Gobierno de TI con énfasis en seguridad de la información para hospitales públicos

Darwin Pillo-Guanoluisa[1], Robert Enríquez-Reyes[2]

[1] Facultad de Postgrado, Universidad de las Américas UDLA, José Queri, Quito 170137.

[2] Facultad de Ingeniería, Ciencias Físicas y Matemáticas, Universidad del Ecuador, Av. Universitaria S/N y Av. América y Facultad de Postgrado, Universidad de las Américas UDLA, José Queri, Quito 170137.

Autores para correspondencia: darwin.marcelo.pillo@gmail.com; renriquez@uce.edu.ec

Fecha de recepción: 17 de mayo 2017 - Fecha de aceptación: 2 de agosto 2017

RESUMEN

El trabajo de investigación de carácter científico propone un modelo de Gobierno de Tecnología de Información con enfoque en Seguridad de la Información para Hospitales Públicos, mediante el uso de modelos, estándares y normas que permitan alinear los objetivos de TI con los objetivos del Hospital, creando valor (beneficios, optimización de riesgos y recursos) para los stakeholders. Se realizó un estudio bibliográfico de carácter analítico sobre el marco legal y normativo relacionado con el derecho a la Salud, además se realiza una investigación acerca de estándares y normas internacionales enfocadas al Gobierno de TI y la Seguridad de la Información Sanitaria. Se desarrolló un Modelo de Gobierno de TI para hospitales, mediante la aplicación del artefacto nuevo generado a través del mapeo entre COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008. Los resultados de la investigación muestran que el Ecuador ha invertido en el sector Salud aproximadamente 11000 millones de dólares y garantiza el derecho a la Salud mediante la Constitución de la República del año 2008. En cuanto a salvaguardar la confidencialidad, integridad y disponibilidad de la información Sanitaria, el Ecuador no posee una regulación o norma propia, como la HIPAA de Estados Unidos o el reglamento 2016/679 de la Unión Europea. La implementación del modelo de Gobierno de TI proporcionará una visión clara del nivel de capacidad de cada proceso del Hospital, definiendo los planes de acción para cerrar las brechas.

Palabras clave: Gobierno de TI, gestión de proyectos, COBIT 5, ISO/IEC 27002, ISO 27799, HIPAA, salud pública Ecuador, seguridad de la información sanitaria.

ABSTRACT

The research proposes a model of IT Governance with focus on Information Security for Public Hospitals, consisting of models, standards and norms that allow alignment of the IT objectives with the Hospital objectives, creating added value (benefits, risk optimization and resources) for stakeholders. An analytical bibliographical study was carried out on the legal and normative framework related to the right to Health. Additionally, research was conducted on international standards with focus on IT Governance and Health Information Security. An IT Governance Model for hospitals was developed, a new tool combining COBIT 5 and the ISO / IEC 27002:2005 and ISO 27799:2008 standards. The results of the investigation show that Ecuador invested approximately 11 billion dollars in the Health sector and guarantees the right to Health through the Constitution of the Republic of 2008. In terms of safeguarding the confidentiality, integrity and availability of sanitary information Ecuador does not have its own law, such as the HIPAA of the United States or the regulation 2016/679 of the European Union. The implementation of the IT Governance model will provide a clear vision of the capacity level of each hospital process, allowing the creation of activities to meet the objectives.

Keywords: IT governance, project management, COBIT 5, ISO/IEC 27002, ISO 27799, HIPAA, public health Ecuador, information security in hospitals.

1. INTRODUCCIÓN

El uso de las TI en las organizaciones de la Salud ha proporcionado grandes beneficios para el sector; sin embargo esto ha ocasionado que dichas organizaciones se vuelvan más críticamente dependientes de los sistemas de información que apoyan la prestación de atención médica, resulta evidente que los eventos en los que se produzcan pérdidas de integridad, disponibilidad y confidencialidad de la información pueden tener un alto impacto clínico y que los problemas derivados de dichos impactos representarían fallas en las obligaciones éticas y legales inherentes a un deber de cuidado por parte de las entidades de salud. Situaciones que concuerdan con el informe de health care and cyber security que indica que en los "últimos dos años, el 81% de hospitales y aseguradoras de Salud han sufrido una brecha en sus datos" (Bell & Ebert, 2015). Además, Bell & Ebert (2015) afirman que "todos estos incidentes provocaron pérdida en los datos, mostrando que los incidentes registrados no se tratan solo de un malware o un virus, sino que además se trata de una exfiltración por parte del personal que pertenece a la organización".

De igual manera en los Hospitales el involucramiento de las TI puede ser considerada una espada de doble filo, puesto que a través de las TI se puede mitigar el riesgo, en lo que respecta a la comprobación de la interdependencia de las enfermedades, la contraindicación de los medicamentos, la satisfacción del cliente / paciente, los errores médicos y el seguimiento de los medicamentos erróneos, y los costos operativos. Pero de igual manera una inadecuada gestión de los riesgos relacionados con las TI en los hospitales puede afectar considerablemente a la continuidad de los servicios de salud. Por lo cual es necesario el uso de marcos de gobernanza basado en estándares específicamente para TI, que permitan asegurar que los objetivos estratégicos de las organizaciones de salud se encuentren alineadas con las metas de TI, así como una adecuada gestión / control de los riesgos relacionados con TI. Existen referencias sobre casos de éxito en la aplicación de COBIT como un marco de referencia relacionado al Gobierno de TI y aplicado en organizaciones de la salud como son: "Sunnybrook Health Sciences Centre" (Curtis, 2013) y "Takeda General Hospital" (Kajimoto, 2012).

Las instituciones adscritas al Sistema Nacional de Salud (SNS) y de forma particular los Hospitales públicos del Ecuador requieren cumplir con sus objetivos estratégicos y desarrollar su misión y visión social a través de prestar con eficiencia su cartera de servicios médicos. De ahí que para asegurar el logro de los objetivos del Hospital a través de TI se hace necesario alinear los objetivos de TI con los objetivos estratégicos de la casa de salud, creando valor (realización de beneficios, optimización de riesgos y recursos) para los interesados. En lo que respecta a Seguridad de la Información aplicable al sector sanitario, el Ecuador actualmente no posee una regulación propia y específica para proporcionar seguridad y confidencialidad a la información; por lo cual en la investigación se desarrolla un artefacto nuevo que contenga el mapeo entre el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008. Esto supone una mejora en los procesos de Gobierno y Gestión de TI que tienen relación con la Seguridad de la Información para las organizaciones del sector salud.

Por consiguiente, el trabajo de investigación propone un modelo de Gobierno de Tecnologías de la Información para Hospitales Públicos con énfasis en la Seguridad de la Información, tomando como caso de estudio al Hospital General Docente de Calderón.

2. MATERIALES Y MÉTODOS

La investigación realizada propone un modelo de Gobierno de TI con énfasis en la Seguridad de la Información que sirva como referencia para los Hospitales Públicos del Ecuador. Teniendo en cuenta que el marco de Gobierno de TI sobre el que se apoya el trabajo realizado es COBIT 5, se generó un instrumento que mapea los procesos y prácticas de COBIT 5 con las normas de Seguridad de la Información aplicable a los Hospitales Públicos del Ecuador. Al respecto la Secretaría Nacional de la Administración Pública (2013) dispone que las "entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva, el uso obligatorio de las Normas Técnicas

Ecuatorianas NTE INEN ISO/IEC 27000 para la Gestión de Seguridad de la Información (SGI)" (Secretaria Nacional de la Administración Pública, 213, pág. 2), siendo la norma utilizada por las instituciones de públicas como referencia para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Las normas de la familia ISO/IEC 27000, utilizadas en el modelo fueron la norma ISO/IEC 27002:2005 que presenta directrices para los controles de seguridad de la información que son genéricas para todas las organizaciones y la norma ISO 27799:2008 que aborda el área de Seguridad de la Información personal de Salud y cómo proteger su confidencialidad e integridad.

2.1. Relación entre la Norma ISO/IEC 27002:2005 e ISO 27799:2008

En este ítem se determinó qué valor aporta la norma ISO 27799:2008 a la norma ISO/IEC 27002:2005 para satisfacer las necesidades de gestión de la Seguridad de la Información del sector sanitario. Se realizó una comparación de alto nivel entre las dos normas que muestran las similitudes y diferencias en la estructura general de las mismas. Posteriormente se realizó una comparación detallada entre las cláusulas, categorías de seguridad y controles de la norma ISO/IEC 27002:2005 y la ISO 27799:2008, que nos permitió identificar las nuevas o enmendadas cláusulas, categorías de seguridad y controles incluidos en la norma ISO 27799:2008.

2.2. Combinación entre COBIT 5 e ISO/IEC 27002:2005

Para establecer la relación entre los procesos de COBIT 5 e ISO/IEC 27002:2005 se utilizó la guía de implementación proporcionada por ISACA denominada, COBIT 5 for Information Security (COBIT 5 para seguridad de la información) como una guía que según afirma ISACA (2012a) "se centra en la seguridad de la información y proporciona una orientación más detallada y práctica para los profesionales de la Seguridad de la Información y demás partes interesadas en todos los niveles de la empresa" (pág. 13).

2.3. Combinación entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008

Las prácticas que contiene cada proceso de COBIT 5 fue el nivel de granularidad utilizado para la integración con las normas ISO/IEC 27002:2005 e ISO 27799:2008. La información utilizada para la combinación es: el mapeo entre COBIT 5 e ISO/IEC 27002:2005, la comparación de las Cláusulas, Categorías de Seguridad y Controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008, las publicaciones oficiales de las normas ISO/IEC 27002:2005 e ISO 27799:2008, y la guía proporcionada por la organización ISACA denominada "Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa" (IT Governance Institute, 2008). Siendo todos estos la base documental para mapear las prácticas de Gobierno y Gestión de COBIT 5 con las categorías de seguridad de la norma ISO/IEC 27002:2005 e ISO 27799:2008. Para facilitar la integración de combinación entre COBIT 5, ISO/IEC 27002:2005 e ISO 27799:2008 se realizaron los siguientes pasos:

a) Identificación de los procesos de COBIT 5 que serán parte del modelo.
b) Establecimiento de la metodología de mapeo con énfasis en Seguridad de la Información aplicado al sector Salud.

   En esta sección se definió los criterios generales utilizados para el mapeo de las categorías de seguridad de las normas ISO/IEC 27002:2005 e ISO 27799:2008, con las prácticas de Gobierno y Gestión de COBIT 5. Dado el alto número de controles que poseen el marco de trabajo y las normas incluidas en el mapeo, es importante definir de qué modo se considerará que un control tiene relación con otro. La metodología utilizada se ha adaptado a partir de la propuesta realizada por ISACA en su libro "Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa" (IT Governance Institute, 2008), los cuales se detallan a continuación:

   √ Parcial (P): El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es más amplia que el/los controles especificados por las normas ISO/IEC 27002:2005 e ISO 27799:2008. Significa que a efectos del modelo propuesto se evidencia un nivel de

cumplimiento satisfactorio con la práctica de COBIT 5, sobreentendiéndose que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 están cubiertos por las actividades de la práctica de COBIT 5.

- √ Completo (C): El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es semejante y pueden considerarse iguales con los controles de la norma ISO/IEC 27002:2005 e ISO 27799:2008. Para efectos del modelo propuesto en el mapeo completo se debe tomar en cuenta que discernir entre usar una u otra modalidad no es un proceso matemático y por tanto puede estar sujeto a interpretaciones o al entorno de la organización. En este caso puede entenderse la relación como bidireccional, por lo que, si se demuestra el cumplimiento en uno de los lados del mapeo, se podrá entender que el otro lado también está cubierto. Se recomienda tomar en cuenta las guías y controles adicionales sugeridos por la norma ISO 27799:2008 debido que el modelo tiene una aplicabilidad en el sector sanitario.
- √ Excede (E): El conjunto de actividades comprendidas dentro de la práctica de COBIT 5 es menos amplia que el conjunto de controles especificados por la norma ISO/IEC 27002:2005 e ISO 27799:2008. Esto significa que el conjunto de controles de las normas de referencia tiene un alcance mayor que las actividades definidas por COBIT 5. En este caso para efecto del modelo propuesto con aplicabilidad en el sector sanitario se debe obligatoriamente tomar en cuenta las guías y controles adicionales sugeridos por la norma ISO 27799:2008.

Para mostrar un ejemplo de mapeo tipificado como excede se ha escogido la práctica DSS05.01 relativo a proteger contra software malicioso (malware). En COBIT 5 se definen seis actividades como se muestra en la Tabla 1.

Tabla 1. DSS05.01: Proteger contra software malicioso (malware). Tomado de (ISACA, 2012b, pág. 192).

DSS05´Prácticas, Entradas/Salidas y Actividades del Proceso				
Prácticas de Gestión	*Entradas*		*Salidas*	
DSS05.01 Proteger contra software malicioso (malware) Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía – spyware – y correo basura)	De	Descripción	Descripción	A
			Política de prevención de software malicioso	AP001.04
			Evaluaciones de amenazas potenciales	AP012.02 AP012.03
Actividades				
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.				
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera o semi-automáticamente.				
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.				
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).				
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).				
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.				

Seguidamente, observamos el resultado del mapeo entre las actividades de la práctica DSS05.01 de COBIT 5 con los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008. Como se muestra en la Tabla 2.

Tabla 2. Mapeo de la práctica DSS05.01: Proteger contra software malicioso (malware).

COBIT 5	ISO/IEC 27002:2005	ISO 27799:2008	Mapeo
DSS05.01 Proteger contra software malicioso (malware)	6.1 Organización interna: 6.1.7 Contacto con grupos de interés especial. 7.1 Responsabilidad sobre los activos: 7.1.3 Acuerdos sobre el uso aceptable de los activos 10.4 Protección contra software malicioso y código móvil: 10.4.1 Controles contra software malicioso. 10.4.2 Medidas y controles contra códigos móviles (cliente).	7.3.2 Organización interna: 7.3.2.4 Contacto con las autoridades, contacto con grupos de intereses especiales y revisión independiente de la seguridad de la información. 7.4.1 Responsabilidad sobre los activos de información de salud: 7.7.4 Protección contra software malicioso y código móvil: 7.7.4.1 Controles contra software malicioso. 7.7.4.2 Medidas y controles contra códigos móviles (cliente).	E

En este caso la Tabla 2, se ha definido como excede, puesto que los controles de las normas ISO/IEC 27002:2005 e ISO 27799:2008 cubren por completo a las actividades de la práctica de COBIT 5, y además agregan controles adicionales dedicados a proteger la información contra software malicioso (malware) y brindan un mejor detalle para el cumplimiento del objetivo de la práctica de gestión de COBIT 5. Entre los controles adicionales se tiene la creación de "planes adecuados de continuidad de negocio para la recuperación de los ataques de código malicioso, políticas contra la descarga y uso de código no autorizado por el cliente" (ISO/IEC 27002:2005, pág. 53) y "mantener el contacto adecuado con grupos especializados en seguridad de la información" (ISO/IEC 27002:2005, pág. 22). Además, la norma ISO 27799:2008 sugiere una "capacitación de concientización para protegerse contra software malintencionado, de una forma diferenciada y apropiada para el personal médico y administrativo" (ISO 27799:2008, pág. 32) de la organización de Salud.

2.4. Guía de implementación del modelo

Para la implementación del modelo propuesto se utilizó la Guía del PMBOK, tomando en cuenta que la "aplicación de conocimientos, habilidades, herramientas y técnicas aumenta las posibilidades de conseguir los objetivos de un proyecto" (PMI, 2013, pág. 2). En la Figura 1 se representa un esquema del modelo propuesto, mediante el uso de marcos de referencia y buenas prácticas de la industria.

Fase 1: Iniciación

En la etapa de iniciación según afirma PMI (2013) se debe "desarrollar un documento que autoriza formalmente la existencia de un proyecto y confiere al director del proyecto la autoridad para asignar los recursos de la organización a las actividades del proyecto" (pág. 54). Las entradas de esta fase están en base a los procesos y necesidades actuales del Hospital, así como también que estén alineados a los objetivos estratégicos de la institución. Finalmente, el principal beneficio de esta fase es generar un documento denominado Acta de Constitución del Proyecto el cual marque el inicio, los límites, la creación de un registro y el establecimiento de una forma directa para que la dirección general acepte formalmente y se comprometa con el proyecto.

Fase 2: Planificación

La fase de planificación está "compuesta por aquellos procesos realizados para establecer el alcance total del esfuerzo, definir y refinar los objetivos, y desarrollar la línea de acción requerida para alcanzar dichos objetivos" (PMI, 2013, pág. 55). El beneficio clave es un documento central denominado Plan para la Dirección del Proyecto que "define la estrategia y las tácticas, así como la línea de acción o ruta para completar con éxito el proyecto. El contenido del Plan para la Dirección del Proyecto es variable en función del área de aplicación y de la complejidad del proyecto" (PMI, 2013, pág. 74).

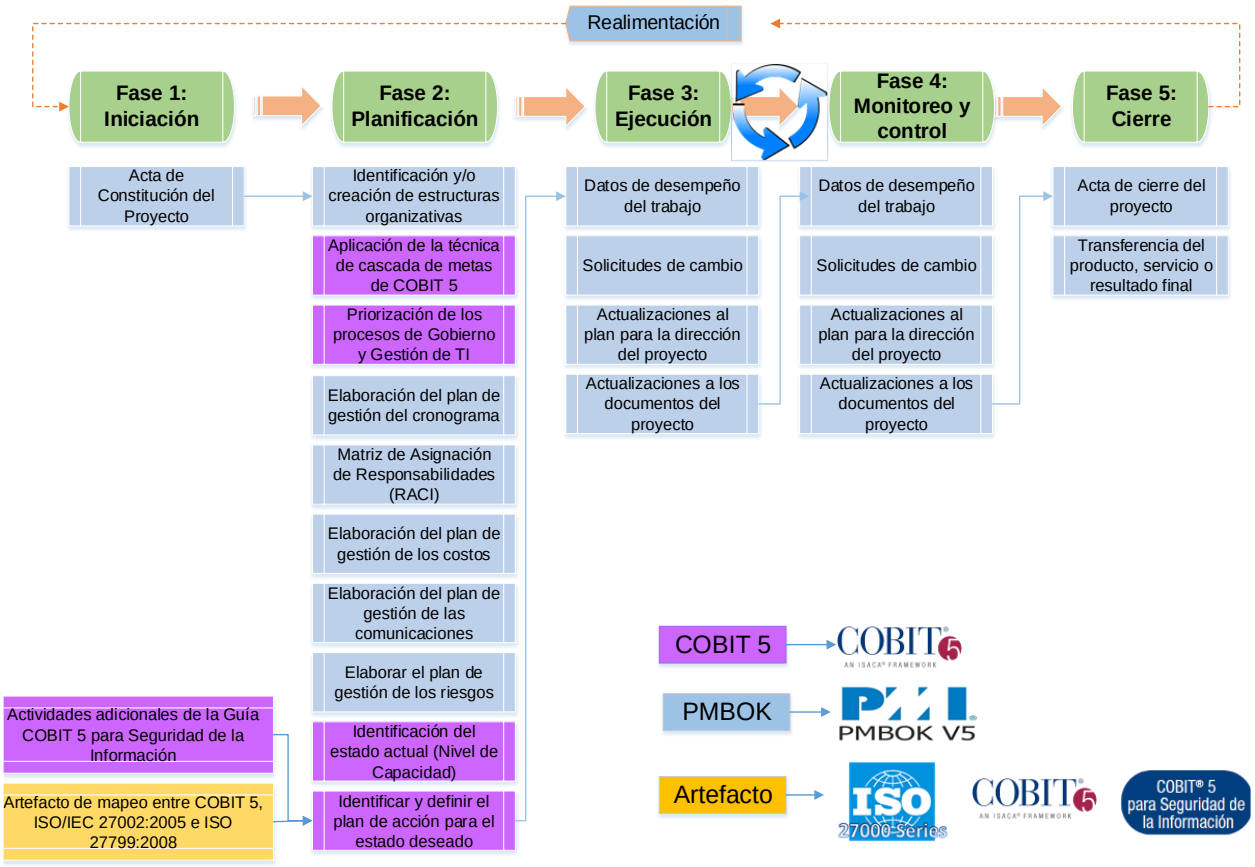

Figura 1. Modelo de Gobierno de TI con énfasis en la Seguridad de la Información para Hospitales Públicos del Ecuador.

Fase 3: Ejecución

En esta fase se ejecuta el proyecto autorizado por la dirección general del Hospital en la fase de inicio y se realizarán una a una, las actividades diseñadas en la fase de planificación. Es así que la fase de ejecución efectúa "la coordinación de personas y recursos, se gestiona las expectativas de los interesados, así como la integración y realización de las actividades del proyecto conforme a la planificación establecida en la fase anterior" (PMI, 2013, pág. 56).

Fase 4: Monitoreo y control

Esta fase tiene como objetivo dar seguimiento, revisar e informar el avance a fin de cumplir con los objetivos de desempeño definidos en el Plan para la Dirección del Proyecto diseñado en la fase de planificación.

Fase 5: Cierre

Los procesos de la fase de cierre se encargan de finalizar todas las actividades a través de todos los grupos de procesos de la dirección de proyectos, permitiendo completar formalmente el proyecto.

3. RESULTADOS

3.1. Implementación del Modelo de Gobierno de TI con énfasis en Seguridad de la Información en el Hospital General Docente de Calderón

El Hospital General Docente de Calderón Figura 2, fue inaugurado el jueves 16 de julio del 2015, es un Hospital público de segundo nivel que beneficia a los habitantes del norte de Quito y parroquias aledañas. El Hospital tiene 156 camas y cuenta con 21 especialidades, como ginecología, pediatría, odontología, traumatología, neurocirugía, entre otros. Esta nueva casa de salud cuenta con un área de emergencia que funciona las 24 horas, como también posee una ludoteca y una sección para residencia médica. En la construcción del Hospital el Estado ha "invertido aproximadamente 74 millones de dólares que incluye la infraestructura y equipamiento" (Ministerio de Salud Pública, 2016).

Figura 2. Hospital General Docente de Calderón. Tomado de Andes (2012).

La implementación del modelo asegura el logro de los objetivos estratégicos del Hospital a través de TI, permitiendo a la casa de salud cumplir con su Misión y Visión social. El Proyecto incluye los siguientes entregables que son desarrollados y formalizados con la Gerencia Hospitalaria en el transcurso de las diferentes fases del modelo:

a) Acta de Constitución del Proyecto.
b) Plan de Gestión del Alcance.
c) Plan de Gestión del Cronograma.
d) Plan de Gestión de los Recursos Humanos.
e) Plan de Gestión de los Costos.
f) Plan de Gestión de las Comunicaciones.
g) Plan de Gestión de Riesgos.
h) Documentación sobre el estado de capacidad actual de los procesos de Gobierno y Gestión de TI seleccionados.
i) Documentación sobre el estado de capacidad objetivo de los procesos de Gobierno y Gestión de TI seleccionados.
j) Documentación sobre las actividades que permitan alcanzar el estado deseado.
k) Informe del desempeño en la ejecución del proyecto y gestión de solicitudes de cambio.
l) Acta de Cierre del Proyecto.

Entre los entregables del proyecto, se define la estructura organizativa del Hospital que proporcionará el apoyo necesario en todo el ciclo de vida de implementación del Gobierno de TI. Para la identificación se utilizó la estructura orgánica definida en el Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del MSP y las recomendaciones de COBIT 5 en su Guía un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa.

Tabla 3. Identificación de la estructura organizativa. Adaptada de Ministerio de Salud Pública (2012) y de ISACA (2012b, pág. 76).

Hospital General Docente de Calderón	Función	Roles y Estructuras Organizativas de COBIT 5
1. Proceso Gobernante		
1.1 Gerencia Hospitalaria	Gerenciar el funcionamiento global del Hospital como máxima autoridad y representante legal de la institución, en el marco de las directrices y acuerdos emanados por el Ministerio de Salud Pública y en cumplimiento de la normativa legal vigente.	Director General Ejecutivo CEO
1.2 Comité de Gestión y Direccionamiento Estratégico del Hospital	Responsables del Gobierno del Hospital como autoridades máximas de cada proceso interno, en el marco de las directrices y acuerdos emanados por el Ministerio de Salud Pública y en cumplimiento de la normativa legal vigente.	Consejo de Administración
2. Procesos Agregadores de Valor		
2.1 Gestión Asistencial	Dirigir y coordinar actividades médico sanitarias de todas las especialidades, a fin de que éstas otorguen al paciente los servicios médicos y hospitalarios con oportunidad, alta calidad, eficiencia y efectividad. Garantizar el funcionamiento de los departamentos productores de salud dentro de los parámetros estandarizados de eficiencia y calidad.	Ejecutivo de Negocio
3. Procesos Habilitantes de Asesoría		
3.1 Gestión de Planificación, Seguimiento y Evaluación de Gestión	Articular los recursos, procedimientos y planes de salud en función de las estratégicas y objetivos institucionales. Implementar sistemas de seguimiento y control que contribuyan a la evaluación del cumplimiento de objetivos y metas y a la reducción de la brecha de oferta y demanda de los servicios de salud que ofrece el Hospital, con el propósito de generar satisfacción de los clientes internos, externos y el mejoramiento de los servicios que se ofrece a la población.	Oficina de Gestión de Programas y Proyectos (PMO)
3.2 Gestión de Asesoría Jurídica	Asesorar en temas relacionados a la correcta aplicación de la carta magna, leyes, reglamentos, acuerdos, decretos y otros instrumentos legales relacionados con el andamiaje legal, a fin de que la institución y su gestión se encuentren siempre amparada en la ley.	Cumplimiento
3.3 Gestión de Calidad	Velar por la implementación y el cumplimiento del sistema integral de gestión de calidad y de los procedimientos e indicadores de calidad de cada uno de los servicios provistos por el hospital para satisfacer las necesidades de la demanda y la interacción con otros sistemas en su contexto.	Propietario del Proceso de Negocio
4. Procesos Habilitantes de Apoyo		
4.1 Gestión de Talento Humano	Administrar, seleccionar y desarrollar el talento humano del Hospital, garantizando su desarrollo constante mediante una verdadera capacitación,	Jefe de Recursos Humanos

	bienestar social y seguridad, con el fin de potencializar las habilidades y capacidades de su personal en cumplimiento a la ley, reglamentos, normas, políticas y otros documentos legales vigentes.	
4.2 Gestión Financiera	Administrar, organizar y controlar las actividades financiero-contables del Hospital, proporcionando ágil, oportuna y transparentemente los recursos financieros requeridos para la ejecución de los planes, programas y proyectos de la institución.	Director General Financiero (CFO)
4.3 Gestión Administrativa	Administrar con eficiencia, eficacia y efectividad los recursos materiales, suministros, bienes y servicios requeridos para la ejecución de los planes, programas y proyectos de la institución.	Director General Operativo (COO)
4.4 Gestión de la Tecnologías de la Información y Comunicaciones	Aplicar las normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones, orientadas a la optimización de los recursos y fortalecimiento de la red interna para mejorar la eficiencia en la atención a los pacientes.	Director de Informática/Sistemas (CIO)

Posteriormente, como parte del modelo propuesto se designó a la técnica de cascada de metas de COBIT 5 como la herramienta para asegurar el alineamiento de TI con los objetivos estratégicos y metas del Hospital General Docente de Calderón. En la Tabla 4 se muestran los procesos de Gobierno y Gestión de TI.

Tabla 4. Procesos de COBIT 5 con énfasis en la Seguridad de la Información para el Hospital General Docente de Calderón.

1	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno
2	APO01	Gestionar el Marco de Gestión de TI
3	APO07	Gestionar los Recursos Humanos
4	APO09	Gestionar los Acuerdos de Servicios
5	APO12	Gestionar los Riesgos
6	APO13	Gestionar la Seguridad
7	BAI02	Gestionar la Definición de Requisitos
8	DSS04	Gestionar la Continuad
9	DSS05	Gestionar los Servicios de Seguridad

A continuación, se identificó el estado actual y deseado de los procesos que contribuirán a conseguir los objetivos estratégicos del Hospital, para la situación actual se realiza una evaluación de capacidad de procesos a través del PAM (Modelo de Evaluación de Procesos) de COBIT 5 como método de evaluación.

En la Tabla 6 se presenta el orden de implementación de los procesos de Gobierno y Gestión de TI del Hospital, de acuerdo con el nivel de valoración obtenido en la cascada de metas de COBIT 5 y la importancia otorgada por los miembros del Equipo de Proyecto.

Tabla 5. Identificación del nivel de capacidad alcanzado y deseado.

Núm.	Código	Nombre del proceso	Nivel de capacidad alcanzado	Nivel de capacidad deseado	Puntuación deseada
1	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	0	1	L
2	APO01	Gestionar el Marco de Gestión de TI	0	1	L
3	APO07	Gestionar los Recursos Humanos	0	1	L
4	APO09	Gestionar los Acuerdos de Servicios	0	1	L
5	APO12	Gestionar los Riesgos	0	1	L
6	APO13	Gestionar la Seguridad	0	1	L
7	BAI02	Gestionar la Definición de Requisitos	0	1	L
8	DSS04	Gestionar la Continuad	0	1	L
9	DSS05	Gestionar los Servicios de Seguridad	0	1	L

Tabla 6. Orden de implementación de los procesos de Gobierno y Gestión de TI del Hospital.

Núm.	Código	Nombre del proceso	Sumatoria	Nivel de Importancia
1	APO01	Gestionar el Marco de Gestión de TI	18	Muy importante
2	APO13	Gestionar la Seguridad	17	Muy importante
3	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	14	Muy importante
4	DSS05	Gestionar los Servicios de Seguridad	14	Muy importante
5	APO12	Gestionar los Riesgos	14	Importante
6	APO07	Gestionar los Recursos Humanos	13	Importante
7	DSS04	Gestionar la Continuidad	15	Poco importante
8	BAI02	Gestionar la Definición de Requisitos	14	Poco importante
9	APO09	Gestionar los Acuerdos de Servicios	13	Poco importante

Para alcanzar el estado deseado se identificó y definió el plan de acción para cada proceso. De igual manera debido al detalle de las actividades a realizar, a manera de ejemplo se muestra en la Tabla 7 la evaluación de capacidad y en la Tabla 8 el plan de acción del proceso EDM01.

Tabla 7. Resultados de la evaluación del proceso EDM01.

Nombre de Proceso: EDM01 – Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno										
Niveles de capacidad	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Puntuación de los criterios		P	N	N						
Nivel de capacidad alcanzado	0									
Escala de calificación	N: No logrado (0 a 15%)		P: Parcialmente logrado (>15 a 50%)		L: Logrado en gran medida (>50 a 85%)			F: Logrado totalmente (>85 a 100%)		

El nivel de capacidad alcanzado por el proceso TI de gobierno EDM01 - Asegurar el establecimiento y mantenimiento de un marco de trabajo de gobierno es cero (0). Mostrando que las decisiones o iniciativas de TI para aportar a los objetivos estratégicos del Hospital, actualmente son gestionadas por las áreas de planificación y administrativa - financiera del Hospital. Por lo tanto, existen decisiones, como la provisión de nuevos servicios o el abastecimiento de infraestructura TI, sin una previa planificación e investigación del retorno de inversión, realizada por prestigio interinstitucional. Además, por iniciativa propia la Unidad de Gestión de Tecnologías de la Información y Comunicaciones realiza encuestas de satisfacción a los usuarios sobre los servicios de TI proporcionados, para un posterior reporte a la Gerencia Hospitalaria. Sin embargo, por no encontrarse bien definidos los roles y responsabilidades dentro del sistema de gobierno del Hospital dichos informes son desestimados o revisados en forma tardía.

Conforme a la metodología de aplicación del modelo propuesto, a continuación, en la Tabla 8 se plantea una serie de actividades a realizar en el proceso EDM01, con la finalidad de alcanzar el nivel de capacidad deseado. Se debe resaltar que las actividades están en base al artefacto nuevo generado mediante la combinación entre las prácticas de Gobierno y Gestión de COBIT 5 con las categorías de seguridad de la norma ISO/IEC 27002:2005 e ISO 27799:2008.

Tabla 8. Plan de acción para alcanzar el estado deseado en el proceso EDM01.

EDM01 – Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno
Para garantizar que las decisiones relativas a TI se han adoptado en línea con los objetivos del Hospital, garantizando el cumplimiento de los requerimientos regulatorios y legales, así como también que se han alcanzado los requerimientos de Gobierno de la Gerencia Hospitalaria, se recomienda: a) *Evaluar el Sistema de Gobierno*: Identificar y comprometerse continuamente con las partes interesadas del Hospital, realizar una estimación del diseño actual y futuro del Gobierno de TI de la casa de salud. Para lo cual se sugiere las siguientes actividades: • Analizar e identificar los factores del entorno interno y externo (obligaciones legales, contractuales y regulatorias) y tendencias en el entorno de prestación de servicios de salud pública que pueden influir en el diseño del Gobierno de TI. • Determinar la relevancia de TI y su papel con respecto a prestación de servicio de salud. • Alinear las capacidades de TI con los intereses de la Gerencia y Comité de Gestión, así como también con los objetivos, misión y visión del Hospital. • Articular los principios de un modelo de toma de decisiones, para que las TI sean efectivas y estén alineadas con los objetivos estratégicos, Misión y Visión del Hospital. • Acordar un modelo de delegación, que determine los niveles apropiados para la delegación de autoridad dentro del Hospital, incluyendo reglas de umbrales, para las decisiones de TI. • Identificar en qué medida la Seguridad de la Información cumple con las necesidades del negocio del Hospital. • Establecer principios que guíen el diseño de facilitadores de la Seguridad de la Información y promueven un ambiente positivo para la seguridad. • Determinar con la Gerencia y Comité de Gestión del Hospital un modelo óptimo en la toma de decisiones para la Seguridad de la Información. b) *Orientar el Sistema de Gobierno*: Comunicar los principios del Gobierno de TI a la Gerencia Hospitalaria y obtener su apoyo, su aceptación y su compromiso. Así mismo se deberá orientar que las estructuras, procesos y prácticas para que el Gobierno de TI estén en línea con: • Comunicar los principios del Gobierno de TI (alineamiento estratégico, entrega de valor, gestión de riesgos, gestión de los recursos y medición del desempeño) y acordar con la Gerencia Hospitalaria la manera de establecer un liderazgo informado y comprometido. • Establecer las estructuras, procesos y prácticas del Gobierno de TI en el Hospital, procurando que estén en línea con los principios de diseños de Gobierno, los modelos de toma de decisión y de delegación acordados.

4. DISCUSIONES

El modelo de Gobierno de TI propuesto se realizó en base a un estudio bibliográfico de carácter analítico de los estándares internacionales y marcos de trabajo enfocados al Gobierno de TI y la Seguridad de la Información sanitaria. La combinación de las normas ISO/IEC 27002 e ISO 27799 con COBIT 5, permite aportar objetivos de control y controles específicos de Seguridad de la información del sector Salud a los procesos de Gobierno y Gestión de COBIT 5. De igual manera el uso de las buenas prácticas en gestión de proyectos como el PMBOK, aumenta las posibilidades de conseguir los objetivos del modelo propuesto, puesto que contiene la información necesaria para iniciar, ejecutar, supervisar, monitorear y cerrar un proyecto.

Investigaciones similares sobre el uso de normas y regulaciones específicas de Seguridad de la Información aplicada al sector Salud, como la investigación *Triple A (Autenticación, Autorización y Contabilidad) en atención de Salud* en una de sus conclusiones indica que es "conveniente requisitos de

la ley HIPAA de Estados Unidos en el diseño de sistemas sanitarios, donde algunos de los requisitos cubren temas como el uso de identificadores únicos, derechos de acceso, encriptación, etc." (De Haan, 2008, pág. 63). Así como también en la investigación *Modelando Control de Acceso para Sistemas de Información de Salud* en una de sus conclusiones indica que "las políticas y normas de control de acceso para sistemas de información de Salud deben integrar normativas, legislación y necesidades específicas de los usuarios" (Margarida, 2010, pág. 144). Considerando lo anterior el modelo propuesto hace uso combinado de las normas ISO/IEC 27002 e ISO 27799, tomando en cuenta además que el sector sanitario es un entorno muy complejo. No siempre es posible compararlo con sectores como la Banca, el Comercio o incluso con el Gobierno, donde los datos también son muy sensibles; pero sin embargo en el sector Salud se maneja información que está relacionada directamente con la vida de las personas. Podemos indicar que es complicado controlar, hacer cumplir y asegurar que todos los procesos de TI funcionen siempre eficientemente y que las vidas humanas o información de los pacientes no estén comprometidas por sistemas de TI mal ejecutados. Sin embargo, hay que esforzarse por garantizar el cumplimiento de las normas y regulaciones en las organizaciones sanitarias que permitan mitigar dichos riesgos.

En cuanto a la Gobernanza de Tecnologías de la Información en organizaciones sanitarias del Ecuador, no se tiene una referencia válida o investigación realizada en el país como si existen en áreas como en Telecomunicaciones (Gallegos & Murillo, 2015), en Instituciones Educativas (Lozano & Utreras, 2014) y (Tintín & Vásquez , 2015), en Instituciones Financieras (Coronel, 2013), etc. Las conclusiones y resultados de las investigaciones mencionadas concuerdan en que el Gobierno y Gestión de TI "actualizan y normalizan los procesos de la organización de forma que se cumplan las metas del negocio, obtengan beneficios, reduciendo costos y riesgos existentes" (Tintín & Vásquez , 2015, pág. 153). Así como también resaltan que la implementación de "marcos de referencia internacionales sobre Gobierno, Riesgos y Cumplimiento de TI generan ventajas competitivas a las organizaciones que las aplican" (Coronel, 2013, pág. 68). De ahí que en concordancia con lo antes mencionado el modelo propuesto de Gobierno de TI con énfasis en Seguridad de la Información para Hospitales Públicos utiliza COBIT 5 como marco de referencia principal. En donde se puede agregar que existen casos de éxito en la aplicación de COBIT como un marco de referencia relacionado al Gobierno de TI y aplicado en organizaciones de la salud como son: "Sunnybrook Health Sciences Centre" (Curtis, 2013) y "Takeda General Hospital" (Kajimoto, 2012).

Sobre la inversión en TI de las organizaciones sanitarias públicas se basa habitualmente por la petición de una unidad o área de la organización, la existencia de presupuesto para realizar la adquisición o el desarrollo, así como también una solicitud de la máxima autoridad. De igual manera a menudo el responsable de TI de los Hospitales no participa directamente en el Comité de Dirección, dificultando el alineamiento entre los objetivos del Hospital y objetivos del departamento de TI. El modelo de Gobierno de TI a través de la metodología propuesta involucra al responsable de TI en las decisiones estratégicas del Hospital que tienen relación con TI, en concordancia con estudios realizados en otros países, como el publicado por Gartner que durante cuatro años entrevistó a 97 responsables de sistemas de información de hospitales Americanos señalando que "debe existir participación de los responsables de sistemas de información asistenciales, en el Comité de Dirección teniendo como responsabilidad asegurar el alineamiento de las inversiones de TI con la estrategia corporativa" (Shaffer & Lovelock, 2009), y otra investigación realizada en los hospitales de Madrid – España indico que para obtener "mejores resultados hospitalarios del sistema de Salud a través de las prácticas de Gobierno de Tecnologías de la Información, debería haber una participación activa del departamento de TI en el Comité de Dirección del Hospital, análisis de riesgos y evaluación del retorno de la inversión" (Muria, 2015, pág. 137).

Finalmente, sobre la implementación de marcos de referencia de Gobierno de TI y normas de Seguridad de la Información en investigaciones internacionales, Lepage (2014) realizó una investigación para las empresas prestadoras de servicios de Salud privadas que ofrecen servicios de atención de Salud con infraestructura propia y de terceros, que están sujetos a los controles de la Superintendencia de Entidades Prestadoras de Salud de Perú. Dicho modelo tiene como objetivo "encontrar los recursos y capacidades necesarias para abastecer sus sucursales y poblarlos de la infraestructura tecnológica necesaria para brindar atención y a su vez soportar sus sistemas organizacionales y cumplir con las regulaciones a las cuales se encuentran sujetas" (Lepage, 2014, pág.

55). Así como también está "enfocado a determinar roles y políticas de Seguridad de Información para procesos específicos de admisión, atención y egreso del paciente" (Lepage, 2014, pág. 74) para la empresa privada prestadora de servicios de Salud. En comparación con el modelo propuesto en la investigación realizada, el campo de aplicación son los Hospitales Públicos del Ecuador y los objetivos estratégicos de carácter social que tiene cada casa de Salud, además de la combinación de las normas ISO/IEC 27002 e ISO 27799 con COBIT 5 que permite aportar objetivos de control y controles específicos de Seguridad de la Información del sector Salud. De igual manera el uso de las buenas prácticas en Gestión de Proyectos como el PMBOK, habilita que el Modelo de Gobierno de TI propuesto pueda ser repetible y acoplarse a diferentes Hospitales Públicos.

5. CONCLUSIONES

El marco referencial COBIT 5 es robusto, flexible e integrador, y permite a las organizaciones alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, disminución de costos y riesgos, con un modelo integral que cubre de extremo a extremo a las organizaciones. Además, tiene varios principios, prácticas, herramientas y modelos de análisis que permiten abordar aspectos críticos; por lo que constituyó una base sólida para el diseño del modelo de Gobierno de TI para Hospitales Públicos, con énfasis en la Seguridad de la Información.

El sector de la Salud y, por consiguiente, los sistemas de TI de atención médica están sujeto a una gran cantidad de normas y regulaciones que se refieren a la Seguridad de la Información. Sin embargo, debido a factores como la escasa coordinación y normalización internacional la mayoría de dichas normas y regulaciones son específicos para cada país o región. Actualmente, las normas y regulaciones más reconocidas en el tratamiento de la información de salud son la norma ISO 27799, la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) de Estados Unidos y el reglamento 2016/679 de la Unión Europea.

La herramienta generada a través del mapeo entre el marco de referencia COBIT 5 y las normas ISO/IEC 27002:2005 e ISO 27799:2008, mejora la aplicación de los procesos de Gobierno y Gestión que tienen relación con la Seguridad de la Información para las organizaciones del sector Salud. Debido a que los controles de las normas de referencia ISO/IEC 27002:2005 e ISO 27799:2008 tiene un alcance mayor que las actividades definidas por COBIT 5 en las prácticas del proceso.

El uso de las buenas prácticas en Gestión de Proyectos aumenta las posibilidades de conseguir los objetivos del modelo Gobierno de TI con énfasis en la Seguridad de la Información, ya que contiene la información necesaria para iniciar, planificar, ejecutar, supervisar y controlar, y cerrar un proyecto. Es así como el Modelo de Gobierno de TI propuesto puede ser repetible y acoplarse a diferentes Hospitales Públicos.

La priorización de procesos a través del mecanismo de la cascada de metas de COBIT 5, identifica los procesos críticos de Gobierno y Gestión de TI que se necesitan para asegurar resultados exitosos en la implementación del modelo de Gobierno de TI con énfasis en la Seguridad de la Información para hospitales públicos del Ecuador.

La implementación del modelo de Gobierno de TI con énfasis en la Seguridad de la Información en el Hospital General Docente de Calderón proporciona una visión clara del nivel de capacidad en que se encuentra cada proceso del Hospital, permitiendo definir los planes de acción para cerrar las brechas y alcanzar el estado deseado. Para asegurar el logro de los objetivos estratégicos del Hospital y crear valor (realización de beneficios, optimización de riesgos y recursos) para el Comité de Dirección del Hospital.

AGRADECIMIENTO

A todos quienes contribuyeron de distinta manera para la realización de la investigación y en forma especial al Hospital General Docente de Calderón por haber auspiciado el proyecto.

BIBLIOGRAFÍA

Andes, A. (2012). *Obras en el sector social de Ecuador no se detendrán en 2016 reitera Presidente Correa*. Recuperado el 01 de Octubre de 2016, de http://www.andes.info.ec/es/noticias/obras-sector-social-ecuador-no-detendran-2016-reitera-presidente-correa.html

Bell, G., & Ebert, M. (2015). *Health care and cyber security* (Vol. 1). Recuperado el 2016 de Octubre de 02, de https://www.kpmg.com/LU/en/IssuesAndInsights/Articlespublications/Doc

Coronel, K. (2013). *Metodología de evaluación del gobierno, riesgos y cumplimiento de la tecnología de información en instituciones del sistema financiero Ecuatoriano.* Quito, Ecuador: Pontificia Universidad Católica del Ecuador. (Tesis Maestria).

Curtis, J. (2013). *ISACA.* Obtenido de https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Sunnybrook-Health-Sciences-Centre.aspx

De Haan, M. (2008). *Triple A (Autenticación, Autorización y Contabilidad) en atención de Salud.* Groningen, Holanda: Universidad de Groningen. (Master Thesis).

Gallegos, F., & Murillo, M. (2015). *Metodología de gestión de seguridad de la información enfocada a las industrias de Telecomunicaciones en el Ecuador.* Quito, Ecuador: Escuela politécnica nacional. (Tesis de Maestria).

ISACA. (2012a). *COBIT 5: For Information Security.* Rolling Meadows, Illinois.

ISACA. (2012b). *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa* (ISBN 978-1-60420-282-3 ed.). Estados Unidos de America.

ISO 27799. (2008). *Health informatics - Information security management in health using ISO/IEC 27002.*

ISO/IEC 27002. (2005). *Information technology - Security techniques - Code of practice for information security management.*

IT Governance Institute. (2008). *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business.* Rolling Meadows, USA.

Kajimoto, M. (2012). *ISACA.* Obtenido de https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Using-COBIT-to-Aid-in-Hospital-Risk-Management.aspx

Lepage, D. (2014). *Diseño de un modelo de gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0*. Lima, Peru: Pontificia Universidad Catolica del Peru.

Lozano, A., & Utreras, J. (2014). *Diseño de un marco referencial de Gobierno de TI basado en COBIT para instituciones educativas k-12 radicadas en el Ecuador.* Quito: Universidad de Las Américas. (Tesis de Maestria).

Margarida, A. (2010). *Modelando Control de Acceso para Sistemas de Información de Salud.* Canterbury, England: The University of Kent. (PhD in Computer Science).

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

Ministerio de Salud Pública. (2016). *Planes y programas de la institución en ejecución - MSP.* Recuperado el 10 de Noviembre de 2016, de http://instituciones.msp.gob.ec/images/Documentos/Ley_de_Transparencia/2016/Julio/k-Planes-y-programas-en-ejecucion.pdf

Muria, J. (2015). *Relación entre Gobierno de Tecnologías de la Información y resultados del sistema sanitario en hospitales del servicio Madrileño de salud.* Valencia, España: U. P. Doctoral, Ed.

PMI. (2013). *Guía de los fundamentos para la dirección de proyectos - PMBOK.* Pensilvania, USA: Project Management Institute.

Secretaria Nacional de la Administración Pública. (213). *Esquema Gubernamental de Seguridad de la Información.* Recuperado el 2016 de Diciembre de 17, de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2016/02/Esquema-Gubernamental-de-Seguridades-de-la-Informacion.pdf

Schaffer, V., & Lovelock, J.-D. (2009). *Results of the Gartner-AMDIS Survey of chief medical informatics officers.* Stamford, Connecticut: Gartner, Inc.

Tintín , C., & Vásquez, R. (2015). *Aplicación de COBIT 5.0 en el diseño de un gobierno y gestión de TI para el centro de educación continúa.* Quito, Ecuador: Escuela Politécnica Nacional.