imposible emplear distintas contraseñas, sin importar cuantas medidas de seguridad, recomendaciones y técnicas existentes, los usuarios emplean el mismo tipo de contraseña ya sean números determinados, fechas especiales, eventos, nombres familiares o de mascotas, con esta información se pretende salvaguardar toda la información, esto sin importar lo contraproducente que puede ser, ya que al emplear una contraseña para toda la información virtual y esta contraseña se rompe es decir es vulnerada esto permite el acceso a toda la información del usuario; a esto debemos aunar que también existen obstáculos que permiten recordar las contraseñas ya que algunos usuarios emplean contraseñas complejas, extensas, o compuestas de símbolos y letras

[13] Tomado de https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/ (Anonymus, 2017)

y que con su uso infrecuente no permite que la contraseña sea efectiva para la protección de la información.

Un reportaje realizado por la BBC en Reino Unido señala que una persona utiliza un promedio de 26 cuentas con clave de acceso, mientras que las contraseñas que utiliza para protegerlas son apenas seis, lo que incrementa las posibilidades de que sean hackeadas.[14]

Frente a la problemática establecida en esta investigación encontramos que los aplicativos y computadores en el servicio de salud y a cargo de los funcionarios se encuentran protegidos por contraseñas que tienen medidas de seguridad de cifrado y creación; sin embargo no se ha prestado atención a la necesidad de capacitación al personal de salud en prácticas de seguridad informática, es así como en el artículo Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario[15] presenta un estudio realizado en el Hospital General Universitario Reina Sofía de Murcia en el año 2014 donde se buscó índices sobre buenas prácticas de seguridad y privacidad entre personal sanitario, utilizando bases de datos relacionadas con el ámbito de la salud y la seguridad informática, de los 205 profesionales consultados, 180 accedieron a participar en el estudio. La edad media de los participantes fue de 45,2 años (desviación estándar: 8,9)[16].

Se presenta a continuación, la tabla con los hallazgos de este estudio:

[14] Tomado de http://www.semana.com/vida-moderna/articulo/las-contrasenas-de-internet-historia-de-un-fracaso/363975-3 (Tecnologia, 2013)

[15] (Luis Fernández-Alemán et al., 2015 Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario)

[16] Ídem

Características de la muestra	Muestra desglosada según BPS			OR (IC95%) BPS
	N (%)	N (%) BPS	N (%) no BPS	
Edad (años)				
18-30	24 (13,3)	4 (16,7)	20 (83,3)	0,70 (0,20-2,44)
31-50	102 (56,7)	20 (19,6)	82 (80,4)	0,85 (0,38-1,91)
51-67	54 (30,0)	12 (22,2)	42 (77,8)	1
Sexo				
Femenino	142 (78,9)	114 (80,3)	28 (19,7)	1,08 (0,44-2,62)
Masculino	38 (21,1)	30 (78,9)	8 (21,1)	1
Nivel de estudios				
Enseñanza obligatoria o inferior	4 (2,2)	1 (25,0)	3 (75,0)	1,11 (0,10-11,68)
Enseñanza secundaria	51 (28,3)	7 (13,7)	44 (86,3)	0,53 (0,19-1,47)
Diplomados universitarios	73 (40,6)	16 (21,9)	57 (78,1)	0,93 (0,40-2,19)
Licenciados universitarios y doctores	52 (28,9)	12 (23,1)	40 (76,9)	1
Ocupación				
Personal de administración	30 (16,7)	5 (16,7)	25 (83,3)	0,62 (0,18-2,10)
Celador	7 (3,9)	2 (28,6)	5 (71,4)	1,24 (0,20-7,55)
Técnico de laboratorio/radiología	11 (6,1)	0 (0,0)	11 (100,0)	0,00 (-)
Enfermero/a	61 (33,8)	14 (23,0)	47 (77,0)	0,92 (0,35-2,41)
Auxiliar de enfermería	34 (18,9)	6 (17,6)	28 (82,4)	0,66 (0,20-2,12)
Médico	37 (20,6)	9 (24,3)	28 (75,7)	1
Experiencia en el puesto actual (años)				
>25	15 (8,3)	4 (26,7)	11 (73,3)	1,14 (0,31-4,16)
21-25	18 (10,0)	4 (22,2)	14 (77,8)	0,89 (0,25-3,17)
16-20	21 (11,7)	7 (33,3)	14 (66,7)	1,57 (0,52-4,66)
11-15	19 (10,6)	2 (10,5)	17 (89,5)	0,37 (0,07-1,80)
6-10	49 (27,2)	5 (10,2)	44 (89,8)	0,35 (0,11-1,07)
0-5	58 (32,2)	14 (24,1)	44 (75,9)	1
Experiencia en otro puesto del sector sanitario (años)				
>25	8 (4,5)	2 (25,0)	6 (75,0)	1,51 (0,28-8,13)
21-25	9 (5,0)	2 (22,2)	7 (77,8)	1,29 (0,24-6,78)
16-20	21 (11,7)	5 (23,8)	16 (76,2)	1,41 (0,45-4,39)
11-15	24 (13,3)	6 (25,0)	18 (75,0)	1,51 (0,52-4,37)
6-10	24 (13,3)	4 (16,7)	20 (83,3)	0,90 (0,27-2,99)
0-5	94 (52,2)	17 (18,1)	77 (81,9)	1

OR: *odds ratio;* IC95%: intervalo de confianza del 95%; BPS: buenas prácticas de seguridad.

Ilustración 2 Características de la muestra y porcentaje de participantes con buenas prácticas de seguridad según las variables sociodemográficas.[17]

[17] Ídem

Como podemos evidenciar en los resultados presentados, el mayor porcentaje de funcionarios que no tienen buenas prácticas de seguridad son aquellos con menor experiencia dentro del sistema de salud, por ende, podemos inferir que dentro de la formación del personal de salud se debe contemplar la necesidad de adiestramiento en el dominio de seguridad de contraseñas, ya que la mayoría emplean nombres de personas, fechas especiales, o datos personales, sin emplear caracteres especiales o números, permitiendo descifrar fácilmente sus contraseñas y dejando vulnerable la información de los pacientes.

Entre las técnicas que encontramos para establecer contraseñas con mayor seguridad es crear contraseñas criptográficas, esto se logra por medio de una cadena de caracteres que transforman una frase normal en un código, se logra manualmente al establecer una frase de uso privado tomando la primera letra y agregando caracteres, símbolos, números y alternando Mayúsculas y minúsculas, por ejemplo: *Have a nice day* se puede tomar la primera letra de cada palabra e intercalar caracteres o números en determinado orden es decir se puede cambiar a **h**2**A**(**n**$**D**7 o **H**1**a**@**n**%**D**8 y así sucesivamente, creando una clave única, sin embargo aún tenemos la problemática de que necesitamos manejar más de 26 contraseñas únicas teniendo en cuenta que en promedio manejamos diversos accesos de cuentas personales, datos bancarios, software estudiantil, y software laboral.

Es importante establecer que las amenazas informáticas pueden provocar diversos incidentes amenazando todos los elementos que conforman los sistemas de información, sin importar si son causados por la negligencia de los trabajadores de salud, o no, las amenazas surgen a partir de la existencia de vulnerabilidades como por ejemplo la falta de capacitación y concientización en el uso de la tecnología por parte de los trabajadores del sector de salud.

Capítulo 3: Legislación aplicada en seguridad informática para el sistema de salud

Estas son algunas leyes vigentes en Colombia en lo referente a Seguridad de la Información:[18]

Para mayor información verificar anexo 3.

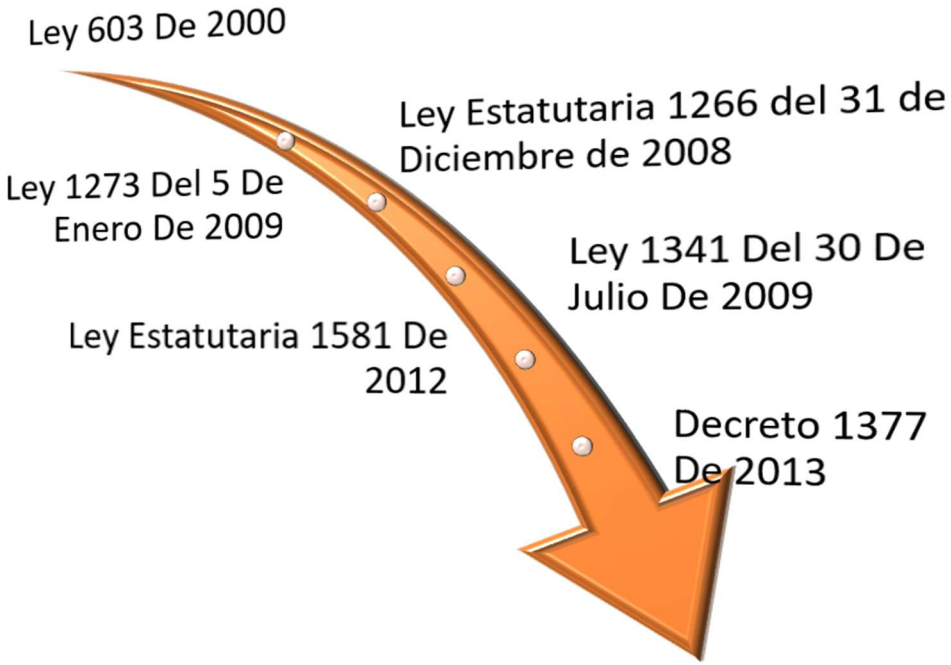

Ilustración 3 Legislación Vigente Historias Clínicas Digitares Colombia

[18] Tomado de https://www.minsalud.gov.co/salud/Documents/Evaluaci%C3%B3n%20de%20Tecnologias%20en%20Salud.pdf (Turriago, De Apoyo, & Reforma De Salud, n.d.)

Capítulo 4: Proposición de Encuesta a los Trabajadores de Salud

Se ha presentado durante esta monografía aspectos sobre las historias clínicas digitales y sus pretensiones a nivel nacional, también una visualización a nivel de la conceptualización de vulnerabilidad en otros países, al igual que la legislación involucrada que soporta los cambios que se deben aplicar y que pueden beneficiar a todos los involucrados dentro del sistema.

Por tanto, para conceptualizar en materia desde el punto de vista de los trabajadores de salud se va a realizar por medio de la web, una encuesta virtual en la cual se expondrán diferentes aspectos sobre la seguridad informática, vulnerabilidad de la información, incidencia y participación del personal de salud; lo cual permitirá evaluar aspectos como conocimientos y percepciones personales a través de la experiencia o educación.

Las preguntas estipuladas dentro de esta encuesta son de carácter social, de conocimientos generales, y de experiencias dentro del ámbito de vulnerabilidad de las historias clínicas, las preguntas que se enviaron a los voluntarios se encuentran en el Anexo 1 de esta monografía.

Capítulo 5: Presentación de Resultados de Encuesta

Se aplicaron un total de 153 encuestas virtuales distribuidas en 22 IPS, así:

1- Nombre del establecimiento de Salud donde trabaja actualmente (Si trabaja en más de uno, debe seleccionar el establecimiento en el cual labora más horas)

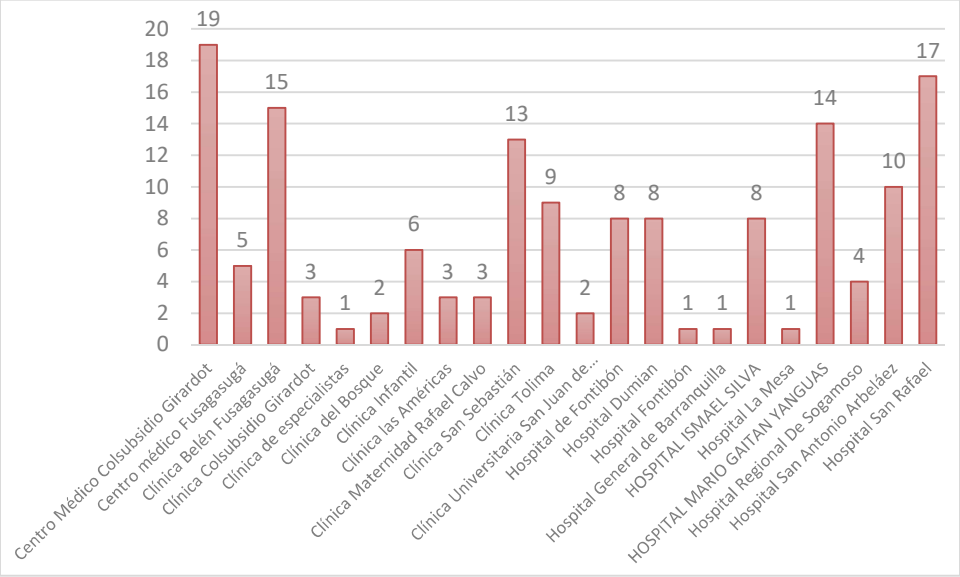

Ilustración 4 IPS aplicadas con la encuesta virtual

La encuesta se aplicó en 22 IPS en 11 municipios de los departamentos de Cundinamarca, Bolivar, Tolima, Atlantico, Boyaca y Bogotá

2- Clase de Entidad

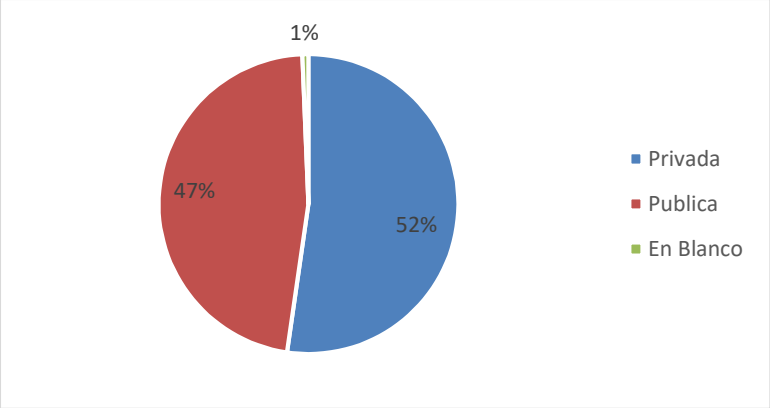

Ilustración 5 Clase de IPS

Aquí se presenta la clasificación del sector al que pertenece la IPS donde laboran los colaboradores que participaron en la encuesta.

3- Edad

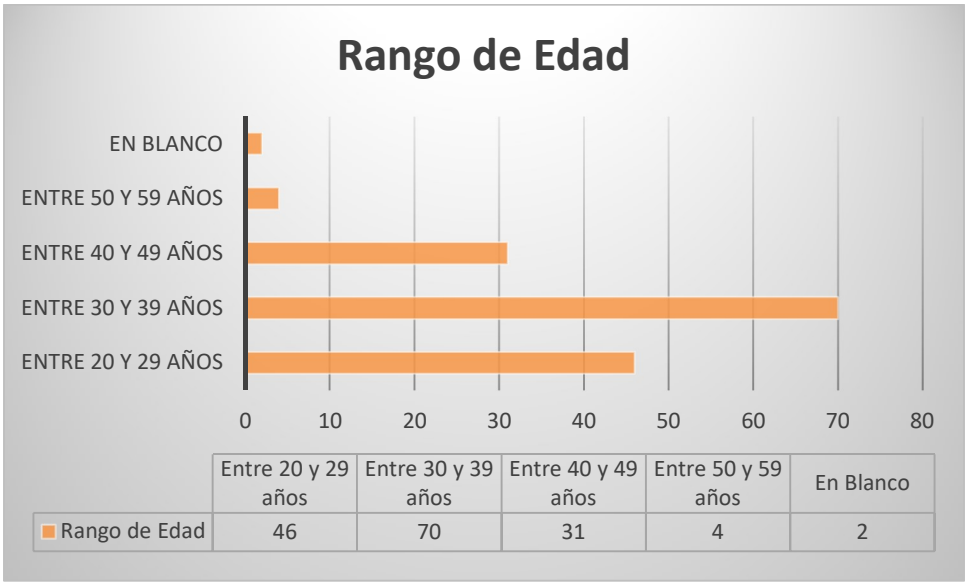

Ilustración 6 Rango de edad

Gran porcentaje de los colaboradores se encuentran en el rango de 30 a 39 años.

4- Cargo que desempeña dentro del establecimiento de Salud

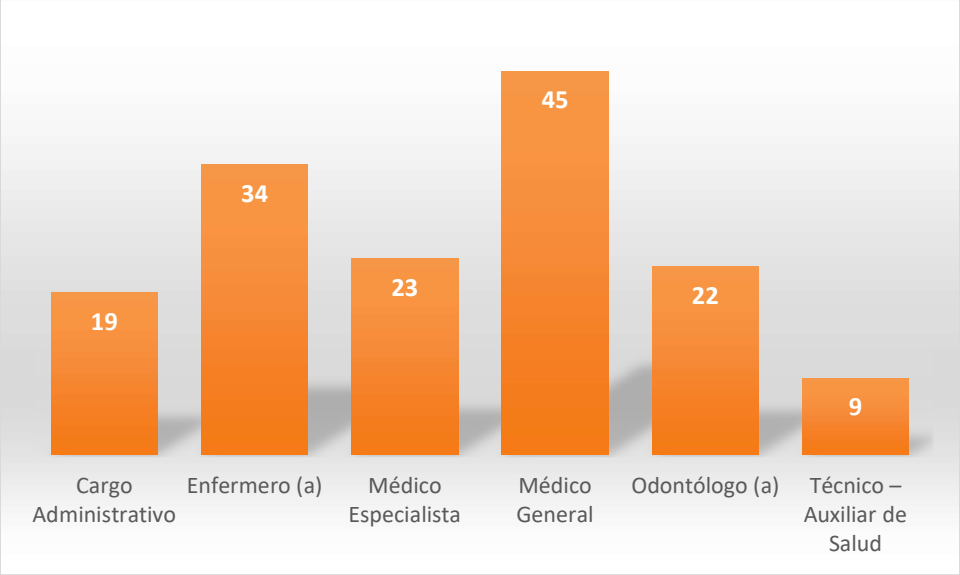

Ilustración 7 Cargo desempeñado dentro de la IPS

El 29.6 % de los encuestados se desempeñan como médicos generales en las IPS donde laboran

5- Para usted la seguridad de información de las Historias Clínicas es

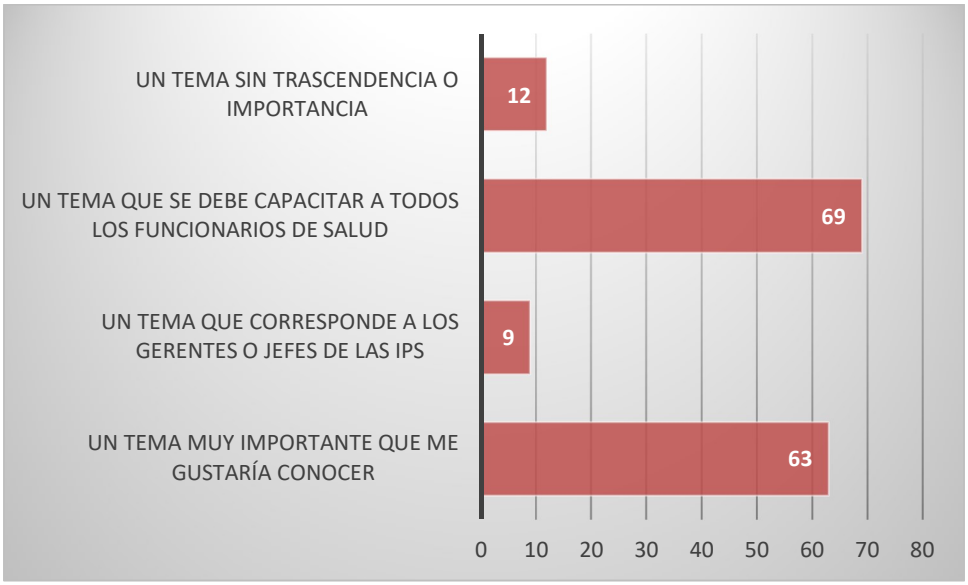

Ilustración 8 Importancia de la seguridad informática

Se logra evidenciar la aceptabilidad del tema por parte del personal de salud

6- ¿Qué sistema de información maneja dentro de su sitio de trabajo?

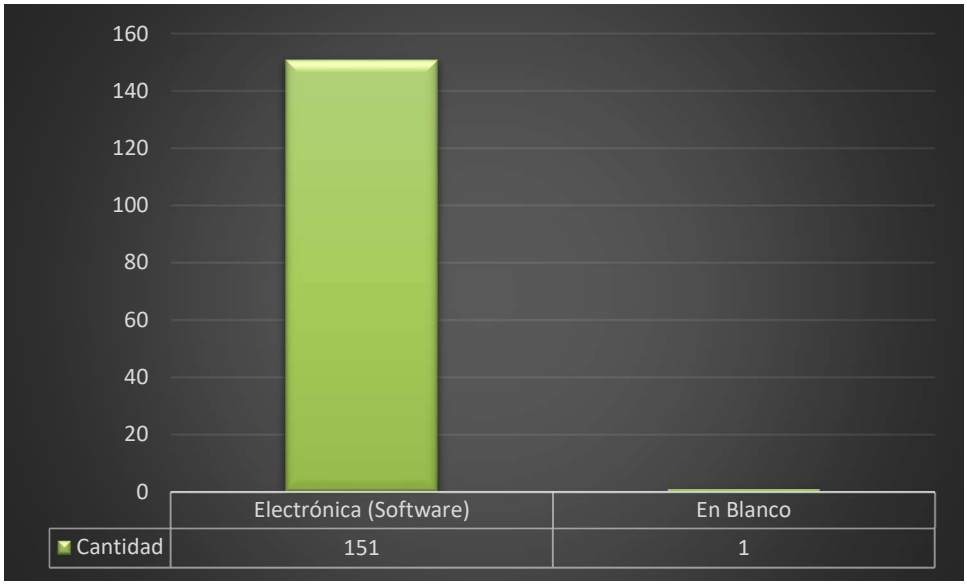

Ilustración 9 Tipo de Sistema de Información que maneja la IPS

El manejo de un sistema de información tipo Software en el 99% de las IPS donde laboran los colaboradores que respondieron la encuesta nos permite evidenciar que sus respuestas serán en base al manejo del tipo de historia clínica digital.

7- ¿Cuántos años tiene de experiencia en el cargo actual?

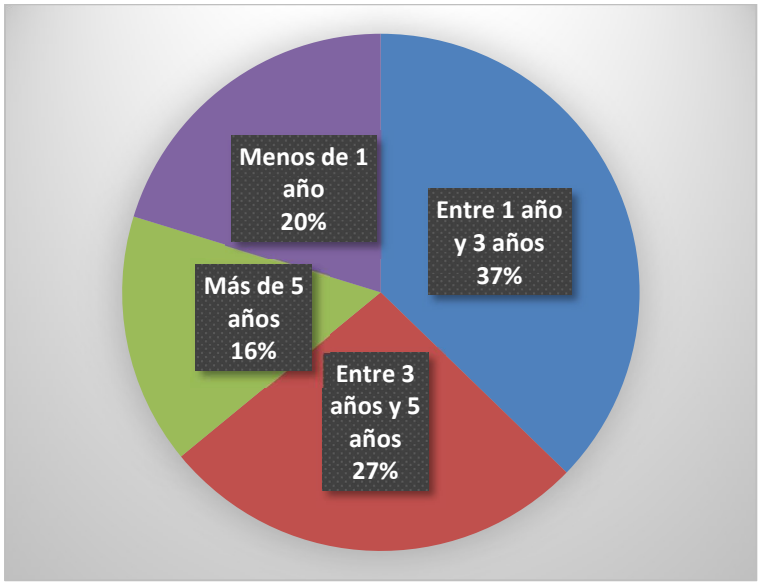

Ilustración 10 Experiencia medida en años en el cargo actual

El mayor porcentaje 37,5% de los colaboradores tienen entre 1 a 3 años de experiencia en el cargo que desempeñan en la actualidad en la IPS

8- ¿Cree usted que el software que utiliza para realizar el proceso de registro de los pacientes es seguro?

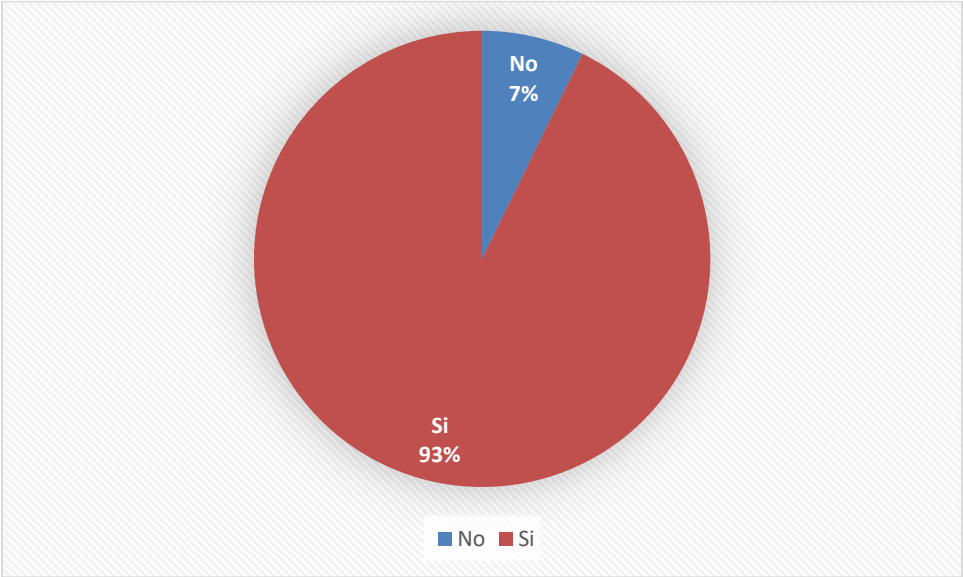

Ilustración 11 Perspectiva de Seguridad frente al Software empleado

De los encuestados 142 opinan que el sistema de Software que emplea la IPS es seguro sin embargo 10 opinan que no ofrece medidas que garanticen la seguridad de la información de los pacientes.

9- Para ingresar al software en donde se maneja las historias clínicas de su IPS. ¿Lo hace con usuario y contraseña personal?

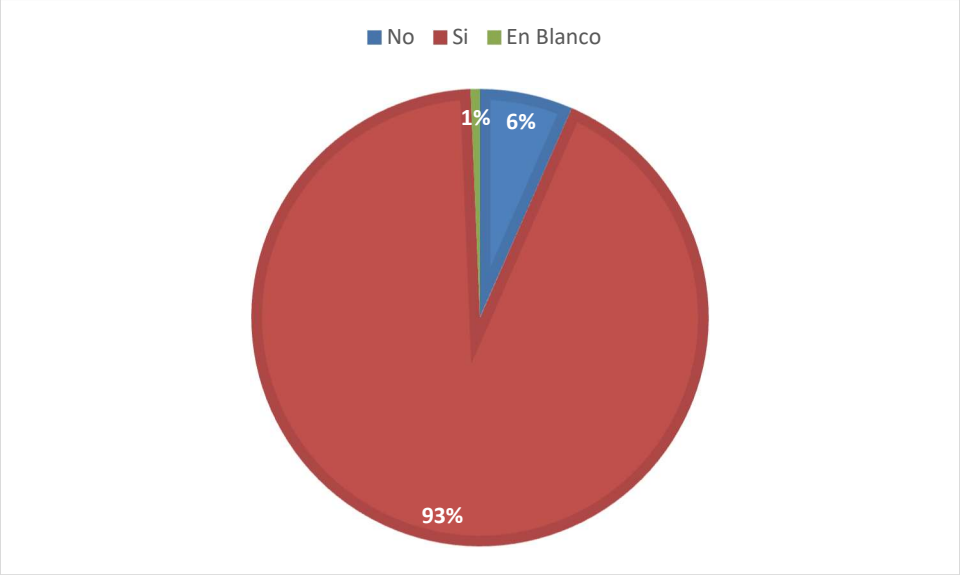

Ilustración 12 Ingreso al sistema con usuario y contraseña

Al igual que en el punto anterior tenemos 142 personas que emplean usuario y contraseña para el ingreso al software y 9 que no emplean ninguna medida seguridad para el ingreso al sistema.

10- ¿Para usted una contraseña es segura cuándo?

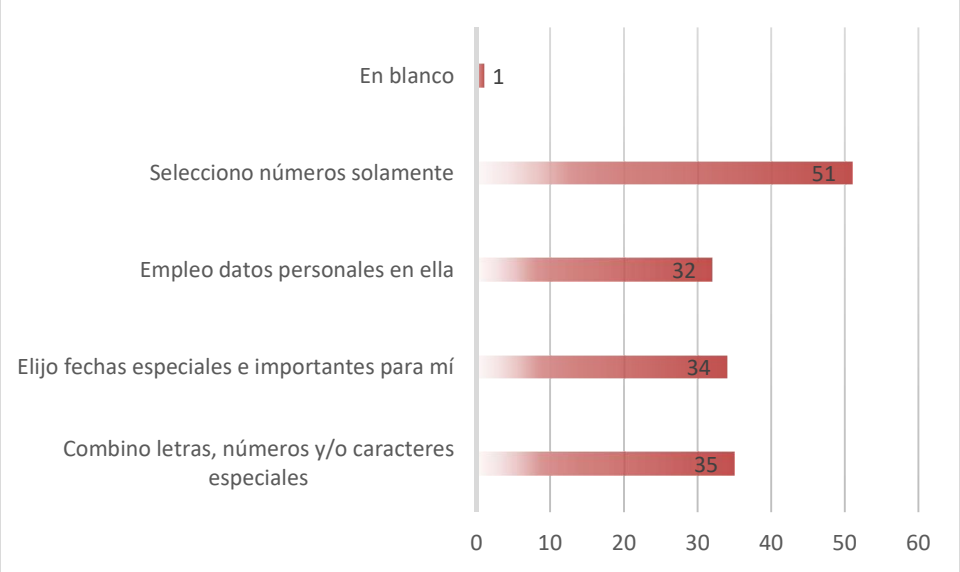

Ilustración 13 Seguridad de contraseña

Esta es una de las gráficas que proporcionan gran valor de información ya que permite vislumbrar la opinión de cada colaborador frente a una contraseña segura.

11- ¿Cree usted que la contraseña que utiliza para el ingreso a la aplicación en donde se maneja las historias clínicas es segura?

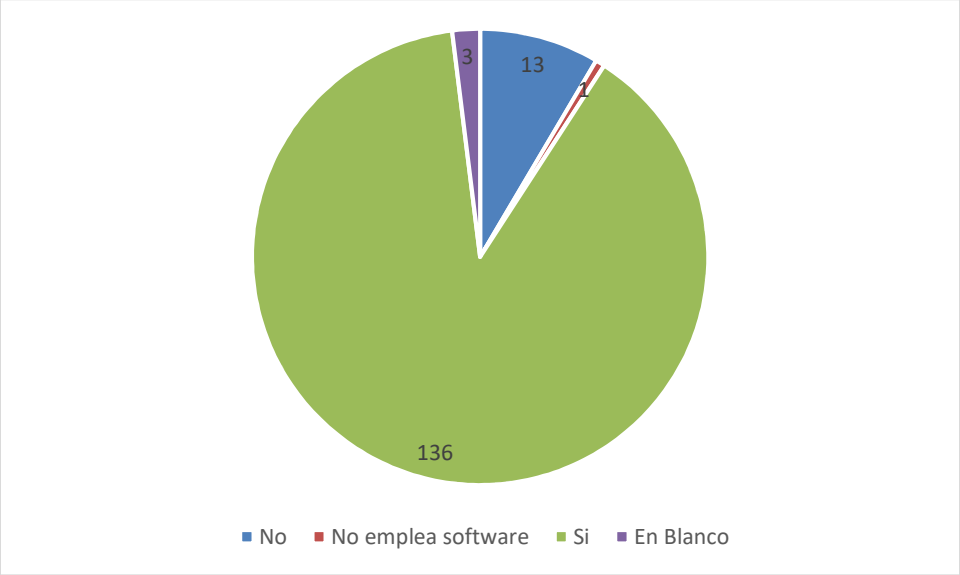

Ilustración 14 Seguridad de Contraseña

Esta grafica ratifica los hallazgos de la pregunta anterior ya que el 89% de los colaboradores concuerdan en que la contraseña que emplean es segura.

12- ¿Cuándo se levanta rápidamente de su lugar de trabajo, siempre bloquea el equipo de cómputo donde se encuentra realizando sus labores diarias?

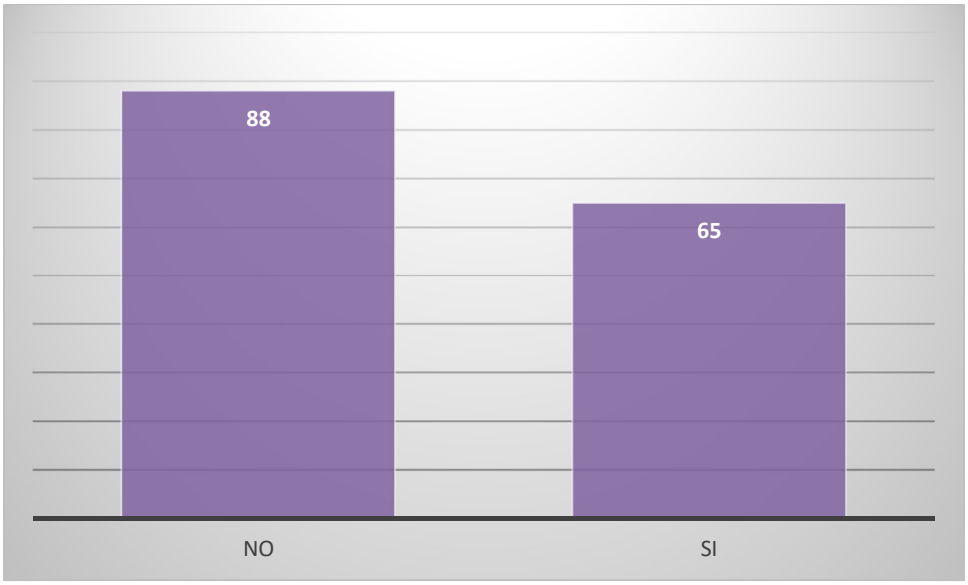

Ilustración 15 Seguridad en el proceso de información en el equipo de Computo

Una de las formas de vulnerabilidad de información es cuando el usuario del equipo de cómputo no bloquea la pantalla permitiendo a terceras personas el ingreso a la información.

13- Si un compañero le sugiere que le preste su usuario y contraseña ¿Usted lo haría?

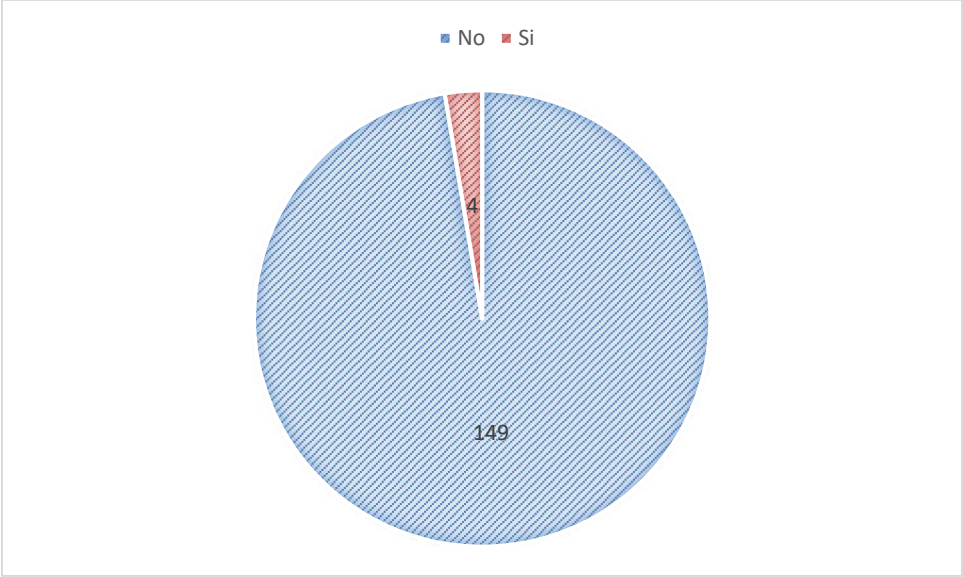

Ilustración 16 Uso personal de usuario y contraseña

Aquí evidenciamos que el 98% de los encuestados consideran que el uso de usuario y contraseña es personal e intransferible.

14- Considera que el usuario y contraseña de los sistemas a los cuales tiene acceso es de uso exclusivo suyo

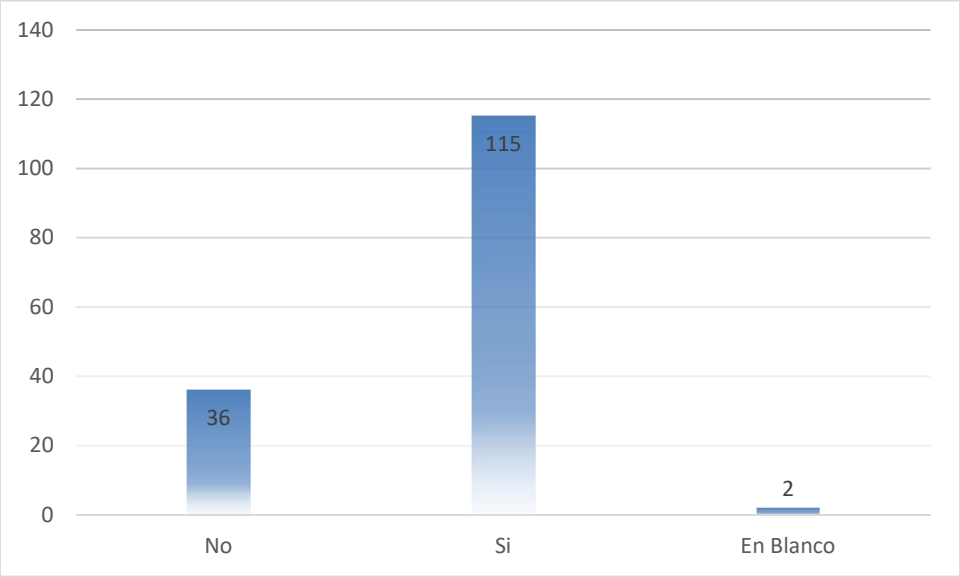

Ilustración 17 Percepción de seguridad en uso de contraseña

El 24% de los encuestados considera que a pesar de tener usuario y contraseña que le permite el ingreso al software este no es garantía de que el ingreso sea exclusivamente del funcionario.

15- La IPS en la que labora promueve un ambiente de seguridad de información por medio de capacitación e información

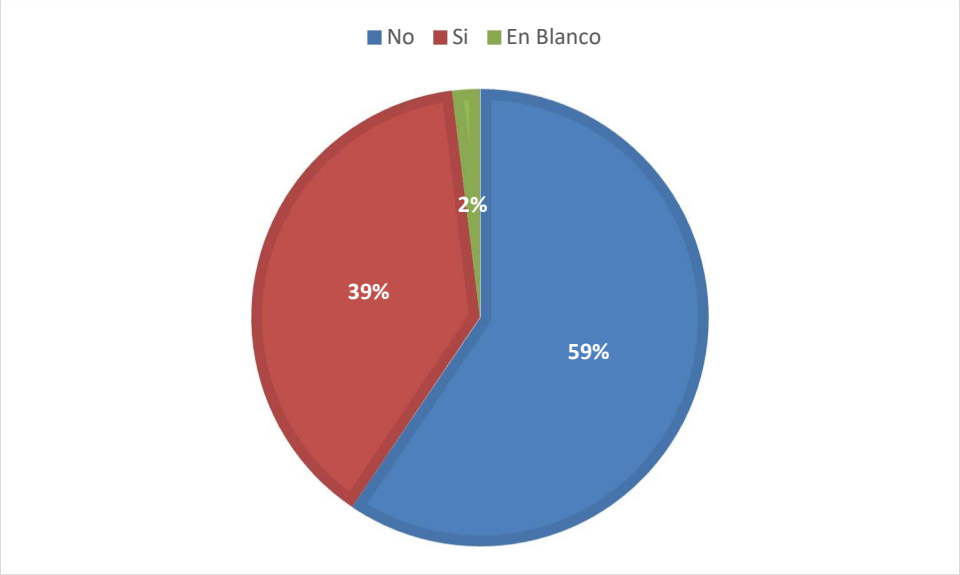

Ilustración 18 Percepción de capacitación sobre seguridad de la Información

Un alto porcentaje de los colaboradores considera que no cuentan con la capacitación sobre seguridad de la información.

16- Si en su IPS no emplean software para el registro de historias clínicas por favor explique brevemente como se realiza el proceso. Si emplea software conteste NO.

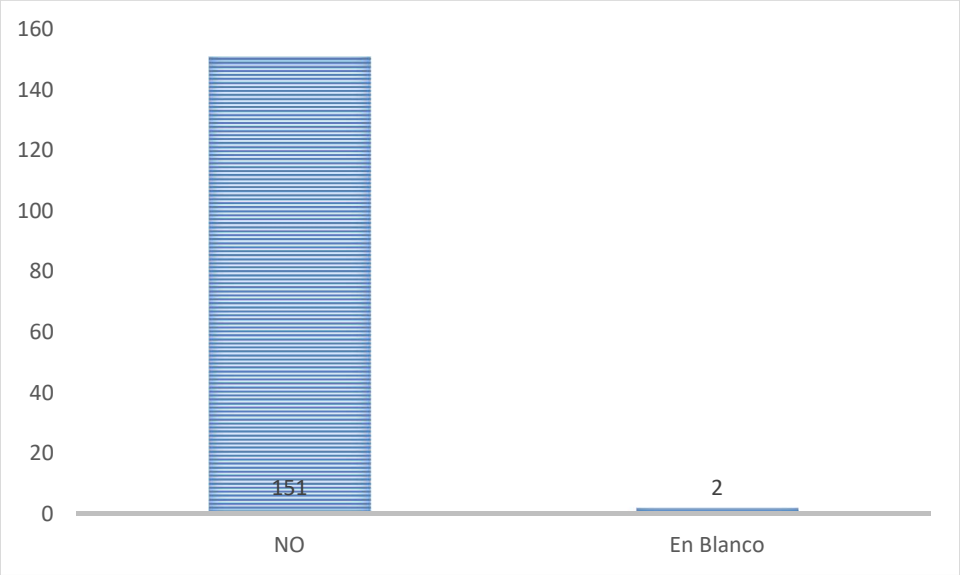

Ilustración 19 Empleo de Software como sistema de ingreso de Historias Clínicas

Se realizó la tabulación de esta pregunta por medio de grafica teniendo en cuenta que no se presentaron respuestas afirmativas para analizar el proceso de historias clínicas físicas.

17- Conoce el protocolo de seguridad de información de la IPS

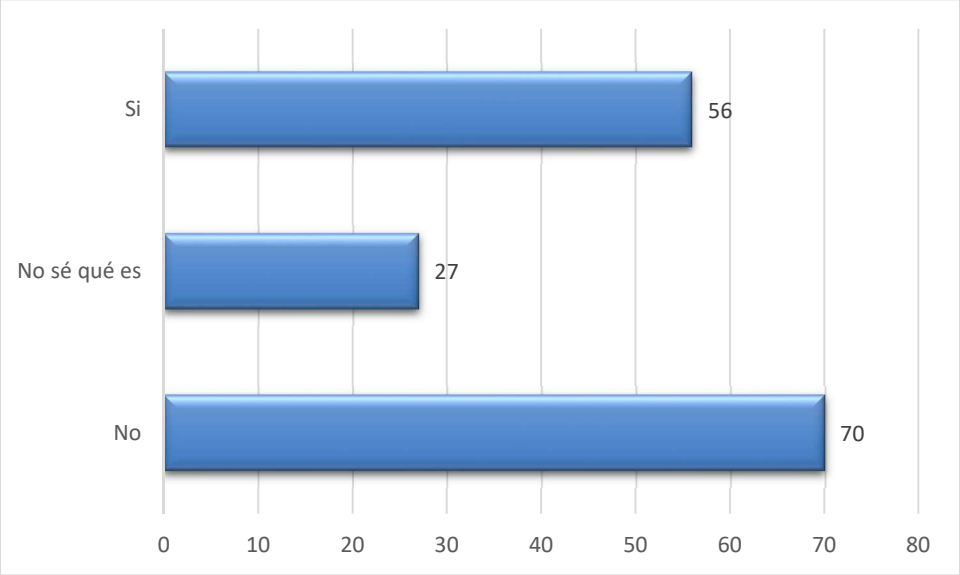

Ilustración 20 Conoce el Protocolo de seguridad de información de la IPS

46% de los encuestados afirman no conocer el protocolo de seguridad que emplea la IPS y el 37% afirma si conocer los protocolos que maneja la IPS.

Capítulo 6: Análisis de Resultados

De acuerdo a los resultados obtenidos, logramos evidenciar que el 86% de los encuestados considera de importancia el conocimiento de la seguridad de las historias clínicas, esto permite establecer el grado de aceptación por parte del personal en salud para capacitaciones, recomendaciones y protocolos de acceso que permitan garantizar la protección de la información.

Frente al sistema de información que manejan las EPS donde laboran el personal de salud encuestadas el 99% informa que maneja Software donde es ingresada la información de la historia clínica de los pacientes; el personal encuestado se encuentra distribuido en personal asistencial y administrativo donde alrededor del 30% de los encuestados son médicos generales, y el ingreso al sistema de información es realizado a través de usuario y contraseña, sin embargo al verificar las respuestas frente a los parámetros empleados encontramos que:

- 33% emplea números
- 20% emplea datos personales
- 22% emplea fechas importantes o especiales

Estas características son fáciles de descubrir por parte de Hackers, la composición y la privacidad de la contraseña s on factores cruciales para mantener la eficacia de este mecanismo como base de protección frente accesos no autorizados al sistema de información sanitario19. En la siguiente tabla se encuentran algunas recomendaciones frente a la creación de contraseñas:

Parámetro	Recomendación
Contraseñas fuertes	Se debe cambiar mínimo cada 90 días

[19] (Sánchez-Henarejos et al., 2014b)

	Debe contener mínimo 8 dígitos Componerla de letras mayúsculas y mi número y algún carácter especial La contraseña no debe contener fechas personales ni información personal La contraseña no debe apuntarse en ningún sitio tampoco se debe almacenar digitalmente o ser enviada por correo electrónico La contraseña debe de ser diferente a las que se emplean en cuentas de carácter personal Las contraseñas no se deben compartir

Con respecto a lo anterior el 88% considera que la contraseña que emplea es segura y el 97% no compartiría la contraseña con otro compañero

De igual manera dentro de la encuesta aplicada se expuso un factor de riesgo y vulnerabilidad cuando se pregunta al usuario que si al levantarse de su lugar de trabajo, siempre bloquea el equipo de cómputo donde se encuentra realizando sus labores diarias, el 57% respondió negativamente, esta situación permite el acceso a personas externas a los sistemas de cómputo y por ende a los sistemas de información creando situaciones de riesgo al acceso no autorizado de la información.

De igual manera dentro del desarrollo de la encuesta era necesario establecer aspectos sobre la empresa (IPS) donde labora el personal de salud, identificando la percepción del colaborador frente a las actividades que desarrolle o no la entidad, promoviendo la seguridad de los sistemas de información, al respecto podemos concluir que el personal de salud considera que no se promueven dichos espacios, sin capacitaciones y sin

conocimiento sobre los protocolos de seguridad se da lugar a posibilidades de errores involuntarios por parte del personal que generen espacios de vulnerabilidad en la información de las historias clínicas.

Capítulo 7: Perspectiva de Ingeniería de Sistemas en la problemática

Debido a que cada vez se dan más delitos en los sistemas informáticos, las medidas de seguridad siguen avanzando, puesto que las compañías **necesitan contar con sistemas altamente protegidos**. Los hackers suelen realizar sus acciones principales en la red, aunque también hay que tener especial cuidado con el software y el hardware, por este motivo, existe seguridad informática para cada uno de estos tres elementos:

- Seguridad online
- Seguridad en software
- Seguridad en hardware

La seguridad para la red

Contar con unas buenas medidas de seguridad en nuestra red es uno de los aspectos que más debemos tener en cuenta, puesto que es en ella donde se suelen dar los mayores hackeos o delitos informáticos. Es decir, seguro que te suenan **los virus, los robos de identidad, las intrusiones ilegales…** todo esto forma parte de los delitos en la red y estos fallos pueden provocar daños muy graves e incluso irreparables. Para ello existen herramientas que nos ayudarán a mejorar la seguridad de nuestra red que son sencillas de utilizar y además ofrecen unos buenos resultados. Nos estamos refiriendo, por ejemplo, a los antivirus, aunque también debemos hacer uso de los programas antispyware. De igual modo, si necesitas una mayor seguridad informática para tu red los cortafuegos o las redes privadas virtuales son también una muy buena solución.

El objetivo de todos estos elementos no es otro que dar la mayor protección a la red en la que trabajamos y así **evitar lo máximo posible la entrada de amenazas** que puedan provocar grandes problemas en el funcionamiento de la misma. Para que estas herramientas sean efectivas, los expertos suelen crear sus propias estrategias de

seguridad, incluyendo en este caso establecer diversos niveles para que así siempre que se esté trabajando a través de la red la seguridad quede intacta.

La innovación, seguridad para el software

Hasta hace muy poco, no se tenía en cuenta el software en relación a la seguridad informática, sin embargo, de forma progresiva este elemento ha adoptado un mayor protagonismo en este sentido, puesto que se ha detectado que los fallos en el mismo **pueden dañar seriamente nuestro sistema** y ser una puerta abierta para los ciberdelincuentes. Las herramientas de seguridad informática de software son relativamente nuevas y se han creado para proteger a este elemento de errores frecuentes que han sido el foco de numerosos problemas. Entre otros podemos hablar de fallos a la hora de implementar el propio software o incluso un pequeño defecto de diseño, cualquier detalle puede ser determinante.

El hardware también necesita seguridad

El hardware es otro elemento que necesita seguridad, por lo que los fabricantes han creado herramientas que ofrecen este servicio, principalmente los cortafuegos y los firewalls de hardware, aunque también hay que decir que cada vez se confía más en los servidores proxy. Lo que hacen estas herramientas es **controlar de forma exhaustiva el tráfico que se produce en la red**, dotando al mismo tiempo al hardware con una seguridad mucho más potente. Así mismo, dentro de este contexto, también hay que destacar los módulos de seguridad de hardware, conocidos como HSM, que se encargan de proteger el cifrado. La seguridad de hardware es una de las más completas, ya que además de todo esto, otra de sus funciones es garantizar que los equipos informáticos no se expongan a grandes riesgos.

Para conocer estos tipos de sistemas de seguridad en el entorno informático es conveniente que los profesionales se formen de una forma exhaustiva y para ello son

recomendables cursos como el máster en seguridad informática o el máster en seguridad empresarial.[20]

7.1 Antecedentes de ataques cibernéticos

Es de aclarar que a pesar de las medidas de seguridad tomados por las entidades esto no exime de la posibilidad de ataques por ciberdelincuentes, por ejemplo, la publicación web del diario español *eldiario.es* del 09/09/2015, presenta tres casos donde entidades de salud estadounidenses fueron afectadas.

Los sistemas informáticos de la sanidad estadounidense están en el punto de mira de los cibercriminales en los últimos tiempos. La compañía UCLA Health ha reconocido ser víctima de un ciberataque: los atacantes habrían podido acceder a los datos personales y médicos de 4,5 millones de pacientes porque no estaban debidamente cifrados. No es la primera vez. Los datos de 80 millones de personas se vieron comprometidos a principios de año por un ataque a la aseguradora de salud Anthem, cuando los ciberdelincuentes consiguieron las credenciales de cinco profesionales con accesos de alto nivel al sistema. Poco después, otra compañía de seguros, Premera Blue Cross, hizo un anuncio similar, con 11 millones de pacientes afectados.[21]

De igual manera en la página web del periódico colombiano *El Tiempo* el 30 de Agosto de 2016 publico que la firma de seguridad Cisco identificó una variante de ramsomware, un tipo de virus que secuestra datos, especialmente enfocados en el área de la salud. Se llama Samsam y es capaz de infiltrarse en los servidores a través de redes, para cifrar las bases de datos de los hospitales, incluyendo la historia clínica de los pacientes, la

[20] Tomado de https://www.obs-edu.com/int/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta 27 de abril 2019

[21] Tomado de https://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-seguridad_informatica-ciberataques-datos-privacidad_0_427657312.html 27 de Abril de 2019

lista de visitantes, etcétera. Para descifrar los datos es necesaria una clave, liberada por los hackers mediante un pago de miles de dólares[22].

[22] Tomado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/historias-clinicas-electronicas-34248
27 de Abril de 2019

Conclusiones

- Los avances legislativos en nuestro país han avanzado exponencialmente frente al tema de protección de información y procesos virtuales; y si bien las historias clínicas cuentan con soporte de seguridad en su parte legislativa, no es nada beneficioso para el usuario (paciente) del sistema de salud ya que una de las grandes fallas es la falta de conocimiento por parte del personal de salud, sobre los temas que regulan y legislan las historias clínicas virtuales en nuestro país, esto permite un aumento los índices de vulnerabilidad y de riesgo de pérdida o mal uso de información.

  Con los resultados obtenidos con la aplicación de la encuesta se observa un claro desconocimiento sobre la importancia del papel que tienen como actores dentro del proceso de seguridad de la información el personal de salud, aunque se evidencia disponibilidad e interés en el tema, la percepción sobre la capacitación del tema por parte de las IPS es negativa lo que genera adicionalmente mayores aspectos por mejorar en estos procesos.

  Sin embargo, se debe considerar que legalmente las IPS están obligadas a garantizar la protección de la información registrada en las historias clínicas, por tanto, sería necesario validar con las IPS los protocolos de seguridad que emplean para la protección de los sistemas de información y más aún como estos protocolos son impartidos o divulgados dentro del personal de salud.

- La norma ISO 27002 establece el protocolo de las buenas prácticas en relación al tratamiento de los riesgos, implantación de controles y garantía de seguridad con las recomendaciones sugeridas para historias clínicas digitales, la norma ISO 27799 proporciona apoyo para la interpretación y aplicación de la ISO 27002, estas dos se complementan con el fin de determinar un conjunto de controles específicos de protección de la seguridad de la información mediante mejores prácticas,

normas como estas se implementan en países como España, donde la historia clínica digital se encuentra unificada para todos los centros de salud, de esta manera el personal de salud ingresa a la historia clínica del paciente sin importar el centro de salud donde es atendido y puede evidenciar todo su historial de atención en salud; la implementación de este modelo permite al personal de salud brindar una mejor, integral y completa atención que el paciente requiere, sin embargo a pesar de los mecanismos legislativos y de capacitación el sistema se ha visto envuelto en situaciones de vulnerabilidad y perdida de información, que han sido generados en parte por la vulnerabilidad propia del sistema (software y hardware) y al igual manera por parte del personal de salud.

- Mirando la situación del Sistema de Salud en Colombia y los avances tecnológicos que permiten mejorar los procesos de accesibilidad, continuidad y permanencia para los pacientes, direcciona a la unificación de la historia clínica virtual en nuestro país, sin embargo, este proceso se debe seguir realizando paso a paso, aprendiendo de los modelos de otros países, como el instaurado en España, donde podemos aprender de sus aciertos y desaciertos, de esta manera se lograra garantizar la privacidad de la información y la veracidad de la misma.

  Teniendo en cuenta que los funcionarios de salud son los que tienen un acceso directo a las historias clínicas para crear, duplicar, modificar, eliminar y guardar, se hace necesario tener protocolo de seguridad que garantice la disminución en los índices de vulnerabilidad que se crean por descuidos, olvidos, distracciones, etc., de los funcionarios de salud, este protocolo debe incluir herramientas tecnológicas (software o hardware) que cierren las aplicaciones o bloqueen los equipos de cómputo en el momento en el que el funcionario de salud se aleja o presente cierta inactividad en el aplicativo para evitar que terceras personas accedan a información privada de los usuarios; otro aspecto que debe incluir el protocolo es la capacitación por parte de los funcionarios de salud sobre legislación que involucre los pros y contras del ejercicio de sus actividades en la vulnerabilidad de las Historias Clínicas.

- Dentro de la guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario de salud[23], documento emitido para el país de España establece algunas recomendaciones que se pueden tener en consideración para aplicar en los sistemas de información en Colombia

  Recomendaciones de uso de certificado digital

  Un certificado digital es un conjunto de datos que permiten la identificación del titular del certificado ante terceros, intercambiar información con otras personas y entidades de manera segura, y firmar electrónicamente los datos que se envían, manteniendo su integridad y conociendo su procedencia. Su uso se está generalizando desde la entrada en vigor del DNI electrónico, y requiere una contraseña que debe ser mantenida bajo las reglas del apartado anterior.

  Recomendaciones de uso del correo electrónico

  Como regla general, nunca se debe utilizar el correo electrónico para intercambiar datos de salud, y si fuera imprescindible, siempre debe hacerse entre cuentas corporativas de la organización de salud, firmando y cifrando los datos trasmitidos utilizando un certificado electrónico, e incluyendo una cláusula de confidencialidad advirtiendo de la naturaleza sensible de la información. Se debe evitar abrir archivos adjuntos o pinchar en enlaces recibidos a través del correo electrónico, aunque procedan de cuentas de personas conocidas. Bajo estos archivos puede haber software malicioso (los troyanos) que acceda, controle y dañe la información del ordenador bajo una apariencia inocua, sin que sea advertido por el profesional sanitario.

  Recomendaciones de uso y acceso a Internet e Intranet

  La visualización de un vídeo, el ingreso en un enlace encontrado en una red social, en una ventana emergente de un anuncio o tras una simple búsqueda on-line, puede poner en peligro la seguridad y la privacidad de los datos sanitarios. Es

[23] Tomado de (Sánchez-Henarejos et al., 2014a)

fundamental que el trabajador esté informado de cuáles son las buenas prácticas de navegación por Internet y siga algunos consejos básicos: disponer de herramientas de seguridad (antivirus, firewall, antispam) actualizadas; realizar análisis con el antivirus periódicamente; no descargar ni ejecutar ningún archivo de sitios desconocidos, pues puede incluir software malicioso; nunca entregar datos personales o circunstancias familiares a desconocidos o en páginas no seguras (que no comiencen por https://); no aceptar contactos desconocidos en redes sociales y mensajería instantánea; nunca pulsar el botón aceptar de una ventana sin leer y entender el mensaje, y finalmente buscar un técnico informático para actualizar y configurar el navegador y el sistema operativo de forma segura.

Recomendaciones de uso de dispositivos extraíbles

Conectar un dispositivo extraíble a un ordenador del centro de AP supone un riesgo alto de entrada de virus a la Intranet del centro. Para evitar infecciones, no se deben conectar dispositivos extraíbles que hayan sido utilizados en otros equipos informáticos. Hay que cifrar con un certificado digital la información que salga del centro, y cuando ya sea desechable, hacer un borrado irreversible con alguna utilidad de borrado seguro. Estas aplicaciones incluyen funciones para limpiar el área de memoria ocupada por los ficheros, con el fin de no dejar rastro de la información generada y almacenada en su ordenador durante su uso (contraseñas, datos personales, etc.).

Recomendaciones de uso de equipos informáticos

La medida más segura para proteger la pantalla de visualización de datos y otros periféricos cuando se ausente, es bloquear el ordenador con una contraseña. Asimismo, hay que borrar los documentos de la memoria de impresoras y fotocopiadoras utilizando las opciones de ajuste y configuración particulares de cada dispositivo. Especial precaución se debe tener al depositar ficheros en directorios o dispositivos compartidos con otros usuarios, de manera que solo accedan a la información usuarios autorizados. En el caso de advertir alguna circunstancia en la que usuarios no autorizados puedan acceder a datos

personales de salud, se debe comunicar inmediatamente al Departamento de Informática del centro de AP.

Recomendaciones de instalación de software

Desconfiar del software disponible en Internet, pues suele contener software malicioso e incluso software espía que pone en riesgo los datos personales de salud. Preferentemente, descargar software procedente de webs oficiales, utilizar un antivirus y siempre consultar antes con un técnico informático. Para disminuir riesgos, evitar la instalación de software no relacionado con el puesto de trabajo en su centro de AP.

Recomendaciones de incidencias de seguridad

Es crucial concienciar a los trabajadores de la necesidad de comunicar los problemas de seguridad en el equipamiento informático del centro de AP, de manera que la organización establezca las medidas correctivas pertinentes para minimizar el impacto de las incidencias de seguridad y subsanar los daños derivados del mismo.

Referencias y Enlaces

(Alventosa-del-Río, 2003; García-Ortega; Cózar-Murillo; Almenara-Barrios, 2004; Jiménez-Pérez, 2001). Informatización de la historia clínica en España. (Spanish). El Profesional De La Información, 19(3), 231-239.

DocSlide. (n.d.). TELEOLOGÍA Y FUNDAMENTOS DE LA INVESTIGACIÓN JURÍDICA - Documents. Retrieved November 30, 2017, from https://docslide.net/documents/teleologia-y-fundamentos-de-la-investigacion-juridica.html

Luis Fernández-Alemán, J., Sánchez-Henarejos, A., Manuel García-Amicis, V., Toval, A., Belén Sánchez-García, A., & Hernández-Hernández, I. (2015). Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario. Gaceta Sanitaria, 29, 74–76. https://doi.org/10.1016/j.gaceta.2014.06.007

MinisterioSalud. (1999). Resolucion 1995 de 1999. Retrieved from https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCIÓN 1995 DE 1999.pdf

Nacional, E., Seguridad, D., De Términos, G., & Abreviaturas, Y. (2011). (). Retrieved from https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/800-Glosario_de_terminos_y_abreviaturas/800-Glosario_de_terminos_ENS-mar11.pdf

Tecnología. (2013). Las contraseñas de internet: historia de un fracaso. Revista Semana. Retrieved from http://www.semana.com/vida-moderna/articulo/las-contrasenas-de-internet-historia-de-un-fracaso/363975-3

Anonymus. (2017). Día de la Contraseña: una breve historia de su origen. Retrieved November 1, 2018, from 2017 website: https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/

DocSlide. (n.d.). TELEOLOGÍA Y FUNDAMENTOS DE LA INVESTIGACIÓN JURÍDICA - Documents. Retrieved November 30, 2017, from 2016 website: https://docslide.net/documents/teleologia-y-fundamentos-de-la-investigacion-

juridica.html

Luis Fernández-Alemán, J., Sánchez-Henarejos, A., Manuel García-Amicis, V., Toval, A., Belén Sánchez-García, A., & Hernández-Hernández, I. (2015). Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario. *Gaceta Sanitaria*, *29*, 74–76. https://doi.org/10.1016/j.gaceta.2014.06.007

MinisterioSalud. (1999). *Resolucion 1995 de 1999*. Retrieved from https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCIÓN 1995 DE 1999.pdf

Nacional, E., Seguridad, D., De Términos, G., & Abreviaturas, Y. (2011). (). Retrieved from https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/800-Glosario_de_terminos_y_abreviaturas/800-Glosario_de_terminos_ENS-mar11.pdf

Rondon, J., & Eslava, W. (2014). *Seguridad de la Información*. Retrieved from http://es.calameo.com/read/0037208432fca1aa7329d

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo de Gea, J. M. (2014a). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atención Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo de Gea, J. M. (2014b). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atención Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Tecnologia. (2013). Las contraseñas de internet: historia de un fracaso. *Revista Semana*. Retrieved from http://www.semana.com/vida-moderna/articulo/las-contrasenas-de-internet-historia-de-un-fracaso/363975-3

Turriago, L. C., De Apoyo, P., & Reforma De Salud, L. (n.d.). *EVALUACIÓN DE TECNOLOGÍAS EN SALUD: APLICACIONES Y RECOMENDACIONES EN EL SISTEMA DE SEGURIDAD SOCIAL EN SALUD COLOMBIANO*. Retrieved from https://www.minsalud.gov.co/salud/Documents/Evaluación de Tecnologias en

Salud.pdf

CCN-CERT. Esquema Nacional de Seguridad. Guía de Seguridad CCN-STIC-800). Esquema Nacional de Seguridad. Glosario de Términos y Abreviaturas. Centro Criptológico Nacional. 2011 [consultado Ago 2013]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema Nacional de Seguridad/800-Glosario de terminos y abreviaturas/800- Glosario de terminos ENS-mar11.pdf

Anonymus. (2017). Día de la Contraseña: una breve historia de su origen. Retrieved November 1, 2018, from 2017 website: https://www.welivesecurity.com/la-es/2017/05/04/dia-de-la-contrasena-origen/

DocSlide. (n.d.). TELEOLOGÍA Y FUNDAMENTOS DE LA INVESTIGACIÓN JURÍDICA - Documents. Retrieved November 30, 2017, from 2016 website: https://docslide.net/documents/teleologia-y-fundamentos-de-la-investigacion-juridica.html

Luis Fernández-Alemán, J., Sánchez-Henarejos, A., Manuel García-Amicis, V., Toval, A., Belén Sánchez-García, A., & Hernández-Hernández, I. (2015). Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario. *Gaceta Sanitaria*, *29*, 74–76. https://doi.org/10.1016/j.gaceta.2014.06.007

MinisterioSalud. (1999). *Resolucion 1995 de 1999*. Retrieved from https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCIÓN 1995 DE 1999.pdf

Nacional, E., Seguridad, D., De Términos, G., & Abreviaturas, Y. (2011). (). Retrieved from https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/800-Glosario_de_terminos_y_abreviaturas/800-Glosario_de_terminos_ENS-mar11.pdf

Rondon, J., & Eslava, W. (2014). *Seguridad de la Información*. Retrieved from http://es.calameo.com/read/0037208432fca1aa7329d

https://doi.org/10.1016/j.aprim.2013.10.008

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo de Gea, J. M. (2014b). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal

sanitario en atención primaria. *Atención Primaria*, *46*(4), 214–222. https://doi.org/10.1016/j.aprim.2013.10.008

Tecnologia. (2013). Las contraseñas de internet: historia de un fracaso. *Revista Semana*. Retrieved from http://www.semana.com/vida-moderna/articulo/las-contrasenas-de-internet-historia-de-un-fracaso/363975-3

Turriago, L. C., De Apoyo, P., & Reforma De Salud, L. (n.d.). *EVALUACIÓN DE TECNOLOGÍAS EN SALUD: APLICACIONES Y RECOMENDACIONES EN EL SISTEMA DE SEGURIDAD SOCIAL EN SALUD COLOMBIANO*. Retrieved from https://www.minsalud.gov.co/salud/Documents/Evaluación de Tecnologias en Salud.pdf

Barona, R. Legislación y Jurisprudencia (n.d.) DERECHOS Y OBLIGACIONES EN LA RELACIÓN MÉDICO – PACIENTE.

ISO 27001 Health informatics -- Electronic health record communication [consultado Sept 2018]. Disponible en: http://www.iso.org/iso/home.htm

ISO 27002 Health informatics -- Electronic health record communication [consultado Oct 2018]. Disponible en: http://www.iso.org/iso/home.htm

ISO 27799 Health informatics -- Electronic health record communication [consultado Sept 2018]. Disponible en: http://www.iso.org/iso/home.htm

Tipos de seguridad más importantes para conocer y tener en cuenta, disponible en: https://www.obs-edu.com/int/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta 27 de abril 2019

La seguridad en los hospitales españoles: tu salud y tus datos, ¿en peligro?, Disponible en: https://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-seguridad_informatica-ciberataques-datos-privacidad_0_427657312.html

Las historias clínicas electrónicas ahorran tiempo y salvan vidas, Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/historias-clinicas-electronicas-34248

Anexos

Anexo 1. Encuesta virtual Trabajadores en Salud

1- Nombre del establecimiento de Salud donde trabaja actualmente (Si trabaja en más de uno, debe seleccionar el establecimiento en el cual labora más horas)

_____

2- Clase de Entidad

- Publica
- Privada
- Mixta

3- Edad

_____

4- Cargo que desempeña dentro del establecimiento de Salud

- Cargo Administrativo
- Enfermero (a)
- Médico General
- Médico Especialista
- Técnico – Auxiliar de Salud
- Odontólogo (a)

5- Para usted la seguridad de información de las Historias Clínicas es:

- Un tema muy importante que me gustaría conocer
- Un tema sin trascendencia o importancia
- Un tema que corresponde a los gerentes o jefes de las IPS
- Un tema que se debe capacitar a todos los funcionarios de salud

6- ¿Qué sistema de información maneja dentro de su sitio de trabajo?

- Física (manual-papel)
- Electrónica (Software)

7- ¿Cuántos años tiene de experiencia en el cargo actual?

- Menos de 1 año
- Entre 1 año y 3 años
- Entre 3 años y 5 años
- Más de 5 años

8- ¿Cree usted que el software que utiliza para realizar el proceso de registro de los pacientes es seguro?

- Si
- No
- No emplea software

9- Para ingresar al software en donde se maneja las historias clínicas de su IPS. ¿Lo hace con usuario y contraseña personal?

- Si
- No
- No emplea software

10-Para usted una contraseña es segura cuando

- Empleo datos personales en ella
- Selecciono números solamente
- Elijo fechas especiales e importantes para mí
- Combino letras, números y/o caracteres especiales
- No utilizo contraseñas

11-¿Cree usted que la contraseña que utiliza para el ingreso a la aplicación en donde se maneja las historias clínicas es segura?

- Si
- No
- No emplea software

12-¿Cuándo se levanta rápidamente de su lugar de trabajo, siempre bloquea el equipo de cómputo donde se encuentra realizando sus labores diarias?

- Si
- No
- No emplea software

13-Si un compañero le sugiere que le preste su usuario y contraseña ¿Usted lo haría?

- Si
- No
- No emplea software

14-Considera que el usuario y contraseña de los sistemas a los cuales tiene acceso es de uso exclusivo suyo.

- Si
- No
- No emplea software

15-La IPS en la que labora promueve un ambiente de seguridad de información por medio de capacitación e información

- Si
- No
- No emplea software

16-Si en su IPS no emplean software para el registro de historias clínicas por favor explique brevemente como se realiza el proceso.

_____
_____
_____

17-Conoce el protocolo de seguridad de información de la IPS

- Si
- No
- No sé qué es

Anexo 2. Resolución 1995 de 1999

A continuación, se encuentran los artículos de la Resolución 1995 el cual establece las normas para el manejo de la historia clínica, y para el adecuado entendimiento del tema es necesario transcribir algunos artículos, así:

ARTÍCULO 1.- DEFINICIONES.	*a) La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.* *b) Estado de salud: El estado de salud del paciente se registra en los datos e informes acerca de la condición somática, psíquica, social, cultural, económica y medioambiental que pueden incidir en la salud del usuario.* *c) Equipo de Salud. Son los Profesionales, Técnicos y Auxiliares del área de la salud que realizan la atención clínico asistencial directa del Usuario y los Auditores Médicos de Aseguradoras y Prestadores responsables de la evaluación de la calidad del servicio brindado.* *d) Historia Clínica para efectos archivísticos: Se entiende como el expediente conformado por el conjunto de documentos en los que se*

	efectúa el registro obligatorio del estado de salud, los actos médicos y demás procedimientos ejecutados por el equipo de salud que interviene en la atención de un paciente, el cual también tiene el carácter de reservado. *e) Archivo de Gestión: Es aquel donde reposan las Historias Clínicas de los Usuarios activos y de los que no han utilizado el servicio durante los cinco años siguientes a la última atención.* *f) Archivo Central: Es aquel donde reposan las Historias Clínicas de los Usuarios que no volvieron a usar los servicios de atención en salud del prestador, transcurridos 5 años desde la última atención.* *g) Archivo Histórico. Es aquel al cual se transfieren las Historias Clínicas que por su valor científico, histórico o cultural, deben ser conservadas permanentemente.*
ARTÍCULO 3.- CARACTERÍSTICAS DE LA HISTORIA CLÍNICA.	*Las características básicas son:* *Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionado*

	con sus dimensiones personal, familiar y comunitaria. *Secuencialidad: Los registros de la prestación de los servicios en salud deben consignarse en la secuencia cronológica en que ocurrió la atención. Desde el punto de vista archivístico la historia clínica es un expediente que de manera cronológica debe acumular documentos relativos a la prestación de servicios de salud brindados al usuario.* *Racionalidad científica: Para los efectos de la presente resolución, es la aplicación de criterios científicos en el diligenciamiento y registro de las acciones en salud brindadas a un usuario, de modo que evidencie en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo.* *Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.* *Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.*

ARTÍCULO 4.- OBLIGATORIEDAD DEL REGISTRO.	*Los profesionales, técnicos y auxiliares que intervienen directamente en la atención a un usuario, tienen la obligación de registrar sus observaciones, conceptos, decisiones y resultados de las acciones en salud desarrolladas, conforme a las características señaladas en la presente resolución.*
ARTÍCULO 6.- APERTURA E IDENTIFICACIÓN DE LA HISTORIA CLÍNICA.	*Todo prestador de servicios de salud que atiende por primera vez a un usuario debe realizar el proceso de apertura de historia clínica.* *A partir del primero de enero del año 2000, la identificación de la historia clínica se hará con el número de la cédula de ciudadanía para los mayores de edad; el número de la tarjeta de identidad para los menores de edad mayores de siete años, y el número del registro civil para los menores de siete años. Para los extranjeros con el número de pasaporte o cédula de extranjería. En el caso en que no exista documento de identidad de los menores de edad, se utilizará el número de la cédula de ciudadanía de la madre, o el del padre en ausencia de ésta, seguido de un número consecutivo de acuerdo al número de orden del menor en el grupo familiar.*
ARTÍCULO 8.- COMPONENTES.	*Son componentes de la historia clínica, la identificación del usuario, los registros específicos y los anexos.*

ARTÍCULO 9.- IDENTIFICACIÓN DEL USUARIO.	*Los contenidos mínimos de este componente son: datos personales de identificación del usuario, apellidos y nombres completos, estado civil, documento de identidad, fecha de nacimiento, edad, sexo, ocupación, dirección y teléfono del domicilio y lugar de residencia, nombre y teléfono del acompañante; nombre, teléfono y parentesco de la persona responsable del usuario, según el caso; aseguradora y tipo de vinculación.*
ARTÍCULO 10.- REGISTROS ESPECÍFICOS.	*Registro específico es el documento en el que se consignan los datos e informes de un tipo determinado de atención. El prestador de servicios de salud debe seleccionar para consignar la información de la atención en salud brindada al usuario, los registros específicos que correspondan a la naturaleza del servicio que presta.* *Los contenidos mínimos de información de la atención prestada al usuario, que debe contener el registro específico son los mismos contemplados en la Resolución 2546 de julio 2 de 1998 y las normas que la modifiquen o adicionen y los generalmente aceptados en la práctica de las disciplinas del área de la salud.* *PARAGRAFO PRIMERO. Cada institución podrá definir los datos adicionales en la historia clínica, que resulten necesarios para la adecuada atención del paciente.*

	PARAGRAFO SEGUNDO. Todo prestador de servicios de salud debe adoptar mediante el acto respectivo, los registros específicos, de conformidad con los servicios prestados en su Institución, así como el contenido de los mismos en los que se incluyan además de los contenidos mínimos los que resulten necesarios para la adecuada atención del paciente. El prestador de servicios puede adoptar los formatos y medios de registro que respondan a sus necesidades, sin perjuicio del cumplimiento de las instrucciones impartidas por las autoridades competentes.
ARTÍCULO 12.- OBLIGATORIEDAD DEL ARCHIVO.	*Todos los prestadores de servicios de salud, deben tener un archivo único de historias clínicas en las etapas de archivo de gestión, central e histórico, el cual será organizado y prestará los servicios pertinentes guardando los principios generales establecidos en el Acuerdo 07 de 1994, referente al Reglamento General de Archivos, expedido por el Archivo General de la Nación y demás normas que lo modifiquen o adicionen.*
ARTÍCULO 13.- CUSTODIA DE LA HISTORIA CLÍNICA.	*La custodia de la historia clínica estará a cargo del prestador de servicios de salud que la generó en el curso de la atención, cumpliendo los procedimientos de archivo señalados en la presente resolución, sin perjuicio de los señalados en otras normas legales vigentes. El prestador podrá entregar copia de la historia clínica al usuario o a su representante legal cuando este lo solicite, para los efectos previstos en las disposiciones legales vigentes.*

	PARÁGRAFO PRIMERO. Del traslado entre prestadores de servicios de salud de la historia clínica de un usuario, debe dejarse constancia en las actas de entrega o de devolución, suscritas por los funcionarios responsables de las entidades encargadas de su custodia. *PARÁGRAFO SEGUNDO. En los eventos en que existan múltiples historias clínicas, el prestador que requiera información contenida en ellas, podrá solicitar copia al prestador a cargo de las mismas, previa autorización del usuario o su representante legal.* *PARÁGRAFO TERCERO. Modificado por el art. 1, Resolución del Min. Protección 1715 de 2005. En caso de liquidación de una Institución Prestadora de Servicios de Salud, la historia clínica se deberá entregar al usuario o a su representante legal. Ante la imposibilidad de su entrega al usuario o a su representante legal, el liquidador de la empresa designará a cargo de quien estará la custodia de la historia clínica, hasta por el término de conservación previsto legalmente. Este hecho se comunicará por escrito a la Dirección Seccional, Distrital o Local de Salud competente, la cual deberá guardar archivo de estas comunicaciones a fin de informar al usuario o a la autoridad competente, bajo la custodia de quien se encuentra la historia clínica.*

ARTÍCULO 14.- ACCESO A LA HISTORIA CLÍNICA.	*Podrán acceder a la información contenida en la historia clínica, en los términos previstos en la Ley:* *1) El usuario.* *2) El Equipo de Salud.* *3) Las autoridades judiciales y de Salud en los casos previstos en la Ley.* *4) Las demás personas determinadas en la ley.* *PARÁGRAFO. El acceso a la historia clínica, se entiende en todos los casos, única y exclusivamente para los fines que de acuerdo con la ley resulten procedentes, debiendo en todo caso, mantenerse la reserva legal.*
ARTÍCULO 16.- SEGURIDAD DEL ARCHIVO DE HISTORIAS CLÍNICAS.	*El prestador de servicios de salud, debe archivar la historia clínica en un área restringida, con acceso limitado al personal de salud autorizado, conservando las historias clínicas en condiciones que garanticen la integridad física y técnica, sin adulteración o alteración de la información.* *Las instituciones prestadoras de servicios de salud y en general los prestadores encargados de la custodia de la historia clínica, deben velar por la conservación de la misma y responder por su adecuado cuidado".*

Anexo 3. Legislación vigente para historias clínicas digitales en Colombia

Ley 603 De 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. Determina a el software como un activo, protegido por el los Derechos de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley Estatutaria 1266 del 31 de Diciembre de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales para ser aplicada por todas las entidades públicas y privadas a nivel nacional, esta ley tiene en cuenta la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 Del 5 De Enero De 2009

Esta ley modifica parte del Código Penal, crea un nuevo bien jurídico tutelado -denominado “la protección de la información y de los datos”- y conserva completamente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 Del 30 De Julio De 2009

Define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dicta otras disposiciones.

Ley Estatutaria 1581 De 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado la sanción de esta Sentencia C-748 establece que toda entidad pública o privada, tiene un plazo de seis meses para crear las políticas internas de manejo de datos personales, estableciendo los procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma, esto da el primer paso para la sistematización de datos de los usuarios del Sistema al cual las entidades de registro y control, pueden tener acceso con previa autorización del usuario, y de esta manera globalizar electrónicamente el acceso a la información.

Aspectos a resaltar de esta normatividad[24]:

1. Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

2. Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

3. Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

[24] Tomado de Ley Estatutaria 1581 De 2012

4. Crea una especial protección a los datos de menores de edad.

5. Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

6. Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

7. Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

8. Crea el Registro Nacional de Bases de Datos.

9. Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

Decreto 1377 De 2013

Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Estos procesos se encuentran con estandarización Internacional mediante normas ISO, para dar claridad es necesario recordar que La ISO (International Standarization Organization) es una organización internacional encargada de asistir las normas de fabricación, comercio y comunicación a nivel mundial. Entre las normas ISO más utilizadas se encuentran las referentes a las medidas de papel

- ISO 216, que contempla los tamaños
- ISO 639 los nombres de lenguas

- ISO 9000, 9001 y 9004 los sistemas de calidad
- ISO 14000 de gestión medioambiental
- ISO/IEC 80000 para signos y símbolos matemáticos y magnitudes del sistema internacional de unidades, y muchos más.
- ISO 9660 para sistemas de archivos de CD-ROM;
- ISO 13606-1: 2008 especifica la comunicación de parte o la totalidad del registro electrónico de salud (EHR) de un único sujeto identificado de cuidado entre los sistemas EHR, o entre los sistemas EHR y un repositorio centralizado de datos EHR.

  También se puede usar para comunicación EHR (electronic health record) entre un sistema EHR o repositorio y aplicaciones clínicas o componentes de middleware (como componentes de soporte de decisión) que necesitan acceder o proporcionar datos EHR, o como la representación de datos EHR dentro de un registro distribuido (federado) sistema.

- ISO 13606-1: 2008 se utilizará predominantemente para apoyar la atención directa brindada a personas identificables, o para apoyar sistemas de monitoreo poblacional tales como registros de enfermedades y vigilancia de salud pública. El uso de registros de salud para otros fines tales como enseñanza, auditoría clínica, administración e informes, administración de servicios, investigación y epidemiología, que a menudo requieren la agregación de registros individuales, no son el centro de la ISO 13606-1: 2008, pero dichos usos secundarios también podría encontrar útil este documento[25].

  Esta norma se encuentra en la actualidad en modificaciones por la norma ISO/DIS 13606-1 y la ISO/TC 215 las cuales brindaran un alcance y aclaración sobre la estandarización en el campo de la informática sanitaria, para facilitar la captura, el

[25] Tomado de https://www.iso.org/standard/40784.html

intercambio y el uso de datos, información y conocimientos relacionados con la salud para respaldar y habilitar todos los aspectos del sistema de salud26.

[26] Tomado de https://www.iso.org/committee/54960.html