MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001: PARA SOPORTE DE ÁREAS DE ADMISIÓN Y ATENCIÓN DE UN HOSPITAL PÚBLICO

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante: Erik Ramiro Mazorra Olmedo

Bajo la dirección de: Rubén Antonio Pacheco Villamar

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Marzo del 2019

Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información ISO/IEC 27001: Para soporte de áreas de admisión y atención de un hospital público.

Methodology for the implementation of a System of Security Management of Information ISO / IEC 27001: For support of areas of admission and attention of a public hospital.

[1]

Resumen

El presente estudio analiza la manera de obtener y proponer una metodología que sea aplicable, desde el punto de vista práctico y de su posible adaptación local al momento de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) ISO/IEC 27001 para hospitales públicos en Ecuador, a partir de metodologías existentes en instituciones similares y otras verticales de la industria. Con base en el objetivo planteado, se revisó y ponderó la importancia que tienen las TICs en el soporte a los procesos internos que tienen los hospitales en sus diversas áreas y, por otro lado, se analizó la necesidad de políticas y procedimientos de seguridad informática y de su gestión en cada proceso para proteger los recursos financieros, la información, el cumplimiento legal y otros bienes tangibles e intangibles que permitan también salvaguardar la gestión interna de todas las áreas. Por último se describe una metodología adecuada para la implementación de un sistema de gestión basado en: 1) mantener el inventario de activos de información, 2) catalogar los procesos de la organización, 3) gestionar el catálogo de amenazas y vulnerabilidades, 4) calcular la tasación de activos de información, 5) registrar y mantener la identificación de riesgos, 6) gestionar la evaluación de riesgos, 7) gestionar la asignación de responsables de seguimiento y de las acciones para el tratamiento de riesgos, 8) registrar la asociación de evidencia documental, 9) generar reportes y consultas de seguimiento para la gestión de controles de la Norma y 10) generar la declaración de aplicabilidad.

Palabras clave: ISO 27001, metodología para la implementación, procesos hospitalarios, seguridad de información, TICs, sistema de gestión de seguridad de información.

Abstract

The present study analyzes the way to obtain and to propose a methodology that is applicable locally, in a pragmatic way, and dynamic, when implementing an Information Security Management System (ISMS), based on ISO / IEC 27001 for public in Ecuador, by studying similar projects in the health area, in other countries, and even in other industry verticals. Therefore, the importance of ICTs for the internal processes that hospitals have was analyzed and discussed. Once, the level of the importance of the ICTs was understand and determined, the need for information security in each process was analyzed to protect financial resources, information, legal situation and other goods, tangible and intangible, that also allow the internal management of all areas to be safeguarded. Finally, an adequate methodology is proposed for the implementation of a management system based on: 1) maintaining the inventory of information assets, 2) cataloging the processes of the organization, 3) manage the catalog of threats and vulnerabilities, 4) calculate the appraisal of information assets, 5) record and maintain the identification of risks, 6) manage the risk assessment, 7) manage the assignment of responsible for monitoring and actions for the treatment of risks, 8) record the association of documentary evidence, 9) generate reports and queries of monitoring for the management of controls of the Standard and 10) generate the declaration of applicability.

Key words ISO 27001, methodology for implementation, hospital processes, information security, TICs, system of security management of information.

[1] Ingeniero en Telecomunicaciones, Master of Science en Ingeniería en Telecomunicaciones. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

INTRODUCCIÓN

La demanda creciente en relación a la mejora de la eficiencia y eficacia de los servicios de salud proporcionados al paciente (atención, diagnóstico, comunicación, entre otros), conjuntamente acompañada con los aspectos de privacidad y seguridad, están incentivando un proceso general de transformación tecnológica, además del impulso al desarrollo de iniciativas de salud dentro de los organizaciones. Por otro lado, el incremento de la movilidad de profesionales, pacientes y usuarios, ha llevado a que la disponibilidad y ubicación de la información de salud empiece a configurarse como un objetivo clave para la mejora de los procesos asistenciales (Ministerio de Sanidad y Consumo, 2013).

En la Unión Europea este proceso tuvo sus inicios a mediados del año 2000, aspecto que de cierta forma coincidió con las iniciativas para el desarrollo de la Sociedad de la Información en el marco de la Agenda de Lisboa. A partir, de ese momento, la Comisión Europea a lo largo de los diferentes años ha ido desarrollando una labor importante encaminada al fomento de la investigación y la innovación en el área de eHealth, que comprende el uso y aplicación de tecnologías de la información como soporte en el cuidado de la salud de los pacientes. De igual forma, durante los últimos quince años en la mayor parte de países se han puesto en marcha planes ambiciosos en relación a la innovación en el campo de la salud (Mahecha & Coello, 2016).

Durante los últimos años, el sector de la salud en relación a la utilización de las TICs presenta un crecimiento notable. Solo en Estados Unidos alrededor de $ 3,2 billones de dólares fueron invertidos dentro de este ámbito, facilitando el trabajo de galenos y usuarios que a diario requieren de herramientas informáticas que ayuden a optimizar el trabajo dentro de los diferentes hospitales, sean estos públicos o, a su vez, privados (Cisco, 2017).

Inicialmente, las aplicaciones informáticas destinadas al sector de la salud fueron desarrolladas ad-hoc. Sin embargo, hoy en día, se cuenta con complejos sistemas de información capaces de comunicar a través de redes de datos distribuidas. Es por ello que, los servicios de salud en muchas comunidades han seguido varias estrategias de incorporación de las tecnologías de la información, lo que ha llevado a diferentes niveles de desarrollo, encontrándose en la actualidad sistemas de identificación de usuarios, digitalización de los registros clínicos de cada paciente, desarrollo de sistemas que soportan y relacionan entre sí los procesos necesarios para hacer efectiva la prestación farmacéutica (prescripción, visado y dispensación), iniciativas para agilizar la citación de los pacientes con los profesionales de la salud, dispositivos de diagnóstico y tratamiento a distancia, sin dejar de lado, servicios de gestión económico-administrativos (Ministerio de Sanidad y Consumo, 2013).

Bajo este contexto, se ha ido incorporando, gradualmente durante los últimos años a los sistemas de salud nuevas aplicaciones clínicas, soluciones de telemedicina o sistemas informáticos para la gestión de la salud. Hoy la hospitalización a domicilio, la gestión digital de las imágenes radiológicas o la prescripción electrónica de recetas son una realidad.

En este sentido, se considera que durante los próximos años, el uso de las TICs continuará siendo un ámbito de actuación clave. Debido a que los retos que se tiene por delante son numerosos, se pueden resaltar los siguientes: las exigencias de interoperabilidad, la necesidad de contar con una inversión sostenida que ayude a desarrollar proyectos escalables, las crecientes garantías de seguridad de las infraestructuras y sistemas desplegados, así como la adecuada gestión del cambio y la adaptación de la cultura institucional a los nuevos procesos.

Como es evidente y tratándose de uno de los pilares que encaminan el éxito y continuidad de una sociedad, como los servicios de salud que brindan instituciones públicas o privadas, conjuntamente con los tres escenarios de aplicación antes mencionados mantienen su importancia estratégica, por lo que su implementación debe realizarse obligatoriamente en entornos protegidos,

entiéndase, seguros en todos los ámbitos, pero por sobre todo en el ámbito de las tecnologías de información y comunicaciones, caso contrario, nos enfrentaríamos a graves problemas que pueden fácilmente escalar en su impacto negativo, como los ya ocurridos recientemente en instituciones de salud a nivel mundial, y que son de dominio público, cuyos sistemas de salud se vieron secuestrados o inutilizados por ataques de extorsión o virus informáticos.

Según el Instituto Ponemon (2017) las violaciones de datos le cuestan a la Industria de la Salud alrededor de 6,2 millones de dólares por año en los Estados Unidos. Además de acuerdo a un estudio reciente el 90% de organizaciones encuestadas tuvo violación de datos en los últimos dos años. Como dato resaltable, en el 2016 un hospital de Los Ángeles sufrió un ataque malicioso que cerró y dañó significativamente las computadoras, y tuvieron que cancelar alrededor de $17000 en bitcoin para retomar el control de sus sistemas.

Para lograr la implementación de un sistema de gestión de seguridad informática existe una amplia experiencia acumulada por los profesionales de las TICs, expresada en soluciones tecnológicas, normas, buenas y mejores prácticas, y marcos de referencia. En lo referente a la NORMA ISO/IEC 27001, el eje central de su aplicación es proteger la confidencialidad, integridad y disponibilidad de la información, y uno de los componentes más importantes para garantizar que dicha aplicación sea eficaz, es contar con un Sistema de Gestión de la Seguridad de la Información (SGSI) coherente, completo y dinámico, que incluya su continua auto evaluación y actualización. Pero, Miranda (2013) describe que en la práctica existen diversas formas, con diferentes matices y niveles de profundización para llevarlo a cabo en instituciones de salud, en específico; se debe buscar un cierto nivel de éxito y disminuir la incertidumbre en los resultados, para adoptar un enfoque, que permita abordar desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de la gestión de seguridad informática.

Para identificar los elementos que intervienen en la gestión de seguridad informática se han realizado varias investigaciones con anterioridad y entre los principales resultados encontrados se destaca la metodología propuesta por (Valencia & Orozco, 2017), la misma que contempla cinco fases secuenciales: 1) aprobación de la dirección del Hospital Público para iniciar el proyecto, 2) definir el alcance, los límites y la política del SGSI, 3) análisis de los requisitos de seguridad de la información, 4) valoración de riesgos y planificación del tratamiento de riesgos y 5) diseño del SGSI. Por otro lado, Sánchez (2013) dentro de su estudio propone una metodología de implementación fundamentada en seis aspectos: 1) definición del alcance y los límites del SGSI, 2) definición de la política de la seguridad de la información, 3) identificación de la política de la seguridad de la información, 4) control de riesgos, 5) fijación de controles y objetivos de control y 6) definición de la declaración de la aplicabilidad. Finalmente, Bojaca (2016) destaca 4 fases necesarias, para el Sistema de Gestión de Seguridad Informática: 1) planificar (análisis diferencial y de riesgos para la definición del alcance y otras actividades de planeación), 2) hacer (propuesta para implementar el diseño del SGSI), 3) verificar (seguimiento, supervisión y revisión del SGSI) y 4) actuar (mantener y mejorar el sistema).

Bajo este contexto, y tomando como referencia lo expuesto en diferentes investigaciones (Bojaca, 2016; Sánchez, 2013; Valencia & Orozco, 2017), para cumplir con el objetivo de esta investigación, y como resultado de ella se bosquejó una metodología resumida que toma como referencia únicamente lo indispensable de cada una de las fuentes, con el fin de hacerla aplicable, pero, al mismo tiempo, coherente y completa, quedando la metodología propuesta para hospitales públicos de la siguiente manera: 1) mantener el inventario de activos de información, 2) catalogar los procesos de la organización, 3) gestionar el catálogo de amenazas y vulnerabilidades, 4) calcular la tasación de activos de información, 5) registrar y mantener la identificación de riesgos, 6) gestionar la evaluación de riesgos, 7) gestionar

la asignación de responsables de seguimiento y de las acciones para el tratamiento de riesgos, 8) registrar la asociación de evidencia documental, 9) generar reportes y consultas de seguimiento para la gestión de controles de la Norma, 10) generar la declaración de aplicabilidad.

MARCO TEÓRICO

El primer paso es analizar el impacto que tienen las TICs en los procesos de los hospitales, para identificar si la incorporación de estas promueven un cambio que mejore la calidad de vida de los usuarios, (Ministerio de Salud Pública, 2012), a la vez que exige a los hospitales replantearse la forma de prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada.

Como ilustración de lo encontrado en el primer paso, tenemos que en las instituciones de salud a nivel mundial, las TICs constituyen la herramienta fundamental en el proceso de implantación de innovaciones en la sociedad de la información. En las primeras etapas de la introducción de soluciones en tecnología de información se logró un 20% de aumento en la eficiencia de un hospital en Dinamarca (Healthcare, 2017), y los resultados fueron similares o mejores en la gran mayoría de los países de la UE. Estas tecnologías han ido impregnando todas las áreas de desempeño y actividades de la sociedad durante los últimos años y en la actualidad se encuentran presentes en todos los ámbitos.

Desde otra perspectiva, lo mencionado anteriormente no es factible, si no se analiza también el segundo paso, debido a que en el mismo se determina como la seguridad de información colabora y se vuelve fundamental en cada proceso ejecutado. Los hospitales deben proteger los recursos financieros, información administrativa y de sus pacientes, reputación, situación legal y otros bienes tangibles e intangibles para minimizar riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada, o, en general, mal intencionada (Gil & Gil, 2017). En definitiva, como lo enuncia (Valeria & Orozco, 2017), una metodología para implementar y aplicar un sistema de gestión de seguridad de la información denominada ISO/IEC 27001.

Expertos (Anvari, 2007; Yaduvanshi & Sharma, 2017) especulan que los médicos asumirán con el paso del tiempo roles más especializados como la atención médica más dependiente de la tecnología, entrenados específicamente para cumplir con las tareas complejas de las TICs dentro de la institución incluyendo entre estas actividades: la adecuada gestión de correos electrónicos, administración de bases de datos, mantenimiento de los diferentes sistemas y control de la seguridad de la información.

Cabe recalcar que, las TICs soportan una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, que a menudo transmiten datos a través de las redes de telecomunicaciones; cuyo principal objetivo radica en fortalecer e impulsar el desarrollo económico y social de un país (Organización para la Cooperación y el Desarrollo Económico, 2013).

De lo anterior se deriva la importancia que tiene el establecer el impacto que las TICs han tenido sobre la operación de los hospitales, dado que, el uso en la atención en salud constituye una herramienta para mejorar el impacto de las intervenciones en la comunidad, permitiendo un acceso más equitativo y eficiente a los servicios, mejorando la oportunidad de la atención y la relación costo/efectividad de los tratamientos e impulsando la generación de conocimientos (Avella, 2013).

El uso de TICs en salud, supone la integración del trabajo de profesionales, pacientes y la misma sociedad para dar un uso correcto y eficiente a estas tecnologías; se requiere además el trabajo interdisciplinario de varias áreas del conocimiento, no sólo de las ciencias de la salud, sino también de la ingeniería en sistemas, entre otros ámbitos profesionales.

La implementación de innovaciones tecnológicas en el sector salud se debe reflejar de manera positiva en la optimización de los recursos

económicos y humanos a través de la implementación y posterior evaluación del uso de tecnologías en salud, como instrumento para la toma de decisiones en sus diferentes niveles (CEPAL, 2010).

Según el Instituto Ponemon (2017) las violaciones de datos le cuestan a la Industria de la Salud alrededor de 6,2 millones de dólares por año en los Estados Unidos. Además de acuerdo a un estudio reciente el 90% de organizaciones encuestadas tuvo violación de datos en los últimos dos años. Como dato resaltable, en el 2016 un hospital de Los Ángeles sufrió un ataque malicioso que cerró y dañó significativamente las computadoras, y tuvieron que cancelar alrededor de $17000 en bitcoin para retomar el control de sus sistemas.

Aplicación de las TICs en Salud

Las TICs constituyen una herramienta que aporta beneficios a los médicos y pacientes; sin embargo, a medida que los hospitales recopilan información, el riesgo de fuga de información o incumplimiento de privacidad es alto, por lo que se debería prestar atención a los problemas de seguridad de acuerdo a normas, leyes o regulaciones. Hay muchas preocupaciones legales en cuanto al uso y funcionamiento de las tecnologías, especialmente, si la red de Internet es su principal recurso, como por ejemplo en farmacias en línea, telemedicina, sistemas de información de salud, entre otras.

La aplicación de las TICs se realiza en un amplio rango de aspectos que afectan el cuidado de la salud, relacionada no solamente con la atención médica que requieren las personas en forma individual sino incluyendo los servicios de salud, la salud pública y la formación de profesionales y pacientes. En la prevención, diagnóstico, tratamiento y rehabilitación de pacientes se podría decir que las TICs son aplicables en todos los campos médicos; esto ha dado lugar, por ejemplo, al desarrollo de la telemedicina que, actualmente, incluye distintos servicios tales como cirugía, teleconsultas, teleradiología, telefotografía y diagnóstico remoto por imagenología digital térmica (Buitrón, Gea, & García, 2016).

Además, la salud constituye un tema muy sensible, dependiendo de las características del sistema de cada país, la aplicación de las TICs tendrá un impacto mayor o menor en cada uno de sus componentes. Bajo este contexto, se entiende como sistema de salud a las instituciones, las personas y los recursos implicados en la prestación de atención de salud a todos los individuos (Ministerio de Salud, 2012).

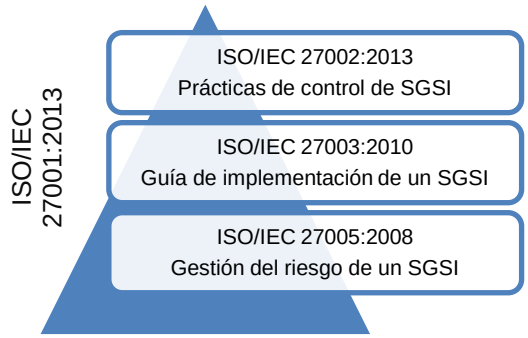
Por lo tanto, para la aplicación de las TICs hay que tener en cuenta factores como: el sector salud tiene un alto grado de regulación por parte del gobierno o los profesionales de la salud; está altamente fragmentado, en él coexisten los servicios públicos, privados, tradicionales o alternativos donde participan muchos actores y culturas diversas; la gestión es fundamentalmente pública; y el financiamiento es a través de impuestos u otros mecanismos, agentes financieros, quienes recaudan fondos y los asignan a proveedores o compran servicios a nivel nacional y otros niveles que financian directa e indirectamente los proyectos (Avella, 2013). Por lo que se determina que se puede dar soporte a las áreas de admisión y atención de un hospital público de la presente investigación.

Estándares de seguridad de la información

Como requisito indispensable para implementar un SGSI en una organización es importante conocer estándares, estructura, componentes, y la relación existente entre cada uno de ellos. Las normas para la implementación de un SGSI pertenecen a la serie denominada ISO/IEC 27000 mismas que son publicadas por la Comisión Electrotécnica Internacional (IEC) y la Organización Internacional de Normalización (ISO), ambas entidades instauraron 17 normas, las cuales se clasifican en cuatro categorías diferentes: 1.- la norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000; 2.- las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006; 3.- las normas guía desarrolladas a través de 10 normas que son: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008,

ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032 y 4) las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017 (Valencia & Orozco, 2017).

Figura 1. Principales normas para implementar un SGSI basado en los estándares de la familia de normas ISO/IEC 27000



Fuente: Adaptado de Valencia, F. y Orozco, M. (2017).

Como se evidencia en la figura 1, la norma ISO/IEC 27001:2013 contiene otras tres normas dado que todas están relacionadas con la implementación de un SGSI para las organizaciones.

Collste, George, & Hedstrom, (2012) explican que la Internet se utiliza cada vez más para brindar información médica, consultas y recetas médicas. La seguridad es un tema muy importante cuando se trata de lidiar con información, especialmente cuando se refiere al cuidado de la salud, donde la información es crítica y confidencial. (Ayatollahi & Shagerdi, 2017). Por esta razón el proceso de gestión de información debe estar bien estructurada y con la seguridad adecuada la confidencialidad en aspectos médicos va enlazado directamente con el cuidado de la salud de la persona.

Los sistemas de información en el área de salud se utilizan generalmente para almacenar, acceder y transmitir datos electrónicos; así mismo, se describen actividades que incluyen bases de datos computarizadas para facilitar el intercambio de la información. En comparación a la información de registros físicos, los registros electrónicos se pueden acceder fácilmente. Por lo tanto, se plantea muchas preocupaciones legales tales como mantener la privacidad del paciente, mantener los datos confidencialmente y lograr la fiabilidad de datos del paciente. (Collste, George, & Hedstrom, 2012)

Cline & Luiz, (2013) indican que los sistemas de información hospitalaria automatizan las funciones administrativas del paciente y las funciones de atención clínica (por ejemplo, notas clínicas, prescripciones computarizadas, resultados de laboratorio en línea, imágenes radiológicas digitales) porque tienen la capacidad de eliminar procesos en papel dentro del entorno clínico. De acuerdo a la información recabada a una enfermera del Hospital Sebokeng de Sudáfrica, los sistemas hospitalarios antiguos (manuales) eran perjudiciales para la atención del paciente porque requerían parte del tiempo del profesional de salud para cumplir con ellos, es decir, llenarlos o completarlos. Al hablar de seguridad en la información y confidencialidad del paciente, el 75% del personal administrativo y de enfermería indicó que la información que manejaban los sistemas electrónicos era más segura que los que manejaban de manera física. Sin embargo, no todos los médicos encuestados estuvieron de acuerdo, demostrando más del 58% su desconfianza de este método, como se puede evidenciar se identifica claramente al estándar de riesgo en el mal manejo de la información de forma física y del posible riesgo en sistemas electrónicos.

Se puede argumentar que los registros electrónicos tienen la capacidad de ofrecer acceso restringido por contraseña a la información electrónica del paciente; sin embargo, el personal del hospital se desanimó por el hecho de que una vez que un usuario inicia sesión en el sistema, esa persona tiene acceso completo a todos los registros del paciente, independientemente de quién sea el médico tratante o a qué sala se asigna al paciente, en este punto el estándar para la administración de la seguridad de información, demuestra que todas los miembros de organización de salud tiene acceso a los datos de cualquier paciente que haya sido ingresado a la misma.

Los riesgos de seguridad en el sector salud se han incrementado, puesto que con equipos sofisticados siempre existe el peligro de perder información valiosa o que ésta se difunda sin restricción. El proceso para administrar los riesgos inherentes a la seguridad de las tecnologías de información de la salud es similar al de la seguridad de dispositivos médicos. Estos escenarios brindan una descripción resumida de algunos problemas de entrega de atención médica y los impactos negativos que se desarrollan con las tecnologías de información. Las amenazas vienen cuando existe un impacto directo sobre la protección de la privacidad. Un solo evento de privacidad del paciente puede ser de un impacto de extrema variedad. La revelación irreversible de difundir información acerca de un paciente con ciertas condiciones patológicas, puede convertirse en un factor financiero devastador. En consecuencia, los sistemas únicos pueden llegar a divulgar, destruir o modificar datos personales sin autorización. (MITA; COCIR; JIRA, 2007)

Menachemi & Collum, (2011) explican que la implantación de un sistema electrónico, disminuye el riesgo de violaciones de la privacidad del paciente, lo cual es una preocupación creciente para estos debido a la cantidad cada vez mayor de información de salud intercambiada electrónicamente. Los sistemas pueden causar varias consecuencias involuntarias, como un aumento de errores médicos, emociones negativas, cambios en la estructura de poder y una dependencia excesiva de la tecnología.

Según Mehraeen, Ayatollahi, & Ahmadi, (2016), el uso de los sistemas de información del hospital tiene muchas ventajas para los proveedores de atención médica y los pacientes. Este sistema tiene potencial para aumentar el acceso a la información y mejorar la investigación clínica y de salud pública. Los problemas que debe enfrentar es cómo mantener la confidencialidad y evitar que personas ajenas al hospital puedan acceder a datos clínicos, situación difícil de lograr, cuando, por un lado, la información del paciente es altamente confidencial y los proveedores de servicios de salud necesitan acceder a ellos. Por lo tanto, la seguridad de la información no es un problema local, sino que es necesario considerarlo a nivel macro para cumplir con las normas nacionales. A pesar de que, se ha considerado a las prácticas de seguridad como problemas técnicos, lo cierto es que debe cambiarse este pensamiento al integrar soluciones técnicas con cultura de seguridad organizacional.

Por otra parte CISCO, (2016) menciona que los registros de atención médica se encuentran entre los datos más *pirateados* en el mundo. Se estima que la información médica vale de 10 a 20 veces más en el mercado negro que los datos de tarjetas de crédito debido a que son un potencial para fraude, robo de identidad y abuso.

Entre algunas de las recomendaciones está el capacitar a los nuevos empleados en temas de responsabilidades para proteger la información. (Mehraeen, Ayatollahi, & Ahmadi, 2016); Mientras que Bulgurcu, Cavusoglu, & Benbasat, (2010) explican que los riesgos relacionados con la seguridad de la información son el principal desafío para muchas organizaciones, ya que estos riesgos pueden tener consecuencias nefastas, incluida la responsabilidad corporativa, la pérdida de credibilidad y daño monetario.

Por lo descrito anteriormente, se deben tomar medidas y hacer conciencia en los profesionales de la industria para garantizar que la seguridad y la privacidad de la información se incluyan en la seguridad en general del sistema y la arquitectura de diseño de acuerdo con la función de gestión de riesgos del propio sistema. (Ayatollahi & Shagerdi, 2017)

Norma ISO/IEC 27001:2013

La norma se enfoca en: Tecnologías de Información, Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información (SGSI) y Requerimientos; por ende, se especifica los requerimientos para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI debidamente formalizado.

METODOLOGÍA

El artículo de investigación es de carácter cualitativo porque se presenta una revisión descriptiva y bibliográfica-documental con referencia al tema de investigación. Seguidamente se analiza la norma ISO/IEC 27001 para implementar un sistema de gestión de seguridad de la información enfocado al soporte de áreas de admisión y atención de un hospital público para Ecuador.

La metodología utilizada dentro del presente estudio se centra bajo un enfoque cualitativo, dado que la información recabada proviene de fuentes de información secundarias, es decir, libros, investigaciones realizadas con anterioridad, revistas, entre otros elementos, los mismos que fueron procesados en su totalidad escogiendo información relevante que se encuentra descrita a lo largo del manuscrito. Por ejemplo, un estudio desarrollado en España revela el progreso que ha experimentado durante los últimos años el uso de las TICs dentro del ámbito de la salud, encontrando hoy en día nuevas aplicaciones clínicas, infraestructura y redes de comunicación, identificación de pacientes y profesionales de la medicina, historia de salud electrónica, receta electrónica, gestión telemática de citas, entre otros (Ministerio de Sanidad y Consumo, 2013). Otro aspecto importante encontrado en la recopilación de información es la importancia del uso de las TICs en la salud como respuesta a las necesidades de planificación, gestión de información, investigación, diagnóstico y tratamiento, además, generalmente se habla de implementación de TICs para la salud teniendo en cuenta tres escenarios grandes de aplicación: 1) software médico o sistemas de gestión institucional, 2) acceso a servicios de información para pacientes y profesionales de la salud y 3) soporte en comunicación a las actividades asistenciales, médicas y quirúrgicas (Avella, 2013).

RESULTADOS

Tabla 1. Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013

Fases	Etapas	Numerales de la norma ISO/IEC 27001:2013 relacionados
Fase 1. Obtener la aprobación de la Dirección del Hospital Público para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI	1. Conocimiento de la institución y de su contexto.
	Definir el alcance preliminar del SGSI	2. Entendimiento de las necesidades y expectativas de las partes interesadas.
	Creación del plan del proyecto para ser aprobado por la Dirección	3. Compromiso y Liderazgo 4. Recursos
Fase 2. Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites de las Tecnologías de Información y Comunicaciones	5. Determinación del alcance del sistema de gestión de seguridad de la información.
	Definir el alcance y los límites físicos	
	Integrar cada alcance y los límites para obtener el alcance y los límites del SGSI	
	Desarrollar la política del SGSI y obtener la aprobación de la Dirección	6. Compromiso y Liderazgo 7. Objetivos de seguridad de la información y planes para cumplir.
	Definición de roles, responsabilidades del SGSI	8. Responsabilidades, roles y autoridades de la institución. Competencia.
Fase 3. Realizar el análisis de los requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso SGSI del Hospital Público. Identificar los activos dentro del alcance del SGSI	9. La institución debe determinar la seguridad de la información. 10. Valorar los riesgos de seguridad de la información
	Realizar una evaluación de la seguridad de la información	
Fase 4. Realizar la valoración de riesgos y planificar el tratamiento de riesgos en caso de que surja en el Hospital Público	Realizar la valoración de riesgos	11. Valorar los riesgos de seguridad de la información.
	Seleccionar los objetivos de control y los controles	12. Procesamiento de riesgos de la seguridad de la información. Objetivos de seguridad de la información y planes para lograrlo
	Obtener la autorización de la Dirección para implementar y operar el SGSI	13. Compromiso y Liderazgo
Fase 5. Diseñar el SGSI	Diseñar la seguridad de la información de la organización	14. Comunicación Información documentada Planificación y control operacional 15. Valoración de riesgos de seguridad de la información.
	Diseñar la seguridad específica de un SGSI	
	Producir el plan del proyecto final del SGSI	

	Procesamiento de riesgos de seguridad de la información. 16. Seguimiento, medición, análisis y evaluación Auditoría interna Revisión por la Dirección con referencia a alguna incidencia con los empleados.

Fuente: Elaboración propia

Se registran diferentes maneras de llevar a cabo la implementación de un SGSI en una institución: sin embargo, para alcanzar un nivel de éxito y disminuir en cierta medida la incertidumbre en sus resultados, se debe adoptar un enfoque que permita abordar, desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de la implementación de un SGSI. La implementación contempla cinco fases secuenciales, a continuación, se detalla cada una de ellas (Valencia & Orozco, 2017).

Fase 1: Aprobación de la Dirección del Hospital Público para iniciar el proyecto

Uno de los aspectos que necesariamente se debe tomar en consideración, y que con frecuencia no es comprendido de forma clara, es que un proyecto de SGSI no constituye un propósito exclusivo del área de Tecnologías de Información, sino que representa un proyecto institucional y como tal necesita en primera instancia la aprobación y posterior a ello, el apoyo de la alta dirección y la parte administrativa para continuar con su implementación adecuada (Valencia & Orozco, 2017).

Establecimiento de las prioridades de la institución para desarrollar un SGSI

Para desarrollar esta actividad resulta indispensable conocer a ciencia cierta las prioridades que tiene la institución para llevar a cabo la implementación de un SGSI, es por ello, que se recomienda tomar en consideración los elementos siguientes: 1) objetivos estratégicos de la institución, 2) requisitos normativos o de terceros relacionados con la seguridad de la información, 3) sistemas de gestión existentes (Valencia & Orozco, 2017).

Definición del alcance preliminar del SGSI

Constituye la definición de que recursos se desea proteger y con base a ello, se puede determinar de forma preliminar el alcance. Es decir, de acuerdo a lo que estipula la norma en estudio, el alcance preliminar debe incluir: un resumen de los requerimientos establecidos por la administración y las obligaciones impuestas de manera externa a la institución.

Creación del plan del proyecto para ser aprobado por la Dirección: Si bien es cierto que la implementación de un SGSI dentro de cualquier institución constituye una tarea permanente, el primer paso para promover su diseño e implementación parte de la estructuración de un proyecto que ayude a delimitar con precisión los tiempos, recursos y personal requerido, para ello, es necesario utilizar herramientas de gestión de proyectos existentes en el mercado. Adicionalmente, dentro de esta actividad también se aprueba el presupuesto del plan de mitigación de riesgos resultante del análisis de riesgos (Valencia & Orozco, 2017).

Fase 2: Definir el alcance, los límites y la política del SGSI

La importancia de establecer el alcance se encuentra fundamentada en la delimitación del proceso de gestión de riesgos y, por lo

cual, pone en alerta a todo el proceso de ejecución del SGSI.

El producto final del alcance, constituye por lo general, un enunciado, en donde se resume los recursos que se están protegiendo dentro de la institución, además forma parte del documento de certificación que es entregado a aquellas instituciones que han logrado cumplir con los requisitos demandados.

Definición de políticas y objetivos de seguridad

La política de seguridad refleja lo que la institución desea hacer con relación a la seguridad de la información, los objetivos que se intenta lograr, observando los requisitos legales y reglamentarios aplicables, además hay que tomar en consideración el compromiso de la parte administrativa para lograr conseguirlos (Díaz, Collazos, Cortéz, Ortíz, & Herazo, 2012).

Aprobación de la Administración

Una de las maneras de demostrar el apoyo de la Administración de forma inicial, constituye, la aprobación tanto de los objetivos como de las políticas del SGSI dentro del alcance definido.

Fase 3: Análisis de los requisitos de seguridad de la información

En relación a lo definido dentro de la norma, para establecer los requisitos de seguridad de la información necesariamente hay que tomar en consideración los siguientes elementos: 1) identificar los activos de información importantes, 2) identificar la visión de la institución y sus efectos acerca de los futuros requisitos de procesamiento de información, 3) identificar las formas actuales de procesamiento de información, 4) identificar los requisitos legales, 5) identificar el nivel de toma de conciencia sobre seguridad de la información y los requisitos de educación y formación en el aspecto de seguridad (Valencia & Orozco, 2017).

Identificar los activos dentro del alcance del SGSI

Las instituciones poseen un sinnúmero y variedad de activos tecnológicos, y tratar de establecer y clasificar estos activos puede ser una difícil tarea, sobre todo en instituciones grandes, dado que, es probable que, dentro de ella, se registren datos electrónicos, almacenes de documentos y miles de dispositivos y personas que forman parte de los activos tecnológicos de dicha institución. A partir de aquello, y según la norma, los activos dentro del contexto del SGSI, constituyen cualquier activo de información, sea este lógico o físico que tiene valor para la institución (Information Systems Audit and Control Association, 2013).

La norma en estudio establece activos de dos tipos: primarios y de soporte. Los primeros constituyen los procesos de negocio y la información, mientras que los últimos constituyen aquellos de los cuales dependen los activos primarios y pueden clasificarse de la siguiente manera: software, hardware, personal, redes, estructura, instalación y ubicación de la institución.

Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos

Esta fase, sin duda alguna constituye el eje fundamental del SGSI, para lo cual es necesario tener en cuenta los siguientes aspectos:

Establecimiento de contexto

Esta fase toma en consideración la preparación de los diferentes elementos que demanda el proceso de gestión de riesgos de seguridad de la información, es decir, alcance, objetivos, políticas y parámetros de evaluación del riesgo.

Parámetros de probabilidad

Para establecer el parámetro de probabilidad es necesario realizar una tabla de frecuencias de la posible ocurrencia de las amenazas, con los niveles requeridos en relación a las diferentes necesidades de la institución.

Los parámetros de impacto

Estos parámetros son definidos en función de las consecuencias que podrían tener cualquier amenaza sobre la información o los activos de información en lo referente a la integridad, confidencialidad y disponibilidad.

Determinación de la vulnerabilidad

Corresponde a la sensibilidad de la institución en relación a la posible materialización de una amenaza sobre la información empresarial. Por lo tanto, en términos generales la vulnerabilidad es medible en términos porcentuales, además en función de los parámetros definidos anteriormente (probabilidad e impacto).

Los criterios de aceptación de riesgo ayudan a definir el riesgo que tiene la institución y corresponde a los parámetros que define una entidad para establecer si un riesgo es aceptable o no.

La valoración del riesgo, según lo establecido en la norma contempla tres fases: identificación de los escenarios de riesgo, estimación del riesgo y evaluación del riesgo.

- El propósito de la identificación de riesgos es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.
- Para estimar el riesgo, se puede llevar a cabo: análisis cualitativo, semi cuantitativo o cuantitativo, o bien, una combinación de los tres. En cualquier caso, el tipo de análisis que se lleve a cabo debe ser congruente con los criterios desarrollados.
- La evaluación del riesgo consiste en realizar una comparación de las vulnerabilidades resultantes de cada riesgo y confrontarlas contra el nivel de aceptación de riesgo (Vanegas & Pardo, 2014).

Los resultados obtenidos de la evaluación de riesgos ayudan a diseñar informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que ayudan a monitorear el nivel de avance en la gestión del riesgo.

La fase de tratamiento de riesgos establece las acciones a desarrollar, mediante los controles propuestos, para llevar el riesgo detectado a un nivel aceptable dentro de la institución.

Fase 5: Diseñar el SGSI

El diseño del SGSI se encuentra conformado por tres componentes: la documentación que debe tener el sistema, la implementación de los controles previstos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información (Pallas, 2009).

La información documentada que necesariamente debe tener un SGSI engloba los requisitos estipulados en la norma ISO/IEC 27001, las mismas que tienen su origen a partir de la implementación de sus diferentes fases.

La implementación del plan de tratamiento de riesgos aprobado por la Administración con los recursos asignados para tal fin, y el mantenimiento de los controles existentes, es lo que permite garantizar niveles aceptables de seguridad de la información.

La evaluación del desempeño del SGSI se realiza mediante la supervisión, medición, análisis y evaluación del sistema; las auditorías habituales y la verificación de la parte administrativa de la institución.

La supervisión, medición, análisis y evaluación del SGSI se realiza, por lo general, mediante la definición de indicadores. Estos son desarrollados de

forma común a nivel general del SGSI, a nivel de indicadores de gestión de riesgos y de los indicadores que permiten evaluar la eficacia y eficiencia de los controles que hacen parte de la declaración de aplicabilidad definida para el sistema.

Tabla 2. Estudio comparativo Sistema de Gestión de Seguridad Informática

Adaptación de las Normas ISO 27001 e HIPAA para la Reducción de Riesgos en la Seguridad en Hospitales Nivel I del IESS	**Diseño de un Sistema de Gestión de Seguridad Informática basado en la Norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá**	**Desarrollo de un Sistema de Información para gestionar la implantación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013**	**Diseño de un Sistema de Gestión de la Seguridad de la Información para comercio electrónico basado en la ISO 27001 para Pequeña y Medianas Empresas en la ciudad de Quito**	**Conclusión**
En las normativas ecuatorianas aplicadas en el sector de la salud, para la seguridad de los sistemas de información no se posee un conjunto de políticas claras que asegure los datos contenidos en las historias clínicas de manera electrónica, la adaptación de la Norma permite asegurar la información contenidas en las historias clínicas en hospitales. Las Normas ISO 27001 e HIPAA tienen puntos en común dentro de las políticas de seguridad de la información como políticas de sanciones, copias de seguridad, establecimiento de responsabilidades, el análisis y gestión de riesgos que permiten establecer ventajas de cada una	El diseño de un sistema de gestión de seguridad informática ha permitido evidenciar las diferentes vulnerabilidades y amenazas a las que se ven expuestas los activos de información del área administrativa y de historias clínicas del hospital, por lo que resulta indispensable que se tomen medidas preventivas con la finalidad de proteger los activos de información y garantizar el normal funcionamiento del hospital. Los procesos de	Se desarrolló la ISO 27005 como metodología para la gestión de riesgos y con base a este estándar se programaron todas las reglas de negocio relacionadas con la gestión de activos de información y la gestión de riesgos. Es decir, que se releva el hecho de que los activos estén relacionados con los procesos empresariales y que sus riesgos definan causas en función de pares amenaza-vulnerabilidad. Se consigue con este sistema que la tasación	Establecer un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001 se convierte en una herramienta de control idónea, dado que permite de una forma sistemática salvaguardar y administrar la información sensible de la institución, para que esta permanezca protegida, evaluando de forma permanente las metodologías, los controles, procesos, etc., situación que fortalece la seguridad, el acceso, disponibilidad, el control, la autenticidad, la integridad, la confidencialidad y la conservación de la	Todas las investigaciones mencionadas dentro del presente estudio se enfocan en el diseño e implementación de un Sistema de Gestión de Seguridad Informática basado en la Norma ISO 27001 la misma que se enfoca en gestionar la seguridad de la información en una institución. El punto central de la normativa ISO

como la generalidad de la ISO y la orientación al sector de la salud con la HIPAA; y las desventajas de no tener un marco de trabajo y políticas de seguridad de la información que permitan reducir la probabilidad de ocurrencia de los riesgos o vulnerabilidades presentes en la información.	seguridad establecidos previos al desarrollo del proyecto eran mínimos, dado que muchos de los equipos donde se almacena la información y su acceso a ella no contaba con protocolos de autenticación para los pacientes por lo que cualquier individuo podía tener acceso a ella poniendo en riesgo su confiabilidad, autenticidad, integridad y disponibilidad. Con el diseño se propone la implementación para hacer más seguros sus procesos informáticos en el área administrativa y de historias clínicas.	de los activos de información que es el proceso de valoración del impacto que tiene cada activo en función de disponibilidad, confidencialidad e integridad y haciendo uso de una escala predefinida, sea realizada por definición directa del responsable de seguridad de información pero también se brinda la alternativa de que los involucrados con el activo como los propietarios y dueños del proceso puedan realizar una valoración individual como en una votación y al final se tenga un valor consolidado en función de estas votaciones.	información, frente a posibles hackeos, y de esta forma permite a la institución cumplir con sus objetivos institucionales, implementando sistemas que tengan un especial cuidado con la información que maneja la entidad. Independientemente de que la norma 27001 proponga una serie de documentos estándar para tomar medidas preventivas y reactivas para resguardar y proteger la información, es la propia institución la que decide cómo manejar la seguridad de la información y que medidas desea implementar, con base a lo que considera que es importante medir o evaluar.	27001 constituye la protección de la confidencialidad, integridad y disponibilidad de los datos, aspecto que es desarrollado investigando los problemas potenciales que podrían afectar a la información, es decir, realizando la evaluación de riesgo y posterior a ello definiendo lo que es necesario hacer para evitar que estos problemas aparezcan.

Fuente: Elaboración propia a partir de (Barragán, 2017; Bojaca, 2016; Mahecha & Coello, 2016; Sánchez, 2013)

Tal como se evidencia en la Tabla 2, se eligieron varios estudios para identificar el impacto de ISO/IEC en la seguridad de un sistema de información, de los cuales demostraron que la implementación del SGSI no obtuvieron los sistemas de eficacia esperados por diferentes razones entre ellas se encuentran el no identificar procesos, el inadecuado personal operativo encargado del área, deficiente capacitación y desconocimiento de objetivos comunes que vayan en sintonía con lo que se espera obtener. Esto permitió tener una visión más amplia de lo que genera un sistema de gestión de seguridad de la Información ISO/IEC y la aceptación al proceso.

Algo similar se determinó en el estudio realizado por Barragán (2017) en el hospital del IESS de Nivel I de la ciudad de Guaranda donde se encontró que los sistemas de información no poseen un conjunto de políticas claras que aseguren los datos contenidos en las historias clínicas de manera electrónica acompañada del desconocimiento por parte del Talento Humano en el manejo de sistemas de información en dicha área. En estas investigaciones se nota claramente la necesidad de un personal altamente capacitado y competente para poder lograr la eficacia requerida en la implementación, además, de la interacción íntima en el desarrollo de las actividades en la dirección del personal del hospital y del personal de servicio, como manifiesta el estudio de (Anchatipán, 2015) quien implementó en el Hospital Quito N°1 de la Policía Nacional una norma similar.

Lo interesante en estas cuatro investigaciones (Barragán, 2017; Bojaca, 2016; Mahecha & Coello, 2016; Sánchez, 2013) es que aseguran haber minimizado el riesgo y haber aumentado la calidad en los servicios mejorando la gestión administrativa en comparación con el procedimiento normal, obviamente por la premura del tiempo y la falta de un acompañamiento para apoyar el monitoreo, seguimiento y evaluación, estas cuatro investigaciones se quedaron en un plan piloto, en el que recomiendan optar por el desarrollo de indicadores de control y de mejora continua para una adecuada implementación en los hospitales.

Cada hospital es una entidad con culturas y métodos organizativos diferentes, por lo tanto, se recomienda también adoptar sistemas de auditoría externa que fortalezcan las debilidades que posee cada área o cada hospital basada en la opinión del propio personal, quienes son los principales entes fomentadores de la calidad y la creación de valor hacia los pacientes que buscan ser atendidos de forma rápida y eficiente.

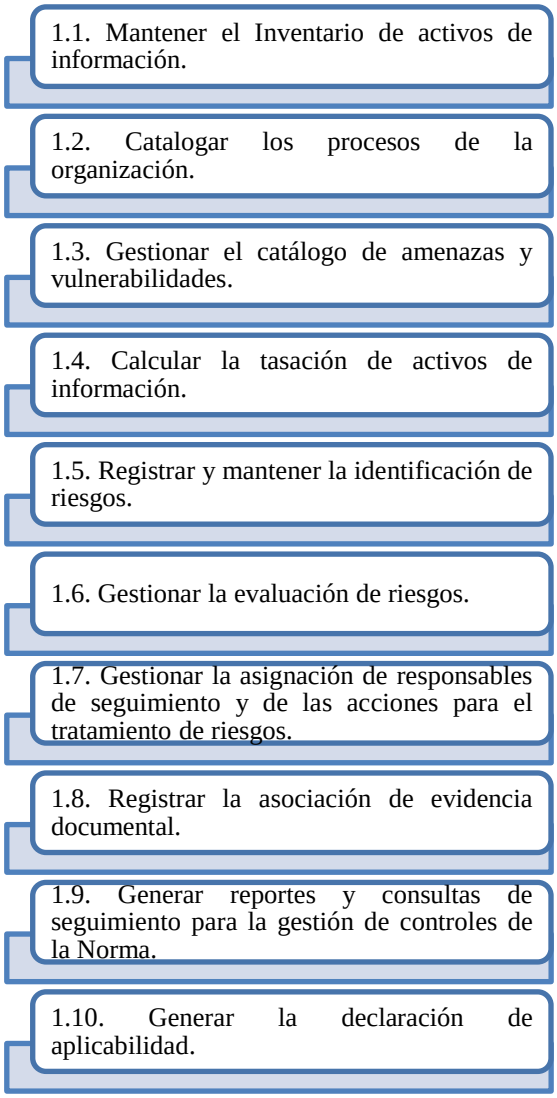
Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información para el Hospital Público

Como se evidenció en los resultados, existen diversas formas de llevar a cabo una implementación de un SGSI, tanto en una organización pública, como privada, no obstante, para llegar a la certificación deben lograr un cierto nivel de éxito y disminuir la incertidumbre en sus resultados para alcanzar la norma ISO/IEC 27001 (Carnicero & Fernandez, 2012).

El desarrollo de un sistema de información ayuda a administrar las fases y los objetos señalados dentro del SGSI. En consecuencia, el sistema representa un aplicativo web, mismo que es accesible desde la intranet de la institución tomando en consideración la gestión de permisos y la integración con otros módulos empresariales como, por ejemplo, registro de bienes, documentos, empleados y otros archivos desde el gestor documental del SGSI.

De forma general, y con base en lo expuesto por Anchatipán (2015) a continuación, se detallan los apartados que deben ser trabajados para la implementación del sistema en estudio:

Figura 2. Procesos para la implementación del SGSI



Fuente: Adaptado de Mahecha & Coello (2016)

Bajo este contexto, el beneficio principal en relación a la utilización del sistema de información propuesto constituye el poder visibilizar el progreso de la implementación de la Norma, aportando un mayor control de forma sistematizada que permite tomar acciones oportunas cuando se presenten contratiempos. La automatización de las actividades requeridas en la Norma impacta en el tiempo de implementación, la productividad de los involucrados y en el control de recursos lo cual aporta para una eficaz puesta en marcha de la Norma (Bojaca, 2016). Otro aspecto a destacar con la implementación del sistema es la disponibilidad de la información que solicitan las diferentes instituciones de control, además de actuar también como un repositorio central de indicadores y documentación establecidos en la Norma.

CONCLUSIONES

Una vez culminado el presente estudio se ha llegado a las siguientes conclusiones:

- A nivel general, es evidente el crecimiento en la utilización de las TICs en el ámbito de la salud, en donde sus inicios se remontan al año 2000 con el desarrollo de las primeras aplicaciones informáticas ad-hoc, a las que, con el paso del tiempo y viendo los beneficios de la incorporación de las tecnologías de la información a este campo, se fueron vinculando diferentes soluciones y estrategias, como por ejemplo: sistemas de identificación de pacientes, digitalización de los registros clínicos, sistemas que soportan y relacionan entre si los procesos necesarios para hacer efectiva la prestación farmacéutica, sistemas para gestionar citas con los pacientes, entre otros.

- La investigación se centró en el análisis de estudios realizados con anterioridad, y principalmente en las conclusiones obtenidas en dichos estudios, donde la propuesta final coincidía, como no podría ser de otra manera, en enfocarse en el diseño de una metodología, su respectiva implementación y posterior operación de proyectos piloto de un Sistema de Gestión de la Seguridad de la Información, bajo la normativa ISO/IEC 27001, cuyo objetivo estuviera direccionado, de una manera medible y sustentable, a proteger la

confidencialidad, integridad y disponibilidad de la información de salud.

- Finalmente, y tomando como referencia estudios previos se bosquejó una metodología práctica y aplicable, la misma que recogía los aspectos más importantes de cada uno de esos estudios, adaptándolos a las necesidades concretas de un hospital público del país. El modelo propuesto es esencialmente práctico, al tiempo que pretende evitar omisiones que pudieran afectar al objetivo primordial de estos sistemas, que es controlar las políticas, las soluciones y la gestión misma de la seguridad de información, es decir, de las actividades que deben proteger la información de salud, garantizando su confidencialidad, integridad y disponibilidad. Como resultado del estudio comparativo de esta propuesta con las otras metodologías, se concluye que la presente es alcanzable, posible, coherente y completa, además de ser apta para generar, una vez implementado el SGSI, cambios positivos y sostenibles en el manejo seguro de la información de la institución, dado el rol clave que cumple la información en, prácticamente, cada proceso hospitalario, y para minimizar riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada.

- En general, se concluye que la importancia del aporte de la implantación de un SGSI radica en la reducción de un gran porcentaje del riesgo presente en las violaciones de la privacidad del paciente (datos, historias clínicas, recetas, tratamientos, etc.), además, de generar o propender a actualizar políticas de seguridad adecuadas, una cultura institucional en seguridad y hábitos del personal en el manejo seguro de la información para agilitar procesos de gestión encaminados a la consecución de los objetivos y metas organizacionales.

Entre las limitaciones encontradas durante el desarrollo del presente estudio están los escasos estudios desarrollados en materia de la Normativa ISO/IEC 27001 aplicada al sector de la salud en el Ecuador, generando un sinnúmero de inconvenientes en relación al manejo general de la información relevante en estas instituciones.

En futuras investigaciones se propone adaptar la metodología propuesta en diferentes instituciones que no necesariamente estén inmersos dentro del sector de la salud sino que esté disponible para organizaciones que necesiten manejar un Sistema de Gestión de la Seguridad de Información con la finalidad de salvaguardar la información existente.

REFERENCIAS BIBLIOGRÁFICAS

Anchatipán Tapia, S. F. (2015). *Propuesta de diseño de un plan de implementación de la norma NTE ISO 15189-2009 en el Hospital Quito N°16 de la Policia Nacional*. Universidad Central del Ecuador.

Anvari, M. (2007). Impact of information technology on Human Resources in Healthcare. *Healthcare Quarterly*, *10*(4), 84–88.

Avella Martínez, L. Y. (2013). *Tecnologías de la información y la comunicación (TICS) en el sector Salud*. Universidad Nacional de Colombia.

Barragán Quizhpe, C. F. (2017). *Adaptación de las Normas ISO 27001 e HIPPA para la reducción de riesgos en la seguridad en Hospitales Nivel I del IESS*. Escuela Superior Politécnica de Chimborazo.

Bojaca Garavito, E. A. (2016). *Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 - 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá*. Universidad Nacional Abierta y a Distancia.

Buitrón Vega, M. E., Gea Izquierdo, E., &

García Oquendo, M. V. (2016). Tecnologías en información y comunicación sanitaria. *Revista PUCE*, (102), 273–289.

Carnicero, J., & Fernandez, A. (2012). Manual de salud electrónica para directivos de servicios y sistemas de salud. *Naciones Unidas (ONU)*, 414.

CEPAL. (2010). Salud y TIC, *12*, 6–8.

Cisco. (2017). The Digitization of the Healthcare Industry: Using Technology to Transform Care. *CISCO*, *1*, 12. https://doi.org/10.1057/978-1-349-95173-4

Díaz, A. F., Collazos, G. I., Cortéz Lozano, H., Ortíz, L. J., & Herazo Pérez, G. A. (2012). Implementacion de un sistema de gestión de seguridad de la información (SGSI) en la Comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la Norma ISO 27001, *2*(2), 1–12.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional : un modelo de simulación basado en dinámica de sistemas. *Scientia et Technica*, *22*(2), 193–197.

Healthcare Denmark. (2017). Hospital Logistics. *Innovating Better Life*, *1*, 28.

Information Systems Audit and Control Association. (2013). *Manual de preparación al exámen CISA 2013*. (Information Systems Audit and Control Association, Ed.). New York.

Mahecha Guzmán, M. L., & Coello Falcones, G. R. (2016). *Desarrollo de un sistemae información para gestiona la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la norma ISO 27001-2013*. Escuela Superior Politécnica del Litoral.

Ministerio de Salud. (2012). *Manual del Modelo de Atención Integral de Salud-MAIS*. Quito. https://doi.org/10.1017/CBO9781107415324.004

Ministerio de Salud Pública. (2012). *Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales*. Quito.

Ministerio de Sanidad y Consumo. (2013). *Las TIC en el Sistema Nacional de Salud: el programa sanidad en línea*. Madrid.

Miranda, K. (2013). *Guía metodológica para implementar un sistema de gestión de seguridad en instituciones*. Universidad de Piura. Recuperado a partir de https://pirhua.udep.edu.pe/bitstream/handle/11042/2787/MAS_DET_012.pdf?sequence=1

Organización para la Cooperación y el Desarrollo Económico. (2013). *Tecnologías de la información y de la comunicación: perspectivas de la OCDE sobre la tecnología de la información*. Paris.

Pallas Mega, G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico*. Universidad de la República.

Sánchez Solá, Á. P. (2013). *Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para Pequeñas y Medianas Empresas en la ciudad de Quito*. Pontificia Universidad Católica del Ecuador.

Valencia Duque, F. J., & Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de la Información*, *22*, 73–88. https://doi.org/10.17013/risti.22.73

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO / IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información*, (22), 73–88. https://doi.org/10.17013/risti.22.73

Vanegas Devia, G. A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT. *Revista S&T*, *12*(30), 35–48.

Yaduvanshi, D., & Sharma, A. (2017). Lean Six Sigma in Health Operations: Challenges and Opportunities—'Nirvana for Operational Efficiency in Hospitals in a Resource Limited Settings'. *Journal of Health Management*, *19*(2), 203–213. https://doi.org/10.1177/0972063417699665