ANÁLISIS DE SEGURIDAD PARA EL MANEJO DE LA INFORMACIÓN MÉDICA EN TELEMEDICINA

SECURITY ANALYSIS FOR MEDICAL INFORMATION MANAGEMENT IN TELEMEDICINE

Edward Paul Guillén Pinto
Ingeniero Electrónico, M.Sc. Líder Grupo de Investigación Grupo GISSIC
Universidad Militar Nueva Granada, Bogotá, Colombia
edward.guillen@unimilitar.edu.co

Leonardo Juan Ramírez López
Ingeniero Electrónico, PhD. Líder Grupo de Investigación Grupo TIGUM
Universidad Militar Nueva Granada, Bogotá, Colombia
leonardo.ramirez@unimilitar.edu.co

Edith Paola Estupiñán Cuesta
Ingeniero en Telecomunicaciones. Asistente de investigación Grupo GISSIC
Universidad Militar Nueva Granada, Bogotá, Colombia
edith.estupinan@unimilitar.edu.co

Fecha de recepción: 28 de julio de 2011
Fecha de aprobación: 9 de diciembre de 2011

RESUMEN

La Telemedicina hace posible realizar de forma remota, varios procedimientos médicos y clínicos como: exámenes, diagnósticos y supervisión de tratamientos, utilizando recursos tele informáticos como computadores, servidores, equipos de procesamiento de imágenes, Internet y equipos de transmisión y recepción de información. La transmisión de la información de los pacientes crece día con día, vinculando otra serie de problemas relacionados con el tráfico y seguridad de los datos. En el tema de la seguridad, aún existe divergencia en los criterios de almacenamiento, acceso y transmisión de información de los pacientes porque los requerimientos físicos y lógicos varían para cada empresa, equipo desarrollador o intereses particulares. El presente trabajo hace un análisis respecto del tema de la seguridad informática sobre una red de Telemedicina. Incluye un análisis sobre los procedimientos de los servicios de Telemedicina más característicos y sus requerimientos de seguridad. Los requerimientos fueron estudiados y seleccionados a partir de los estándares internacionales regulatorios que se adapten a las necesidades básicas de seguridad de los servicios de Telemedicina.

Palabras clave: telemedicina, servicios, requerimientos, seguridad, información. HIPPA, CALDICOTT.

ABSTRACT

Tele-medicine allows making a wide variety of medical procedures such as health screening, diagnosis procedures, and treatment supervision in a remote way by using IT resources such as computers, servers, image processing equipments, Internet, and communication networks.

Transmission of patients' information is growing every single day with the subsequent increasing of traffic and data information problems. With information on Tele-medicine applications, there is no consensus in the criteria associated to storage, access and transmission of patient information because of the variety requirements of companies, developers, designers, or interests. This paper presents an analysis of informatics security on Tele-medicine service oriented networks. The paper includs an analysis about the most important procedures in telemedicine services and the security requirements of each one. The requirements were studied and chosen from the international regulatory standards that supplies the basic security needs on telemedicine services.

Keywords: tele-medicine, services, requirements, security, information, HIPPA, CALDICOTT.

INTRODUCCIÓN

Por lo general, la Telemedicina alude al uso de las tecnologías de comunicación e información sobre servicios médicos a distancia. Estas tecnologías permiten intercambiar datos con el fin de examinar, diagnosticar y tratar un paciente, y facilitar el acceso de la población, independiente del área geográfica donde habite [1].

La seguridad y confiabilidad sobre redes de Telemedicina, son dos de los aspectos más relevantes para almacenar, acceder y transmitir de información médica de los pacientes. Analizar estos dos aspectos, previene amenazas y ataques a los sistemas de Telemedicina. Para un sistema de Telemedicina como para cualquier sistema, una falla particular puede causar la caída del sistema por completo. En general, las amenazas y ataques sobre una red de datos, obligan a establecer parámetros para prevenir o mitigar estas falencias, por medio de regulaciones y estándares. Por esta razón, surge la necesidad de estudiar qué estándares regulatorios existen y se adaptan a los servicios de Telemedicina [2]. Dentro de las regulaciones más relevantes, están la Ley de Transferibilidad Responsabilidad de Seguros de Salud HIPPA (Health Insurance Portability and Accountability), el Informe sobre la Revisión de Información de Identificación del Paciente perteneciente al comité CALDICOTT y Los Objetivos de Control para Información y Tecnologías COBIT [3] y [4].

La información médica que se maneja y en Telemedicina, es en general de tipo confidencial y por lo tanto, requiere resguardarse de ataques y amenazas que puedan afectar el derecho a la intimidad, la privacidad y la protección de los datos de los pacientes [5]. Todas las redes de datos son vulnerables a ataques que buscan provocar el colapso de los sistemas y sustraer datos privados. Estos ataques pueden afectar los datos que se encuentren encriptados o no, mediante técnicas de hurto de información como lo son los programas espía (spyware), los virus y los troyanos, el acceso no autorizado a la información, la alteración o deterioro total o parcial de la misma. En el caso particular de las redes de Telemedicina, éstas pueden ser atacadas por el aprovechamiento de sus vulnerabilidades entre las cuales se destacan la falta de sistemas de seguridad informática, sistemas inestables de autenticación, fallos en los procedimientos de

transmisión y almacenamiento de la información, y manejo inadecuado de la información por parte del personal encargado [6]. Un ejemplo claro de un ataque a redes médicas, es la sustracción de información privada por parte de los funcionarios, en el mes de abril del año 2011, en el Midstate Medical Center, Estados Unidos. El Caso se presentó cuando un empleado del centro médico que quiso trabajar desde su casa, transfirió información confidencial de más de 93.500 pacientes del hospital a un sitio externo, utilizando la red de la institución y dejando vulnerable la información de la entidad de salud. La información incluía datos privados de las personas como nombres, direcciones, fechas de nacimiento e información médica confidencial [7]. Otro ejemplo de afectación a la información médica, es el robo de identidad que consiste en un ataque por medios informáticos, mediante el cual el atacante obtiene información personal de otras personas y la utiliza ilegalmente: en Birmingham, Estados Unidos, en el mes de junio del año 2011, una mujer fue acusada de haber robado la identidad de más de 4.000 personas de una fuente de información del Hospital de Birmingham, accediendo a los recursos informáticos dentro de la entidad de salud. La información fue utilizada para hurtar correo, y pretendía usarse en fraudes bancarios, usando el número de seguro social de los pacientes [8].

Los servicios de Telemedicina manejan diferentes tipos de información, datos de señales, imagen, video, registros, etc., que permiten la comunicación a distancia entre diferentes especialistas [9]. Existe un amplio conjunto de servicios de Telemedicina entre los cuales se encuentran los servicios de Tele-consulta, Tele-diagnóstico, Tele-terapia y Telemetría. Estos servicios utilizan aplicaciones que se soportan en sistemas multimedia de video, voz y datos sobre el Protocolo de Internet (IP), regulados por protocolos como H.323, el Protocolo de Inicio de Sesión (SIP) o el Protocolo de datagrama de usuario (UDP) [10] y [12]. Los servicios de Telemedicina realizan la transmisión de archivos de texto e imágenes, en formatos como Digital Imaging and Communication in Medicine (Dicom) [13], y Health Level 7 (HL7), [14] a través de un servidor de transferencia de ficheros [15].

La implementación de buenas prácticas en el manejo y protección de información y de sistemas de seguridad en Telemedicina, ha llevado a varias organizaciones a tener éxito al desarrollar sus proyectos relacionados con el tema. Como un claro ejemplo, nacional, se destaca el proyecto Galaxia, un Programa de Telemedicina de la Fundación Cardiovascular de Colombia, aplicado a la Salud Pública, para desarrollar y mantener de una red de servicios médicos local, regional y nacional, con el fin de facilitar el acceso a la consulta especializada a través del uso de la Tecnología [16]. El proyecto Galaxia se inició en el departamento de Santander como una iniciativa para acercar la medicina especializada a pacientes que requerían tratamientos exclusivos, pero se encontraban en municipios y zonas apartadas de las zonas urbanas. Otro caso de éxito, es el del Centro de Telemedicina de Colombia que desde 2003, está trabajando en beneficio de personas a quienes la Telemedicina facilita sus tratamientos médicos, enfocado en la Telemedicina y salud en línea en países de América Latina y el Caribe [17].

Este trabajo presenta un análisis detallado de los servicios de Telemedicina que actualmente se ofrecen en Colombia, definiendo los procedimientos básicos, las normas y regulaciones usan en el manejo de la información médica, para luego realizar un filtro de los requerimientos relevantes

sobre el manejo de información médica. Con esto, es posible ofrecer una propuesta de análisis de los requerimientos acorde con los servicios ofrecidos en una red de Telemedicina, determinando características y criterios de seguridad respecto del manejo de información médica y las regulaciones existentes [18].

1. INTRODUCCIÓN A LA TELEMEDICINA

En la actualidad, la Telemedicina es considerada como una nueva forma de atención médica que se caracteriza por entregar servicios de salud a distancia. La Telemedicina promueve una mejor atención a los pacientes, brindando un diagnóstico rápido y eficiente. El uso de la informática y las Telecomunicaciones en el área de la salud, debe estar acompañado de medidas de seguridad adecuadas para garantizar la confidencialidad, disponibilidad e integridad de la información médica, ofreciendo protección a los pacientes, los profesionales de la salud y al recurso humano en general. La Telemedicina contribuye a reducir los costos y la concentración de pacientes en las entidades de salud [19].

Una red de Telemedicina por lo general, está compuesta por pacientes, centros de salud y referencia (Médicos Especialistas), periféricos médicos, equipos de comunicaciones y medio de transmisión (enlaces de baja velocidad para conexiones entre especialistas de la salud y pacientes en un centro de la salud y enlaces de alta velocidad para la conexión entre las entidades de salud). Una aproximación a este tipo de redes, se puede ver en la Figura 1, donde se detalla de manera muy general, los principales componentes de una red de Telemedicina. Esta red cuenta con servidores que permiten implementar aplicaciones médicas y con usuarios que dependiendo su categoría, tienen cierto tipo de privilegios [20].

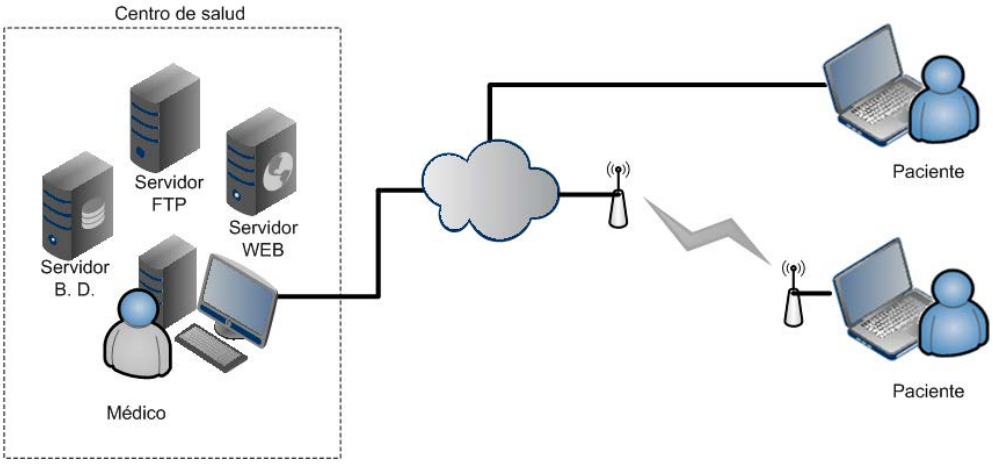

Figura 1. Típica Red de Telemedicina

Una red de Telemedicina se caracteriza por contar con personal encargado de registrar signos vitales, toma de fotografías y videoconferencias. Estas actividades tienen la finalidad de enviar datos mediante una red de comunicación definida por una tecnología en particular (3G, GSM, Internet, etc.). Estos datos se almacenan en un servidor y son accedidos por el especialista médico, para analizar datos almacenados y al final, dar un diagnóstico [21] y [22].

2. SERVICIOS DE TELEMEDICINA: UNA VISIÓN GENERAL

Con el pasar del tiempo, el número de servicios médicos y especialidades aumenta y suple distintas necesidades [23] y [24]. Los servicios de Telemedicina tienen la posibilidad de ser clasificados de diferente manera. Las posibles clasificaciones tienen características principales en común, pero pueden variar un poco en las especialidades consideradas. Por ejemplo: una clasificación por el tipo de información para transmitir (datos, audio o imágenes), o por la tecnología usada o el tipo de especialidades derivadas de los servicios en Telemedicina [25] y [26].

Tabla 1. Servicios y especialidades de Telemedicina

Servicios de Telemedicina	Especialidades
Tele-consulta	Registro Clínico Electrónico
Tele-diagnóstico	Tele-endoscopia
	Tele-dermatología
	Tele-oftalmología
	Tele-otorrinolaringología
Tele-terapia	Tele-psiquiatría
	Tele-fisioterapia
	Tele-prescripción
Telemetría	Tele-radiología
	Tele-patología
	Tele-cardiología

La organización Panamericana de la Salud con el aval de la Organización Mundial de la Salud OPS/OMS, hizo una clasificación de los servicios de Telemedicina de acuerdo con las especialidades derivadas de cada una de ellas, lo cual se puede apreciar en la Tabla 1 [27]. A partir de esa clasificación, este artículo enfocará su análisis. Es importante destacar que los resultados que se presentan a continuación, son producto de un proyecto de investigación titulado *Validación de Políticas de Seguridad en la Práctica Social,* desarrollado por el Grupo de investigación GISSIC en la Universidad Militar Nueva Granada en el año 2010 [28].

2.1 Actividades en Telemedicina

Para cumplir con su finalidad principal la Telemedicina requiere la especificación de distintas actividades. La definición de estas actividades en la telemedicina, es lo que después puede permitir clasificarlas para llamarlas servicios o especialidades. Las actividades pueden variar de

acuerdo con la finalidad del centro de salud y la importancia dada a ciertos servicios en particular [29]. Otro punto por destacar, es que la mayoría de las actividades de la telemedicina se desprende de las partes involucradas, como se muestra en la figura 2.

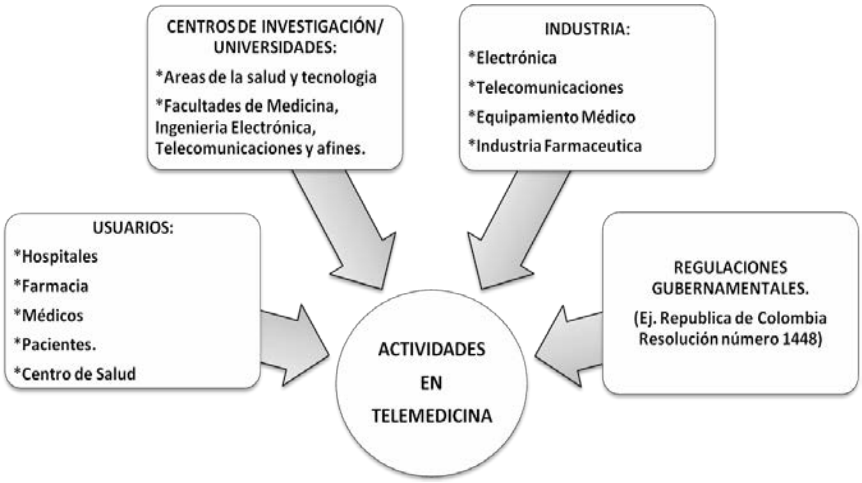

Figura 2. Partes involucradas en las actividades de la Telemedicina

De todas las partes involucradas en la Telemedicina (Figura 2), se desglosan actividades particulares vinculadas con cada parte. Actividades relacionadas con la investigación, están enfocadas en generar nuevos procesos en telemedicina para optimizar los existentes y generar nuevos procesos. Las Actividades relacionadas con los usuarios, están relacionadas con el control de los pacientes (consulta y registro), diagnóstico preventivo y terapéutico, tratamientos, monitoreo remoto, lectura de diagnóstico e interpretación de los procedimientos realizados a los pacientes y consulta. Las Actividades relacionadas con los equipos, involucran directamente a las industrias dedicadas a su fabricación y al mantenimiento y control de los equipos. Finalmente, las actividades gubernamentales están enfocadas en definir la normatividad y las regulaciones necesarias para poder ejecutar correctamente los servicios de telemedicina [29].

2.2 Servicios de Telemedicina

A continuación, de acuerdo con la clasificación propuesta en este artículo se detallan las características relevantes de los servicios y de sus especialidades.

2.2.1 Tele-Consulta

El servicio de Tele-consulta se utiliza en la especialidad del Registro Clínico Electrónico (RCE). Los RCE son bancos de almacenamiento de información médica de pacientes asociados en una entidad de salud. Los registros de cada paciente incluyen datos básicos como información personal, datos demográficos, información sobre visitas médicas y progreso en tratamientos,

alergias, medicamentos, signos vitales, antecedentes médicos, historia familiar, registro de hospitalizaciones, vacunas, datos de laboratorio e informes de radiología.

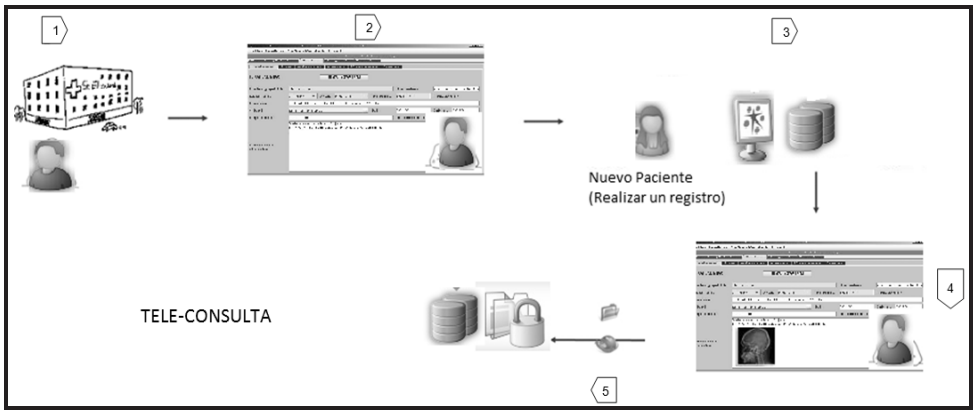

Figura 3. Procesos básicos para generar un registro clínico electrónico

La Figura 3 muestra una aproximación del proceso de Tele-consulta [30], donde cada numeral se relaciona a continuación:

1. Ingreso paciente en la entidad de salud
2. Identificación del paciente
3. Registro del nuevo paciente (diligenciamiento datos personales)
4. Actualización de datos del paciente(si ya existe en la base de datos)
5. Almacenamiento del registro clínico en la base de datos

2.2.2 Tele-diagnóstico

El servicio de Tele-diagnóstico es una práctica que permite a los especialistas, generar un diagnóstico del paciente, estando a kilómetros de distancia y ahorra recursos humanos y tecnológicos.

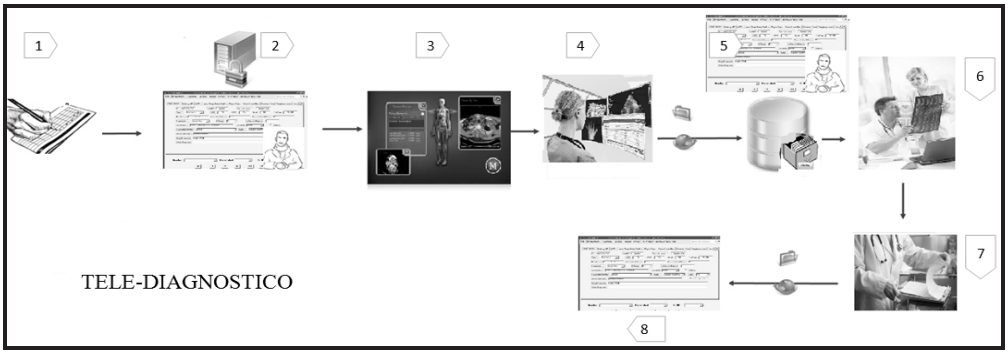

Figura 4. Procesos básicos de Tele-diagnostico

En la Figura 4, se muestran las características principales del servicio de Tele-diagnóstico y de sus especialidades, y en la tabla 2, se muestran los procedimientos básicos de de este servicio y sus especialidades, cuyos numerales se relacionan a continuación:

1. Registro del paciente
2. Identificación del paciente
3. Registro inicial del procedimiento
4. Almacenamiento de imágenes y videos en el registro del paciente
5. Análisis e interpretación de las imágenes obtenidas
6. Diagnostico por el especialista con base en el informe de resultados
7. Actualización de información en el registro clínico

Tabla 2. Procedimientos básicos del servicio de Tele-diagnóstico y sus Especialidades

TELE-DIAGNÓSTICO				
Especialidades / **Procedimientos**	**Tele-endoscopia**	**Tele-Dermatología**	**Tele-Oftalmología**	**Tele-Otorrino-laringología**
Definición del tipo de comunicación en tiempo real, diferido o hibrido		✓		
Ingreso del paciente	✓			
Registro del paciente	✓	✓	✓	✓
Identificación del paciente	✓	✓	✓	✓
Registro inicial del procedimiento	✓	✓	✓	✓
Ingreso del paciente en la entidad de salud, si es necesario		✓		
Preparación del paciente	✓	✓	✓	✓
Ejecución del procedimiento	✓	✓	✓	✓
Captura de imágenes y videos		✓		✓
Captura de imágenes del fondo del ojo hecha por expertos			✓	
Almacenamiento de imágenes y videos en el registro del paciente	✓	✓	✓	✓
Análisis e interpretación de las imágenes obtenidas			✓	✓
Videoconferencia/teleconferencia (especialista- paciente), de ser necesario		✓		
Elaboración de informe con resultados del procedimiento	✓	✓	✓	✓
Diagnóstico por el especialista con base en el informe de resultados.	✓	✓	✓	✓
Informe de consulta presencial al paciente de ser necesario			✓	
Actualización de información en el registro clínico	✓	✓	✓	✓

Dentro de las especialidades del Tele-diagnóstico, se encuentran:

Tele-Endoscopia: La endoscopia convencional es un examen para observar los conductos y cavidades del cuerpo por medio de instrumentos ópticos que proporcionan información visual acerca de órganos internos que son inaccesibles de modo externo. Para la Tele-endoscopia, los sistemas de adquisición están conectados a un sistema de videoconferencia o de digitalización de imágenes de video, con el fin de almacenar los resultados para su posterior diagnóstico. La información adquirida se almacena y luego es analizada por el especialista para hacer un diagnóstico del estado del paciente [31].

Tele-Dermatología: La dermatología es el estudio de la piel, su estructura y las enfermedades que pueda presentar. La Tele-dermatología permite estudiar la piel por medio de sistemas de videoconferencia o Teleconferencia y por lo general, se realiza en tiempo real. Las imágenes adquiridas son capturadas por una cámara digital que permite el almacenamiento posterior en un servidor y en el registro clínico de cada paciente, lo cual permite que el especialista acceda a la información en tiempo diferido, para generar un diagnóstico sobre el estado del paciente [31].

Tele-Oftalmología: Es el estudio del globo ocular con base en un sistema de captura de imágenes del fondo ocular sin generar dilatación de la pupila. La Tele-oftalmología se realiza a través de sistemas oftalmoscopios que se conectan a sistemas de digitalización de imágenes o video y sistemas de videoconferencia. Los especialistas emiten luego, un diagnóstico del estado ocular del paciente [32].

Tele-otorrinolaringología: Es una especialidad medico quirúrgica a distancia, que examina y estudia las enfermedades relacionadas con el oído, la nariz, la faringe, la laringe, la patología del cuello y las glándulas salivares. En esta especialidad, se realiza un adecuado manejo quirúrgico relacionado con el oído, la nariz, los senos paranasales, los problemas de voz, el ronquido con apnea del sueño, las cirugías de amígdalas sin extracción, entre otras. Para este tipo de exámenes, general se usa tecnología láser [33].

2.2.3 Tele-Terapia

La Tele-terapia es un servicio que permite a los especialistas, controlar y supervisar tratamientos clínicos en pacientes que se encuentran topográficamente separados [34]. En la Figura 5, se muestran las características principales del servicio de Tele-terapia y en la Tabla 3, se muestran los procedimientos básicos de este servicio y sus especialidades. Cada numeral se relaciona a continuación:

1. Registro del paciente
2. Consulta del registro clínico EHR
3. Establecimiento de videoconferencia especialista-paciente
4. Almacenamiento de información en base de datos
5. Envío de información del estado del paciente a especialistas
6. Análisis e interpretación de las imágenes obtenidas

7. Diagnostico por el especialista
8. Actualización de información en el registro clínico
9. Finalización de sesión de video conferencia

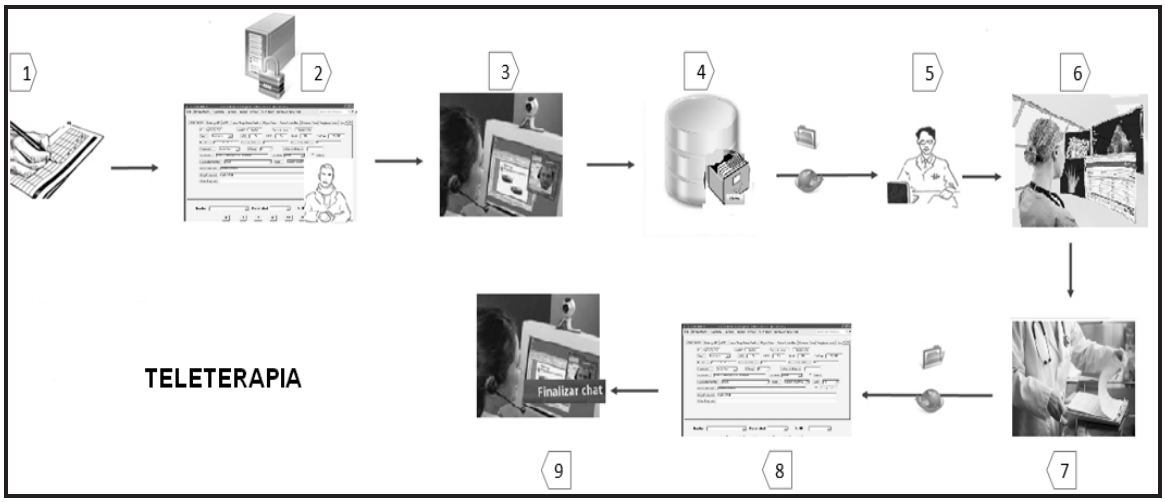

Figura 5. Proceso Básico de Servicio Tele-terapia

La Tele-terapia se divide en las siguientes especialidades:

Tele-Psiquiatría: Se refiere a la aplicación de la Telemedicina a la salud mental, y se define como el uso de las tecnologías de comunicaciones que permite el contacto entre un paciente y un especialista en salud mental. La Tele-psiquiatría facilita actividades de diagnóstico, educación, tratamiento, consulta y transferencia de datos médicos [35].

Tabla 3. Procedimientos básicos del servicio de Teleterapia y sus Especialidades

TELETERAPIA			
Especialidades / **Procedimientos**	**Tele-psiquiatría**	**Tele-fisioterapia**	**Tele-prescripción**
Registro del paciente	✓	✓	✓
Consulta de registro clínico electrónico EHR	✓	✓	✓
Establecimiento de videoconferencia Especialista-paciente	✓	✓	✓
Programación de examen (si es necesario)			✓
Registro del procedimiento indicado	✓	✓	
Almacenamiento de información en base de datos	✓	✓	✓
Envío de información del estado del paciente a			✓

especialistas			
Análisis e interpretación de las imágenes	✓	✓	
Diagnostico por el especialista	✓	✓	✓
Asignación de nueva consulta	✓		
Actualización de información en el registro clínico	✓	✓	✓
Finalización de sesión de video conferencia	✓	✓	✓

Tele-fisioterapia: Esta especialidad permite aplicar la Telemedicina al tratamiento de lesiones que afectan el movimiento corporal humano. Además, brinda la posibilidad de hacer un seguimiento desde casa por medio de la videoconferencia. También puede establecer comunicaciones entre familiares y pacientes para consultar dudas al especialista. La aplicación permite el contacto entre el paciente y el especialista, así como un monitoreo exhaustivo del paciente, controlando el tratamiento y la evolución de su estado de salud [36].

Tele-prescripción: Esta especialidad define un proceso en el cual el médico especialista se entera de los síntomas del paciente y hace un examen físico en busca de signos que representen alguna particularidad, y confronta los datos adquiridos con la conversación y el examen médico, para decidir una acción. Si la acción es terapéutica, surge la prescripción médica [37].

2.2.4 Telemetría

El servicio de Telemetría permite a los especialistas de la salud, por medio de imágenes y videos, recolectar información de forma remota acerca del estado de salud de los pacientes para consulta y diagnóstico [38]. En la Figura 6, una aproximación de este servicio y en la Tabla 4, se ven los procesos básicos de las especialidades del servicio.

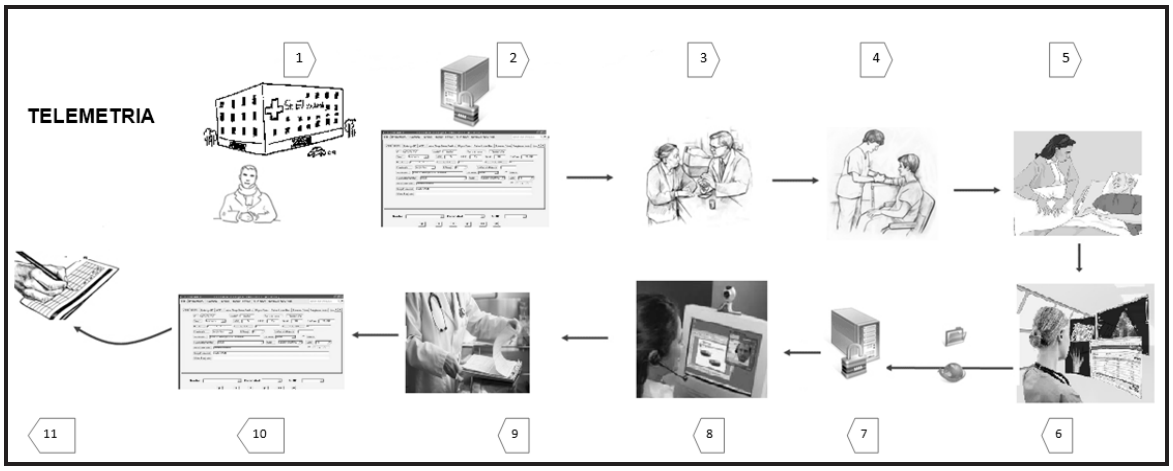

Figura 6. Procesos Básicos de Telemetría

Cuyos numerales se relacionan a continuación:

1. Ingreso del paciente a la entidad de salud.
2. Identificación del paciente.
3. Explicación del procedimiento al paciente para su aprobación.
4. Exámenes rutinarios al paciente y su almacenamiento en EHR.
5. Preparación del paciente para el procedimiento..
6. Captura y digitalización de imágenes.
7. Almacenamiento de imágenes y videos en el registro del paciente.
8. Videoconferencia Especialista- paciente.
9. Diagnóstico por el especialista con base en las imágenes tomadas.
10. Actualización de información en el registro clínico.
11. Programación de nueva consulta.

Tabla 4. Procedimientos básicos del servicio de Telemetría y sus Especialidades

TELEMETRÍA			
Especialidades / Procedimientos	**Tele-Radiología**	**Tele-Patología**	**Tele-Cardiología**
Ingreso del paciente en la entidad de salud	✓	✓	✓
Identificación del paciente	✓	✓	✓
Explicación del procedimiento al paciente para su aprobación	✓	✓	✓
Registro inicial del procedimiento	✓	✓	✓
Exámenes rutinarios al paciente y su almacenamiento en EHR	✓	✓	✓
Asignación de consulta previa al paciente para evaluación de exámenes de ser necesario	✓	✓	✓
Preparación del paciente para el procedimiento	✓	✓	✓
Captura de imágenes radiológicas	✓		
Captura de imágenes ECG		✓	
Adquisición de imágenes de microscopio			✓
Captura y digitalización de imágenes			✓
Compresión de imágenes	✓		✓
Almacenamiento de imágenes y videos en el registro del paciente	✓	✓	✓
Administración de los datos e imágenes (consultas de datos, transmisión de imágenes e impresión)	✓	✓	✓
Asignación de consulta previa al paciente para evaluar exámenes	✓	✓	✓
Utilización del software para manejo y transmisión de imágenes entre especialistas	✓		✓
Videoconferencia Especialista- paciente		✓	✓
Integración del diagnóstico presuntivo, exámenes de rutina ECG.		✓	

Diagnóstico por el especialista con base en las imágenes tomadas	✓	✓	✓
Actualización de información en el registro clínico	✓	✓	✓
Programación de nueva consulta de ser necesario.	✓	✓	✓

Las especialidades que se derivan del servicio de Telemetría son:

Tele-radiología: Es el servicio destinado a capturar imágenes médicas en equipos de resonancia magnética nuclear para la transmisión y posterior consulta por el especialista. El especialista realiza una interpretación de las imágenes transmitidas con fines de diagnóstico. En este tipo de especialidad, el especialista no tiene contacto directo con el paciente, y por eso, es una aplicación en tiempo diferido [38].

Tele-cardiología: Esta aplicación se orienta a la prevención, diagnóstico y tratamiento de enfermedades cardiovasculares. La transmisión de la información puede emplear diferentes medios de comunicación, y se elige, dependiendo de las necesidades del paciente. Esta especialidad permite grabar y enviar electrocardiogramas, señales cardíacas, sonidos, mensajes e imágenes [39].

Tele-patología: Esta especialidad se encarga de la captura y transmisión de imágenes digitales de anatomía patológica con fines de consulta, diagnóstico, investigación o docencia. La Tele-patología estática utiliza imágenes fijas, mientras que la dinámica se basa en el envío de imágenes obtenidas con videocámara [40].

3. ESTÁNDARES REGULATORIOS EN TELEMEDICINA

Para una correcta administración de la seguridad de la información médica, se debe establecer controles y procedimientos que la preserven. Las diferentes regulaciones buscan mantener la confidencialidad, integridad y disponibilidad de la información médica [41].

3.1 Normas Internacionales para seguridad en Telemedicina

La existencia de estándares regulatorios sobre el manejo de información médica, ha permitido que las entidades de salud alcancen mayores índices de confiablidad en la transmisión de información. Dentro de los estándares más representativos, se destacan *HIPAA, COBIT, CALDICOTT, ISO Y ITU-T.* Estos estándares establecen parámetros para preservar la regulación de transmisión de información. A continuación se hará una breve descripción de cada estándar.

La Ley de Transferibilidad y Responsabilidad de Seguros de salud, llamada por sus siglas en inglés HIPPA, es un conjunto de estándares que aseguran la protección de información médica en aspectos como la transmisión, almacenamiento y acceso a la información de salud. Esta Ley se fundamenta en dos documentos principales 45 CFR PART 160 y 45 CFR PART 164. La primera

parte especifica los requerimientos administrativos generales y la segunda, requerimientos de seguridad para la información médica, registro médico electrónico, fundamentos del análisis de riesgos de seguridad, gestión de riesgos y requerimientos para proteger de la información médica [42].

COBIT (Objetivos de control para tecnología de la información y relacionadas), es un conjunto de mejores prácticas para seguridad, calidad, eficacia y eficiencia en las tecnologías de la información necesarias para identificar riesgos, gestionar recursos y medir el rendimiento que permitan alcanzar los objetivos de una organización [43].

El departamento de Salud en su organización CALDICOTT, establece parámetros para permitir la protección de información relacionada con la identificación personal en servicios de salud. Por otra parte, este comité define qué información es de alta calidad y debe ser protegida contra divulgación indebida e inapropiada. Esta norma mediante documentos de confidencialidad como reportes de cumplimiento de principios de protección de datos, políticas, procedimientos para la salud e informes sobre identificación del paciente, permite recopilar los requerimientos para mantener la integridad de la información médica de los pacientes [44].

Las normas ISO 27000 están diseñadas para administra la seguridad de la información. Estas normas especifican aspectos necesarios para implantar un óptimo Sistema de Gestión de la Seguridad de la Información (SGSI), además de definiciones generales, guía de buenas prácticas y requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de la seguridad de la información [45].

La organización internacional de Tele-comunicaciones (ITU-T), por medio de sus normas permite garantizar la compatibilidad y eficacia de las operaciones de red, y ayudar a proteger la infraestructura de Tele-comunicaciones y los servicios que en prestan. Las normas permiten revisa los requisitos de seguridad en redes de datos, para aplicar en redes de Telemedicina en la recomendación X.805 y X1051 [46].

3.2. Requerimientos comunes: almacenamiento, acceso y transmisión de información médica según COBIT, HIPPA y CALDICOTT

Las reglamentaciones para manejar de información médica exponen de forma muy detallada qué requerimientos existen para almacenamiento, acceso y transmisión de la información. Estas regulaciones determinan características como por ejemplo: los equipos que se manejan en estas redes ya sea de cómputo o de diagnóstico. A partir de estas normas, es posible definir qué requerimientos son relevantes. En las tablas 5, 6 y 7 se ven algunos de los requerimientos más importantes para manejar información médica, establecidos por CALDICOTT, HIPAA Y COBIT respectivamente.

Tabla 5. Requerimientos comunes el almacenamiento, acceso y transmisión de información médica según CALDICOTT [47] y [48].

Requerimiento	ID
Los sistemas de tecnología de información y protección de información clínica deben ser apropiados en las entidades de salud para recopilar y analizar un volumen considerable de información de pacientes en bases de datos.	CA 1
Las condiciones de salud del paciente y el progreso deben poderse verificar	
Las transmisiones de información médica relacionada con estadísticas hospitalarias, deben hacerse de forma anónima y el acceso a esta información debe tener una identificación estrictamente controlada.	CA 2
Se debe asignar un número de identificación único conocido, para recolectar datos relacionados con medicina general.	CA 3
La información que se proporcione a entidades de salud externas, debe tener un propósito legítimo, con políticas y protocolos claros para garantizar que quienes reciban dicha información cumplan con los estándares dentro de la entidad de salud.	CA 4
Es necesario utilizar identificadores codificados de referencia para los pacientes	CA 5
La información debe ser cifrada	CA 6
El identificador de cada paciente debe ser un número de diez dígitos y únicamente funciona cuando los números se introducen en un computador que automáticamente lleva a cabo la validación del paciente.	CA 7
Un error en el número de identificación debe detectar una entrada inválida, refiriéndose al paciente equivocado.	CA 8
Cada entidad de salud que intercambie información con entidades externas y organizaciones asociadas, debe establecer un protocolo de comunicación que permita supervisar el intercambio y la transferencia de información.	CA 9
Se debe definir protocolos estrictos para identificar personas autorizadas para acceder a la identidad del paciente y bajo qué circunstancias el acceso debe ser autorizado.	CA10
Se debe permitir la separación de información de la base de datos relacionada con identificación del paciente de información relacionada con tratamientos o condición del paciente	CA 11
El diseño de nuevos sistemas para transferir datos de prescripción, debe poder adaptarse a los sistemas ya existentes.	CA 12
Las tecnologías usadas deben garantizar la privacidad de los datos.	CA 13
En un extremo debe existir protección de contraseña simple en el punto de acceso. (encripción de datos y mecanismos sofisticados de control de acceso).	CA 14
Debe existir control de acceso a los equipos de cómputo y medidas de seguridad básicas.	CA 15
Se debe realizar un control sobre el acceso al sistema por medio del uso de contraseñas o autenticaciones.	CA 16
Se debe intercambiar datos en un formato que no sea totalmente anónimo, pero los atributos de identificación de los datos se restringen sólo a un grupo de individuos.	CA 17
El uso de una firma donde el emisor usa clave privada, y el receptor la puede verificar por medio de la clave pública del emisor.	CA 18
Los procesos que se aplican a la transmisión de datos entre dos partes independientes también pueden ser aplicados al almacenamiento de datos.	CA 19
Cualquiera de los procesos que se aplican a la transmisión de datos entre dos usuarios también pueden ser aplicados a al almacenamiento de datos.	CA 20
Manejar base de datos por separado, una en donde se encuentren los datos principales del paciente y otra con los datos que permiten a un individuo ser identificado.	CA 21
El enlace entre las bases de datos, se controla mediante la adopción de tecnologías que mejoran la privacidad, como la encripción de datos de identificación.	CA 22

Tabla 6. Requerimientos comunes el almacenamiento, acceso y transmisión de información médica según HIPPA [49]

Requerimientos	ID
Implementar procedimientos para verificar la identidad de la persona o entidad que solicite el acceso a la información de salud.	HIPPA 1
Exigir a cada persona una contraseña o PIN	
Definir guías de procedimientos que garanticen la confidencialidad, privacidad y seguridad de la información.	HIPPA 2
Exigir algún tipo de dato biométrico como huellas dactilares, patrones de voz, patrones faciales o del iris	
Implementar mecanismos electrónicos para corroborar que la información de salud protegida no haya sido alterada o destruida de forma no autorizada.	HIPPA 3
Usar protocolos de comunicaciones de red que garanticen que los datos enviados sean los datos recibidos.	
Implementar mecanismos para cifrar y descifrar la información protegida de salud electrónica.	HIPPA 4
Implementar hardware y software para registrar y examinar la actividad en los sistemas de información que contengan o utilicen la información de salud.	HIPPA 5
El Recurso Humano debe estar acreditado para ofrecer sus servicios según la reglamentación vigente para cada profesión u oficio.	HIPPA 6
Establecer políticas y procesos para actuar frente una emergencia que altere los sistemas que contengan información de salud protegida.	
Las instituciones deben certificar que cuentan con personal capacitado para manejar la tecnología utilizada en los procedimientos de Telemedicina.	HIPPA 7
Gestionar el almacenamiento físico de toda la información del sistema	HIPPA 8
La información capturada debe tener identificadores, lo mismo que la información médica mínima requerida para establecer un diagnóstico adecuado.	HIPPA 9
Los dispositivos de captura que tengan contacto con el paciente, deben cumplir con los requisitos mínimos que garanticen su integridad física.	HIPPA 10
Los sistemas de Telemedicina requieren de conexiones remotas.	HIPPA 11
Los dispositivos de diagnóstico médico requieren de un ancho de banda específico y sofisticadas interfaces con el usuario.	
Contar con una conexión a Internet (Banda ancha), y equipos con ciertas características de capacidad en disco duro, memoria RAM y procesador.	
Implementar políticas y procedimientos para garantizar que todos los miembros de un equipo de trabajo, tengan acceso adecuado a información electrónica de salud de acuerdo con lo establecido.	HIPPA 12
Implementar políticas y procedimientos para garantizar que quienes no tengan acceso no conozcan la información médica.	HIPPA 13
Realizar evaluaciones técnicas y no técnicas de manera periódica, basadas en la aplicación de normas.	HIPPA 14

Tabla 7. Requerimientos para almacenamiento, acceso y transmisión de información médica según COBIT. [50]

Requerimiento	ID
Implementar procedimientos para verificar la identidad de la persona o entidad que solicite el acceso a la información electrónica de salud protegida.	CO 1
Debe existir una limitante en los intentos de acceso.	CO 2
Copias de seguridad guardadas en sitio diferente.	CO 3
Para transmitir la información médica, se debe usar protocolos de comunicaciones de red que garanticen que los datos enviados sean los datos recibidos.	CO 4

Implementar mecanismos para cifrar y descifrar la información protegida de salud electrónica.	CO 5
Mantener registro de accesos, autorizados y denegados a la información medicas y guardar estos registros durante dos años.	CO 6
Inventarios de los equipos que tiene la institución médica.	CO 7
La configuración de los equipos de despliegue debe cumplir los estándares mínimos para garantizar la interpretación adecuada de la información por parte del receptor.	CO 8
Exigir a cada persona, una contraseña o PIN	CO 9

De acuerdo con cada uno de los servicios de Telemedicina y los requerimientos que se concentran en las normas evaluadas, se puede establecer que todos los servicios necesitan de cada requerimiento anteriormente especificado, respecto del almacenamiento, acceso, transmisión de información, recurso humano y equipos. La implementación de los requerimientos varía de acuerdo con el nivel de complejidad del servicio y de la entidad que presta dicho servicio.

4. ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE TELEMEDICINA

Para poder establecer mecanismos de prevención y protección de la información en redes de Telemedicina, se debe determinar las debilidades y defectos denominados vulnerabilidades [51].

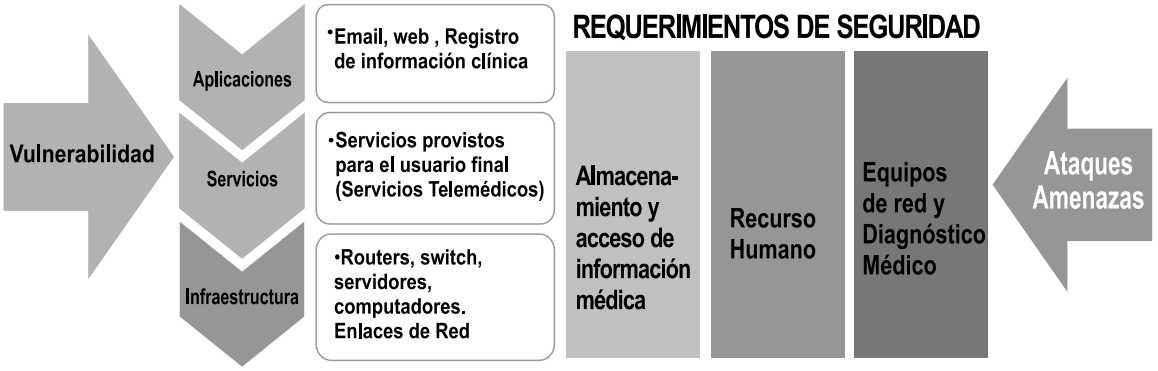

Figura 7. Vulnerabilidades en Redes de Telemedicina

La seguridad y la interoperabilidad se consideran dos de los requisitos importantes en los sistemas de Telemedicina. Por lo general, se intercambia información médica, velando por la protección de datos y prevención del uso no autorizado, mientras se mantiene un alto grado de accesibilidad. La interoperabilidad permite establecer acuerdos de seguridad entre las entidades de salud para el intercambio de datos. Es importante analizar las posibles fallas en redes de Telemedicina, para luego conocer los estándares que ofrecen supervisión y mecanismos para mitigar estas fallas requerimientos de seguridad. En la Figura 7, se describe un esquema que permite ver que las amenazas en una red, siempre están presentes y pueden afectar las aplicaciones sobre una red de Telemedicina [52] y [53].

4.1 Análisis de vulnerabilidades y riesgos

El análisis de los riesgos a los cuales se expone la información en una red de Telemedicina, permite determinar el alcance de los posibles daños a la integridad de la información médica, generados por las vulnerabilidades en una red de Telemedicina.

Al igual que las redes de datos, las redes de Telemedicina están expuestas a una gran cantidad de amenazas debidas a las vulnerabilidades del sistema. La presencia de vulnerabilidades y amenazas en la red, genera un riesgo asociado a la afectación total o parcial de la información. El riesgo puede definirse como el daño potencial causado por una amenaza que puede explotar las vulnerabilidades de un activo; el activo en el caso de la Telemedicina, es la información médica que se maneja sobre la red.

El riesgo se determina por la presencia de una amenaza y al menos, una vulnerabilidad. Las amenazas se refieren a la probabilidad de ocurrencia de un evento que puede afectar el sistema en un tiempo dado, y las vulnerabilidades se refieren a la magnitud de la intensidad de los daños sufridos frente al impacto de un evento [54].

4.1.1 Nivel de efecto: El efecto es la repercusión negativa sobre el rendimiento de la red, causada por la explotación de una vulnerabilidad [55]. En la Tabla 8, se puede apreciar la clasificación del efecto, de acuerdo con el nivel de exposición del sistema a determinada vulnerabilidad.

Tabla 8. Clasificación del efecto [55]

Nivel	Descriptor	Descripción
3	Alto	Pérdida total de la información. Cambios o daños irreversibles. Copias de la información por personas inescrupulosas.
2	Medio	Daños reversibles a la información, requiere de una serie de procesos para recuperar los datos perdidos o modificados. Ayuda externa para buscar solución al problema
1	Bajo	Acceso a la información de personas no autorizadas, sin sufrir modificaciones o pérdidas. Procedimientos locales para solucionar el problema.

4.1.2 Nivel de riesgo: El nivel de riesgo define la clasificación del riesgo asociado a la afectación del activo, según la estimación de la probabilidad de que una amenaza se haga efectiva. La clasificación del riesgo puede apreciarse en la Tabla 9.

Tabla 9. Clasificación del riesgo [55]

Nivel	Descriptor	Descripción
3	Alto	Se genera un riesgo en el sistema con una probabilidad igual o mayor al 40% de que una amenaza se haga efectiva.
2	Medio	Se genera un riesgo en el sistema con una probabilidad de entre el 20% y el 40% de que una amenaza se haga efectiva.
1	Bajo	Se genera un riesgo en el sistema con una probabilidad menor al 20%.

Para determinar el nivel de riesgo promedio en donde se encuentra el activo, es necesario aplicar la ecuación 1 [55].

$$\overline{Nivel\ de\ riesgo} = \frac{\sum Clasificación\ del\ Riesgo}{Número\ de\ Activos} \quad \textbf{(1)}$$

La fórmula anterior determina en cuál nivel de la clasificación de riesgo se encuentra la información médica, para poder evaluar de acuerdo con las vulnerabilidades, amenazas y requerimientos de seguridad, las medidas preventivas o correctivas necesarias para evitar daños a la información de los pacientes.

4.2 Estrategias de Implementación de seguridad sobre los servicios de Telemedicina

Es importante tener en cuenta que la información médica que se maneja en Telemedicina, es en general de tipo confidencial y por lo tanto, requiere ser protegida de ataques y amenazas que puedan afectar el derecho a la intimidad, la privacidad y la protección de los datos de los pacientes. Estos ataques pueden afectar los datos que se encuentren encriptados o no, por medio de técnicas de hurto de información como lo son los programas espía (spyware), los virus y troyanos, el acceso no autorizado a la información, la alteración o deterioro total o parcial de la información. Para ello, es importante definir metodologías y estándares que puedan ser aplicados y así garantizar la seguridad sobre el manejo de información médica en Telemedicina.

El proceso para garantizar la seguridad informática tiene varios puntos para tener en cuenta. La definición de estrategias es uno de los primeros pasos y trae consigo el estudio de la situación actual y de la definición de requerimientos, de acuerdo con el objetivo de la aplicación o servicio de Telemedicina. Después de la definición, se debe realizar producción y ejecución de las estrategias. Pero no basta con la simple ejecución de las estrategias para garantizar la seguridad sobre la información médica; también es necesario el monitoreo de estas estrategias. El monitoreo permite identificar vulnerabilidades sobre las estrategias para fortalecer los mecanismos usados para mantener la seguridad. Para definir una estrategia, cada proceso se

realimenta con los otros, sí generando un ciclo entre los procesos principales como se ve en la Figura 8 [56].

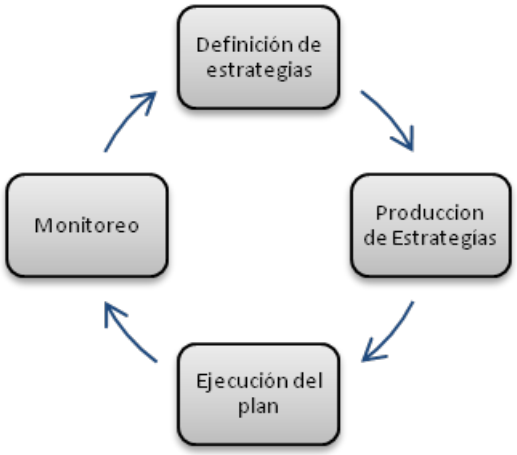

Figura 8. Ciclo de planeación de estrategias de implementación de seguridad en un sistema

Específicamente para Colombia, no existe una estrategia, normatividad o metodología específica que pueda ser tomada y aplicada como referencia con respecto de la seguridad informática en salud; aún así, existen las Resoluciones 1448 de 2006 y 3763 de 2007 que rigen la Telemedicina en el País [57] y [58], pero no existen estándares generales que puedan ser aplicados en las entidades de salud colombianas. Por esta razón, este artículo trabaja sobre las normas HIPPA, COBIT y CALDICOTT para definir de requerimientos y conservar la integridad de los datos del paciente, sin dejar de lado que existen otras normas que ayudan a regular estos procesos como la ITU- SG 16 y 17, ITU- D, entre otras [59] y [61].

Por otra parte los servicios de Telemedicina y sus respectivas especialidades, para poder ser llevados a cabo, requieren de aplicaciones como videoconferencia, teleconferencia, transferencia de archivos, chat/mail y acceso a web. Estas aplicaciones pueden ser usadas por uno o varios servicios, dependiendo del tipo de servicio. Por esta razón, la seguridad sobre la información médica debe estar considerada sobre estas aplicaciones que respaldan los servicios de Telemedicina.

La seguridad en una videoconferencia no es sólo de vital interés para una empresa, sino que debe ser considerada siempre en cualquier ámbito. Recientes regulaciones gubernamentales como HIPAA y la Ley Sarbanes-Oxley de 2002, establecen que los proveedores médicos, instituciones financieras y otras corporaciones deben proteger todos los datos electrónicos asociados con sus clientes y pacientes. Esto incluye todas las transmisiones electrónicas de datos personales del cliente e incluso, las videoconferencias [62] y [63].

La teleconferencia es otra aplicación presente en la Telemedicina, y sus principios de seguridad están enfocados sobre el control de acceso. Las conferencias telefónicas son "sólo por invitación", como un evento, cuando cierto control en el acceso se integra en el proceso de invitación. Los servicios de seguridad deseados por las partes, varía según la naturaleza de la teleconferencia y por lo general, la confidencialidad de datos tiene prioridad sobre los requisitos de seguridad [64] y [65].

La Telemedicina tiene un contexto más amplio que sólo las aplicaciones de la teleconferencia y el video conferencia, debido a que también requiere de la transferencia de archivos. Esta aplicación permite intercambiar archivos que contienen la historia clínica del paciente se encuentra información confidencial y sensible a la cual no deben acceder personas no autorizadas; para proteger la privacidad del paciente. La manera más común de proteger esta información es por medio del uso de la criptografía [66] y [68]. Gracias a que la Telemedicina permite a las entidades medicas aumentar la eficiencia de sus operaciones, mantener y administrar las aplicaciones que utilizan una interfaz de navegador de Internet, uno de sus objetivos es proporcionar a los especialistas, la seguridad necesaria en comunicación para la transferencia y almacenamiento de datos e imágenes médicas [69] y [70].

Una vez se definen las estrategias de implementación de seguridad sobre las aplicaciones que soportan los servicios de telemedicina, viene el proceso para verificar el manejo de estas estrategias. Mediante un análisis, el monitoreo y la verificación permiten determinar vulnerabilidades de alto riesgo como huecos de seguridad, con alta tasa de explotación que permitan acceso total no monitoreado sin dejar rastro o que puedan poner vidas en peligros. Estas vulnerabilidades deben ser reportadas al cliente con una solución práctica tan pronto sean encontradas. La verificación hace un seguimiento del cumplimiento de los requerimientos con herramientas y pruebas como negación de Servicio. Los resultados de los análisis esperan dar información recopilada sobre una ventana de tiempo para proveer una revisión adecuada de los sistemas y procesos de seguridad e incluir soluciones prácticas orientadas a resolver los problemas de seguridad encontrados y no sólo las medidas de seguridad fallidas [71].

5. EVALUACIÓN DE LOS SERVICIOS DE TELEMEDICINA

A partir de los requerimientos estudiados en la sección anterior, se establecen algunas comparaciones y características de los servicios de Telemedicina, comprobando particularidades comunes de uso del servicio y lo concerniente al manejo de la información médica. De acuerdo con las características de los servicios de Telemedicina, en la Tabla 10 se presenta la relación entre aquellos y las principales aplicaciones que pueden intervenir en sus procesos. Algunas aplicaciones se usan por varios servicios, lo cual facilita que estos últimos puedan ser ejecutados, reduciendo la necesidad de implementar infraestructuras especiales para cada uno.

Tabla 10. Servicios y aplicaciones de Telemedicina

Aplicaciones / Servicios	Video-conferencia	Tele-conferencia	Transferencia de archivos	Chat/mail	Acceso web
EHR			√		√
Tele-Endoscopia	√		√	√	√
Tele-Dermatología	√	√	√	√	√
Tele-Oftalmología	√	√	√	√	√
Tele-Otorrinolaringología	√		√	√	√
Tele-Psiquiatría	√	√		√	√
Tele-Fisioterapia	√			√	
Tele-Prescripción	√	√	√		
Tele-Radiología			√	√	
Tele-Patología	√		√	√	
Tele-Cardiología	√	√	√		√

La evaluación de los servicios y sus aplicaciones, muestra que hay servicios que pueden llegar a utilizar todas las aplicaciones, mientras que otros sólo emplean algunas de ellas. En cualquiera de los casos, según el tipo de aplicaciones que se involucren en los servicios, se generan algunos requerimientos en cuanto a seguridad de la información, que hace necesario tomar algunas medidas preventivas para su protección. Los principales mecanismos de seguridad para proteger la información en Telemedicina, se muestran en la Tabla 11.

Tabla 11. Mecanismos de seguridad para las aplicaciones de Telemedicina

Medidas de seguridad / Aplicaciones	Autenticación	Acceso a la información por parte del paciente	Cifrado de la información	Copias de seguridad de la información
Teleconferencia / llamadas Telefónicas	√	√	√	
Videoconferencia	√	√	√	
Intercambio de mensajes entre especialistas	√		√	
Envío del diagnóstico por el especialista	√	√	√	√
Registro, consulta y actualización de la información del paciente	√		√	√
Consultas y actualización del EHR	√		√	√

Para ejecutar todas las aplicaciones utilizadas por los servicios, es necesario que los usuarios y administradores que utilicen los servicios de Telemedicina, puedan autenticarse con un nombre de usuario y una contraseña única. Los pacientes pueden tener o no, acceso a la información médica generada en los procedimientos que se realizan en las sesiones de Telemedicina. Cierta información médica debe ser cifrada para impedir el acceso de persona no autorizada a la información médica. La Tabla 12 muestra la relación entre la relación de autorización y el acceso a la información médica según el tipo de usuario, en un esquema en donde se involucran especialistas, pacientes y el tipo de información al cual cada uno de ellos puede acceder.

Tabla 12. Relación de autorización y acceso a la información según el tipo de usuario

PROFESIONALES	Acceso a la base de datos de la información médica	Acceso al EHR de cada paciente	Permisos para establecer sesiones de Tele- y videoconferencia	Permisos para enviar y recibir resultados de exámenes	Información acerca del servicio, hoja de vida de profesionales
Admon. de red	√		√		√
Enfermera		√	√	√	√
Médico	√	√	√	√	√
Especialista	√	√	√	√	√
Paciente			√	√	√
Usuario externo					√

Es importante mencionar que el grupo de trabajo médico se compone de médicos, especialistas y enfermeras. Los especialistas médicos tendrán acceso total de información médica relacionada con pacientes, mientras que las enfermeras tendrán un acceso parcial. La Tabla 13 muestra los principales requerimientos de seguridad que demandan la transmisión y el manejo de la información médica, y establece una relación con los estándares mencionados en la sección 3, para cumplir con estos requerimientos. Además, se clasifica cada requerimiento según el tipo de riesgo que generaría su ausencia en el sistema y el nivel de impacto que causaría una amenaza, si no se cumple con cada requerimiento.

Tabla 13. Requerimientos/vulnerabilidades de seguridad y estándares para información médica

ID	Estándar / Requerimientos	HIPAA	COBIT	CALDICOT	Nivel de riesgo	Nivel de impacto
R_1	Sistemas de autenticación e identificación de personas que acceden a la información.	√	√	√	3	2
R_2	Exigir contraseña o PIN de acceso a cada persona.	√	√	√	3	2
R_3	Límite de los intentos de acceso.		√		3	2
R_4	Normas, políticas, protocolos o guías para garantizar la confidencialidad, privacidad y seguridad de la información	√		√	2	1
R_5	Cifrado de la información antes de ser enviada	√	√	√	2	1

R_6	Acceso a Internet a las redes de Telemedicina	√			1	1
R_7	Protocolos o estándares de comunicaciones de red que garanticen que los datos enviados sean los datos recibidos (no repudio).	√	√	√	3	3
R_8	Registro del número de accesos autorizados y denegados a la información médica por persona.		√	√	3	2
R_9	Interoperabilidad entre nuevos sistemas y sistemas existentes.			√	2	1
R_{10}	Formato de intercambio de información para permitir que sólo los miembros de un grupo de trabajo tengan acceso a la misma.	√		√	3	3
R_{11}	Firma asíncrona: el emisor usa una clave privada, y el receptor puede verificar su autenticidad por medio de la clave pública del emisor.			√	3	2
R_{12}	Los procesos para transmitir datos pueden ser aplicados al almacenamiento de datos			√	2	1
R_{13}	El Recurso Humano debe estar acreditado para ofrecer sus servicios según la reglamentación vigente.	√			3	2
R_{14}	Es necesario establecer políticas y procesos para actuar frente a una emergencia u otro incidente en el cual se pueda alterar los sistemas que contienen información de salud.	√			3	3
R_{15}	Debe hacerse copias de seguridad de la información y guardarlas en sitio diferente al sitio donde se encuentren los sistemas.		√		3	3
R_{16}	Los sistemas de Telemedicina requieren de conexiones remotas.	√			2	1
R_{17}	Es recomendable manejar bases de datos separadas, una en donde se encuentre el contenido de los datos principales del paciente y otra con los datos que permiten identificar a un individuo.			√	2	2
R_{18}	Los dispositivos de captura que tengan contacto con el paciente, deben cumplir con los requisitos mínimos para garantizar su integridad física.	√			2	1
R_{19}	Realizar evaluaciones periódicas basadas en la aplicación de normas y en respuesta a cambios ambientales u operacionales que afectan la seguridad de la información	√			3	2
R_{20}	Implementar políticas y procedimientos para garantizar que quienes no tienen acceso, no conozcan la información médica, y quienes sí, lo hagan bajo ciertas circunstancias.	√		√	3	3

Los valores que fueron asignados en la Tabla 13 para evaluar el impacto de la no implementación de un requerimiento en una red de Telemedicina, se evalúan según los niveles de efecto y riesgo descritos en las Tablas 8 y 9, respectivamente. Las matrices evaluadas

permiten observar que los estándares regulatorios especialmente diseñados para el manejo de la información médica, establecen requerimientos básicos y complejos de seguridad que varían de acuerdo con la finalidad del servicio y la infraestructura en particular, donde se implementan los requerimientos. La Figura 9 muestra de manera grafica, el nivel de riesgo e impacto en donde se encuentra un sistema de Telemedicina, si no cumple con cada requerimiento establecido anteriormente. La falta de implementación de requerimientos relacionados para garantizar la confiabilidad de la información (R7), limitar el acceso (R10, R20), y mantener respaldo de la información médica (R14 y R15), representan el nivel de riesgo e impacto más alto, como se observa en la Figura 9.

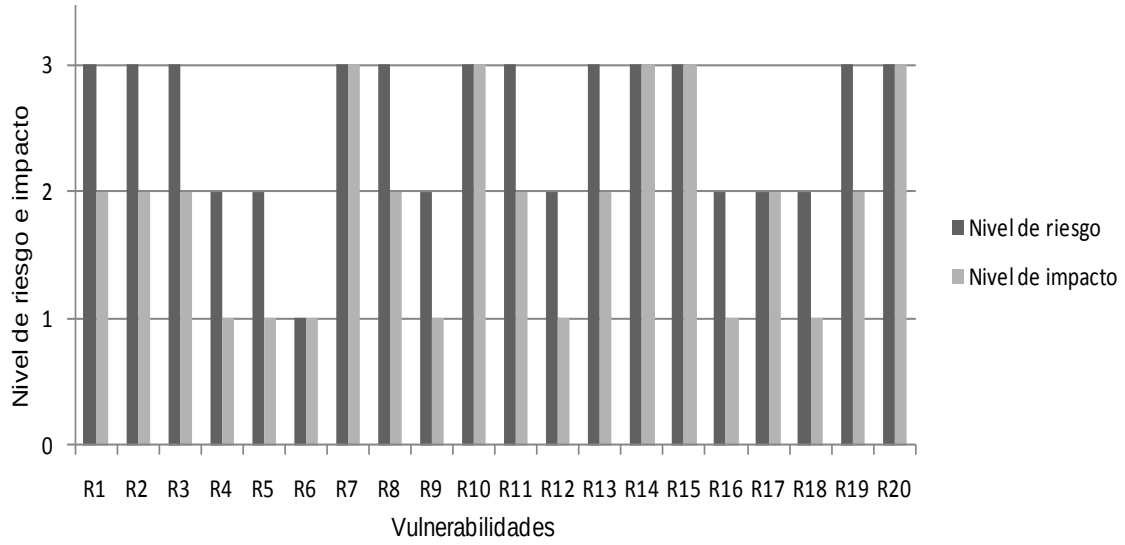

Figura 9. Nivel de riesgo e impacto de las vulnerabilidades de las Redes de Telemedicina

Cada requerimiento de seguridad representa la existencia de una vulnerabilidad en el sistema, es decir, si el sistema no cumple con alguno de los requerimientos, se corre el riesgo de que alguna amenaza de afectación o modificación a la información médica, pueda generar un impacto negativo en la integridad de la misma. La ecuación 1 nos brinda la posibilidad de conocer en qué nivel de riesgo se encuentra un sistema de Telemedicina, debido a la falta de implementación de requerimientos.

$$\overline{Nivel\_de\_riesgo} = \frac{51}{20} \qquad \overline{Nivel\_de\_riesgo} = 2{,}55 \approx 2$$

Con lo cual se puede concluir que un sistema de Telemedicina que no cumpla con los requerimientos propuestos anteriormente, se encontraría en un nivel de riesgo alto, con una probabilidad entre el 40% y el 100% de que una amenaza se haga efectiva.

Además, en la Tabla 14, se muestra la relación de los requerimientos de seguridad básicos tomados de la Tabla 13 para cada especialidad médica que se tuvo en cuenta para desarrollar este artículo. Los requerimientos necesarios para cada servicio se marcan sobre cada servicio con una (x). Esta tabla fundamentalmente está reflejando qué requerimientos (R_n) se consideran básicos en las especialidades en Telemedicina. La tabla permite ver que existen requerimientos que son necesarios para todas las especialidades. También es importante destacar que toda la información proveniente de cada especialidad, está condensada en el registro clínico electrónico (EHR); por esta razón, este es el servicio que incluye la mayoría de los requerimientos.

Tabla 14. Requerimientos básicos de seguridad para el acceso de los servicios de Telemedicina

Servicios / Requerimientos	A	B	C	D	E	F	G	H	I	J	K
R_1	x					x		x			
R_2	x	x	x	x	x	x	x	x	x	x	x
R_3	x					x		x			
R_4	x	x	x	x	x	x	x	x	x	x	x
R_5	x	x	x	x	x		x		x	x	x
R_6	x							x			
R_7	x	x	x	x	x	x	x	x	x	x	x
R_8	x							x			
R_9	x	x	x	x	x	x	x	x	x	x	x
R_{10}	x	x	x	x	x	x	x		x	x	x
R_{11}	x							x			
R_{12}	x	x	x	x	x			x	x	x	x
R_{13}	x	x	x	x	x	x	x	x	x	x	x
R_{14}	x	x	x	x	x	x	x	x	x	x	x
R_{15}	x										
R_{16}	x	x	x	x	x	x	x	x	x	x	x
R_{17}	x					x		x			
R_{18}		x	x	x	x		x		x	x	x
R_{19}	x	x	x	x	x	x	x	x	x	x	x
R_{20}	x							x			

Rn=Requerimientos, A=EHR, B= Tele-endoscopía, C= Tele-dermatología, d= Tele-oftalmología, E= Tele-otorrinolaringología, F= Tele-psiquiatría, G= Tele-fisioterapia, H= Tele-prescripción, I= Tele-radiología, J= Tele-patología, K= Tele-cardiología

6. CONCLUSIONES

Los estándares y regulaciones sobre el manejo y transmisión de la información médica como HIPPA y CALDICOTT, son herramientas que permiten mitigar las vulnerabilidades que pueden presentarse en servicios de Telemedicina, reduciendo la necesidad de implementar sistemas de seguridad para cada servicio.

HIPAA define de manera muy detallada y completa, los requerimientos para manejar información médica. Esta norma evalúa distintos aspectos para conservar la integridad de la

información médica, la exigencia de recurso humano calificado, planes de contingencia, evaluaciones periódicas de operación, y transmisión de información médica. De acuerdo con el detalle que se maneja en HIPPA en el aspecto de seguridad, hace que esta norma sea considerada entre los demás estándares de regulación de información médica, como una de las más solidas y utilizadas en redes de Telemedicina.

Las entidades de salud que prestan servicios de Telemedicina deben implementar mecanismos para proteger de la información médica de los pacientes. Estos mecanismos están definidos en regulaciones internacionales diseñadas específicamente para manejar la información del sector salud. La implementación de estos mecanismos permite mejorar la calidad del servicio hacia los pacientes.

De acuerdo con el análisis realizado en este artículo, es posible concluir que la definición de requerimientos sobre seguridad en redes de Telemedicina, está enfocada sobre cuatro puntos principales: Almacenamiento y acceso de la información médica de los pacientes, Transmisión de la Información, Recurso Humano y Equipos de red y diagnóstico médico. Las matrices evaluadas permiten ver que los estándares regulatorios definidos para manejar la información médica, determinan requerimientos fundamentales y de mayor complejidad que varían de acuerdo con la finalidad del servicio y la infraestructura en particular, donde se implementan los requerimientos.

Luego de analizar los principales requerimientos de seguridad en redes de Telemedicina, se evaluó el nivel de riesgo e impacto que puede generar la no implementación de estos requerimientos y poner en peligro la confiablidad de la información médica o del sistema de Telemedicina. A partir de la evaluación, se hace evidente que evadir requerimientos tales como: implementar protocolos de comunicaciones, mantener un respaldo de la información médica, limitar acceso de personal y definir políticas de acceso a la información médica, generan niveles de riesgo alto que afectarían de manera considerable una red de Telemedicina.

REFERENCIAS BIBLIOGRÁFICAS

[1] Komiya, R. A proposal for Tele-medicine reference model for future standardization. HEALTHCOM 2005. Proceedings of 7th International Workshop.

[2] Yajiong, Xue and Huigang, Liang. Analysis of Tele-medicine Diffusion:The Case of China. IEEE transactions on information technology in biomedicine. Vol. 11(2), march 2007.

[3] Health Insurance Portability and Accountability Act (HIPAA). Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices 1996.

[4] Caldicott, Dame Fiona Report on the review of patient-identifiable information Department on Heath and British Medical association, December 1997.

[5] Ferrante, F. Maintaining Security and Privacy of Patient Information. Proceedings of the 28th IEEE EMBS Annual International Conference New York, aug 30 - sept 3, 2006.

[6] Maji, A.K., Mukhoty, A., Majumdar, A.K. ; Mukhopadhyay, J., Shamik, Sural, Paul, S., and Majumdar, B. Security analysis and implementation of web-based Tele-medicine services with a four-tier architecture Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare 2008.

[7] En: http://www.phiprivacy.net/?p=6389

[8] En:http://www2.alabamas13.com/news/2011/jun/29/alabaster-woman-indicted-hospital-patient-informat-ar-2043896/

[9] Estándar ISO/TR 16056-1. Health Informatics: Interoperability of Tele-health Systems and Networks ISO Press.

[10] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., and Schooler E. SIP: Session Initiation Protocol IETF RFC 3261, junio 2002.

[11] International Tele-communication Union (ITU) Recomendación ITU-T H.323, diciembre de 2009.

[12] Postel J. User Datagram Protocol IETF RFC 768, agosto 1980.

[13] Documentación de Digital Imaging and communications in Medicine En: http://dicom.nema.org/

[14] Documentación Health Level 7 (HL7).En: http://www.hl7.org/

[15] Sheng, O., Hu, P., Chih-Ping, W., and Pai-Chun, Ma. Organizational management of Tele-medicine technology: conquering time and space boundaries in health care services. Engineering Management, IEEE Transactions, 2002.

[16] Miserque N. Programa Galaxia Fundación Cardiovascular de Colombia Floridablanca – Santander. Departamento Nacional de Medicina Área de Telemedicina. En: Revista eSalud. Vol. 1. Fesalud. 2005.

[17] Centro de Telemedicina de Colombia. En : http://www.colombianTelemed.com/content/blogcategory/1/2/lang,spanish/

[18] Zhang G. H., Carmen, C. Poon Y., Member, IEEE, Ye. Li, and Zhang Y. T. A Biometric Method to Secure Tele-medicine Systems. 31st Annual International Conference of the IEEE EMBS Minneapolis, september 2-6, 2009.

[19] Wallauer Jader, von Wangenheim Aldo, Andrade Rafael, Macedo Douglas D. J. de, A Telemedicine Network Using Secure Techniques and Intelligent User Access Control, 21st IEEE International Symposium on Computer-Based Medical Systems, pp. 1-3.

[20] Bingyi Hu, Jing Bai, and Datian, Ye. An internet based communication server for Telemedicine. The Department of Electrical Engineering, The School of Life Science and Engineering Tsinghua University, Beijing. Proceedings-19th International Conference - IEEE/EMB, oct. 30 - nov. 2, 1997 Chicago.

[21] Shaikh, Asadullah y Misbahuddin, Muhammad. A system design for a Tele-medicine health care system, Tesis de Maestría en Ingeniería de Software y Gestión. University of Goteborg. Department of Applied information Technology, 2007.

[22] Zvikhachevskaya, Anna, Markarian, Garik, and Mihaylova, Lyudmila. Quality of Service consideration for the wireless Tele-medicine and e-healt services WCNC 2009 proceedings, IEEE, 2009.

[23] Yajiong, Xue and Huigang, Liang. Analysis of Tele-medicine Diffusion:The Case of China. IEEE transactions on information technology in biomedicine, Vol. 11 (2), march 2007.

[24] Sicurello, Francesco Some Aspects on Tele-medicine and Health Network Referent of Italian Ministry of Foreign Affairs for Tele-medicine, CNR- Institute of Biomedical Advanced Technology, Milan.

[25] Toninelli, Alessandra Montanari, Rebecca, and Corradi Antonio, Enabling secure service discovery in mobile healthcare enterprise networks. University of Bologna. In: IEEE Wireless Communications Magazine june 2009.

[26] Sicurello Francesco Some Aspects on Tele-medicine and Health Network Referent of Italian Ministry of Foreign Affairs for Tele-medicine. CNR- Institute of Biomedical Advanced Technology, Milan.

[27] Organización Panamericana de la Salud OPS/OMS, ORAS-CONHU Organismo Andino de Salud. Aplicaciones de Tele-comunicaciones en la salud en la Subregión Andina. Serie Documentos Institucionales, 2000.

[28] Guillén, E., y Ramírez, Leonardo. Validación de Políticas de Seguridad en la Práctica Social. Universidad Militar Nueva Granada, 2010.

[29] Andriyan B., Suksmono U., Sastrokusumo L.R., Overview of Telemedicine Activities in Indonesia: Progress and Constraints. IEEE 2004.

[30] Fliedner T.M., Weiss, M., Grossmann, H.P., Pieper B., Akleyev, A.V., and Varfolomeyeva, T.A. Tele-consultation in Radiation Medicine Results of regular Tele-medicine consultations between the Health Sciences Centre of the University of Ulm, Germany and Urals Research Centre for Radiation Medicine, Chelyabinsk, 2002.

[31] Grupo de Investigación GITEM Manual de estándares de las condiciones tecnológicas mínimas para las prestación de servicios de salud por Telemedicina Universidad Distrital Francisco José de Caldas, 2004.

[32] Baos G. Tele-oftalmología: Telemedicina en Oftalmología. En: Archivo de la Sociedad Española de Oftalmología, 2. 1998.

[33] Heneghan C., Sclafani A.P,. Stern J., Ginsburg J., Tele-medicine applications in otolaryngology. In: Engineering in Medicine and Biology Magazine. IEEE, 1999.

[34] Reddy N.P, and Gupta V., Computerized biofeedback systems for home care and Tele-therapy. In: Engineering in Medicine and Biology, 1999.

[35] F. da Costa Dias, De Azevedo R.R., Rodríguez C., Danas E, Dias G., and De Barros R. Onto sic: Leveraging the Knowledge in the Treatment and Diagnosis of Tele-psychiatry. Network and System Security. 4th International Conference, 2010.

[36] Foo Siang Fook V., Zhuo Hao S., Phyo Wai A., Jayachandran M., Biswas J., Siew Yee L., and Yap P., Innovative platform for Tele-physiotherapy. In: E-health Networking, Applications and Services. HealthCom 2008. 10th International Conference.

[37] Observatorio Regional de la Sociedad de la Información (ORSI). La Telemedicina al servicio de la Sociedad del Conocimiento. Estrategia Regional para la Sociedad Digital del Conocimiento de Castilla y León (ERSDI), 2007.

[38] Knisley J.R., and. Werchan H.A. Tele-metry: enhancing tactical network management ctical Communications Conference, 1994. Vol. 1. Digital Technology for the Tactical Communicator, 1994.

[39] Ozen N., and Karli B., A Tele-cardiology system design with real-time diagnosis and Tele-consultation. Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008. First International Conference, 2008.

[40] Alfaro L., AlviraM. , M. Coma, Ferrer O., y García M.. Manual de Tele-patología. Club de Informática Aplicada de la Sociedad Española de Anatomía Patológica Pamplona, 2001.

[41] International Tele-communication Union. UIT-T International Tele-communication Union – Tele-communication Sector, 1993.

[42] Health Insurance Portability and Accountability Act (HIPAA) Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices, 1996.

[43] Brand, Koen & Boonen, Harry, "IT Governance based on COBIT 4.0: a management guide Van Haren Publishing, 2004.

[44] Caldicott, Dame Fiona. Report on the review of patient-idetifiable information Department on Heath and British Medical association, December, 1997.

[45] International Organization for Standardization ISO and International Electro technical Commission IEC International Standard ISO/IEC 27000:2009..

[46] International Tele-communication Union UIT-T International Tele-communication Union – Tele-communication Sector, 1993.

[47] CALDICOTT, Dame Fiona. Report on the review of patient-idetifiable information Department on Heath and British Medical association, diciembre, 1997.

[48] Williams, A. The confidentiality, security and sharing of personal data Policy and Procedures for the local health community Version 1.3 Compiled,. 2001.

[49] Melczer H. Security and Privacy Workgroup. 45 CFR PART 160 –general administrative requirements and 45 CFR PART 164 – security and privacy, 2003.

[50] Brand, Koen & Boonen, Harry IT Governance based on COBIT 4.0: a management guide Van Haren Publishing, 2004.

[51] International Tele-communication Union UIT-T International Tele-communication Union – Tele-communication Sector, 1993.

[52] Amiya K. Maji, Arpita Mukhoty, Arun K. Majumdar, Jayanta Mukhopadhyay, Shamik Sural, Soubhik Paul, Bandana Majumdar. Security Analysis and Implementation of Web-based Tele-medicine Services with a Four-tier Architecture. IEEE. Indian Institute of Technology Kharagpur.

[53] Maglogiannis Ilias and Zafiropoulos Elias. Modeling Risk in Distributed Healthcare Information Systems. Proceedings of the 28th IEEE EMBS. Annual International Conference New York City, aug 30- sept 3.

[54] Dillar, Kurt y Pfost, Jared. Guía de administración de riesgos de seguridad. Capítulo 4: Evaluación del riesgo. Microsoft Corporation, 2004.

[55] Echeverry, Juan. Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada. Trabajo de grado. Programa de Ingeniería en Telecomunicaciones, 2009.

[57] Ministerio de la Protección Social. Resolución 1448, 8 de mayo de 2006. En: http://www.fcv.org/Portal/telemedicina/normatividad/1448.pdf (24 de marzo 2012)

[58] Ministerio de la Protección Social Resolución 3763, 18 de octubre de 2007. En: http://www.fcv.org/Portal/telemedicina/normatividad/3763.pdf (24 de marzo de 2012)

[59] International Telecommunication Union, ITU-T Study Group 16: e-health and standardization. En: http://www.itu.int/ITU-T/studygroups/com16/index.asp

[60] International Telecommunication Union, ITU-T Study Group 17 Security En: http://www.itu.int/ITU-T/studygroups/com17/index.asp

[61] International Telecommunication Union, ITU-D: ICT Applications for e-health. En: http://www.itu.int/ITU-D/cyb/app/e-health.html

[62] Weinstein, Ira M. Security for videoconferencing A guide to understanding, planning, and implementing secure compliant ISDN &IP videoconferencing security, .2004.

[63] Mahmoud, Y. Information security strategy in Telemedicine and e-Health systems: A case study of England's Shared Electronic Health Record System. 2010.

[64] Stubblebine, Stuart G. Security Services for Multimedia Conferencing" USC Information Sciences Institute, 1998.

[65] Heffernan, Richard J.and Moberl, Michael D. Trends in Proprietary Information Loss" Advancing security Worldwide International, 2007.

[66] Kovacevic, S., Kovac, M., and Knezovic, J. System for Secure Data Exchange in Telemedicine Faculty of Electrical Engineerign and Computing, Zagreb. 9 International Conference on Telecommunication 2007.

[67] Stallings, W. Cryptography and Network Security, 4th ed. Pearson Prentice Hall, 2006.

[68] Kaufman Charlie, Perlman Radia, and Speciner Mike. Network Security, Private Communication in a Public World, 2nd ed. Prentice Hall, 2002.

[69] Blagosklonov, O., Itti, E., Sabbah, R., and Guiderdoni, P. High-secured cardiac imaging network: Imaging CardioWeb Institute In: cardiology 2002, pp. 345-346.

[70] Itti, R, and Guiderdoni P. Internet nuclear cardiac image circulation, processing and storage: The Cardioweb project. In: Radiology 2000, 217 suppl.:704.

[71] Institute for security and open methodologies. P. Herzog. Open Source Security Testing Methodology Manual. OSSTMM 2.1, 2003.