UNIVERSIDAD DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

ESTÁNDARES DE SEGURIDAD EN TELEMEDICINA PARA CENTROS DE SALUD EN EL ESTADO DE QUINTANA ROO

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE

INGENIERO EN REDES

PRESENTA

IVÁN DE JESÚS ALPUCHE TEJERO

SUPERVISORES

M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
M.S.I. LAURA YÉSICA DÁVALOS CASTILLA
DR. JAVIER VÁZQUEZ CASTILLO

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2021

UNIVERSIDAD DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

TRABAJO MONOGRÁFICO TITULADO

"ESTÁNDARES DE SEGURIDAD EN TELEMEDICINA PARA CENTROS DE SALUD EN EL ESTADO DE QUINTANA ROO"

ELABORADO POR:

IVÁN DE JESÚS ALPUCHE TEJERO

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ SUPERVISOR

SUPERVISOR: _____

M.S.I. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE

SUPERVISOR: _____

DR. JAIME SILVERIO ORTEGÓN AGUILAR

SUPERVISOR: _____

M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISORA SUPLENTE: _____

M.S.I. LAURA YESICA DÁVALOS CASTILLO

SUPERVISOR SUPLENTE: _____

DR. JAVIER VÁZQUEZ CASTILLO

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2021

RESUMEN

La telemedicina permite a los profesionales de la salud evaluar, diagnosticar y tratar a pacientes a distancia utilizando la tecnología de telecomunicaciones. El enfoque ha pasado por una evolución sorprendente en la última década y se está convirtiendo en una parte cada vez más importante de la infraestructura de salud.

La telemedicina permite que las evaluaciones médicas puedan llevarse a cabo incluso con menos recursos, tales como la movilidad del paciente, optimización del recurso médico especializado, el tiempo de atención puede disminuir, mejoramiento en la transferencia de datos clínicos: fotografías, radiografías, muestras, audios y cualquier otro referente necesario para el correcto diagnóstico del paciente.

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, puede estar propensa a ataque y a falla que pueden 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.

A nivel estatal en Quintana Roo, se acaba establecer el servicio de Telemedicina para los centros salud rurales (Kantunilkín, Isla Mujeres, José María Morelos y Felipe Carrillo Puerto) con los especialistas en los hospitales urbanos (Playa del Carmen, Chetumal y Cancún).

El presente trabajo monográfico aborda la documentación de estándares de seguridad utilizados en materia de Telemedicina a nivel estatal en Quintana Roo desde los enfoques tecnológico, administrativo, físico y legal, considerando El Centro Nacional de Excelencia Tecnológica en Salud (CENETEC-Salud), normas estatales, el Instituto Nacional de Transparencia (INAI), estándares internacionales, Servicios Estatales de Salud (SESA), y el proyecto llamado “Diseño, implementación y puesta en marcha de un Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED), para ampliar la cobertura y aumentar la calidad de los servicios en salud en comunidades marginadas de Quintana Roo”.

AGRADECIMIENTOS.

En primera instancia quiero agradecer a la institución de la que es derivada este proyecto; la Universidad de Quintana Roo cede Chetumal, muchas gracias a la universidad que me dejo crecer y desenvolverme como un profesionista de calidad, integro y con seguridad en lo que será una guía para mi vida.

Quiero agradecer específicamente a la División de Ciencias, Ingeniería y Tecnología y todo el personal que pertenece a la misma, mis profesores, mis compañeros y los encargados de la parte administrativa que tuve el placer de conocer

Agradecimientos para el ingeniero Rubén González Elixavide por haber sido mi tutor de carrera por los 5 años que crucé, un guía para muchas situaciones y dudas que en su momento ayudo a solucionar. Ahora, siendo un compañero del área de Redes que sepa que le agradezco por mucho lo que me a enseñado tanto como persona como ingeniero.

Agradecimientos para los profesores que me acompañaron en la carrera, el maestro Vladimir Veniamin Cabañas Victoria, la maestra Laura Yesica Davalos Castilla, el doctor Jaime Silverio Ortegón Aguilar, el doctor Javier Vázquez Castillo, y el ingeniero Freddy Ignacio Chan Puc que fueron los principales impulsores de mi carrera y siempre trataron de apoyarme para pequeñas y grandes tareas que lleve a cabo durante mis 5 años en la misma.

DEDICATORIA.

Quiero dedicar este proyecto monográfico con el cual planeo terminar mi estado de egresado y concluir la carrera de Ingeniería en Redes a mi padre Iván Alonso Alpuche Castillo especialmente, quien, debido a la situación en la que nos encontramos no podrá estar presente físicamente a la hora que reciba mi título, nunca fue de muchas palabras, pero siempre supe que tendría su apoyo a mis decisiones, un hombre que me dejo lo que es el trabajo duro y honesto como aprendizaje, espero que sepa que su hijo esta orgulloso de poder siempre decir que es hijo de un hombre como él.

A mi madre, Frine del Carmen Tejero Cervantes, mujer de mucho corazón quien me ha enseñado a disfrutar de la vida, las cosas pequeñas, las cosas grandes, gracias a ella puedo decir que soy alguien que es capaz de decir al mundo, me siento feliz, me siento triste, me siento enojado, frustrado y saber cuando debo afrontar algo solo, y cuando deba pedir ayuda sé que allí estará ella con sus brazos extendidos para mí.

A mi hermano, Javier Martín Alpuche Tejero con quien he tenido diferencias varias, pero a pesar de eso he crecido con él, si soy quien soy el es pare de ello, soy su hermano mayor y quiero dedicarle este éxito que he conseguido gracias a la persona que ayudo a formar.

Quiero agradecer a mis maestros, que al día de hoy puedo decir que siempre serán mis maestros, pero que también puedo ver unos amigos en ellos, conviví mas de cerca con algunos que con otros, pero todos pusieron de su parte para formar el estudiante que se presentara como un hombre que sabe que hacer, como hacerlo, y si no lo sabe, solucionarlo si buscar excusas.

Quiero agradecer a mis compañeros quienes estuvieron conmigo en la carrera, se que hemos cambiado desde entrar a la misma, y aunque a algunos probablemente no los vuelva a ver, que sepan que estaré siempre dispuesto a extender una mano, compartimos mucho, compartamos más.

CONTENIDO.

índice de Ilustraciones

CAPÍTULO 1: INTRODUCCIÓN

1.1 Introducción

El proyecto presentado aquí consiste en una recopilación documental de los estándares de seguridad referentes a la telemedicina y aplicados específicamente al estado de Quintana Roo, los estándares abarcados consideraran los aspectos legales, administrativos, físicos y tecnológicos.

El uso de la información médica debe ser regulado por alguna norma, esto incluye desde luego los datos transmitidos por medio de la telecomunicación ya sea de tipo síncrona o asíncrona. Por ello se deben cuidar estos datos desde que el paciente ingresa al consultorio hasta después de que sea dado de alta.

En estos procesos para la protección de datos intervienen varios aspectos, en el legal con respecto a que tienen que seguir una norma ya establecida, el administrativo por las personas físicas que tengan acceso a los datos, en el físico por la intervención directa con los equipos de telecomunicación, y la tecnológica por las medidas de seguridad dentro de la red.

1.2 Objetivo general

Documentar los estándares de seguridad utilizados en materia de Telesalud a nivel estatal desde los enfoques tecnológico, administrativo, físico y legal.

1.3 Objetivos particulares

1. Describir los estándares de seguridad estatales en materia de Telesalud.
2. Recopilar las medidas de carácter preventivo en los procesos de telecomunicación en el ámbito de salud.
3. Documentar los procesos establecidos para tratar con problemas de seguridad en el área de Telesalud.
4. Determinar las acciones después de tratar con un problema de seguridad.

CAPÍTULO 2: MARCO DE REFERENCIA

2.1 Telemedicina y Telesalud.

La Telesalud es la atención médica basada en el uso de tecnologías de la información y comunicación. Contribuye para hacer accesibles los servicios de salud de especialidad a la población alejada geográficamente.

La Telesalud brinda la oportunidad de usar una herramienta tecnológica por algún medio electrónico, para el intercambio de imágenes, voz, datos y video; permite el diagnóstico y opinión de especialistas en casos clínicos; da acceso a la infraestructura y equipos tecnológicos de apoyo a la consulta médica.

A veces se usa el término telemedicina para referirse a telesalud. La telesalud es un término más amplio. Incluye la telemedicina, pero también involucra cosas como capacitación para profesionales de la salud, reuniones administrativas de atención médica y servicios proporcionados por farmacéuticos y trabajadores sociales. (Congreso de los estados unidos mexicanos, 2013)

2.1.1 Beneficios de la Telesalud

- Recibir atención en el hogar: En especial para personas que no pueden acceder fácilmente a las oficinas de sus profesionales de la salud.
- Recibir atención de un especialista que esté en otra locación.
- Recibir atención después del horario de atención.
- Mayor comunicación con sus proveedores de atención de salud.
- Mejor comunicación y coordinación entre los proveedores de atención médica.
- Mayor apoyo para las personas que manejan sus afecciones de salud, especialmente enfermedades crónicas como la diabetes.
- Menor costo, ya que las visitas virtuales pueden ser más baratas que las visitas en persona.

2.1.2 Desventajas de la Telesalud

- Si su visita virtual es con un profesional de la salud que no es su proveedor habitual, es posible que él o ella no tenga todos sus antecedentes médicos.
- Después de una visita virtual, puede que usted deba coordinar su atención con su proveedor habitual.
- En algunos casos, es posible que el proveedor no pueda hacer el diagnóstico correcto sin examinarlo en persona, o su proveedor puede necesitar que venga para una prueba de laboratorio.
- Puede haber problemas con la tecnología, por ejemplo, si pierde la conexión o hay un problema con el software, entre otros.
- Algunas compañías de seguros pueden no cubrir las visitas de telesalud.

2.1.3 Servicios comunes de la Telesalud

- Atención médica general, como visitas de bienestar.
- Recetas para medicamentos.
- Dermatología (cuidado de la piel).
- Exámenes de la vista.
- Asesoría nutricional.
- Consejería sobre salud mental.
- Atención de urgencia para algunas afecciones, como sinusitis, infecciones de las vías urinarias o erupciones cutáneas comunes, entre otras.

2.2 Relevancia de los estándares de seguridad

En México la seguridad informática es prioridad presente para cualquier organización, empresa e institución, deben tener protocolos de seguridad en sus procedimientos para verificar que la confidencialidad de los datos sea segura. Como propuesta de seguridad informática se realizaron normas para la protección de información en las redes de las empresas. Si todas

aquellas instituciones contaran con la protección en su información y seguridad adecuada, existiría la protección idónea para sus usuarios.

Las empresas en la actualidad manejan información y la administran mediante un software, por lo que es necesario realizar evaluaciones de riesgos para la información con el fin de proteger la integridad y cumplir los objetivos de políticas de seguridad informática para evitar pérdidas de información.

El estudio de amenazas y riesgos de pérdidas de información nos han proporcionado ventajas para la implantación de controles con el objetivo de administrar y proteger importantes cantidades de información. También trasciende en el uso correcto de los recursos de hardware para cumplir con el control de seguridad informática.

Durante años ha existido la ciberdelincuencia las cuales mediante virus realizaban sus ataques a los usuarios para el robo de identidad, información confidencial de sectores públicos y privado, los cuales se implementaron como solución antivirus, recientemente se ha tomado como medida la regulación en las leyes para la protección de datos y para castigar aquellas personas que se encuentren realizando ciberdelincuencia. En el 2010 entró en vigor la ley de protección de datos personales en posesión de particulares, Banamex incurrió en faltas por eso fue sancionado con multas por 16 millones de pesos en el 2013, ya que no contaba con la protección de información de sus clientes. (Congreso de los estados unidos mexicanos, 2013)

Toda empresa u organización debe estar a la vanguardia de los procesos de cambio, donde disponer de información continua y confiable en tiempo, constituye una ventaja fundamental. Donde obtener la información es tener poder, la seguridad informática debe tener, disponibilidad, integridad y confidencialidad.

La finalidad de la seguridad informática es permitir que una organización cumpla con todos sus objetivos de protección de datos, implementando nuevos sistemas de tecnologías de información en especial tomando en cuenta a los usuarios. La protección del sistema ante

cualquier amenaza potencial, la cual consiste en no permitir el acceso de una tercera persona al sistema de las empresas, una de las amenazas más frecuentes son los virus ya que se trata de programas maliciosos que generalmente se reproducen y afectan demasiado. La falta de seguridad a incrementado la manipulación, falsificación o alteración de la información, es por eso que los profesionales en el área deben estar conscientes de amenazas de seguridad en las computadoras.

De acuerdo con lo que comenta el Dr. Miguel Ángel Mendoza el apego a los estándares de seguridad permite la aplicación de las mejores prácticas utilizadas en la industria, ya que es posible utilizar un conjunto de acciones, metodologías, herramientas y técnicas, que han sido aplicadas y probadas con resultados favorables.

Un beneficio relacionado con las actividades que establecen los estándares consiste en la aplicación de la mejora continua, concepto que se encuentra implícito en el desarrollo de una organización. La alineación con los estándares contribuye a la mejora de procesos y madurez de las empresas, debido a que se deben documentar, comunicar, monitorear y medir. En niveles más elevados de madurez, las tareas se automatizan y optimizan; en niveles bajos, no se cuenta con procesos o procedimientos, las actividades se realizan de forma desorganizada o se inicia con el seguimiento de patrones regulares.

Además, se llevan a cabo evaluaciones periódicas para conocer la efectividad en la implementación de medidas de seguridad, la información sobre amenazas y vulnerabilidades se recolecta y analiza, se definen e implementan controles de seguridad idóneos para mitigar riesgos, y de manera general, las prácticas de seguridad y la tecnología relacionada se encuentran integrados en los procesos organizacionales. (Congreso de los estados unidos mexicanos, 2013)

2.3 Proveedores de los estándares de seguridad

En México se utilizan estándares establecidos de diferentes instituciones internacionales, nacionales y estatales, entre las cuales se encuentran los generados por:

2.3.1 La Organización Internacional de Estandarización

La Organización Internacional de Estandarización (ISO) es una organización independiente y no-gubernamental formada por las organizaciones de estandarización de sus 163 países miembros. Es el mayor desarrollador mundial de estándares internacionales voluntarios y facilita el comercio mundial al proporcionar estándares comunes entre países. Se han establecido cerca de veinte mil estándares cubriendo desde productos manufacturados y tecnología a seguridad alimenticia, agricultura y sanidad. (ISO, s.f.)

El uso de estándares facilita la creación de productos y servicios que sean seguros, fiables y de calidad. Los estándares ayudan a los negocios a aumentar la productividad a la vez que minimizan los errores y el gasto. Al permitir comparar directamente productos de diferentes fabricantes, facilita que nuevas compañías puedan entrar en nuevos mercados y ayudar en el desarrollo de un comercio global con bases justas. Los estándares también sirven para proteger a los consumidores y usuarios finales de productos y servicios, asegurando que los productos certificados se ajusten a los mínimos estandarizados internacionalmente. Algunos estándares para seguridad que ha establecido la Organización Internacional de Estandarización son los que se señalan a continuación:

Estándar ISO 17799

Establece pautas y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos descritos proporcionan orientación general sobre los objetivos comúnmente aceptados de la gestión de la seguridad de la información. ISO / IEC 17799: 2005 contiene las mejores prácticas de control de objetivos y controles en las siguientes áreas de gestión de seguridad de la información:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y ambiental.
- Comunicaciones y gestión de operaciones.

- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.
- Conformidad.

Los objetivos de control y los controles en ISO / IEC 17799: 2005 están destinados a ser implementados para cumplir con los requisitos identificados por una evaluación de riesgos. ISO / IEC 17799: 2005 está pensado como una base común y una guía práctica para desarrollar estándares de seguridad organizacionales y prácticas de administración de seguridad efectiva, y para ayudar a construir confianza en actividades inter-organizacionales.

Estándar ISO 27000

Proporciona la visión general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones que se usan comúnmente en la familia de estándares ISMS. Este documento es aplicable a todos los tipos y tamaños de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). El ISO 27000 contiene el vocabulario en el que se apoyan el resto de las normas

Estándar ISO 27001

Es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar.

Estándar ISO 27002

Se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles.

Estándar ISO 27003

Es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

Estándar ISO 27004

Describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.

Estándar ISO 27005

Es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.

Estándar ISO 27006

Es un conjunto de requisitos de acreditación de las organizaciones certificadoras.

Estándar ISO 27007

Es una guía para auditar SGSI. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

Estándar ISO 27010

Proporciona directrices además de la orientación proporcionada en la familia de normas ISO / IEC 27000 para implementar la gestión de la seguridad de la información dentro de las comunidades que comparten información.

Esta Norma Internacional proporciona controles y orientación específicamente relacionados con el inicio, la implementación, el mantenimiento y la mejora de la seguridad de la información en las comunicaciones entre organizaciones y entre sectores. Proporciona pautas y principios generales sobre cómo se pueden cumplir los requisitos especificados mediante la mensajería establecida y otros métodos técnicos.

Esta Norma Internacional es aplicable a todas las formas de compartir e intercambiar información sensible, tanto pública como privada, nacional e internacionalmente, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a intercambios de información y compartir información relacionada con la provisión, mantenimiento y protección de la infraestructura crítica de una organización o estado nación. Está diseñado para apoyar la creación de confianza al intercambiar y compartir información confidencial, lo que fomenta el crecimiento internacional de las comunidades de intercambio de información. (ISO, s.f.)

2.3.2 Ley Federal Mexicana de Telecomunicaciones

Capítulo I de las disposiciones generales (Ornelas, s.f.)

Artículo 1º. La presente Ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite.

Artículo 2º. Corresponde al Estado la rectoría en materia de telecomunicaciones, a cuyo efecto protegerá la seguridad y la soberanía de la Nación.
En todo momento el Estado mantendrá el dominio sobre el espectro radioeléctrico y las posiciones orbitales asignadas al país.

Artículo 3º. Para los efectos de esta Ley se entenderá por:

I. Banda de frecuencias: porción del espectro radioeléctrico que contiene un conjunto de frecuencias determinadas;

II. Espectro radioeléctrico: el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz; (Ornelas, s.f.)

III. Estación terrena: la antena y el equipo asociado a ésta que se utiliza para transmitir o recibir señales de comunicación vía satélite;

IV. Frecuencia: número de ciclos que por segundo efectúa una onda del espectro radioeléctrico;

V. Homologación: acto por el cual la Secretaría reconoce oficialmente que las especificaciones de un producto destinado a telecomunicaciones satisfacen las normas y requisitos establecidos, por lo que puede ser conectado a una red pública de telecomunicaciones, o hacer uso del espectro radioeléctrico;

VI. Orbita satelital: trayectoria que recorre un satélite al girar alrededor de la tierra;

VII. Posiciones orbitales geoestacionarias: ubicaciones en una órbita circular sobre el Ecuador que permiten que un satélite gire a la misma velocidad de rotación de la tierra, permitiendo que el satélite mantenga en forma permanente la misma latitud y longitud;

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

IX. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

X. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

XI. Secretaría: la Secretaría de Comunicaciones y Transportes;

XII. Servicios de valor agregado: los que emplean una red pública de telecomunicaciones y que tienen efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida por algún usuario y que comercializan a los usuarios información adicional, diferente o reestructurada, o que implican interacción del usuario con información almacenada; (Ornelas, s.f.)

XIII. Sistema de comunicación vía satélite: el que permite el envío de señales de microondas a través de una estación transmisora a un satélite que las recibe, amplifica y envía de regreso a la Tierra para ser captadas por estación receptora, y

XIV. Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

XV. Servicio de radiodifusión: servicio de telecomunicaciones definido por el artículo 2 de la Ley Federal de Radio y Televisión, y

XVI. Servicio de radio y televisión: el servicio de audio o de audio y video asociado que se presta a través de redes públicas de telecomunicaciones, así como el servicio de radiodifusión.

Artículo 7º. La presente Ley tiene como objetivos promover un desarrollo eficiente de las telecomunicaciones; ejercer la rectoría del Estado en la materia, para garantizar la soberanía nacional; fomentar una sana competencia entre los diferentes prestadores de servicios de telecomunicaciones a fin de que éstos se presten con mejores precios, diversidad y calidad en beneficio de los usuarios, y promover una adecuada cobertura social. (Ornelas, s.f.)

Para el logro de estos objetivos, corresponde a la Secretaría, sin perjuicio de las que se confieran a otras dependencias del Ejecutivo Federal, el ejercicio de las atribuciones siguientes:

I. Planear, formular y conducir las políticas y programas, así como regular el desarrollo de las telecomunicaciones, con base en el Plan Nacional de Desarrollo y los programas sectoriales correspondientes;

II. Promover y vigilar la eficiente interconexión de los diferentes equipos y redes de telecomunicación;

III. Expedir las normas oficiales mexicanas en materia de telecomunicaciones y otras disposiciones administrativas;

IV. Acreditar peritos en materia de telecomunicaciones;

V. Establecer procedimientos para homologación de equipos;

VI. Elaborar y mantener actualizado el Cuadro Nacional de Atribución de Frecuencias;

VII. Gestionar la obtención de las posiciones orbitales geoestacionarias con sus respectivas bandas de frecuencias, así como las órbitas satelitales para satélites mexicanos, y coordinar su uso y operación con organismos y entidades internacionales y con otros países;

VIII. Participar en la negociación de tratados y convenios internacionales en materia de telecomunicaciones, considerando, entre otros factores las diferencias existentes del sector con respecto al de los países con que se negocie, y vigilar su observancia;

IX. Adquirir, establecer y operar, en su caso, por sí o a través de terceros, redes de telecomunicaciones;

X. Promover el fortalecimiento de los valores culturales y de la identidad nacional;

XI. Promover la investigación y el desarrollo tecnológico en materia de telecomunicaciones, la capacitación y el empleo de mexicanos cuyas relaciones laborales se sujetarán a la legislación de la materia;

XII. Interpretar esta Ley para efectos administrativos;

XIII. Supervisar a través de la Comisión Federal de Telecomunicaciones, la elaboración y actualización por parte de los concesionarios del Registro Nacional de Usuarios de Telefonía Móvil, y

XIV. Las demás que esta Ley y otros ordenamientos legales le confieran en la materia. (Ornelas, s.f.)

2.3.3 Código Penal Federal Mexicano

El Código Penal Federal Mexicano regula las sanciones desde el ámbito legal aplicadas a las intervenciones irregulares dentro de la informática, esto incluye la comunicación empleada en el servicio de Telemedicina utilizado en Quintana Roo. (Cuervo, 2018)

Artículo 210. Sobre revelación de secretos.

Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211. Sobre revelación de secretos.

La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 bis. Sobre revelación de secretos.

A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Artículo 211 bis 1. Sobre acceso ilícito a sistemas y equipos de informática.

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2. Sobre acceso ilícito a sistemas y equipos de informática.

Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. (Cuervo, 2018)

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3. Sobre acceso ilícito a sistemas y equipos de informática.

Al que, estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días de multa.

Al que, estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

2.3.4 Normatividad en Tecnologías de la Información para la Secretaría de Salud

A continuación, se mencionarán los artículos que atañen al proyecto (FEDERAL)

Artículo 1. Sobre Lineamientos generales

Se entiende por Tecnologías de la Información -TI, al conjunto de:

a) Equipos de cómputo y comunicaciones. Equipos diversos como equipo médico, que utiliza o se comunica con computadoras o equipos de datos, son considerados como TI.

b) Software y sus licencias

c) Sistemas de Información, en el marco de las atribuciones de la DGTI.

d) Redes de voz, datos y video.

e) Protocolos de intercambio de información.

f) Recursos Humanos especializados en las áreas afines.

g) Equipos y sistemas de Seguridad informática.

h) Datos e información.

i) Centros de cómputo.

j) Contratos y convenios con elementos afines. (Secretaría de Salud, s.f.)

Artículo 4. Sobre Estrategia General

La Secretaría de Salud considerará para sus desarrollos y adquisiciones por igual Software propietario y de Software Libre. Para un mismo propósito, se deberá seleccionar la propuesta más adecuada para los fines que se pretenden, privilegiando la menos costosa en su caso.

Artículo 5. Sobre Estrategia General

La Secretaría utilizará productos que utilicen estándares abiertos para intercambio de información, operación y comunicación (interoperabilidad) en todos los desarrollos posteriores a la emisión de esta normatividad.

Artículo 8. Sobre Dictaminación

La DGTI dictaminará técnicamente, todos los proyectos de TI de los sujetos obligados, tanto los desarrollados con personal o recursos internos como los externos, de acuerdo a los

procedimientos y formatos publicados en http://norma-ti.salud.gob.mx (Al momento de desarrollar este documento, la liga publicada se encontraba fuera de línea, incluso el dominio salud.gob.mx no era reconocido, al realizar la búsqueda lo encontré en la siguiente URL: http://www.comeri.salud.gob.mx/descargas/Historico/Normatividad_Tecnologias_de_la_Informacion_2006.pdf).

Artículo 9. Sobre Dictaminación.

Cada sujeto obligado asignará un responsable de Tecnologías de la Información cuyas funciones quedarán establecidas en la página http://norma-ti.salud.gob.mx

Artículo 10. Sobre Dictaminación.

El responsable de Tecnologías de la Información deberá estar certificado por la DGTI.

Artículo 17. Sobre Infraestructura

Los sujetos obligados deberán contar con el inventario de recursos de TI actualizado y enviarlo anualmente durante el mes de marzo a la DGTI, de acuerdo a los procedimientos aprobados por el COMERI y publicados en http://norma-ti.salud.gob.mx.

Artículo 18. Sobre Infraestructura

El responsable de TI, es el encargado de conformar el inventario de TI y de enviarlo oportunamente.

Artículo 21. Sobre Infraestructura

El servicio de redes de voz, datos, video e Internet será administrado por la DGTI en todas las instalaciones de los sujetos obligados. (Secretaría de Salud, s.f.)

Artículo 22. Sobre Infraestructura

Todo elemento de Tecnologías de la Información deberá utilizarse para los fines institucionales a que este afecto, dándoles un uso y mantenimiento adecuado de acuerdo a sus manuales y guías, además de lo dispuesto por la presente Normatividad. La infraestructura de

comunicaciones para acceso a la red pública y el software de cada equipo deben ser utilizados para intereses y tareas relacionados con el trabajo de la Secretaría.

Artículo 24. Sobre Infraestructura

Debe usarse una interfaz WEB para la interacción con el usuario en todo sistema desarrollado por y para la Secretaría.

Artículo 27. Sobre Centro de Datos y Telecomunicaciones

Todos los servidores deberán residir en el centro o centros de datos de la Secretaría de Salud que la DGTI determine.

Artículo 29. Sobre Centro de Datos y Telecomunicaciones

La información depositada en los servidores de la Secretaría es responsabilidad del área solicitante del recurso asignado en los mismos.

Artículo 38. Sobre Sistemas

Todos los sistemas que sean desarrollados por o para la Secretaría de Salud o que sean adaptados para su utilización en esta, pasarán a ser de su propiedad bajo los lineamientos del "Programa Institucional de Desarrollo de Software de la Secretaría de Salud" y deberán contar con el código fuente y licencia para ser usados, actualizados, modificados conforme a las necesidades y conveniencia de la Secretaría de Salud. (Secretaría de Salud, s.f.)

2.3.5 Políticas y Lineamientos de Seguridad Informática

En el caso exclusivo de estos lineamientos pertenecientes al Estado de México, concorde a la investigación realizada atañen al proyecto y posee posibles sugerencias del manejo de los estándares. (Ornelas, s.f.)

Este documento es publicado por la Dirección de Telecomunicaciones de la Dirección General del Sistema Estatal de Informática en la página de dicha Dirección General en la URL: http://dgsei.edomex.gob.mx/ . Las políticas y lineamientos aplican para su aplicación por todas las áreas de Tecnologías de la Información del Poder Ejecutivo del Estado de México, incluyendo el personal bajo contrato por tiempo determinado, los proveedores y todos los sistemas informáticos y de comunicaciones utilizados por los servidores públicos del Poder Ejecutivo. Estos sistemas incluyen las redes de área local, las computadoras personales (PC) y demás sistemas administrativos, los centros de procesamiento locales de cómputo, de telecomunicaciones y de conmutación, los proveedores de servicios de Internet (ISP) y otros

proveedores externos de servicios de información. Políticas y Lineamientos de Seguridad Informática | Dirección General del Sistema Estatal de Informática (edomex.gob.mx) .

2.3.5.1 Política de seguridad informática

Definición Técnica

La Seguridad Informática implica la protección de la información en términos de:

a) Confidencialidad: divulgar información sólo a las personas y los procesos autorizados.

b) Integridad: garantiza la exactitud e integridad de la información.

c) Disponibilidad: asegura el acceso y la utilización oportunos de la información y los sistemas de información como se requiera, y la protección de los equipos, software y demás activos de tecnología informática.

Alcance

Esta política se aplica a todos los servidores públicos, proveedores, sistemas informáticos, software, documentación o información, equipos y demás recursos de Tecnologías de la Información utilizados por las Unidades de Tecnologías de la Información y la propia DGSEI.

Inventario de activos

Se debe llevar un inventario centralizado y actualizado de los recursos de Tecnología de Información de la institución, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan.

Uso aceptable de activos

Se debe llevar un inventario centralizado y actualizado de los recursos de Tecnología de Información de la institución, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan. (Ornelas, s.f.)

Clasificación de la Información

Los activos informáticos deben estar clasificados con base al impacto que representan en la institución, y además en sus propiedades de seguridad como confidencialidad, disponibilidad

e integridad. Los dueños de los activos de información deben responsabilizarse de las necesidades de la institución para clasificar, valuar y compartir o restringir información, así como del impacto asociado a estas necesidades. Para la incorporación de activos de información al inventario, se debe asignar una clasificación de seguridad y debe ser proporcionada por el dueño del activo.

Etiquetado y manejo de la información

Toda la información que se encuentre almacenada en papel o medios magnéticos y ópticos, se debe etiquetar indicando su tipo de clasificación para facilitar su control, manejo y cuidado por parte del personal. (Ornelas, s.f.)

Capacitación del Personal en materia de Seguridad de la Información

La Dirección General debe considerar en su plan de trabajo el proporcionar a los servidores públicos responsables de Tecnologías de la Información y Comunicaciones, programas de concientización, educación y capacitación adecuados en función de las necesidades, para que estos a su vez lo transmitan hacia los usuarios de los activos de información. El personal debe recibir capacitación periódica (1 vez al año) que lo concientice sobre problemas de seguridad de la información. Los usuarios deben recibir capacitación periódica (1 vez al año) que los concientice a una cultura de seguridad de la información. Deben existir métodos que permitan afianzar la cultura de seguridad en el personal como:

- Correos electrónicos.
- Promover videos institucionales.
- Promover pláticas de seguridad.
- Promover carteles o trípticos en materia de seguridad.

2.4 Sistema de gestión de la seguridad de la información (SGSI)

Independientemente del tipo de actividad y tamaño, cualquier organización recopila, procesa, almacena y transmite información mediante el uso y aplicación de procesos, sistemas, redes y personas internos y/o externos. (Díaz & Rojas, 2015)

En función del contexto (tipo de industria, entorno de actuación, ...) y de cada momento particular en que se desarrollan sus actividades, las organizaciones están inevitablemente expuestas a situaciones de riesgo en base a diversos factores que pueden afectar y que, de hecho, afectan negativamente a los activos de información más necesarios.

La supervivencia de las organizaciones depende en gran medida de una correcta identificación de los factores más relevantes y la apropiada valoración del grado de incertidumbre asociado a la posibilidad real de introducir efectos negativos en los activos de información y la consecución de los objetivos de la organización. (Díaz & Rojas, 2015)

Toda la información almacenada y procesada por una organización está expuesta ante amenazas de ataque (por intereses comerciales, intelectuales y/o chantaje y extorsión), error (intencionado o por negligencia), ambientales (por ej. inundación o incendio), fallo en los sistemas (de almacenamiento de datos, informáticos, redes telemáticas), entre otras y también está sujeta a vulnerabilidades que representan puntos débiles inherentes a su propio uso en el ciclo de vida.

Para poder interrelacionar y coordinar las actividades de protección para la seguridad de la información, cada organización necesita establecer su propia política y objetivos para la seguridad de la información dentro de la coherencia del marco de globales de la organización.

Una vez fijados los objetivos en seguridad de la información necesitamos asegurar el modo de poder lograrlos eficazmente, en definitiva, un sistema de gestión de la seguridad de la información o SGSI en su forma abreviada. (Lara, s.f.)

Un SGSI desde la visión del estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro, ...).

2.4.1 Características de un SGSI

Los SGSI como estructura tienen ciertas características que cumplir para ser eficaz en el cumplimiento de sus objetivos, las principales se nombran a continuación.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO, s.f.)

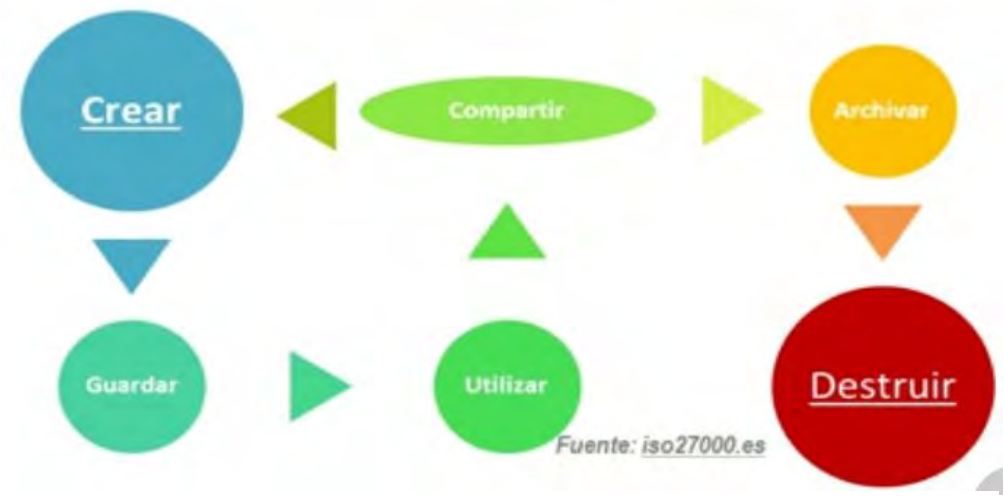

Ilustración 1Características de un SGSI Fuente: ISO27000.es

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran. acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO, s.f.)

2.4.2 Beneficios y costes de un SGSI

Al ser un sistema basado en estándares los beneficios son directos y puntuales mientras que en el lado de los costes son los esperados haciendo mayor referencia a implementación de tiempo y organización que de recursos materiales. (Intedya, 2015)

-Confianza y satisfacción de los requisitos de seguridad de la información por los clientes y otras partes interesadas.

-Establecimiento de una metodología de gestión de la seguridad clara y estructurada cumpliendo con los reglamentos, la legislación y las exigencias de la industria.

-Gestionar los activos de información de manera organizada que facilite la mejora continua y el ajuste a los objetivos organizacionales en cada momento sin una compra sistemática de productos y tecnologías. (Intedya, 2015)

-Reducción del riesgo de pérdida, robo o corrupción de información con la posibilidad de continuar la actividad después de un incidente grave (debido cuidado y diligencia).

Ilustración 2 Costes y Beneficios de un SGSI Fuente: ISO27000.es

2.4.3 Implantación de un SGSI

Las actividades propias para la implantación inicial de un SGSI y su posterior mantenimiento se deben considerar como un proyecto más que aborda la organización mediante la

determinación de unas actividades críticas para el éxito del proyecto que llevan asociadas una planificación con los responsables principales, los recursos necesarios y los posibles riesgos asociados al proyecto. (Intedya, 2015)

Alcance del SGSI

El alcance del SGSI aclara los límites del SGSI en función del contexto o importancia y ubicación de los activos críticos de información de la organización (por ejemplo, unidades, ubicaciones o departamentos) y los riesgos propios o externos asociados (p.ej. leyes y reglamentos, obligaciones contractuales, estrategias y políticas impuestas por organismos centrales).

Se debe tener en cuenta de los flujos de información que cruza los límites del alcance.

Una estrategia de alto nivel impulsada por la organización o una declaración de visión (ya sea hecha o al menos formalmente respaldada por la alta gerencia) es una forma de cristalizar tanto el alcance como el propósito de aplicación del SGSI, y puede ser útil para fines de concientización así como de promoción. (Intedya, 2015)

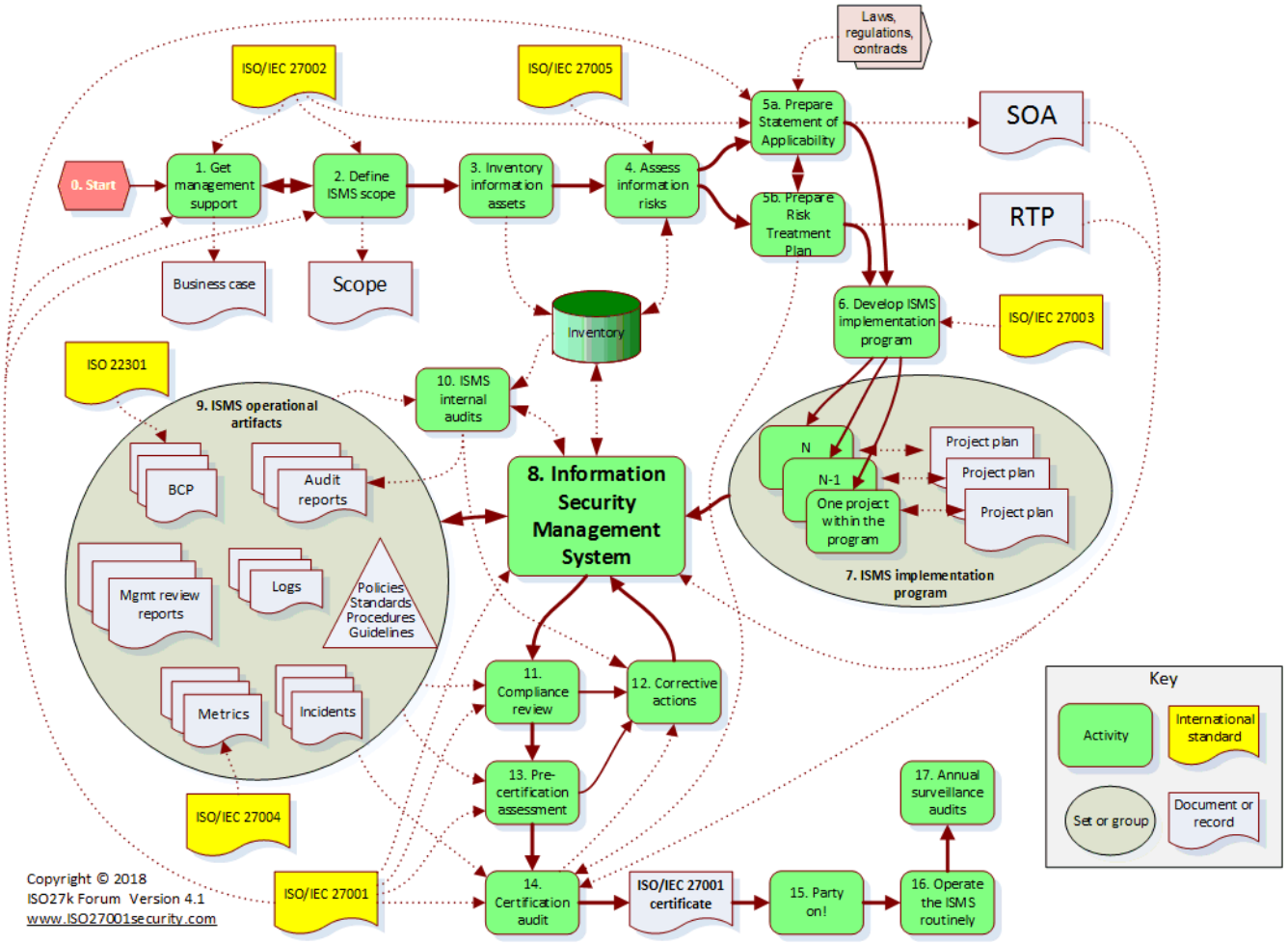

Ilustración 3 Estructura interna de un SGSI Fuente: ISO27000

Política del SGSI

Establece y confirma el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del SGSI, entre otros posibles aspectos relevantes.

La alta gerencia puede preferir una política de tipo de gobierno única, sucinta, amplia / general o puede adoptar un enfoque diferente. (Intedya, 2015)

Evaluación de riesgos

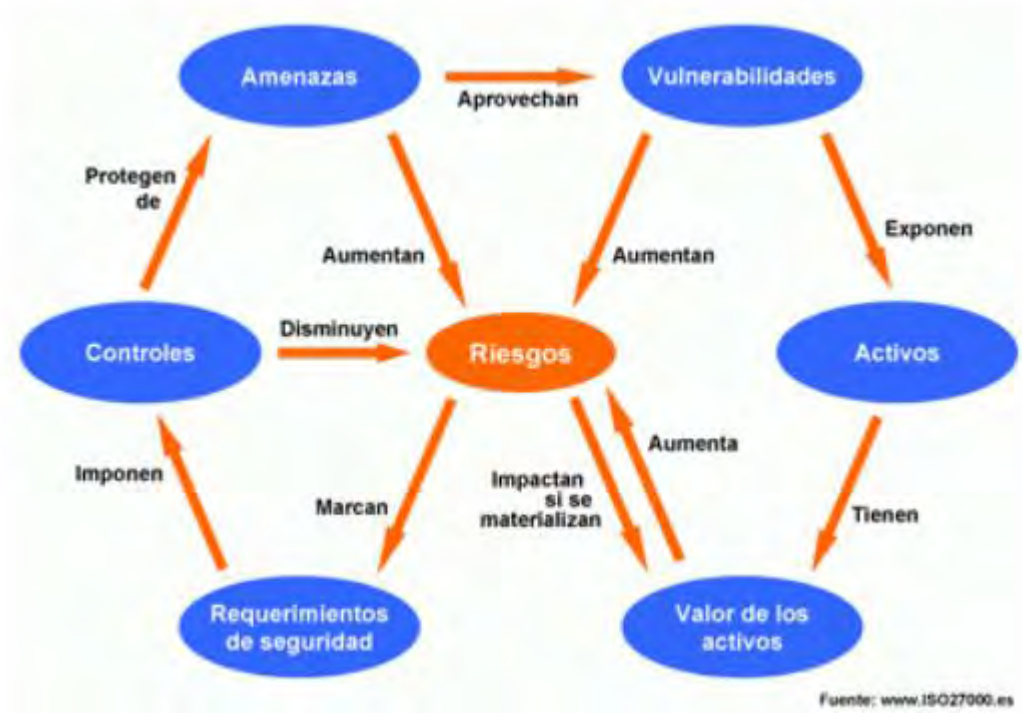

ILUSTRACIÓN 4EVALUACIÓN DE RIESGOS DE UN SGSI FUENTE: ISO27000

2.5 Sistema de Información Hospitalaria

Según Francisco J. Fernández Puerto y Florina Gatica Lara en su compilación para la Universidad Nacional Autónoma de México de la Facultad de Medicina sobre el sistema de Información Hospitalaria, "Es un sistema de información orientado a satisfacer las necesidades de generación de información, planeación y preparación**.** En esta fase se inicia con la Metodología, identificando los usuarios, determinar el alcance y enfoque del método y definir casos específicos de actuación con vías de escalada para almacenar, procesar y reinterpretar datos médico-administrativos de cualquier institución hospitalaria. Permitiendo la optimización de los recursos humanos y materiales, además de minimizar los inconvenientes burocráticos que enfrentan los pacientes. Todo sistema de información hospitalaria genera reportes e informes dependiendo el área o servicio para el cual se requiera, dando lugar a la retroalimentación de la calidad de la atención de los servicios de salud".

2.5.1 Tipos de Sistemas de Información

Entre los tipos de sistemas de información encontramos los siguientes:

a) Sistemas Económico-Financiero.

b) Sistemas Administrativos.

c) Sistemas para Registro Central de Pacientes.

d) Sistema de Manejo de Materiales.

Los sistemas económico-financieros en medicina, llamados sistemas de economía médica se clasifican en:

a) Sistemas de nómina y de personal.

b) Sistema de manejo de materiales.

c) Sistema de cargos y cobros.

d) Sistema de pagos.

e) Sistema de contabilidad.

Los sistemas administrativos, según Huesing, se clasifican en:

a) Sistema para registro central de pacientes.

b) Sistema para admisión, altas y transferencias de pacientes.

c) Sistema para el control de citas y programación de servicios.

d) Sistema para el procesamiento y edición de documentos (historias clínicas, reportes, recetas, etc.).

El sistema para registro central de pacientes es uno de los sistemas medulares, porque permite tener una base de datos de tipo demográfico, información de asegurados, datos clínicos, estadísticos y algunos otros datos de interés administrativo. Se caracterizan por utilizar una identificación numérica para cada uno de los pacientes. Normalmente actúan como sistema base para todos los demás sistemas, ya sean clínicos, financieros o administrativos relacionados con el paciente.

También han sido utilizados como base para obtener datos de poblaciones para modelos de planeación de salud pública. El sistema de manejo de materiales (inventarios), lo más importante de estos sistemas es la dinámica de la información ya que se obtienen cotizaciones, información de precios, proveedores, registro de proveedores, contratos, control de inflación de abusos, tasa de inflación y decisiones de concurso para aprobar la compra de un artículo y evitar abusos, etc. También se orienta mucho al inventario en farmacia, ayudando así a mantener el control de medicamentos y la administración de estos a los pacientes.

2.5.2 Requerimientos tecnológicos de un Sistema de Información Hospitalaria

Todo sistema de información hospitalaria requiere de:

a) Una red de comunicaciones: tipos de redes (Intranet e Internet).

b) Equipo de cómputo (hardware): dependiendo de la infraestructura y la posibilidad económica de las instituciones.

c) Software de base: selección de plataforma con la cual se programará el sistema, que debe ser amigable al usuario.

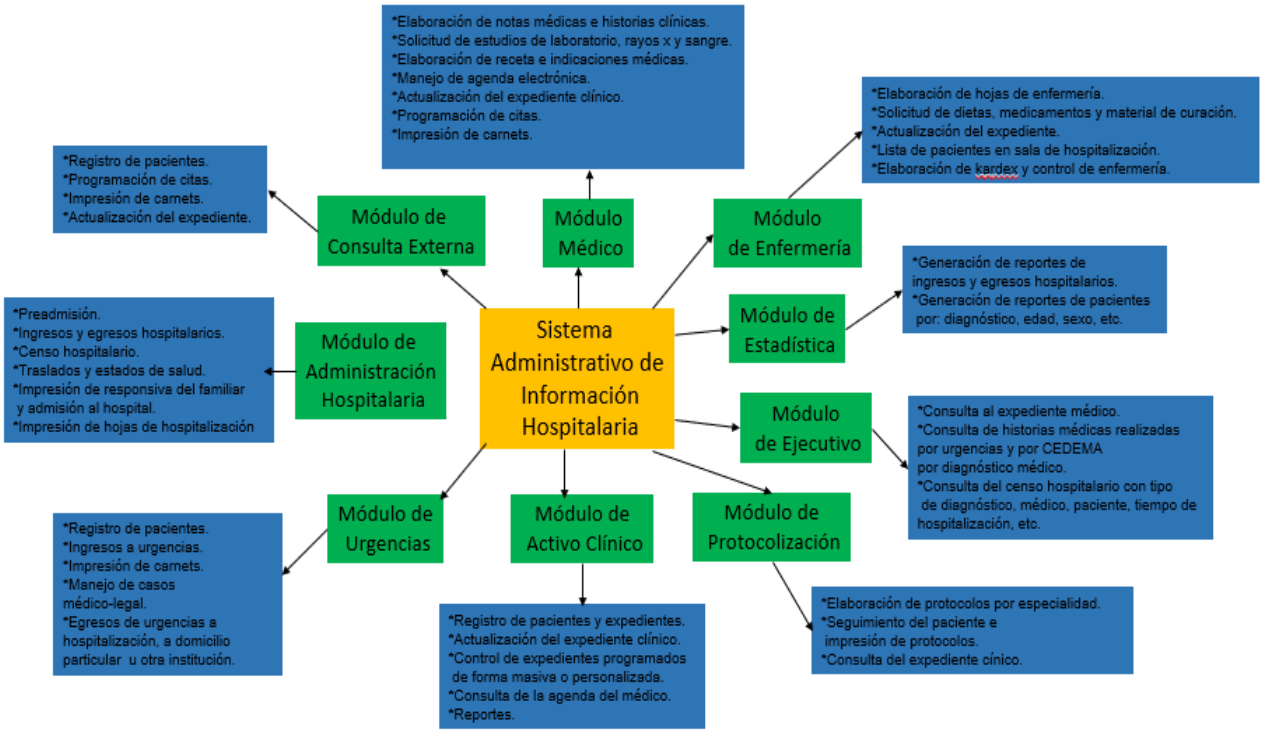

Ilustración 5: Sistema Administrativo de Información Hospitalaria, fuente: compilación para la Universidad Nacional Autónoma de México de la Facultad de Medicina sobre el sistema de Información Hospitalaria.

2.5.3 Electronic Medical Record (Historial Clínico Electrónico)

Los sistemas de EMR fueron inicialmente desarrollados para gestionar los datos de facturación y aseguradora del paciente, pero, a medida que se incrementó el rango de intercambio de datos médicos, estos sistemas fueron desarrollados para uso clínico.

Los sistemas de EMR almacenan electrónicamente datos del paciente de forma eficiente y segura en un repositorio central de datos que puede ser accedido por diversas personas al mismo tiempo, como se muestra en la figura 6.

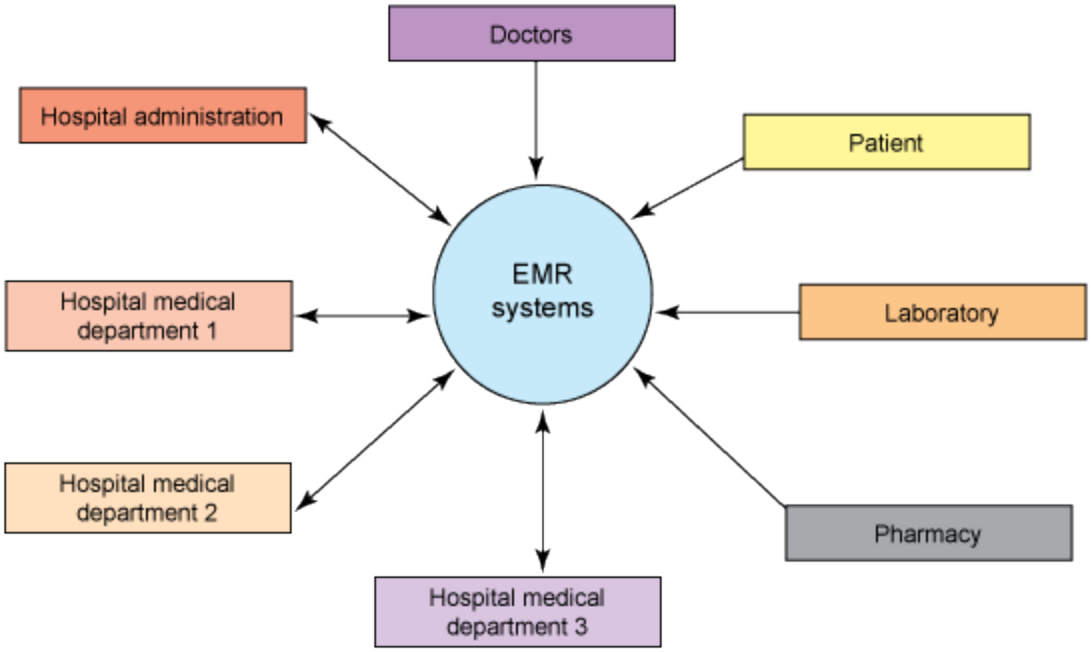

Ilustración 6 Personal afín al Historial Clínico Electrónico fuente; Requerimientos tecnológicos de un Sistema de Información Hospitalaria

2.5.4 Ventajas de utilizar un sistema de EMR

- **Reducción de costos a largo plazo**: Aunque el costo de configuración es alto, con el tiempo, el costo es mucho más bajo que el de un sistema tradicional. El almacenamiento electrónico de datos elimina los costos de almacenamiento de papel.

- **Tiempo de espera reducido**: Los datos están disponibles en la punta de sus dedos con sistemas de EMR, de forma que no necesita esperar los datos del paciente para el diagnóstico y el tratamiento. También, ya que el e-mail es el modo principal de comunicación, el intercambio de datos es muy rápido y efectivo.

- **Sin repeticiones**: Los sistemas de EMR almacenan los datos centralmente donde todos los departamentos puedan accederlos. Esto elimina la repetición de datos de los pacientes a través de los departamentos.

- **Comunicación efectiva**: Ya que el paciente, el hospital, la farmacia y el laboratorio están conectados centralmente, pueden comunicarse entre sí de forma mucho más rápida que con el sistema tradicional.

- **Tratamiento de más alta calidad**: Los registros electrónicos almacenados de forma apropiada no pueden estar mal archivados o en el lugar inapropiado. Con el historial del paciente a la mano, el médico puede analizar las condiciones previas de salud y proporcionar un mejor cuidado.

- **Precisión de los datos**: Un sistema de EMR elimina el problema de entender la letra a mano ilegible de los doctores y enfermeras.

- **Soluciones de software de código abierto**: Las soluciones de software de código abierto son gratuitas y ofrecen una alta calidad de servicio. Muchas instituciones pequeñas están adoptando sistemas de EMR utilizando soluciones de código abierto. Existe una variedad inmensa de estas soluciones disponibles para sistemas de EMR.

  Algunas de las ofertas destacadas de código abierto incluyen:

  1. OpenEMR
  2. OpenMRS
  3. VistA
  4. GNUmed

  Muchos de estos sistemas cumplen con los estándares médicos de software exigidos por el gobierno federal mediante la *National Health Information Infrastructure*.

2.5.5 Estándares médicos de software

Un estándar comprende un grupo de reglas y definiciones que especifican cómo llevar a cabo un proceso. Los estándares son útiles para la IM porque ayudan a armonizar los métodos de

gestión y análisis de información. Estos métodos se basan principalmente en el empleo de un lenguaje común y el uso de terminología médica específica. El uso de un lenguaje estándar permite el intercambio de información entre sistemas de historias clínicas electrónicas (HCE), favorece la extracción eficiente de información de las bases de datos, contribuye al desarrollo de sistemas de soporte diagnóstico, habilita la minería de datos y facilita la evaluación estadística.

2.5.5.1 HL7

Health Level Seven es un conjunto de estándares para facilitar el intercambio electrónico de información clínica. HL7 utiliza una notación formal de modelado (UML) y un metalenguaje extensible de marcado con etiquetas (XML). De esta forma, el estándar define la estructura de los metadatos a intercambiar entre sistemas de HCE, para garantizar así la comunicación sintáctica entre ellos. (Citron Health, 2019)

2.5.5.2 DICOM

Digital Imaging and Communication in Medicine es el estándar reconocido mundialmente para el intercambio de estudios imagenológicos, pensado para su manejo, visualización, almacenamiento, impresión y transmisión. Incluye la definición de un formato de fichero y de un protocolo de comunicación de red. Este último es un protocolo de aplicación que usa TCP/IP para la comunicación entre sistemas. Los ficheros DICOM pueden intercambiarse entre dos entidades que tengan capacidad de recibir imágenes y datos de estudios en formato DICOM. (Citron Health, 2019)

2.5.5.3 SNOMED-CT

SNOMED o SNOMED Términos Clínicos es una colección semánticamente organizada de términos médicos que proporciona los códigos, los términos, sinónimos y definiciones utilizadas en la documentación clínica y los informes. Se considera que es la terminología de la salud clínica más completa y multilingüe en el mundo, cuyo propósito principal es codificar los términos que se utilizan en la información de salud para apoyar la aplicación efectiva del almacenamiento de los datos clínicos con el objetivo de mejorar la atención al paciente.

SNOMED CT ofrece la terminología general para los historiales médicos electrónicos. Su amplia cobertura incluye: hallazgos clínicos, síntomas, diagnósticos, procedimientos, estructuras corporales, organismos y otras etiologías, sustancias, productos farmacéuticos, dispositivos y especímenes. (Citron Health, 2019)

2.5.5.4 CIE 10

La CIE 10 es el acrónimo de la Clasificación Internacional de Enfermedades, Décima Versión correspondiente a la versión en español de la (en inglés) ICD, siglas de *International Statistical Classification of Diseases and Related Health Problems*) y determina la clasificación y codificación de las enfermedades y una amplia variedad de signos, síntomas, hallazgos anormales, denuncias, circunstancias sociales y causas externas de daños y/o enfermedad.

2.5.5.5 LOINC

Logical Observation Identifiers Names and Codes (LOINC) es una base de datos y el estándar universal para la identificación de los exámenes de laboratorio. Desarrollado por primera vez en 1994, que fue creado y es mantenido por el Instituto Regenstrief, una organización de investigación médica sin fines de lucro de Estados Unidos. LOINC fue creado en respuesta a la demanda de una base de datos electrónica para la atención clínica y de gestión y está disponible al público sin costo alguno. Está respaldada por la Asociación Americana del Laboratorio Clínico y el Colegio Americano de Patólogos. (Citron Health, 2019)

2.5.5.6 ATC

El código ATC o Sistema de Clasificación Anatómica, Terapéutica, Química (ATC: acrónimo de *Anatomical, Therapeutic, Chemical Classification system*) es un índice de sustancias farmacológicas y medicamentos, organizados según grupos terapéuticos. Este sistema fue instituido por Organización Mundial de la Salud. El código recoge el sistema u órgano sobre el que actúa, el efecto farmacológico, las indicaciones terapéuticas y la estructura química del fármaco.

2.6 Servicio de Telemedicina en Quintana Roo

2.6.1 Servicios de directorio

Los directorios de dominio permiten administrar objetos de la red y sus relaciones. En ellos se administran usuarios, servidores o máquinas de escritorio, se guarda información personal y de oficina, se otorgan permisos, se agrupan y brinda seguridad. (Secretaría de Salud, 2002)

2.6.1.1 Dominio

Un dominio es una agrupación lógica de objetos que permite la administración central y el control sobre la replicación de esos objetos. Cada organización tiene al menos un dominio, que se implementa cuando se instala el directorio activo en el primer controlador de dominio.

2.6.1.2 Controlador de dominio

Los controladores de dominio de directorio activo son quizás el tipo más importante de servidor de red en una red de Windows. Los controladores de dominio también son uno de los servidores más utilizados en una red de Windows, por lo que es importante evaluar de manera realista los requisitos operativos y el rendimiento del servidor para cada uno.

2.6.1.3 Cuenta de usuario

En el directorio activo, la cuenta de usuario del dominio contiene el nombre de usuario, la contraseña, los grupos de los que el usuario es miembro y otra información descriptiva, como direcciones y números de teléfono, así como muchas otras descripciones y atributos de los usuarios, como seguridad y acceso remoto.

2.6.1.4 Dominio de directorio activo, árboles y bosques

Dentro del directorio, los objetos se organizan mediante una estructura de árbol jerárquica denominada árbol de directorios. La estructura de la jerarquía se deriva del esquema y se utiliza para definir las relaciones padre-hijo de los objetos almacenados en el directorio.
Una agrupación lógica de objetos que permite la administración central de esos objetos se denomina dominio. En el árbol de directorios, un dominio se representa como un objeto. De hecho, es el objeto principal de todos los objetos que contiene. (Secretaría de Salud, 2002)

2.6.1.5 Gestión TCP/IP

El protocolo clave que usará es el Protocolo de control de transmisión/Protocolo de Internet (TCP/IP). TCP/IP es en realidad una colección de protocolos y servicios utilizados para comunicarse a través de una red. Es el protocolo principal utilizado para las comunicaciones entre redes. En comparación con la configuración de otros protocolos de red, la configuración de las comunicaciones TCP/IP es bastante complicada, pero TCP/IP es el protocolo más versátil disponible. (Secretaría de Salud, 2002)

2.6.2 Alcance

Con la implementación de la plataforma de videoconferencias se pretende interconectar los sitios descritos en la tabla número dos, esto con el fin de mejorar la salud de un paciente, (Universidad de Quintana Roo, 2018) permitiendo la comunicación interactiva en tiempo real entre el paciente, y el médico o profesional a distancia.

Tabla 1 Alcance del Proyecto fuente; Diseño, implementación y puesta en marcha de un Sistema de Atención y Capacitación Médica Especializada a Distancia (SACMED)para ampliar la cobertura y aumentar la calidad de los servicios en salud en comunidades marginadas de

Hospital General de Chetumal	Teleconsulta
Hospital General de Chetumal	Auditorio
Uneme Cisame de Chetumal	Sala de usos múltiples
Hospital Integral de José María Morelos	Consultorio
Hospital General de Felipe Carrilo Puerto	Consultorio de medicina interna
Hospital General de Felipe Carrilo Puerto	Sala de enseñanza
Uneme de enfermedades crónicas de Felipe Carrillo Puerto	Sala de usos múltiples
Hospital General de Playa del Carmen	Teleconsulta
Hospital General de Playa del Carmen	Auditorio
Hospital General de Cancún	Teleconsulta
Hospital General de Cancún	Auditorio
Jurisdicción Sanitaria Número 2	Sala de enseñanza
Hospital Comunitario de Isla Mujeres	Consultorio 1
Hospital Comunitario de Isla Mujeres	Aula de usos múltiples
Hospital Integral de Kantunilkín	Consultorio 2
Hospital Integral de Kantunilkín	Aula de prospera

Capítulo 3 CONCLUSIONES

En materia de Estándares de Seguridad relacionados a la Telemedicina en lo que compete al Estado de Quintana Roo; México, hay un proceso bastante elevado de competencia y capacitación, desde luego no es completa ya que durante el proceso de investigación salió a exponer que hay varios procesos que se podrían agregar, modificar o retirar.

Debido al ámbito federal que se maneja en los proyectos de este tema siempre van a estar relacionados a las leyes implementadas en el país, aun así, con los conocimientos recabados a través de proyectos y documentos se puede destacar que hay perspectivas a las que hacer referencia cuando se elaboran proyectos en este sentido, desde la capacitación al personal médico hasta la protección directa del Hardware en el que se transitarán los datos de los pacientes, que es precisamente por quienes se realiza este proceso de investigación, habría que entrar más a fondo respecto que normas son repetidas, competentes y elaborar en torno a ello un solo documento en el que se entienda perfectamente las normas que deben seguir para proyectos independientemente del nivel que se planteen dichos proyectos.

La seguridad dentro de la Informática en ámbito de salud es relevante debido a que muchos datos deben mantenerse en calidad de médico-paciente y no deben ser externados bajo ningún concepto, hablando tanto a nivel de leyes como moralmente son datos delicados que merecen la mayor protección que se pueda brindar. La seguridad como se a mencionado en este proyecto debe iniciar con las personas, pasar por el hardware y terminar en la red ya que con que una sola de esas partes se vea comprometida no importa la protección en cualquiera de las otras.

Los estándares son especialmente eficaces en la implementación de seguridad, son realizados con base en criterios y estudios de diversas organizaciones y personas especializadas, por lo que son los mejores para la elección de lineamientos dentro de empresas o, en este caso, hospitales y siendo de libre conocimiento estos, no hay ventajas sobre estos de elegir soluciones personalizadas.

Los riesgos de no tomar en cuenta los estándares de seguridad se pueden definir entre términos como, robos, estafas, comprometimiento de datos, generación de caos entre otros, se puede concluir como si la información es robada o perdida se puede afectar tanto a las instituciones como a las personas dentro de las mismas.

Referencias

Advisery. (s.f.). Obtenido de 27001 Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

Citron Health. (2019). Retrieved from https://chironhealth.com/telemedicine/what-is-telemedicine/

Congreso de los estados unidos mexicanos. (2013). *Ley Federal de Telecomunicaciones.* Diario Oficial de la Federacion.

Cuervo, I. V. (2018). *Informática Jurídica*. Obtenido de http://www.informatica-juridica.com/legislacion/mexico/#toc-proteccin-de-datos-personales

Díaz, A. R., & Rojas, A. C. (21 de 3 de 2015). *Mediagraphic.com.* Obtenido de https://www.medigraphic.com/pdfs/infodir/ifd-2015/ifd1521b.pdf

Intedya. (01 de 09 de 2015). Obtenido de ISO 27000 y el conjunto de estándares de Seguridad de la Información: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

ISO. (s.f.). *International Organization for Standardization*. Obtenido de https://www.iso.org/search.html?q=17799

Krishna, S. (s.f.). *IBM Developer*. Obtenido de https://www.ibm.com/developerworks/ssa/industry/library/ind-openemr/index.html

Lara, F. J. (s.f.). *Sistema de informacion hospitalaria UNAM*. Obtenido de http://www.facmed.unam.mx/emc/computo/ssa/HIS/his.pdf

Marco Normativo INAI. (s.f.). Obtenido de http://inicio.inai.org.mx/SitePages/marcoNormativo.aspx?a=proteccion

MedLine Plus. (4 de Mayo de 2021). Obtenido de https://medlineplus.gov/telehealth.html

NORMA Oficial Mexicana NOM-024-SSA3-2010. (s.f.). Obtenido de http://www.dof.gob.mx/normasOficiales/4151/salud/salud.htm

Ornelas, F. H. (s.f.). *Politicas y Lineamientos de Seguridad Informatica del estado de mexico*. Obtenido de http://dgsei.edomex.gob.mx/politicas_lineamientos

Secretaría de Salud. (2002). *e-Salud*, Primera Edicion. Obtenido de http://www.salud.gob.mx/unidades/cdi/documentos/esalud.pdf

Secretaría de Salud. (s.f.). *Normatividad en Tecnologías de la Información para la Secretaría de Salud*. Obtenido de http://www.comeri.salud.gob.mx/descargas/Historico/Normatividad_Tecnologias_de_la_Informacion_2006.pdf

Torres, I. V. (s.f.). *Informática Jurídica.com*. Obtenido de http://www.informatica-juridica.com/legislacion/mexico/#toc-proteccin-de-datos-personales

Universidad de Quintana Roo. (31 de 12 de 2018). Obtenido de http://saladeprensa.uqroo.mx/noticias/4489-entregara-uqroo-en-2019-el-sistema-de-atencion-y-capacitacion-medica-especializada-a-distancia/