



INFORME DE TRABAJO

Mesa N° 5

Tema

Telemedicina desde la perspectiva de la ingeniería multidisciplinaria: identificación de aspectos críticos y recomendaciones en el contexto de pandemia COVID-19

Coordinadora responsable

- Gloria Henríquez Díaz

Participantes

- Héctor Barrera Fuentealba (secretario)
- Eduardo Costoya Arrigoni
- Fernando de Mayo Israel
- Antonio Rienzo Renato

Fecha

Agosto - septiembre de 2020



TABLA DE CONTENIDO

| | | |
|-------|--|----|
| 1 | INTRODUCCIÓN | 3 |
| 2 | DIAGNÓSTICO EN RELACIÓN CON LA PANDEMIA DE COVID-19 | 4 |
| 2.1 | SITUACIÓN DE LA TELEMEDICINA EN CHILE PREVIO A LA PANDEMIA..... | 4 |
| 2.1.1 | BREVE HISTORIA | 4 |
| 2.1.2 | ESTADO PRE-PANDEMIA | 4 |
| 2.2 | ASPECTOS CRÍTICOS Y OPORTUNIDADES IDENTIFICADAS PRODUCTO DE LA PANDEMIA.. | 8 |
| 3 | DESCRIPCIÓN DE LOS PRINCIPALES ASPECTOS CRÍTICOS Y OPORTUNIDADES IDENTIFICADOS . | 9 |
| 3.1 | TELECOMUNICACIONES | 9 |
| 3.1.1 | INTRODUCCIÓN | 9 |
| 3.1.2 | SITUACIÓN PRE-PANDEMIA | 11 |
| 3.1.3 | CONTEXTO DURANTE LA PANDEMIA | 13 |
| 3.2 | GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN..... | 15 |
| 3.2.1 | INTRODUCCIÓN | 15 |
| 3.2.2 | SITUACIÓN PRE-PANDEMIA | 17 |
| 3.2.3 | CONTEXTO DURANTE LA PANDEMIA | 19 |
| 3.3 | IoT, TELEMONITOREO Y HOMECARE..... | 22 |
| 3.3.1 | INTRODUCCIÓN | 22 |
| 3.3.2 | SITUACIÓN PRE-PANDEMIA | 23 |
| 3.3.3 | CONTEXTO DURANTE LA PANDEMIA | 26 |
| 4 | RECOMENDACIONES Y CONCLUSIONES | 28 |
| 4.1 | TELECOMUNICACIONES | 28 |
| 4.2 | GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN..... | 28 |
| 4.3 | IOT, TELEMONITOREO Y HOMECARE | 32 |
| 4.4 | RECOMENDACIONES FINALES | 34 |
| 5 | REFERENCIAS..... | 36 |



1 INTRODUCCIÓN

La OMS¹ define la telemedicina como “la prestación de servicios de salud, donde la distancia es un factor crítico, por parte de todos los profesionales de la salud que utilizan tecnologías de la información y la comunicación para el intercambio de información válida para el diagnóstico, tratamiento y prevención de enfermedades y lesiones, investigación y evaluación, y para la educación continua de los proveedores de atención médica, todo ello con el interés de promover la salud de las personas y sus comunidades” [1].

La pandemia de COVID-19 ha mostrado una serie de debilidades en distintos ámbitos, dentro de los cuales la telemedicina no ha quedado exenta y, a pesar de contar con tecnología, infraestructura y expertos en el tema, en países como Chile se ha manifestado cierto grado de desconocimiento conceptual y en procesos (generales y particulares), además de un déficit en disponibilidad de herramientas e instrumentos necesarios para su uso. A esto se agrega que no solo la sociedad, sino que también parte importante de los profesionales de salud y de ingeniería estaban parcialmente en conocimiento de que la telemedicina es una realidad que sucede hace años.

Lo descrito en el párrafo precedente, además de la necesidad impuesta por la situación sanitaria actual, han revelado la necesidad de explorar y usar la telemedicina en todas las áreas que abarca, es decir, desde la teleconsulta hasta el telemonitoreo, pero no solo desde la perspectiva de los profesionales de salud y de los pacientes, sino que también desde la ingeniería y las diferentes disciplinas que esta involucra, dentro de las que se pueden mencionar las especialidades de: eléctrica, electrónica, informática, biomédica, industrial, matemática, entre otras.

El presente documento describe aspectos considerados críticos o que abren espacios u oportunidades en telemedicina producto del contexto de COVID-19 e identificados desde la perspectiva de la ingeniería en las áreas de: (1) telecomunicaciones, (2) seguridad de la información y (3) cuidados domiciliarios a distancia, describiendo la situación previa y durante la pandemia, además de recomendaciones para el periodo posterior.

¹ OMS: Organización Mundial de la Salud



2 DIAGNÓSTICO EN RELACIÓN CON LA PANDEMIA DE COVID-19

2.1 SITUACIÓN DE LA TELEMEDICINA EN CHILE PREVIO A LA PANDEMIA

2.1.1 BREVE HISTORIA

La telemedicina comenzó a desarrollarse en Chile aproximadamente en 1993, investigando dos áreas: comparación de diagnóstico tradicional *versus* tele-diagnóstico y desarrollo de métodos óptimos de colaboración a distancia (educación). Posteriormente, se hicieron transmisiones de imágenes para diagnósticos dermatológicos desde la Isla Juan Fernández vía *e-mail* y módem (1998-1999) y de imágenes radiológicas desde la Antártica (2000-2003), además de la inclusión de internet de alta velocidad para la transmisión de imágenes neuroquirúrgicas (2001) [2], [3].

En los años siguientes, el MINSAL² [2], [4]:

- Implementó el servicio de Tele-electrocardiografía a nivel nacional (2004);
- Creó el Centro de Asistencia Remota en Salud en la Región Metropolitana (2005);
- Creó el Departamento de Asistencia Remota en Salud ampliando Salud Responde a nivel nacional (2007);
- Implementó la Tele-dermatología (2009);
- En 2009 comenzó el Programa Galileo de Telemedicina Cardiovascular como piloto en el Hospital Las Higueras, transformándose luego en un programa oficial de la Macro Red Regional, financiado íntegramente por el MINSAL desde 2012.
- Implementó la Tele-radiología y la Teleasistencia a través de dispositivos móviles (2012);
- Creó la Red de Referencia de Telemedicina en Accidente Cerebrovascular en el Servicio de Salud Metropolitano Sur (2017).

2.1.2 ESTADO PRE-PANDEMIA

Las principales estrategias implementadas en Chile que se han mantenido vigentes en el periodo pre-pandemia se resumen en la Tabla 1 [2].

² MINSAL: Ministerio de Salud



Tabla 1. Principales estrategias implementadas en Chile

| Área | Estrategia | Descripción |
|---|--------------------------|---|
| Tele Informes | Tele Electro-cardiograma | <p><u>Descripción:</u> Pacientes que consultan por dolor torácico acceden a un ECG³ y a su informe a través de una central de informes, confirmándose o descartándose un infarto agudo de miocardio en menos de 20 minutos.</p> <p><u>Implementación:</u> 452 Servicios de Urgencia de Atención Primaria de todo el país.</p> <p><u>Producción:</u> Desde 2005 a diciembre de 2017 se han realizado más de 847.000 informes.</p> |
| | Tele Radiología | <p><u>Descripción:</u> Cubre brechas entre horas contratadas de radiólogos y demanda de informes radiológicos. Compra servicios de informes radiológicos más el servicio de interoperabilidad y transmisión de imágenes.</p> <p><u>Implementación:</u> 34 establecimientos en distintas regiones del país (Unidades de Emergencia y de Paciente Crítico).</p> <p><u>Producción:</u> Desde 2012 a diciembre de 2017 se han realizado 737.498 informes.</p> |
| | Tele Oftalmología | <p><u>Descripción:</u> Screening para detectar Retinopatía Diabética a través de examen de Fondo de Ojo, que es informado por un Oftalmólogo, a través de una plataforma.</p> <p><u>Implementación:</u> 124 Unidades de Atención Primaria Oftalmológicas en 29 Servicios de Salud.</p> <p><u>Producción:</u> Desde 2013 al 31 de diciembre de 2017 se han realizado más de 300.000 informes.</p> |
| Teleconsultas en Atención Ambulatoria, Hospitalización y Urgencia | Tele Dermatología | <p><u>Descripción:</u> Envío de antecedentes clínicos y fotografías por parte de un médico de atención primaria a un especialista dermatólogo, quien evalúa antecedentes y entrega orientación diagnóstica e indicaciones.</p> <p><u>Implementación:</u> 29 Servicios de Salud⁴ a nivel de Atención Primaria.</p> <p><u>Producción:</u> Desde 2009 a diciembre de 2017 se han realizado 79.801 teleconsultas.</p> |

³ ECG: Electrocardiograma

⁴ El MINSAL cuenta con un total de 29 Servicios de Salud a lo largo del país. La Red Asistencial de cada uno está constituida por el conjunto de establecimientos asistenciales públicos más los establecimientos municipales de atención primaria de salud de su territorio y los demás establecimientos públicos o privados que mantengan convenios con el Servicio de Salud respectivo [20].



| | | |
|---|---|--|
| | Teleconsulta Otras Especialidades | <p><u>Descripción:</u> Contacto a distancia entre médicos en etapa de formación, desde Hospitales de Baja Complejidad o Atención Primaria urbana y rural, con especialistas de Hospitales de Mediana o Alta Complejidad.</p> <p><u>Implementación:</u> 28 Servicios de Salud.</p> <p><u>Producción:</u> Desde 2012 a noviembre de 2017 se han realizado 107.705 Teleconsultas.</p> |
| | Teleconsulta en pacientes con Tratamiento Anticoagulante Oral | <p><u>Descripción:</u> Teleconsulta en la especialidad de Medicina Interna, para pacientes que se encuentran con tratamiento anticoagulante oral y requieren control permanente para dosificación de medicamentos.</p> <p><u>Implementación:</u> 5 hospitales de la Región Metropolitana.</p> <p><u>Producción:</u> Desde 2014 a diciembre de 2017 se han realizado más de 13.000 atenciones.</p> |
| Telemedicina en Red de Alta Complejidad y Redes Ges | Telenefrología | <p><u>Descripción:</u> Detección precoz de la enfermedad renal a través del envío de antecedentes clínicos por parte del médico de atención primaria al especialista, quien evalúa y entrega orientación diagnóstica e indicaciones de manejo y/o tratamiento.</p> <p><u>Implementación:</u> 12 Servicios de Salud.</p> <p><u>Producción:</u> Incluida en Teleconsulta Otras Especialidades.</p> |
| | Neuropsiquiatría Infantil | <p><u>Descripción:</u> Evaluación de niños y adolescentes con requerimiento de atención por neuropsiquiatra, a través de videoconferencia móvil.</p> <p><u>Implementación:</u> 11 hospitales a lo largo del país.</p> <p><u>Producción:</u> Desde 2014 a diciembre de 2017 se han realizado 58 atenciones.</p> |
| | Telemedicina en Cáncer | <p><u>Descripción:</u> Implementación de estrategia de telemedicina en la Red de Oncología nacional en cuatro líneas: Comité Oncológico, Patología Oral, Cuidados Paliativos y Alivio del Dolor, Teleconsulta Oncológica.</p> <p><u>Implementación:</u> el Comité Oncológico se encuentra en algunas áreas de trabajo en distintas Macrorregiones, mientras que en otras está presente a nivel nacional; Patología Oral se ha desarrollado en los Servicios de Salud Concepción, Ñuble y Arauco; Cuidados Paliativos ha estado presente en los Servicios de Salud de Talcahuano, Concepción, Araucanía Norte y Viña del Mar.</p> <p><u>Producción:</u> Durante al año 2017 se han realizado 2.427 evaluaciones en comité oncológico, 285 consultas en patología oral y 44 evaluaciones en Cuidados Paliativos.</p> |



| | | |
|-----------------------------------|---|--|
| | Telemedicina en Ataque Cerebro Vascular (ACV) | <p><u>Descripción:</u> Equipo de neurólogos de turno que realicen apoyo a médicos de Unidades de Emergencia de establecimientos que no cuenten con neurólogos de Urgencia, para diagnóstico de ACV en fase aguda y realización de Trombólisis, de acuerdo con indicación y por medio de Tecnologías de Información y Comunicaciones.</p> <p><u>Implementación:</u> 3 hospitales (Regiones Metropolitana y de Atacama).</p> <p><u>Producción:</u> En 2017 se realizaron 293 teleconsultas y 14 teletrombólisis.</p> |
| | Telemedicina en la Red VIH | <p><u>Descripción:</u> Optimizar el manejo de pacientes portadores de VIH/SIDA con complicaciones clínicas y/o dificultades con esquema terapéutico, para lo cual los profesionales reciben asesoría de un equipo de expertos, a través de videoconferencias en las que se plantean orientaciones de manejo y tratamiento.</p> <p><u>Implementación:</u> especialistas de un hospital asesoran al resto de los centros.</p> <p><u>Producción:</u> Desde 2016 reuniones clínicas.</p> |
| | Telemedicina en la Red de Cardiopatías Congénitas Operables | <p><u>Descripción:</u> Comités Cardiológicos en que profesionales de un hospital derivador evalúan a su paciente conjuntamente con especialistas del hospital de referencia, con el fin de determinar plan de acción o de seguimiento, a través de videoconferencia.</p> <p><u>Implementación:</u> un hospital evaluador para 7 Servicios de Salud del país.</p> <p><u>Producción:</u> Durante 2017 se han realizado 17 evaluaciones.</p> |
| | Telemedicina en la Red de Gran Quemado | <p><u>Descripción:</u> Evaluación de pacientes Gran Quemado entre hospital derivador y hospital referente, mediante el envío de antecedentes clínicos y fotografías al especialista a través de una Plataforma.</p> <p><u>Implementación:</u> un hospital de referencia que recibe a pacientes de todo el país.</p> <p><u>Producción:</u> Durante 2017 se evalúa pertinencia de derivación de 113 pacientes.</p> |
| Teleasistencia en la Red de Salud | Salud Responde | <p><u>Descripción:</u> Ofrece un servicio permanente de entrega de información, orientación, educación, asistencia, apoyo y contención en materias de salud, a la que se accede telefónicamente durante las 24 horas del día, los 365 días del año.</p> <p><u>Implementación:</u> destinado a los habitantes de todo el país.</p> <p><u>Producción:</u> Desde 2005 hasta diciembre de 2017 se han realizado más de 6 millones de Teleasistencias.</p> |



2.2 ASPECTOS CRÍTICOS Y OPORTUNIDADES IDENTIFICADAS PRODUCTO DE LA PANDEMIA

El diagnóstico aquí realizado se ha basado en determinar cuáles han sido los aspectos críticos y las oportunidades que se manifestaron al utilizar telemedicina en el contexto de pandemia, identificando los siguientes puntos relevantes:

- Utilización de medios de comunicación para realizar atenciones de salud a distancia;
- Seguridad de la información de las prestaciones de salud realizadas;
- Disponibilidad de equipamiento para la realización de atenciones a distancia.

Los principales aspectos identificados por este equipo de trabajo están en las siguientes tres áreas y se describen en las secciones respectivas:

1. Telecomunicaciones;
2. Gestión de la seguridad de la información;
3. IoT, telemonitoreo y homecare.



3 DESCRIPCIÓN DE LOS PRINCIPALES ASPECTOS CRÍTICOS Y OPORTUNIDADES IDENTIFICADOS

3.1 TELECOMUNICACIONES

3.1.1 INTRODUCCIÓN

La palabra telecomunicaciones conceptualmente se refiere a las comunicaciones a distancia.

Las comunicaciones se pueden clasificar como se muestra en la Figura 1, ya sea en forma conducida o inalámbrica, siempre transportan una onda, solo que en la conducida (como va por un cable) la onda se propaga en forma confinada y guiada.

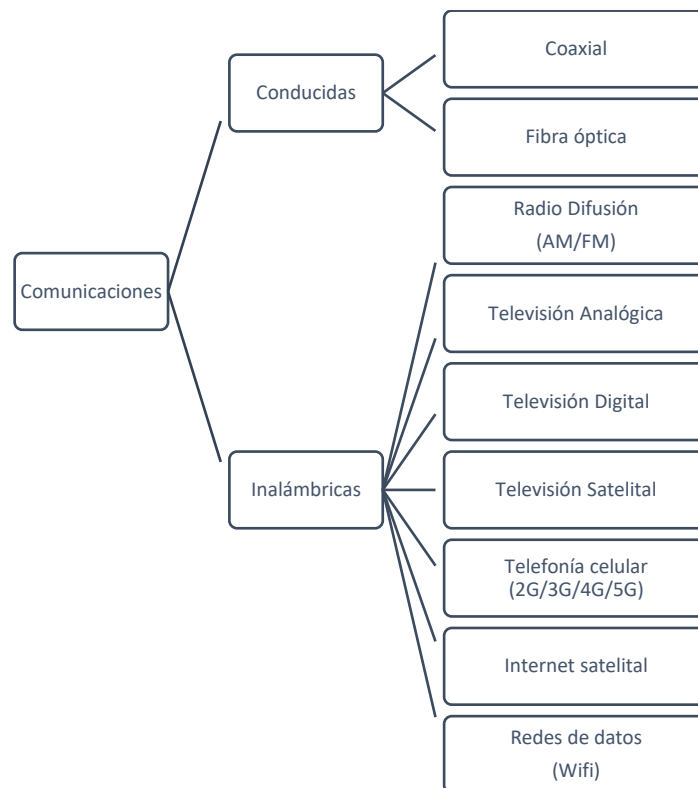


Figura 1. Clasificación de las comunicaciones



Para transmitir información se necesita tres cosas:

- Una portadora (Figura 2);
- Una modulación a través de una señal modulante de variadas formas, por ej., modulación de amplitud (Figura 2);
- Un código: en el caso del código binario la información analógica se transforma en bits.

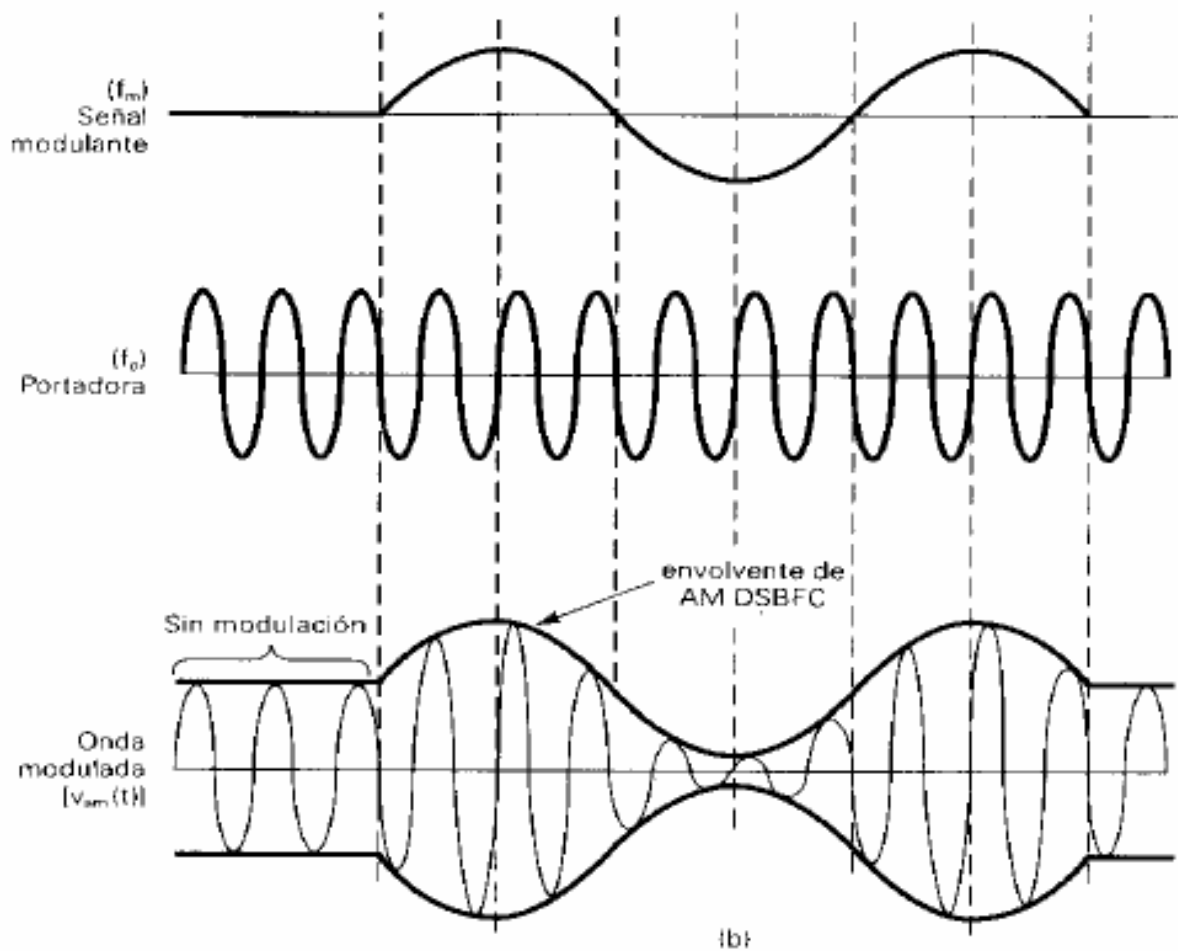


Figura 2. Modulación



Si hay una portadora en F1, al modularla el espectro se ensancha según la magnitud de lo que se va a enviar, lo que ocupa una proporción mayor en el espectro⁵ (Figura 3).

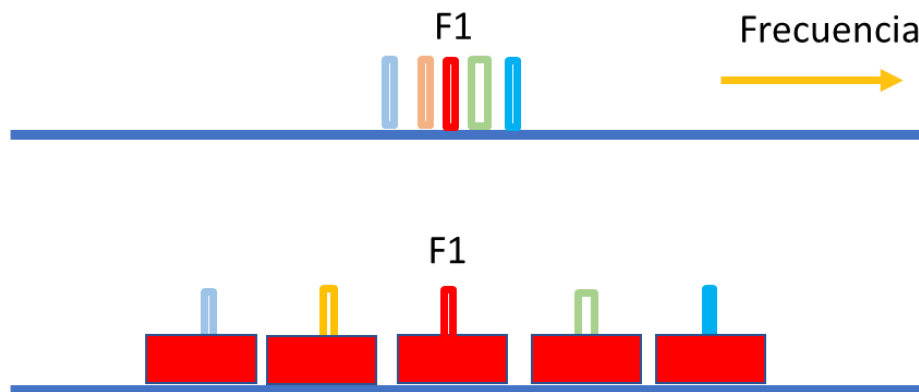


Figura 3. Portadora

3.1.2 SITUACIÓN PRE-PANDEMIA







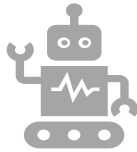
El uso de las telecomunicaciones en telemedicina previo a la pandemia se puede clasificar según el transporte de información como se muestra en la Tabla 2. En ella el orden de los requerimientos no es aleatorio, sino que representa en forma creciente la demanda hacia el sistema de telecomunicación requerido. No obstante, durante la pandemia esta clasificación no ha presentado cambios.

Cabe destacar que la telemedicina, en general, no consume muchos recursos desde la perspectiva de las telecomunicaciones.

⁵ Espectro: es el ordenamiento de frecuencias de todo el espectro electromagnético.



Tabla 2. Información desde la telemedicina a los sistemas de telecomunicaciones para su transporte (Formato digital)

| |  |  |  |  |  |  |  |
|-------------------------|---|---|--|---|---|---|---|
| Orden de requerimientos | 1° | 2° | 3° | 4° | 5° | 6° | 7° |
| Descripción | Alfanuméricos | Información de sensores | Audio | Curvas digitalizadas | Imágenes estáticas de resolución mediana o alta | Imágenes dinámicas de mediana o alta resolución, video | Imágenes bidireccionales dinámicas de alta resolución y baja latencia |
| Ejemplos | Exámenes de laboratorio, instrucciones, etc. | Pulso, saturación de oxígeno, presión arterial, etc. | Interfaz con el paciente, con el tratante, fonoendoscopia, etc. | Electrocardiograma, audiometría, etc. | Scanners, ecografías, radiografías, resonancia magnética. | Angiografía, teleconsulta sincrónica, etc. | Telecirugía y robótica |



3.1.3 CONTEXTO DURANTE LA PANDEMIA

El contexto de las telecomunicaciones durante el periodo de pandemia, incluidos los requerimientos de telemedicina, se puede resumir en la Figura 4. Esta infraestructura se encuentra a nivel de capitales de región, de provincia y ciudades menores (nivel OCDE⁶), pero todavía es deficiente en zonas rurales. Lo que se muestra en color azul es lo que actualmente tiene el sistema y lo verde es lo que se está comenzando a implementar, mientras que las flechas indican la tendencia.

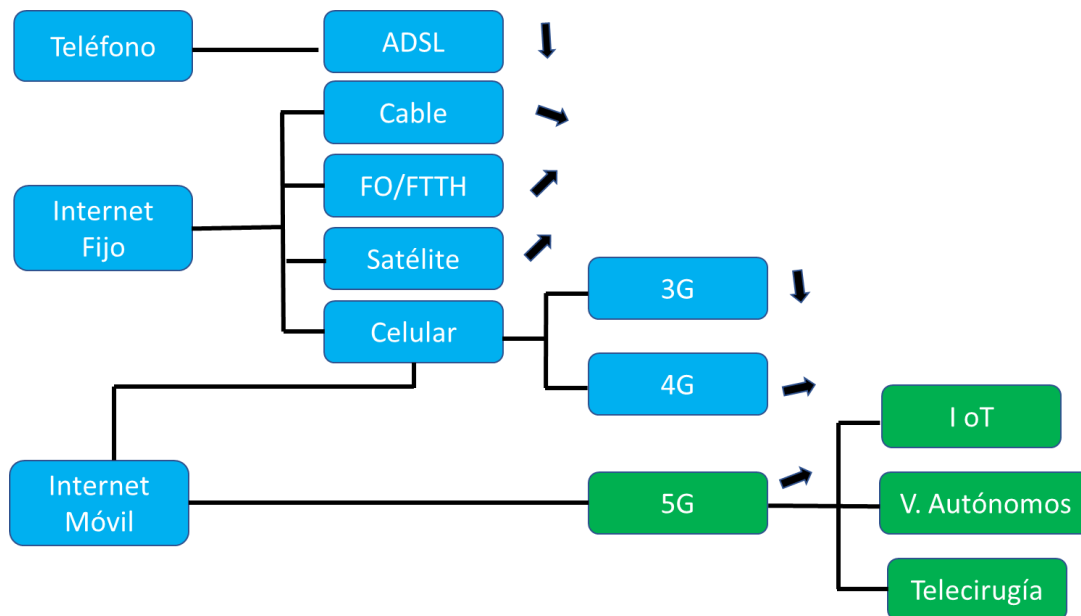


Figura 4. Telecomunicaciones en el presente, futuro y tendencias (Chile)

La telefonía ADSL⁷ (que es teléfono más internet) va en declinación rápida porque no puede dar la velocidad de internet que se requiere en la actualidad.

Internet fijo se transmite por:

- Cable coaxial: va en disminución por costos y capacidad;

⁶ OCDE: Organización para la Cooperación y el Desarrollo Económicos

⁷ ADSL: *Asymmetric Digital Subscriber Line*



- FO⁸ y FTTH⁹: crecimiento exponencial;
- Satélite: los satélites de baja altura (que son los que transmiten internet) van en crecimiento;
- Celular.

Internet móvil se transmite por:

- Celular: lo hace a través de 3G (que está en disminución) y 4G (que va en aumento);
- 5G: está actualmente en licitación y su destino es principalmente para IoT¹⁰, transporte y medicina.

La fibra óptica constituye en la actualidad el medio de mayor capacidad para proporcionar el despliegue de las telecomunicaciones. Chile está en muy buenas condiciones respecto a fibra óptica troncal, sin embargo en la parte rural es notoriamente deficitario. Ello impide el realizar telemedicina básica en zonas rurales apartadas.

El Proyecto FON¹¹, recientemente adjudicado, interconectará 186 comunas en 13 regiones divididas en seis macrozonas, con fibra óptica oscura a disposición de los operadores de sistemas de telecomunicaciones, tanto fijo como móviles (Figura 5). Ello permitiría implementar telemedicina básica en consultorio de regiones apartadas. El proyecto se financia en un 80% por el Fondo de Desarrollo de las Telecomunicaciones.

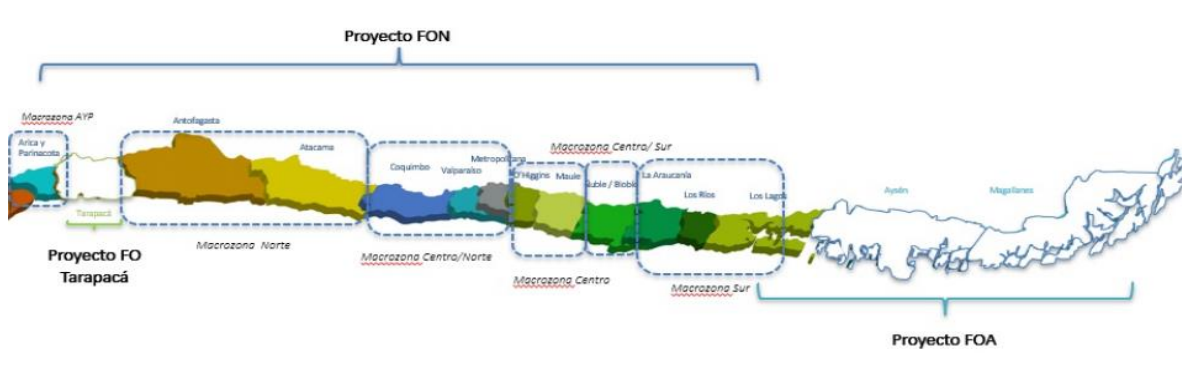


Figura 5. Mapa del Proyecto FON

⁸ FO: Fibra óptica

⁹ FTTH: *fiber to the home*

¹⁰ IoT: *internet of things*

¹¹ FON: Fibra Óptica Nacional



3.2 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.2.1 INTRODUCCIÓN

Si bien con los elementos tecnológicos disponibles en la actualidad la telemedicina es relativamente fácil de desplegar y escalar, mantener cantidades masivas de datos estructurados y no estructurados en forma segura es algo más que un desafío.

Dentro de la atención en telemedicina son intercambiados datos entre el médico y el paciente, los cuales eventualmente pueden ser almacenados. Por otro lado también son intercambiados datos entre distintas unidades de atención, como pueden ser un Servicio de Radiología con un especialista en otra ciudad, región o país.

En este punto es importante tener en cuenta que los datos médicos de una persona (también conocidos como PHI¹²) están clasificados como datos sensibles y especialmente protegidos, por lo que se debe velar por varios aspectos de la seguridad tales como la integridad y privacidad.

En Chile el MINSAL a través de la ley 20584 y la ley 19628 regula aspectos relacionados a distintos aspectos del manejo de la información en el contexto de una atención médica, aspectos que no pueden estar excluidos en el contexto de la telemedicina.

Los datos relacionados a la salud de su persona pueden contener información extremadamente sensible respecto a condiciones que puedan dar motivo a discriminación social, discriminación por parte de compañías de seguros, presiones e intereses comerciales, menoscabo en sus oportunidades laborales o que simplemente se desea mantener en la más estricta esfera privada.

En la Figura 6 podemos ver un mapa con los variados tipos de información sobre la salud de una persona que pueden ser intercambiados y/o almacenados en una atención de telemedicina.

¹² PHI: *Private Health Information*



| | | |
|---|---|--|
| Assessment and Plan of Treatment • Consultation Note • Discharge Summary Note • History & Physical • Imaging Narrative • Laboratory Report Narrative • Pathology Report Narrative • Procedure Note • Progress Note | Laboratory • Tests • Values/Results | Provenance *NEW • Author • Author Time Stamp • Author Organization |
| Care Team Members | Medications • Medications • Medication Allergies | Smoking Status |
| Goals • Patient Goals | Patient Demographics • First Name • Last Name • Previous Name • Middle Name (including middle initial) • Suffix • Birth Sex • Date of Birth • Race • Ethnicity • Preferred Language • Address *NEW • Phone Number *NEW | Unique Device Identifier(s) for a Patient's Implantable Device(s) |
| Health Concerns | Problems | Vital Signs • Diastolic Blood Pressure • Systolic Blood Pressure • Body Height • Body Weight • Heart Rate • Respiratory rate • Body Temperature • Pulse oximetry • Inhaled oxygen concentration • Pediatric Vital Signs *NEW - BMI percentile per age and sex for youth 2-20 - Weight for age per length and sex - Occipital-frontal circumference for children >3 years old |
| Immunizations | Procedures | |

Figura 6. Tipo de información en salud en telemedicina

La información privada de salud se refiere a datos de salud mental y física, ya sea pasada, presente o futura que es creada, recibida, transmitida o almacenada por una entidad de salud y sus asociados. Esta información puede estar relacionada con la provisión de cuidados médicos, las operaciones médicas y los pagos asociados a estas prestaciones.

La información privada de salud incluye toda la información de salud identificable, incluyendo información demográfica, historial médico, resultados de exámenes, información de seguridad social y otra información que pudiera ser usada para identificar un paciente o proveer servicios médicos o coberturas.

Algunos ejemplos de información que debe ser tratado con especial cuidado son [5]:

- Nombres
- Información Geográfica
- Fechas
- Números telefónicos
- Direcciones de correo electrónico
- Números de seguridad social
- Números de registros médicos
- Números de plan de salud
- Números de cuenta corriente
- Números de licencias médicas o certificados
- Número de placa patente de vehículos



- Números seriales o identificadores de aparatos como marcapasos, prótesis, etc.
- Identificadores biométricos como huellas dactilares, de voz, de retina, etc.
- Fotografías
- Información de facturación
- Citas médicas
- Resultados de exámenes de laboratorio
- Resultados de exámenes de imagenología

3.2.2 SITUACIÓN PRE-PANDEMIA

Desde hace más de una década, de la mano de las indiscutibles mejoras en las redes de comunicaciones, es que la telemedicina ha tenido un despegue si bien no masivo, al menos en ciertos nichos en forma firme y constante.

Existe un amplio conjunto de servicios de telemedicina entre los cuales se encuentran los servicios de teleconsulta, telediagnóstico, teleterapia y telemonitorización.

Por ejemplo a nivel nacional es de uso frecuente en consultas de especialidad para zonas rurales, informes médicos de exámenes de imagenología y consultas de salud mental por nombrar algunos casos de uso.

A nivel internacional la práctica de telemedicina está extendida a servicios para cuidado de adulto mayor, así como monitorización de enfermos crónicos mediante dispositivos de IoT, además de cientos de iniciativas públicas y privadas para el desarrollo de aplicaciones que permitan el despliegue de servicios de cuidado y atención médica a distancia con las eficiencias en tiempos y costo que estos implican para el paciente y los profesionales de la salud.

En el modelo de atención presencial, las medidas de seguridad de la información se circunscriben al hospital y sus recursos, pero con la modalidad de telemedicina, se expande el área de recursos en cantidad y distribución geográfica, a ser tomados en cuenta por parte de la gestión de la seguridad de la información.

Si bien la telemedicina es relativamente fácil de desplegar y escalar con las tecnologías de comunicación actualmente disponibles, mantener ingentes cantidades de datos estructurados y no estructurados que esta genera, genera más de un desafío. Por ejemplo, en Estados Unidos, en años anteriores se han perpetrado robos de información médica para realizar fraudes bancarios.

Los datos transitan por ejemplo desde dispositivos de muestreo (IoT) a la terminal del paciente (computadora, *tablet* o *smartphone*), luego a la plataforma del proveedor de salud y luego



al sistema de almacenamiento, en todo el proceso debemos asegurarnos de la integridad del dato así como de su confidencialidad y disponibilidad.

Todas las redes de datos son vulnerables a ataques que buscan provocar el colapso de los sistemas y sustraer datos privados. En el caso particular de las redes de telemedicina, estas pueden ser atacadas por el aprovechamiento de las vulnerabilidades entre las cuales 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.

Un ejemplo claro de 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 90 mil pacientes del hospital a un sitio externo, utilizando la red de la institución y dejando vulnerable la información. Otro ejemplo de afectación a la información médica es el robo de identidad mediante el cual el atacante obtiene información personal de otras personas y la utiliza ilegalmente: en Birmingham, Estados Unidos, en junio del año 2011, una mujer fue acusada de haber robado la identidad de más de 4 mil 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 seguridad social de los pacientes [6].

Por otro lado está el riesgo de que una brecha de seguridad genere un ataque que imposibilite la entrega de la atención médica, ya sea por falta del recurso tecnológico o por falta de los datos necesarios para brindar el tratamiento correcto.

La seguridad y confiabilidad sobre las redes de telemedicina son 2 de los aspectos más relevantes para almacenar, acceder y transmitir la información médica de los pacientes. Analizar estos dos aspectos previene de amenazas y ataques a los sistemas de telemedicina. Dentro de las regulaciones más relevantes existentes que se adaptan a los servicios de telemedicina tenemos:

- ISO 27000, conjunto de estándares internacionales sobre la seguridad de la información;
- COBIT, objetivos de control para información y tecnologías.

Estas normativas deben ser contrastadas con las propias normativas que regulan el manejo de la información en el área de Salud, ya sea a nivel nacional:

- Ley 20584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, entre ellos el derecho de la reserva de la información contenida en la ficha clínica;



- Ley 19628, que regula el trato de los datos de carácter personal, en registros o bancos de datos, por organismos públicos o privados, y es uno de los estatutos normativos más relevantes sobre la materia.

O a nivel internacional:

- HIPPA¹³ (por su acrónimo en inglés), ley de transferibilidad y responsabilidad de seguros de salud;
- Reporte CALDICOTT, informe sobre la revisión de información de identificación del paciente.

A nivel de normativas, un correcto cruce de información sobre las normas propias del ámbito de la salud con aquellas de índole técnico, permiten exponer en forma detallada los requerimientos para el almacenamiento, acceso y transmisión de información médica dentro de la práctica de la telemedicina.

3.2.3 CONTEXTO DURANTE LA PANDEMIA

Es posible observar producto de la crisis COVID un aumento exponencial de las ofertas de atención médica a través de canales remotos, pero sin detallarse explícitamente los compromisos para con la confidencialidad de la información generada en el transcurso de la tele atención.

El tamaño, alcance y velocidad del despliegue de la telemedicina desde el inicio de la crisis COVID es destacable. Hospitales y unidades de atención que nunca antes habían desplegado herramientas de atención remota, aprendieron rápidamente como integrarse a ellas.

Algunos hospitales en Estados Unidos han tenido incrementos del 4000% en las atenciones de telemedicina.

No obstante lo anterior, la urgencia y premura por el despliegue de la telemedicina ha resultado en la flexibilización por parte de los reguladores de las normas, con el resultado de la masificación del uso de herramientas como FaceTime, Skype y Zoom, entre otras. Han aumentado las atenciones remotas y con ello las potenciales amenazas a través de por ejemplo phishing y ataques a servidores de acceso remoto.

Las necesidades urgentes, pero temporales, solucionables a través de la telemedicina no debiesen ser una excusa para la implementación de servicios con bajos estándares de seguridad,

¹³ HIPAA: *Health Insurance Portability and Accountability Act*



con consecuencias nefastas para la confianza en la práctica de la telemedicina, así como en la privacidad de los pacientes.

Un reporte de Ciber Seguridad de HIMMS¹⁴ (organización sin fines de lucro para el fomento de la digitalización en la medicina) señala que durante la crisis COVID ha aumentado las campañas de Phishing dirigidas tanto a clientes finales como a organizaciones, así como en ataques de denegamiento de servicio, y más. En resumen, criminales informáticos están capitalizando el miedo y las preocupaciones de las personas respecto a la crisis COVID para su beneficio [7].

Hospitales y agencias gubernamentales han experimentado ataques distribuidos de denegación de servicio, algunos exitosos y en otros casos solo intentos. En el caso de ataques exitosos, algunas organizaciones han reportado caídas completas de sus redes.

Múltiples campañas de *ransomware* han sido activadas desde abril a la fecha de acuerdo con los informes de especialistas. Protocolos de acceso a servidores remotos, redes privadas virtuales, escritorios virtuales y otros tipos de ambiente virtuales, sistemas operativos legados y dispositivos expuestos a Internet han sido blanco de ataques informáticos.

Interpol y Europol han emitidos avisos a hospitales y organizaciones gubernamentales involucradas en la respuesta global a la crisis COVID que ahora son blanco de ataques de tipo *ransomware* en un esfuerzo por parte de organizaciones criminales de obtener créditos económicos.

Un significativo número de incidentes ha llevado a hospitales a posponer cirugías y redirigir pacientes a otros centros. Varias organizaciones de salud suponen haber sido víctimas de ataques informáticos durante la crisis COVID en servicios de laboratorio, vacunatorios y agendamiento de pacientes.

Con un número importante de trabajadores de la salud ejerciendo funciones en forma remota, las organizaciones han reportado mayor tiempo de sus equipos de seguridad informática para atender dudas de sus usuarios respecto correos electrónicos sospechosos (Phishing). Al respecto las organizaciones han liberado a sus usuarios internos guías para responder las principales dudas sobre seguridad de la información de sus miembros.

Asimismo, ataques basados en troyanos y otros virus para tomar control remoto de las computadoras de los usuarios, han visto un incremento de la mano del uso de la temática COVID (ofertas de antivirales, test de detección, vacunas, material de protección personal, sanitizadores y soluciones antisépticas) como un argumento para incitar a los usuarios a descargar el contenido que sirve de vehículo para estas amenazas.

¹⁴ HIMMS: *Healthcare Information and Management Systems Society*



Otros desafíos a los cuales se ha visto enfrentada la telemedicina es la seguridad en la integración de la información entre los diferentes silos de información de cada uno de los sistemas integrantes de los procesos de telemedicina, como IoT, la terminal del paciente, la plataforma de imágenes, la ficha del paciente, etc. Cada vez se integran nuevos sistemas con nuevas funcionalidades, en el proceso no debemos perder el foco en la seguridad al momento de integrar nuevas tecnologías a las ya existentes o entre ellas mismas. En el ámbito de la confidencialidad, una problemática que se ha presentado es cómo disponer la información de los pacientes para efectos de trazabilidad, control de cuarentenas y análisis epidemiológico de forma confidencial, solo a quienes les resulta imprescindible esa información para realizar en forma correcta su trabajo, dada la discriminación social a la cual se puede ver enfrentado un paciente COVID positivo.

Lo anterior hace necesaria la evaluación de riesgos, la implementación y la normalización de estándares mínimos de gestión de la seguridad de la información con el objetivo de evitar o minimizar las brechas de seguridad que puedan ser explotadas tanto en prestaciones del área privada como del área pública, dada la potencial irrupción permanente que puede adquirir la telemedicina a partir de la crisis COVID.

Con el crecimiento exponencial de la telemedicina producto de la crisis COVID, tanto en volumen como en tipos de prestaciones, se hace necesaria la introducción de nuevas herramientas para acceder a la información en más puntos y en más contextos, con ello se añaden riesgos a lo que se denomina la “superficie de ataque”, como se observa en la Figura 7 [8].

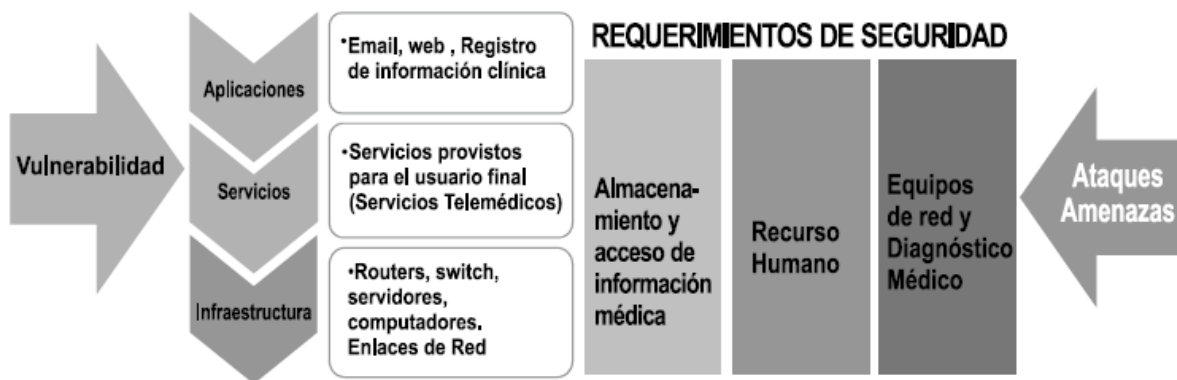


Figura 7. Requerimientos de seguridad

El despliegue masivo de la telemedicina añade exposición a riesgos en las siguientes áreas:

- Fallas en la tecnología, dado el crecimiento en la infraestructura tecnológica necesaria para proveer el servicio;



- Falta de consentimiento informado, dado el desconocimiento de las prestaciones dentro de la práctica médica en la nueva plataforma, por parte de los usuarios (pacientes y trabajadores de la salud);
- Administración del acceso y la identidad, dada la masiva prestación de servicios desde los hogares de los profesionales de la salud;
- Riesgos de seguridad física, por la falta de protocolos de resguardo adecuado de la información como respaldos y procedimientos de contingencia;
- Infraestructura Tecnológica Obsoleta, dada la coexistencia de las nuevas tecnologías desplegadas con la infraestructura tecnológica existente;
- Terminales de usuario con software no actualizado, producto de que los usuarios del sistema utilizan sus equipos personales para conectarse;
- Riesgos en sistemas de terceras partes (por ejemplo dispositivos IoT), por no estar pensados con foco en la seguridad de los datos.

Los riesgos anteriormente enumerados son explotados a través de diferentes técnicas como:

- *Phishing*: ingeniería social para la obtención de claves;
- Escalamiento de privilegios: ejecución por parte de un usuario de actividades no permitidas explícitamente según su nivel de privilegios;
- Accesos no autorizados a través de *Backdoors*: ejecución de código malicioso mediante la explotación de bugs en sistemas con software fuera de soporte por parte del fabricante o sin las últimas actualizaciones de seguridad;
- *Spoofing*: suplantación de identidad a través del acceso a data de autenticación en dispositivos IoT para obtenciones de telemonitoreos relacionados a la salud del paciente.

3.3 IoT, TELEMONITOREO Y HOMECARE

3.3.1 INTRODUCCIÓN

La pandemia de COVID-19 ha producido que se desarrollen nuevas formas de entregar salud y también de tomar algunas que ya existen pero que, al menos en Chile, no son de conocimiento general o cuyos métodos o instrumentos no son comunes en la práctica diaria. En este escenario, aparecen los conceptos IoT, telemonitoreo y homecare, los que se entrelazan cuando se habla de la



atención de pacientes a distancia, sobre todo, si esta atención se realiza con el paciente estando en su domicilio, y que se definen como:

- IoT (*Internet of Things*): Agrupación e interconexión de dispositivos, máquinas, objetos y personas a través de una red de Internet, donde todos ellos pueden ser visibles e interactuar sin necesidad de intervención humana, es decir, interacción máquina a máquina (M2M) o entre dispositivos. Los objetos tienen identificadores únicos y la capacidad para transferir datos en una red de comunicación [9];
- Telemonitoreo: Procedimiento en el cual se recopila información de salud de un paciente por medio de un conjunto de sensores y cuyas mediciones de forma automática se envían a un lugar distante, en el cual hay profesionales de salud que analizan la información y entregan las respuestas respectivas [10]; Esto permite disponer de una amplia base de datos para ayudar a la medicina preventiva;
- Homecare: Es el cuidado que se le entrega a una persona con necesidades especiales que debe permanecer en su casa, dentro de los que pueden estar los adultos mayores, pacientes con enfermedades crónicas, personas en recuperación de cirugía o con alguna discapacidad. Dentro de la gama de servicios que considera el *homecare*, también está incluida la telesalud [11].

En esta sección se aborda el uso de estas tecnologías en relación con las atenciones de salud realizadas principalmente a nivel ambulatorio (es decir, excluyendo el ambiente hospitalario), como forma de suplir total o parcialmente los servicios que habitualmente los pacientes reciben en la consulta médica pública o privada.

3.3.2 SITUACIÓN PRE-PANDEMIA

La IoT, como parte de la transformación digital, ha llegado hace algún tiempo en forma vertiginosa a la vida diaria a través de la conexión de objetos a internet, y no solo con los teléfonos inteligentes, televisores, relojes, máquinas o ciudades inteligentes, sino que también con ese conocimiento acumulado aplicado en el área médica se ha podido contar con mayor tecnología en ámbitos como la medicina preventiva y también optimizar el tratamiento dado a los pacientes, mejorando su calidad de vida, por ejemplo, con sistemas de monitoreo de la salud (Salud Inteligente).



Gracias a las redes de sensores corporales inalámbricos WBAN¹⁵ ha sido posible el desarrollo de un conjunto de sensores biométricos que han permitido la monitorización de la salud de los enfermos y que, dadas sus características (medir parámetros fisiológicos, comunicación entre ellos y con la estación base, además de la recopilación de información en la estación base), se ha conseguido que el proceso sea realizado con el paciente a distancia. Dentro de los que están disponibles o en desarrollo se pueden mencionar los siguientes:

- Sensor piezoeléctrico en la muñeca para medir presión sanguínea,
- Sensor óptico para medir frecuencia de pulso y saturación de oxígeno,
- Micrófonos en el tórax para medir frecuencia cardíaca,
- Micrófonos para evaluar ruido intestinal,
- Sensor para medir frecuencia respiratoria,
- Sensores para medir resistencia vascular sistémica,
- Sensores para ECG,
- Sensores de temperatura del cuerpo,
- Medidores de nivel de sudor,
- Otros.

El desarrollo de la Industrial IoT (IIoT) y la Inteligencia Artificial, ha permitido y dado sentido a sistemas de aprendizaje cognitivo (Cognitive IoT) con grandes innovaciones que implican aspectos como: aprendizaje por sí solo, probabilístico, adaptivo, flexible, dinámico, interactivo y escalable. Esto cobra gran importancia al ver que los mismos desarrollos, avances y descubrimientos han sido aplicados al área médica.

En los últimos años, la disponibilidad de dispositivos de salud inteligentes y el IoT han permitido que un gran segmento de personas hayan adquirido el hábito de mantenerse saludables, lo cual se ha complementado con la conexión en la atención médica, pero no solo eso, sino que también los dispositivos médicos cada vez están más conectados entre sí, mejorando la experiencia de usuario tanto por parte del paciente como del médico y permitiendo una respuesta rápida y oportuna frente a las emergencias. Además, el monitoreo continuo y en tiempo real ayuda a tratar en forma más eficiente a los pacientes. El almacenamiento y el análisis de los registros del paciente han sido importantes en las estrategias de medicina preventiva, brotes de enfermedades y soluciones de salud [12].

Llevando lo anterior a la realidad nacional, en la Tabla 3 se muestran ejemplos de dispositivos que actualmente se encuentran en uso y/o a la venta en Chile y que permiten complementar el examen físico al momento de hacer una teleconsulta, hacer monitoreo de ciertos

¹⁵ WBAN: *Wireless Body Area Networks*. Permiten recolectar datos de parámetros vitales del cuerpo de un paciente para luego ser recogidos por pequeños sensores portátiles o implantables que se comunican utilizando técnicas inalámbricas de corto alcance.



parámetros vitales desde el lugar donde el enfermo se encuentre (telemonitoreo) o que le entregan al paciente una herramienta para autogestionar su salud.

Tabla 3. Ejemplos de dispositivos y tecnologías en uso y/o a la venta en Chile

| Dispositivo o tecnología | Función | Utilidad |
|---|---|--|
| TytoHome [13] | Complemento de examen físico con: <ul style="list-style-type: none"> • Control de temperatura y frecuencia cardiaca, • Examen visual de faringe, oídos y piel, • Examen de ruidos cardiacos, pulmonares y abdominales. | Consulta general |
| Esfigmomanómetro Tel-O-Graph [14] | Telemonitoreo de presión arterial, con: <ul style="list-style-type: none"> • Tarjeta SIM que envía las mediciones directo a la plataforma, o • Conexión bluetooth al smartphone y desde este a la plataforma de monitoreo. | Monitoreo de pacientes crónicos |
| Glucómetro Accu-Check Instant [15] | Telemonitoreo de diabetes mellitus, con conexión bluetooth al smartphone y desde este a la plataforma de monitoreo. | Monitoreo de pacientes crónicos |
| Plataforma de monitoreo Red Carelink [16] | Telemonitoreo de dispositivos cardiológicos implantables: <ul style="list-style-type: none"> • MCP: marcapasos, • DAI: desfibrilador automático implantable, • SRC: sistemas de resincronización cardiaca. | Monitoreo de pacientes crónicos |
| Reloj Apple Watch Series 6 [17] | Complemento o extensión de examen físico y seguimiento de indicaciones con: <ul style="list-style-type: none"> • Medición de oxígeno en sangre, • Electrocardiograma de una derivación, • Notificaciones de frecuencia cardiaca alta o baja, • Notificación de ritmo cardiaco irregular, • Seguimiento de periodos de sueño. | Consulta general y seguimiento de estilo de vida saludable |
| Clip CardiacSense [18] | Monitorización continuamente de presión arterial: <ul style="list-style-type: none"> • Sin manguito inflable, | Monitoreo de pacientes crónicos |



| | | |
|------------|--|------------------|
| | <ul style="list-style-type: none"> • Notificaciones al médico en tiempo real cuando el clip detecta un problema, • El médico tiene acceso a los datos brutos que se almacenan en la aplicación de la nube. | |
| Binah [19] | <p>A través de cualquier dispositivo con cámara (<i>smartphone, Tablet</i>), sin necesidad de un dispositivo adicional y usando una señal de fotopleletismograma puede:</p> <ul style="list-style-type: none"> • Calcular la frecuencia cardiaca, • Calcular la saturación de oxígeno, • Calcular la frecuencia respiratoria. | Consulta general |

3.3.3 CONTEXTO DURANTE LA PANDEMIA

La presencia del COVID-19 produjo varios cambios transitorios en la forma de entregar atenciones de salud a los pacientes. Tanto en el sector público como privado, se suspendieron ciertos tipos de atenciones y procedimientos (como control de enfermedades crónicas y cirugías programadas) para enfocar todos los esfuerzos en el manejo de pacientes con síntomas sugerentes o confirmados de COVID-19 y mantener las atenciones de urgencia de rutina.

Los cambios transitorios en la forma de trabajo están produciendo que aparezcan o se masifiquen otras formas de entregar atenciones de salud, donde la teleconsulta (que es una rama de la telemedicina) ha comenzado a ser más conocida y utilizada, sobre todo porque la atención se puede realizar con el paciente en su domicilio (o en cualquier parte donde se encuentre) evitando principalmente dos cosas: (1) la exposición innecesaria al contagio de COVID-19, (2) un mayor número de pacientes que llegan a los servicios de urgencia u otros centros de salud que pudieran verse saturados de trabajo y (3) menor desplazamiento de personas para acceder los centros de salud. Esta manera de entregar atención de salud ambulatoria, si bien se origina en cambios transitorios, puede transformarse en algo permanente, más eficiente puesto que los distintos usuarios (profesionales de salud y pacientes) han encontrado una nueva herramienta que les permite conectarse y resolver problemas que no necesitan una evaluación presencial.

Sin embargo, la teleconsulta tiene como principal déficit que la atención, al no ser presencial, carece de un elemento fundamental que es el examen físico. Esta carencia, dependiendo de la enfermedad, puede ser minimizada por la entrevista que le realiza el profesional al paciente



y/o por los resultados de exámenes complementarios que los pacientes pueden tener al momento de la teleconsulta. En ese contexto, los dispositivos descritos en este ítem toman un rol importante, puesto que permiten realizar en parte o totalmente el examen físico a distancia, o bien, porque se consideran como una extensión del examen físico.

En otro rubro, no hay una prueba directa, pero algunas compañías estarían monitoreando cambios en cinco o más signos vitales y reconocimiento facial con el procesamiento del resultado, en menos de un minuto, darían la probabilidad de tener COVID-19 (se excluye a los asintomáticos).



4 RECOMENDACIONES Y CONCLUSIONES

4.1 TELECOMUNICACIONES

Actualmente, las telecomunicaciones en Chile ofrecen una estructura que permite realizar telemedicina en casi todos sus ámbitos, siendo la única excepción el 5G que, al encontrarse en etapa de licitación, en el futuro próximo ya será un recurso disponible. Esta estructura está desarrollada y bien establecida principalmente en zonas urbanas, siendo más débil en zonas rurales.

El fortalecimiento de las telecomunicaciones en zonas rurales es una pieza fundamental para llevar telemedicina a todo el país, por lo tanto, se hace primordial que el Proyecto de Fibra Óptica Nacional se efectúe prontamente. Como alternativa, también se propone el uso de satélites de baja altura. Alcanzar esta meta implicará que las personas que viven en zonas alejadas de las grandes ciudades o de difícil acceso puedan recibir atención de salud en forma más oportuna y de mayor calidad, porque de esta manera los pacientes evitarán dificultades como son disponibilidad limitada de transporte, falta de dinero para el transporte o el alojamiento (en caso de que no sea factible regresar el mismo día) u otras, pero además tendrán la posibilidad de acceder a atenciones por especialistas ya sea en forma directa o intermediada por el centro de salud al que pertenecen.

Además de lo anterior, se debe poner énfasis en mantener la seguridad de las telecomunicaciones en dos ámbitos:

- En infraestructura, puesto que se debe asegurar que los sistemas de telecomunicaciones se mantengan permanentemente funcionando y disponibles para que el sistema de salud no se quede sin cumplir su labor diaria, es decir, mantener los flujos de información entre: plataformas, dispositivos IoT, telemonitoreo, entre otros, además de la interconexión entre los mismos centros de atención de salud, ambulancias, redes asistenciales, etc.
- En información, principalmente en lo que se refiere a lo que se interrelaciona con lo descrito en la sección siguiente sobre gestión de seguridad de la información.

4.2 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En una visión integrada de la seguridad de la información en la telemedicina, un factor clave es comunicar en forma simple los procedimientos y políticas de forma que puedan ser entendidas por todos los actores involucrados en el proceso. Aquí es importante hacer hincapié en que la



gestión de la seguridad de la información se basa en 2 pilares, los recursos técnicos y los recursos humanos.

Desde el punto de vista de los recursos humanos, la gestión de la seguridad de la información debe ser vista con un enfoque inclusivo que reúna a todos los actores involucrados (tecnología, médicos, ejecutivos, áreas legales, etc.) y les permita plantear sus preocupaciones con el objetivo de generar los lineamientos generales y políticas.

Es importante educar a los usuarios (pacientes, profesionales de la salud y staff de apoyo) en las mejores prácticas respecto a la seguridad de la información en telemedicina. La capacitación al personal médico y staff de apoyo en las normas, procesos y flujos de trabajo para esta nueva modalidad de atención. Para ello se debe trabajar en la definición de políticas y procedimientos centrados en los usuarios (homologación de estándares de confidencialidad presencial a remota, recomendaciones y toma de conocimiento sobre conductas y riesgos, autenticación del usuario, por nombrar algunos puntos a tomar en consideración).

La concientización sobre la confidencialidad en el uso de usuarios y claves, el control de la identidad de quienes acceden a una sesión y el resguardo de los datos generados son críticos para evitar brechas de seguridad.

Los pacientes también juegan un rol importante pues son actores claves en la ecuación de la privacidad de los datos. Es imperativo que estos sean educados sobre las mejores prácticas de seguridad en el entorno de la telemedicina, conociendo los riesgos, que pueden hacer y que no pueden hacer.

Desde un punto de vista técnico el primer paso es hacer una evaluación del riesgo de seguridad para cada uno de los procesos de telemedicina involucrados, para generar guías relativas a la seguridad para cada uno de los casos de uso de la telemedicina, teniendo en cuenta cuatro principios: seguridad, operatividad, estandarización y simplicidad (Figura 8).

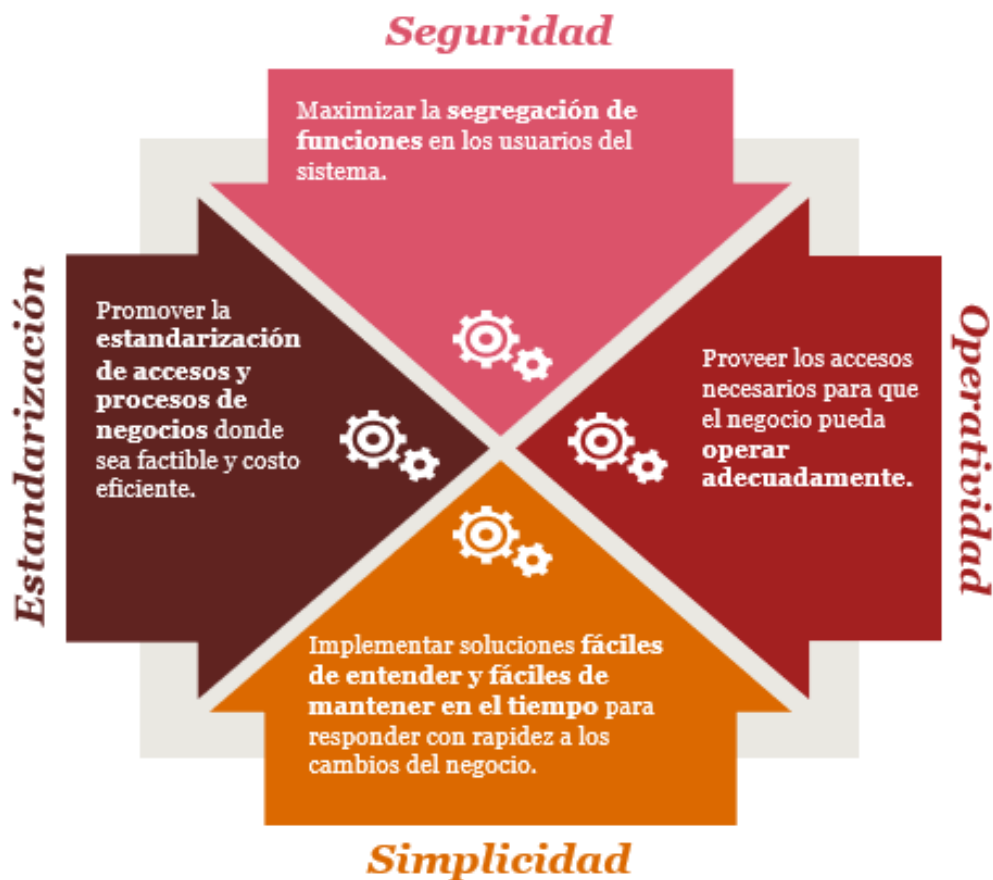


Figura 8. Principios para gestión de seguridad de la información

Teniendo como norte los cuatro principios se identifican las siguientes tareas por realizar:

- Identificar los procesos de telemedicina y establecer las mejores prácticas de seguridad dentro de ellos como parte integral de la cadena de valor;
- Concientizar sobre las mejores prácticas para mantener la seguridad de la información a los usuarios de las distintas plataformas (pacientes, médicos, enfermeras, tecnólogos médicos, personal administrativo, etc.);
- Incorporar en el criterio de evaluación para la incorporación de un activo de telemedicina (software, plataformas o dispositivos); una evaluación del riesgo de seguridad para poder evaluar que tan segura es el activo y a que riesgos nos expone. (Información provista en especificaciones del fabricante del activo según formato MDS2¹⁶);

¹⁶ MDS2: *Manufacturer Disclosure Statement for Medical Device Security*



- Establecer controles de seguridad como prácticas institucionales, asegurándose de tener sistemas auditables y traceables;
- Los datos, a menos que sea absolutamente necesario, no deben ser expuestos en forma directa sino como consultas analíticas que aseguren el anonimato de los pacientes.

Entrando más en detalle podemos definir varios ámbitos o áreas de gestión de la seguridad de la información para empezar a construir nuestro modelo de gestión de la seguridad de la información en telemedicina.

- 1) Definición de políticas y procedimientos centrados en los usuarios (homologación de estándares de confidencialidad presencial a remota, recomendaciones y toma de conocimiento sobre conductas y riesgos, autenticación del usuario);
- 2) Seguridad del canal de comunicación;
- 3) Seguridad del almacenamiento de datos;
- 4) Seguridad del control de acceso a los datos.

A partir de los requerimientos del regulador y las normativas técnicas podemos identificar el siguiente pormenorizado de actividades a revisar y/o implementar como requerimientos comunes de seguridad para telemedicina:

- Los sistemas de tecnología y protección de información clínica deben ser apropiados en las entidades de salud para recopilar y analizar la información de los pacientes en bases de datos.
- 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.
- 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 esa información cumplan con los estándares dentro de la entidad de salud, supervisando el intercambio y transferencia de información.
- Utilizar identificadores codificados de referencia para los pacientes, con el objetivo de permitir la separación de información de la base de datos relacionada con la identificación del paciente de información relacionada con tratamientos o condición del paciente.
- La transmisión de información debe ser siempre por canales cifrados.
- Los accesos a la información del paciente, ya sean exitosos o fallidos, deben ser auditables.
- Se deben definir protocolos estrictos para identificar personas autorizadas para acceder a la identidad del paciente y bajo qué circunstancias el acceso debe ser autorizado.
- Las tecnologías usadas deben garantizar la privacidad de los datos.



- En cada uno de los extremos de la comunicación debe existir protección de contraseña simple en el punto de acceso, encriptación de datos y mecanismos de control de acceso y privilegios.
- Debe existir control de acceso a los equipos de cómputo y medidas de seguridad básicas.
- En el almacenamiento de los datos se deben procurar las mismas precauciones que aplican a la transmisión de datos, como por ejemplo la encriptación de estos.
- Implementar procedimientos para verificar la identidad de la persona o entidad que solicite acceso a la información de salud.
- Definir guías de procedimientos que garanticen la confidencialidad, privacidad y seguridad de la información.
- Exigir algún tipo de dato biométrico como huellas dactilares, patrones de voz, patrones faciales o del iris.
- Implementar mecanismos de control y auditoría para corroborar que la información de salud protegida no haya sido alterada o destruida de forma no autorizada.
- Usar mecanismos de confiabilidad que garanticen que los datos enviados sean los datos recibidos.
- Mantener de forma cifrada la información sensible de salud.
- El recurso humano debe estar capacitado para ofrecer sus servicios en forma remota o no presencial, para ofrecer sus servicios según la reglamentación vigente en materia de privacidad, confidencialidad y confiabilidad.
- Establecer políticas y procedimientos para actuar frente a una emergencia que altere los sistemas que contengan información de salud protegida.
- Las instituciones deben acreditar que cuentan con personal capacitado para manejar la tecnología utilizada en los procedimientos de Telemedicina.
- Gestionar activamente el almacenamiento físico de toda la información del sistema.
- Realizar evaluación técnicas y no técnicas de la seguridad de la información de manera periódica, basadas en la aplicación de normas.
- Mantener copias de seguridad guardadas en sitios diferentes.

4.3 IOT, TELEMONITOREO Y HOMECARE

Los dispositivos para monitoreo o evaluación de los pacientes desde su casa son una realidad instalada en varios países, dentro de los que también se encuentra Chile pero a una menor escala. Un aspecto importante que se debe considerar es el costo monetario que puede significar y quién será el encargado de asumirlo. En este sentido, los precios pueden ser similares con respecto a aquellos que no tienen incorporada la tecnología de monitoreo (por ejemplo, relojes con medición de signos vitales fabricados en China *versus* otros tipos de relojes convencionales) o pueden ser varias veces más caros (por ejemplo, esfigmomanómetros digitales con tarjeta SIM con monitoreo en plataforma especializada en relación con esfigmomanómetros disponibles en cualquier



farmacia). Quien asume el costo es un tema no trivial, puesto que si este va por parte del paciente se puede producir una segregación negativa donde se verán beneficiados solo aquellos que tengan suficiente poder adquisitivo, mientras que si las instituciones son las encargadas de costearlos (tomando como beneficio la mejora o mantención de un buen estado de salud de sus enfermos, lo que se traduce en ahorro económico por menor cantidad de hospitalizaciones, de uso de días cama en cada hospitalización u otras formas de prestaciones de salud como realización de exámenes diagnósticos, pago de licencias médicas, entre otros), el acceso se vuelve transversal y no segrega por capacidad de pago del enfermo.

La existencia de sensores para medir distintos parámetros físicos y la tecnología para transmitir esos datos en tiempo real, además de computadores más poderosos con capacidad para procesar y desplegar esa información, permite que se puedan hacer distintas y variadas evaluaciones en forma sincrónica. En forma similar sucede con las evaluaciones asincrónicas, donde la información se transmite en forma diferida, lo que posiblemente usa menos recursos de los sistemas.

El hecho de que haya un número creciente de recopilación de datos y la posibilidad de tenerlos en forma estructurada (como sucede con varias de las plataformas usadas por los dispositivos descritos en este documento) genera la oportunidad de enriquecer las bases de datos y realizar mejoras u optimizaciones de los sistemas con el uso de inteligencia artificial u otras herramientas que tienen estos fines.

Dentro de todo esto, el recurso humano no puede quedar atrás, se debe educar a los usuarios de salud (desde los pacientes y sus familiares hasta los profesionales y directivos) con respecto a la existencia, uso y potencial de estas tecnologías para que cada vez los pacientes puedan acceder a esta realidad que beneficia a todo el sistema de salud.

En términos de seguridad, se debe asegurar la calidad de los equipos que se estén usando por medio de:

- Certificaciones CE¹⁷, FDA¹⁸ u otra (solicitársela al fabricante y si es un desarrollo nacional tramitar la certificación);
- Capacitaciones técnicas al personal que va a operar y que hará la mantención de estos equipos;
- Promover el uso adecuado por parte de pacientes y personal de salud;
- Mantener disponible la red eléctrica para los pacientes electrodependientes.

¹⁷ CE: Comunidad Europea

¹⁸ FDA: *Food and Drugs Administration* de EEUU



4.4 RECOMENDACIONES FINALES

La telemedicina tiene un importante componente tecnológico que debe ser utilizado de forma correcta y eficiente, para lo cual se requiere un trabajo mancomunado de médicos, tecnólogos, enfermeros, TENS¹⁹ e ingenieros para obtener el mayor impacto en el sistema de Salud. De la mano de esto, se debe mantener el cumplimiento de las regulaciones sanitarias y de las normas de seguridad de la información, además de identificar aquellos campos en los que se deben hacer actualizaciones o generar nuevas normativas que estén acordes a la realidad actual.

También, la telemedicina debe estar para aliviar a los seres humanos de los sufrimientos físicos y psicológicos, además de permitir disfrutar mejor de la vida, para lo cual se espera que a futuro se complemente con los avances en nanoterapia y genética para así mejorar otros aspectos como el envejecimiento.

Existe una diferencia importante entre lo que se necesita y lo que efectivamente se tiene en términos de infraestructura física, aplicaciones, innovaciones y servicios, por lo que se debe trabajar en mejorar los dispositivos, la recopilación y el análisis de los datos, potenciando el avance tecnológico en salud en todos sus ámbitos.

En cuanto al acceso, la telemedicina está presente en la totalidad de Servicios de Salud de Chile (los que suman 29) con al menos una de sus prestaciones, lo cual indica que en el sector público ya se ha dado un primer paso para identificarla como un aporte a los procesos sanitarios. Además, la suma de variadas prestaciones en muchos de los establecimientos tanto públicos como privados permiten que cada vez sean más los pacientes tengan acceso a atenciones, exámenes, asistencia, opiniones de experto, etc. A pesar de esto, queda mucho por hacer para tener un sistema capaz de llegar a los lugares más alejados o de difícil acceso del país (para lo cual el sistema de FON será un gran avance) y que el tipo de prestaciones entregadas cubra la mayor cantidad posible de necesidades de salud de la población.

Con respecto a costos, la telemedicina no suele ser más cara que la medicina realizada en forma presencial. A nivel de instituciones y según el tipo de prestación, se pueden generar ahorros por una menor necesidad de disponer de espacio físico (por ejemplo, en el caso de la teleconsulta en la cual el paciente no va al centro de salud y donde el profesional que realiza la atención solo necesita un escritorio con una silla) o porque al generar acceso a prestaciones a nivel de atención primaria (como la toma de exámenes cuyo informe es realizado a distancia por el especialista correspondiente, comités de expertos, realización de interconsultas entre especialidades, etc.), se pueden realizar diagnósticos en forma precoz, indicación de tratamientos adecuados y ajustes de terapias, entre otras cosas, lo que se traduce en alcanzar o mantener en mejores condiciones de

¹⁹ TENS: Técnico en Enfermería de Nivel Superior



salud a la población, disminuyendo así el número total de hospitalizaciones y la duración de cada una de ellas. Por el lado de los pacientes, sobre todo de zonas rurales donde además hay dificultades en el transporte, la telemedicina evita que tengan que recorrer grandes distancias para llegar a los hospitales principales de su región cuando el motivo de consulta se puede resolver a nivel local, lo que también se traduce en ahorro en el costo del pasaje y, en muchos casos, también en alojamiento (principalmente para aquellos pacientes que disponen de transporte solo algunas veces a la semana). Es por razones como estas que reforzar los sistemas de telemedicina a nivel de atención primaria es fundamental y también lo es el mantener la comunicación entre atención primaria y hospitales de mayor complejidad (donde habitualmente se encuentran los especialistas), tanto a nivel público como privado.



5 REFERENCIAS

- [1] WHO, «Telemedicine: opportunities and developments in Member States. Report on the second global survey and health,» *Global Observatory for e-Health series.*, vol. 2, 2010.
- [2] Subsecretaría de Redes Asistenciales, Ministerio de Salud, «Programa Nacional de Telesalud: En el contexto de Redes Integradas de Servicios de Salud,» 2018. [En línea]. Disponible: <https://www.minsal.cl/wp-content/uploads/2018/03/Programa-Nacional-de-Telesalud.pdf>. [Último acceso: 07 noviembre 2020].
- [3] E. Cosoi, «Telemedicina en el Mundo,» *Revista Chilena de Pediatría*, vol. 73, nº 3, 2002.
- [4] Ó. Ferrari, «Telemedicina, el progreso virtual de la salud,» Saval Net, 02 septiembre 2013. [En línea]. Disponible: <https://www.savallnet.cl/mundo-medico/reportajes/telemedicina-el-virtual-virtual-en-salud.html>. [Último acceso: 02 enero 2021].
- [5] A. T. Tunggal, «UpGuard,» Octubre 2020. [En línea]. Disponible: <https://www.upguard.com/blog/protected-health-information-phi>. [Último acceso: Octubre 2020].
- [6] K. Nader, «el Hospital,» 2018. [En línea]. Disponible: www.elhospital.com/temas/Riesgos-en-la-seguridad-informatica-en-salud+111853?pagina=1. [Último acceso: Octubre 2020].
- [7] Lee King, BS, JD, CISSP, CIPP/US, FHIMSS, «Healthcare and Cross-Sector Cybersecurity Report,» HIMSS, Abril 2020.
- [8] E. Guillen, L. Ramírez y E. Estupiñan, *Análisis de la seguridad para el manejo de la información médica en telemedicina*, Bogotá, Colombia: Universidad Militar Nueva Granada, 2011.
- [9] Deloitte, «IoT - Internet Of Things,» 2020. [En línea]. Disponible: <https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html>. [Último acceso: 20 septiembre 2020].
- [10] AccuHealth, «¿Sabes que es: Telemedicina, Telesalud, e-salud, Telemonitoreo y Hospital remoto?,» 17 marzo 2019. [En línea]. Disponible: https://www.accuhealth.cl/blog_accu/index.php/2019/03/17/sabes-que-es-telemedicina-telesalud-e-salud-telemonitoreo-y-hospital-remoto/. [Último acceso: 29 septiembre 2020].
- [11] Medline Plus, «Home Care Services,» 14 septiembre 2020. [En línea]. Disponible: <https://medlineplus.gov/homecareservices.html>. [Último acceso: 20 septiembre 2020].



- [12] P. K. Dutta Pramanik, B. K. Upadhyaya, S. Pal y T. Pal, «Internet of Things, Smart Sensors, and Pervasive Systems: Enabling the Connected and Pervasive Health Care,» de *Healthcare Data Analytics and Management*, Elsevier, 2019, pp. 3-7.
- [13] TytoCare, «Get answers quickly,» [En línea]. Disponible: <https://www.tytocare.com/>. [Último acceso: 20 septiembre 2020].
- [14] IEM, «eHealth,» [En línea]. Disponible: <https://www.iem.de/en/ehealth/#digitalebde>. [Último acceso: 21 septiembre 2020].
- [15] Roche Diagnostics, «Accu-Chek® Connect: Aplicación para el seguimiento de la diabetes,» [En línea]. Disponible: <https://www.accu-chek.cl/gestion-de-informacion/connect-aplicacion-para-el-seguimiento-de-la-diabetes>. [Último acceso: 18 Octubre 2020].
- [16] Medtronic, «El Carelink Red: manejo para sus pacientes,» Medtronic, 2020. [En línea]. Disponible: <https://www.medtronic.com/us-en/healthcare-professionals/products/cardiac-rhythm/managing-patients/information-systems/carelink-network.html>. [Último acceso: 18 Octubre 2020].
- [17] Apple Inc., «Apple Watch Series 6,» 2020. [En línea]. Disponible: <https://www.apple.com/cl/apple-watch-series-6/>. [Último acceso: 18 Octubre 2020].
- [18] «CardiacSense,» [En línea]. Disponible: <https://www.cardiacsense.com/es/product/el-clip/>. [Último acceso: 09 noviembre 2020].
- [19] «Binai.ai,» 2020. [En línea]. Disponible: <https://www.binah.ai/es/>. [Último acceso: 09 noviembre 2020].
- [20] Ministerio de Salud de Chile, «Servicios de Salud,» Ministerio de Salud, [En línea]. Disponible: <https://www.minsal.cl/servicios-de-salud/>. [Último acceso: 02 enero 2021].