PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

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

Tesis para optar el Título de **Ingeniera Informática** que presenta el bachiller:

Diana Estefanía Lepage Hoces

ASESOR: Moisés Antonio Villena Aguilar

Lima, Abril del 2014

RESUMEN

Con la reciente publicación de la ley de protección de datos personales y la actualización de las dos (2) principales normas de la familia de la ISO 27000, se verifica la importancia de la información dentro de las organizaciones.

En el caso de las empresas prestadoras de servicios de salud, el sector ha ido creciendo tras la necesidad de los clientes por contar con un servicio de excelencia para toda la familia y detección de enfermedades, por ello se crean nuevos programas para tener acceso a estos servicios, teniendo como consecuencia el incremento de datos e información.

Por esa razón, se ven en la necesidad de incrementar y/o mejorar su infraestructura tecnológica para soportar sus procesos de negocio, mejorando la calidad y rapidez de sus servicios, integrando datos provistos por otras entidades y velando por la confidencialidad de la ellos de acuerdo al marco regulatorio al que están sujetas. No obstante, se debe garantizar el alineamiento estratégico y la correspondencia de esta tecnología con los objetivos de negocio que aseguren el retorno de la inversión.

A partir de lo expuesto, se plantea una solución integrada que brinde un enfoque estratégico y comprometa a la Alta Dirección para que participe del cambio que conlleve a que las empresas logren sus objetivos de la mano de tecnología correctamente gestionada. Esta solución es diseñar un Gobierno de Tecnología de Información con enfoque a seguridad de información, velando por el cumplimiento de los cinco (5) pilares que son el alineamiento estratégico, la entrega de valor o retorno de inversión, medición del desempeño de TI, gestión de riesgos y gestión de recursos.

Para el proyecto se empleará un marco de negocio mundialmente reconocido, COBIT 5.0, que brinda buenas prácticas para implementar esta solución dentro de cualquier organización según sea el contexto. Así mismo, integra una serie de marcos reconocidos y permite su uso desde una alta perspectiva de negocio y finalmente presentarse como una alternativa de solución ante una problemática generalizada a nivel estratégico y tecnológico en las empresas prestadoras de servicio de salud.

Índice de contenido

Índice de Tablas

Índice de Ilustraciones

Capítulo 1. Generalidades

1.1 Problemática

En las últimas décadas se han observado constantes cambios dentro de los paradigmas del negocio, ya sean éstos del tipo financiero, comercial, manufacturero, etc. En nuestro país se observa el progreso de las pequeñas y medianas empresas, así como el crecimiento de la actividad empresarial y de algunos sectores económicos en particular. Véase la siguiente tabla en la cual se indican la variación del producto bruto interno para cada rubro:

PERÚ: PRODUCTO BRUTO INTERNO
(Variación porcentual del índice de volumen físico respecto al mismo período del año anterior)
Valores a precios constantes de 1994

Actividades	2012/2011					2013/2012
	I Trim.	II Trim.	III Trim.	IV Trim.	Año	I Trim.
Economía Total (PBI)	**6,0**	**6,5**	**6,8**	**5,9**	**6,3**	**4,8**
Agricultura, Caza y Silvicultura	2,5	7,9	4,0	4,8	5,1	6,6
Pesca	-10,5	-10,6	1,0	-25,4	-11,6	-4,5
Minería e Hidrocarburos	3,4	4,3	3,5	-2,0	2,2	-0,6
Manufactura	-0,7	0,1	3,7	2,2	1,3	-0,2
Electricidad y Agua	6,3	5,1	5,1	4,6	5,2	4,8
Construcción	12,4	16,7	19,3	12,5	15,2	11,9
Comercio	7,9	6,4	6,2	6,4	6,7	5,0
Otros Servicios 1/	7,8	7,2	6,9	7,1	7,3	5,9
Total Industrias (VAB)	**5,9**	**6,3**	**6,7**	**5,8**	**6,2**	**4,8**
DM-Otros Impuestos a los Productos	7,0	8,1	7,8	7,6	7,6	4,8

Incluye Servicios Gubernamentales y Otros Servicios
ota: - Cifras trimestrales ajustadas a las Cuentas Nacionales Anuales.
uente: Instituto Nacional de Estadística e Informática (INEI).

Figura 1.1.1 - Variación del crecimiento de la actividad empresarial por sectores. [INEI, 2013].

Las empresas se trazan objetivos de negocio según el sector laboral y elaboran estrategias o mecanismos para el cumplimiento de los mismos. Sin embargo con la

incorporación de técnicas como el balance scorecard, matriz FODA[1], se pueden elaborar planes para el cumplimiento y la medir el desempeño empresarial.

Algunas de las estrategias consisten en desarrollar, en caso no existan, procesos de negocio que estén alineados con el (los) objetivo(s) de la organización, o de lo contrario optimizar los existentes como parte de la mejora constante. Éstos pueden estar apoyados o soportados por sistemas de información y/o tecnologías de información con la finalidad de automatizarlos y junto con ello, mejorar la imagen institucional de la empresa.

En el caso particular de las empresas prestadoras de servicios de salud, éstas están sujetas a una serie de regulaciones por parte del ministerio de salud adicional a ley de protección de datos personales y tienen como necesidad brindar una mejor calidad de servicio hacia sus clientes. No obstante dicho mercado tiene actores adicionales como las empresas aseguradoras, entidades financiadoras de servicios de salud, empresas que contratan servicios complementarios y por último la misma EPS[2] que brinda atención al público en general.

Estas empresas tienen grandes planes de expansión para los próximos años debido a la demanda de la población por estos servicios [Apoyo Consultoría, 2012]. Este crecimiento estratégico se verá reflejado también a nivel de tecnología de vanguardia para realizar sus actividades (exámenes médicos, detección de enfermedades) y en tecnologías de información que formarán parte de los procesos que lleguen a optimizarse o crearse para cubrir las nuevas reglas de negocio sin dejar de lado la visión empresarial y objetivos estratégicos que persiguen dado el momento oportuno. Esto trae en consecuencia el manejo de proyectos.

Sin embargo, estos proyectos que involucran tecnologías de información, pueden presentar retrasos o problemas producto de las regulaciones no consideradas, adquisición de plataformas que no soportan procesos de negocio, entre otros, que en resumen los conllevan a ser catalogados como proyectos a pérdida, lo cual causaría también consumo de recursos[3] innecesarios.

[1] Matriz FODA: Esquema que permite identificar las Fuerzas, Oportunidades, Debilidades y Amenazas de una organización.
[2] EPS: Empresa que brinda servicios de salud a través de seguros o no. Pueden ser clínicas u hospitales
[3] Recursos: Involucra también tiempo, personal, hardware y software.

A continuación se describen algunos elementos del problema dentro de las organizaciones:

Área - Enfoque	Descripción del problema
Desempeño de las Tecnologías de Información.	• No se analizan a detalle las tecnologías de información de forma que brinden soluciones y mejoras al proceso de negocio. Se priorizan los costos de inversión o las tendencias actuales de la competencia frente a un buen desempeño de tecnología[4]. [ITGI, 2007]. • No se consideran suficientes criterios de medida de desempeño de las tecnologías para aprobar o rechazar un proyecto.
Riesgos de la organización y las tecnologías.	• En relación a la incorrecta medición del desempeño, no se realiza un análisis exhaustivo de todos los posibles riesgos y el nivel de impacto dentro de la organización. [ITGI, 2007]. • En cuanto a la empresa y la tecnología, los planes de contingencia, como parte de la gestión de continuidad de negocio, o mitigación de riesgos no son gestionados de la manera adecuada, por ello los controles implantados no garantizan la protección de activos. Esto se relaciona también con la gestión de recursos de la organización. [ITGI, 2008b].
Recursos de la organización y activos.	• El crecimiento e innovación de tecnologías de información generan tendencias de adquisición inviables debido a sus procesos de negocio. No obstante, por estimación de costos, evaluación de competencia, son incorporadas como soluciones y son gestionadas como tal, lo cual conlleva a cambiar procesos para que sean éstos los que se adapten a la tecnología. [Muñoz y Ulloa, 2011]. • Los recursos de tecnología y servicios no son debidamente monitoreados, es decir no se realiza un seguimiento que permita

[4] Entiéndase por tecnología como tecnologías de información y/o comunicación. (TIC).

	controlar el estado de los mismos y determinar la eficiencia de los activos para apoyar los procesos de la organización. [ITGI, 2008b].
Alineación con los objetivos de la organización	• La gestión inadecuada de proyectos y tecnologías de información, da como resultado que los procesos entregados, o la mejora sobre éstos, no estén alineados a los objetivos de la organización, limitando el crecimiento de la misma y generando insatisfacción de los stakeholders[5]. [ITGI, 2007].
Retorno de valor de las tecnologías de la organización.	• No otorgan el valor de retorno esperado. En otras palabras, no brindan un valor agregado al proceso que genere ganancias a nivel de productividad, debido a que dicha tecnología no es la correcta a emplear o trae consigo riesgos de alto impacto que disminuyen el valor de retorno de las mismas. Esto incluye que los stakeholders no obtienen el valor de inversión esperado. [ITGI, 2009a].

Tabla 1.1.1 - Resumen de problemática.

Para cada uno de los enfoques o áreas señaladas en el cuadro anterior, se desprenden problemas particulares propios de empresas prestadoras de salud. Por ejemplo se tienen los siguientes:

- Las tecnologías de información empleadas actualmente deben estar en capacidad de soportar la expansión departamental y local de estas empresas de forma óptima y eficaz para asegurar el retorno de valor de la inversión.
- En cuanto a los riesgos y la seguridad, se debe de tomar en cuenta todas las regulaciones a las cuales están sujetas estas empresas, tales como la norma técnica para las historias clínica y la nueva ley de protección de datos personales, pues esto obliga a que las empresas implementen mecanismos y controles que incrementen la protección de la información que se maneja de forma interna y externa.
- Se puede mencionar también el problema de comunicación y el trámite documentario a seguir para poder emplear los servicios brindados por estas empresas, como por ejemplo, realizarse algún diagnóstico, internamiento e incluso tratar las emergencias a través de algún tercero tales como empresas aseguradoras y otras instituciones asociadas.

[5] Stakeholders: Partes interesadas del negocio. Entiéndase también como inversionistas.

- Tal como se mencionó, los planes estratégicos apuntan a expandir el negocio hacia otras localidades. Actualmente, se observa que el staff médico está descontento, lo cual produce escases de este recurso primordial y debe de ser considerado y gestionado para evitar ahondar el problema actual y que en el futuro estos nuevos locales operen normalmente.

El siguiente cuadro muestra los problemas más comunes con respecto a las TI en las organizaciones. Se tiene como base países norteamericanos. Sin embargo, comparando la problemática descrita, se coincide que los problemas principales son que el retorno de inversiones no es el esperado, incidentes relacionados seguridad de las tecnologías de información, incidentes operacionales, los cuales tienen impacto en el negocio y las TI.

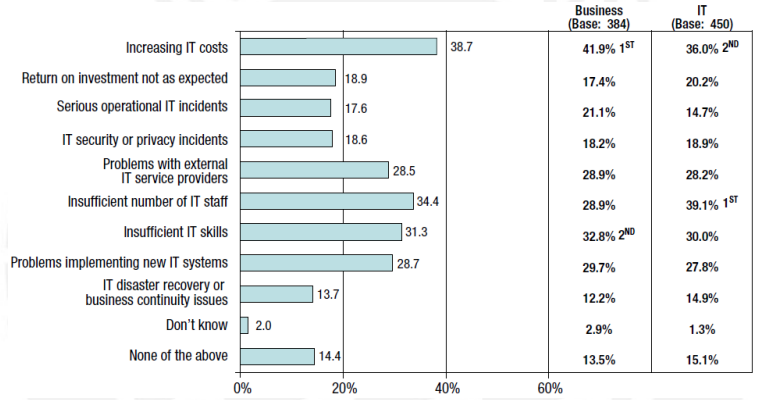


Figura 1.1.2 - Encuesta: Problemas principales con las TI. [ITGI, 2011].

La problemática descrita, que abarca diversos puntos dentro de las organizaciones y relacionada con las tecnologías de información y objetivos estratégicos trazados, da lugar a un tema que en el Perú no ha tenido mayor repercusión, pero que en otros países como Canadá y Reino Unido es una buena práctica para lograr los objetivos de negocio. Esto es el Gobierno de Tecnologías de Información.

El Gobierno de TI[6] pretende gobernar y/o gestionar las tecnologías de información para que puedan alinearse a los objetivos de negocio y que retornen el valor esperado, es decir, sacar el máximo provecho de las TI para beneficio de la organización y los Stakeholders. Se basa en cinco pilares [ITGI, 2003]: Administración de riesgos, Medición de desempeño, Administración de recursos, Entrega de valor y Alineamiento estratégico.

[6] TI: Abreviatura para referirnos a las tecnologías de información.

La organización mundialmente reconocida y que conduce la investigación sobre las prácticas y percepciones de gobierno de TI para las empresas es el *Information Technology Governance Institute* conocido por sus siglas ITGI, establecido en el año 1998 tras la importancia de las tecnologías de información para el éxito de las empresas y que se convirtieron en el camino para lograr los objetivos de negocio.

Todos los años, está organización junto con ISACA -*Information Systems Audit and Control Association*- elabora un reporte mundial sobre el estado del gobierno de TI y las empresas que lo han implantado, permitiendo aclarar el panorama actual de la problemática y las tácticas que siguen las empresas para implantar el gobierno.

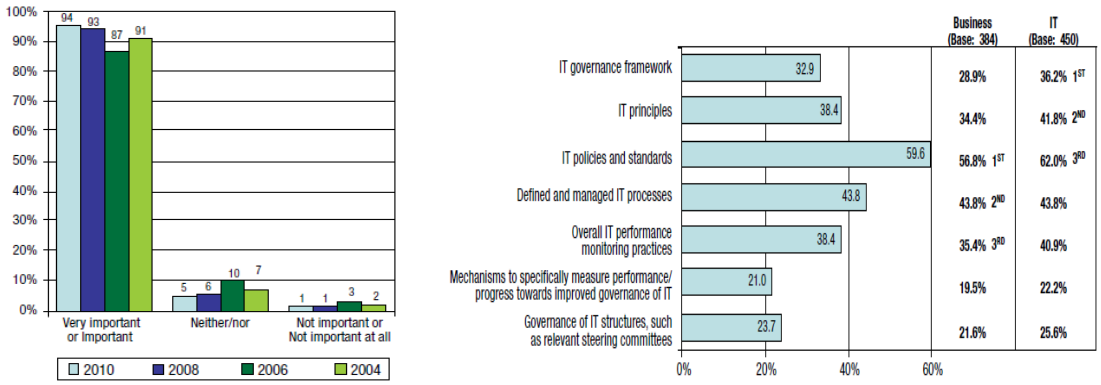


Figura 1.1.3 - Importancia del uso de las tecnologías para aplicar estrategias de la empresa. Prácticas comunes para implantación de Gobierno de TI. [ITGI, 2011].

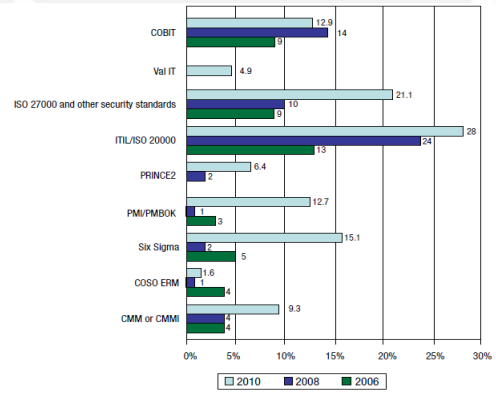


Figura 1.1.4 – Marcos de trabajo comúnmente utilizados para la implantación de gobierno de TI. [ITGI, 2011].

La información mostrada en los cuadros estadísticos se resume en que las empresas consideran cada vez más importante contar con un gobierno de TI y para su implantación hace uso de marcos de trabajo entre los cuales destacan ITIL 2011[7], ISO

[7] ITIL 2011: Última versión actualizada del libro de buenas prácticas.

20000, ISO 27000 y COBIT. Pese a que la estadística no la muestre, la norma ISO 38500 también brinda los estándares y políticas para dicha implantación.

Cada uno de estos marcos de trabajo, para implantar gobierno de tecnologías de información, tiene enfoques distintos pero también comunes entre sí, por lo cual no puede descartarse el uso de uno o más de éstos en el proceso de implantación. Cuentan con versiones diferentes que se adaptan a las necesidades y amenazas actualmente existentes, pues el gobierno de TI abarca diversas áreas que van transformándose y pueden llegar a tomar mayor fuerza a nivel empresarial. Como ejemplo se tiene el área de seguridad de información, la cual en nuestro país ha tomado gran importancia y existen normas que apoyan a un correcto funcionamiento de ésta.

Por todas las razones mencionadas anteriormente y la importancia del cumplimiento de los objetivos de negocio, se propone como solución a la problemática planteada, diseñar un modelo de gobierno de TI en las empresas prestadoras de servicios de salud, de manera que se pueda cumplir con la regulación y alinear los objetivos organizacionales y objetivos de TI, gestionando tecnologías existentes y emergentes y garantizar que éstas contribuyan a lograr sus metas trazadas.
Esto implica que las TI retornen el valor esperado y que estén alineadas a los objetivos de negocio. No obstante, este modelo planteado brinda solución a la problemática con respecto a la gestión de los riesgos de la organización, gestión de recursos y desempeño de las tecnologías de información.

Debido a los enfoques que pretende solucionar el gobierno de TI, se ve necesario el uso de un marco de control para seguir un estándar que brinde las pautas para un diseño de gobierno de TI que pueda ser controlado a mediano y largo plazo. En este caso se toma como referencia el marco de negocio COBIT 5.0, pues integra soluciones y buenas prácticas para ser aplicadas a diversos procesos incluso contemplados en otros marcos y propone mejorar su versión anterior COBIT 4.1 la cual ha traído buenas críticas y grandes resultados en otros países.

Esta última versión lleva aproximadamente un año de publicación y aún no se tienen referencias exactas de implantaciones de gobierno de TI haciendo uso de la última versión de COBIT, por lo cual resulta novedoso e interesante, por las mejoras que ofrece esta nueva versión, su aplicación al contexto ya presentado.

1.2 Objetivo general

Diseñar un modelo de gobierno de tecnologías de información, bajo la óptica del marco de negocios COBIT 5.0 para empresas prestadoras de servicios de salud.

1.3 Objetivos específicos

- **OBJ 1**: Elaborar el Caso de negocio que justifique la implementación del Gobierno de TI en la organización.
- **OBJ 2**: Mapear las fases del ciclo de vida del Gobierno de TI según COBIT 5.0 para la empresa.
- **OBJ 3**: Elaborar el balance scorecard de TI de la empresa que refleje las necesidades y expectativas de los stakeholders.
- **OBJ 4**: Elaborar a declaración de aplicabilidad de COBIT 5.0 para el enfoque de Seguridad de Información dentro de la empresa
- **OBJ 5**: Modelar los procesos de negocio "AS - IS"[8].
- **OBJ 6**: Elaborar las políticas de gobierno de TI a aplicarse dentro de la empresa, "TO-BE"[9].
- **OBJ 7**: Evaluar el estado de los procesos habilitadores, correspondientes a los enfoques de gobierno de TI que aplican en la empresa, su evolución y nivel de madurez.

1.4 Resultados esperados

- **Resultado 1 para el OBJ 1**: Documento que contenga el Business Case que justifica la implementación del Gobierno de TI
- **Resultado 2 para el OBJ 2**: Documento que contenga el resultado del mapeo de las fases del ciclo de vida de gobierno de TI para la empresa.
- **Resultado 3 para el OBJ 3**: Documento que contenga los resultados del balance scorecard de TI de la empresa.

[8] AS-IS: Dentro de este entorno se refiere a modelar los procesos tal como están en la organización.
[9] TO-BE: En relación al tema, se refiere a cómo serán los procesos aplicando el marco de negocio.

- **Resultado 4 para el OBJ 4**: Documento que contenga la matriz de aplicabilidad de procesos habilitadores según COBIT 5.0 en la empresa tomando en cuenta el enfoque de seguridad de información.
- **Resultado 5 para el OBJ 5**: Documento que contenga el modelamiento de los procesos AS-IS de la empresa.
- **Resultado 6 para el OBJ 6**: Documento que contenga las políticas de gobierno de TI aplicadas a la empresa. Incluye matriz de responsabilidades (RACI).
- **Resultado 7 para el OBJ 7**: Documento que contenga el estado de los procesos habilitadores y el respectivo nivel de madurez.

1.5 Métodos, metodologías y procedimientos

1.5.1 Mecanismos para desarrollar los resultados esperados.

A continuación se detallará los métodos y procedimientos optados para la elaboración de los resultados esperados.

- **Metodología 1 para el Resultado esperado 1**

  Un business case es una presentación o una propuesta a una autoridad de una organización que busca financiación, aprobación, o ambos, de la actividad, iniciativa o proyecto. Pone una decisión de inversión propuesta en un contexto estratégico y proporciona la información necesaria para tomar una decisión informada sobre si se debe proceder con la inversión y en qué forma. [Treasury Board of Canada Secretariat, 2009].

  La importancia del business case en el proceso de toma de decisiones continúa durante el ciclo de vida de una inversión. Se utiliza para revisar y revalidar la inversión en cada proyecto programado y cuando se produzca un cambio significativo en el contexto, un proyecto o función de negocios. [Treasury Board of Canada Secretariat, 2009].

  La guía del business case y la plantilla se han desarrollado para alinearse con una variedad de instrumentos y políticas clave. El modelo de business case propuesto en la guía del Treasury Board of Canada Secretariat divide el desarrollo del

business case en tres fases y los pasos claves que colectivamente forman un business case sólido. Estos son [Treasury Board of Canada Secretariat, 2009]:

- Fase 1: Contexto estratégico.
- Fase 2: Análisis y recomendaciones.
- Fase 3: Gestión y capacitación.
- Paso 1: Necesidades del negocio y resultados esperados.
- Paso 2: Análisis de opciones preliminares.
- Paso 3: Opciones viables.
- Paso 4: Justificación y recomendaciones.
- Paso 5: Gestión de la inversión.

Retomando los resultados esperados, para la materialización de este documento, se empleará la **Guía del Business Case**, la cual contiene las actividades para su elaboración. Esta guía presenta un mapeo claro y conciso para las fases de desarrollo y los pasos a seguir para el desarrollo de un business case. Además brinda un enfoque financiero importante para la aceptación del proyecto.

- **Metodología 2 para Resultado esperado 2, 4, 6 y 7**

Para el conjunto de resultados esperados listados se materializaran empleando el **marco de control COBIT 5.0** propuesto para la solución a la problemática. Será utilizado porque este marco involucra una serie políticas y pautas para mapear las fases de gobierno de TI en las empresas. El mapeo de fases del ciclo de vida de gobierno de TI, el cual se desarrolla junto con los stakeholders, es el punto de partida para fijar el alcance por medio de los enfoques seleccionados, los cuales se convierten en los “drivers” para las siguientes etapas dentro del proyecto.

También, según la aplicabilidad definida, COBIT permite identificar los procesos habilitadores para lograr un gobierno de TI y las actividades y políticas a ser aplicadas para la mejora de los procesos involucrados junto con la matriz de responsabilidades respectiva. En este caso se emplea la matriz RACI. Además, COBIT 5.0 basándose en la ISO 15504 permite evaluar el estado de sus procesos y determinar su nivel de madurez.

En el marco conceptual se describe detalladamente este marco de control y se brinda la información necesaria que justifica su elección.

- **Metodología 3 para Resultado Esperado 3**

  Para la materialización de este resultado esperado se tomará en cuenta información y **publicaciones que describan al balance scorecard de** TI y las técnicas para la elaboración. En el marco conceptual se hace referencia a esta teoría. No obstante, se emplea la **cascada de objetivos** propuesta en COBIT 5.0 y descrita en el marco conceptual.

- **Metodología 4 para Resultado Esperado 5**

  Para el modelamiento de procesos se utilizará **Business Process Model and Notation (BPMN 2.0).**

  BPMN es un estándar diseñado por el Object Management Group para normalizar la notación gráfica en el modelado de procesos. El objetivo principal es ser un estándar que permita la rápida elaboración e interpretación de diagramas de procesos de negocio. La versión actual es la 2.0 que fue publicada en el año 2011. [OMG, 2011].

  Este modelo está basado en el Unified Modeling Language (UML) y está orientado a ser compatible con XML. Los elementos básicos de BPMN son [OMG, 2011]:

  - **Flow Objects**: Definen el comportamiento del flujo del diagrama. Pueden ser eventos o actividades.
  - **Data**: Representan a los datos de los procesos, tales como los de entrada como los de salida.
  - **Connecting Objects**: Representan asociaciones entre objetos, secuencias, mensajes, relaciones, etc.
  - **Swimlanes**: Representan un sector del flujo.
  - **Artifacts**: Son grupos o anotaciones en el diagrama.

  La razón por la cual se emplea esta notación es porque, además de ser un estándar reconocido y, según su descripción, de rápida elaboración, presentan compatibilidad entre otros diagramas y elementos. No obstante al ser basado en UML, notación comúnmente usada, su lenguaje y elementos resultan familiares.

1.6 Alcance y limitaciones

1.6.1 Alcance

Como parte del alcance se toma en cuenta los siguientes puntos:

- Para el desarrollo del proyecto, se tomará en cuenta “un enfoque” para diseñar el gobierno de Tecnologías de Información, el cual es definido según los intereses de los stakeholders, en este caso son quienes brindan la información de la empresa prestadora de servicios de salud y señalan cuáles son sus objetivos y necesidades. Aunque dentro de una empresa pueden aplicarse más enfoques, por las limitaciones de tiempo, no es viable que puedan aplicarse y modelarse los procesos de todas las áreas y realizar la evaluación respectiva. El enfoque a tomarse en cuenta para este proyecto es el de **seguridad de información**.

- El proyecto está orientado a empresas prestadoras de servicios de salud. Si bien el marco de gobierno de TI puede aplicarse a todo tipo de empresa, por cuestiones de tiempo para la ejecución del proyecto, por fines académicos no se puede abarcar todos éstos rubros y realizar el análisis para cada uno de ellos.

- Se utilizará el marco de control COBIT 5.0. Algunas empresas cuentan con otros marcos de control que puedan contribuir a la solución, esta solo comprenderá los procesos y políticas de esta nueva versión de COBIT.

1.6.2 Limitaciones

- **Acceso a la información.**
  La principal limitación es el acceso a la información. Según las políticas de la empresa, la información brindada podría resultar insuficiente para el proyecto, o de lo contrario simplemente no se podría tener acceso a ella y en consecuencia no se podría realizar el modelamiento de los procesos involucrados.

- **Poco conocimiento del tema por parte de la empresa.**
  Para la ejecución de este proyecto es necesaria la comunicación con la empresa que apoyará a la definición de los enfoques a ser aplicados. Una limitación puede ser el poco conocimiento de este tema, pues tal como se muestra en la

problemática, en nuestro país no hay evidencia de implantaciones exitosas de un gobierno de TI y para superar los problemas existentes se apoyan de otros recursos distintos al presentado en la solución, lo cual podría dificultar la comunicación y comprensión de los fines de este proyecto, afectando también la etapa de definición de las áreas de enfoque de interés.

- **Evolución de los marcos de trabajo.**
  Aunque COBIT 5.0 es un marco recientemente publicado por ISACA, no se descarta que más adelante durante la ejecución del proyecto se realicen cambios o publicaciones de fe de erratas o documentos complementarios. Así mismo, se debe tomar en cuenta el cambio en las regulaciones o nuevas normas que complementen el marco regulatorio a cumplir.

- **Tiempo de vida del proyecto.**
  El presente proyecto de fin de carrera tiene un tiempo límite como todo proyecto. No obstante, los proyectos relacionados con Gobierno de TI, tienen una duración alrededor de 1 o 2 años en la cual participa toda la organización de TI según sus roles. Sin embargo, para este proyecto se cuenta con un promedio de cuatro (4) meses para lograr todos los objetivos y resultados esperados teniendo como recurso el trabajo de campo realizado con la empresa, simulando un servicio de consultoría.

1.6.3 Riesgos

Durante el proyecto de tesis pueden presentarse riesgos que manifiesten o evidencien las limitaciones descritas, a continuación se presentan algunos posibles riesgos, su impacto y las medidas correctivas en caso su materialización.

ID	Riesgo	Impacto	Medidas correctivas de mitigación
R01	La empresa decide no brindar la información necesaria.	EXTREMO	Cambiar de empresa y realizar los cambios necesarios en el documento en caso se seleccione otro enfoque o se tenga que cambiar el rubro de la empresa.
R02	Pérdida de información	MEDIO	En caso de pérdida de información de la empresa, volver a realizar el levantamiento

			de información y documentarlo realizando el backup respectivo.
			En caso de pérdida de documentos del proyecto reconstruir la información perdida a partir de los avances entregados al asesor en forma digital.
			Ajustar los plazos de entrega realizando tareas paralelas.
R03	Información otorgada inconsistente o incompleta.	MEDIO	Realizar el trabajo de campo para poder completar la información faltante.
			Realizar trabajo de campo y reuniones para la validación de la información entregada.
R04	Disminución de plazos de entrega.	MEDIO	Modificar el cronograma considerando que tareas pueden realizarse en paralelo respetando la ruta crítica del proyecto.
R05	Enfermedad.	BAJO	Realizar los ajustes en el cronograma para ampliar los plazos dependiendo si existe de por medio el descanso médico.
R06	Cambios en los frameworks y/o herramientas empleadas.	ALTO	Realizar los cambios dentro del documento adecuando los cambios realizados en las herramientas.
			Realizar nuevamente la capacitación y entrenamiento en dichas herramientas.
			Ajustar el cronograma del proyecto.
R07	Falta de comunicación con el asesor.	ALTO	Comunicar al coordinador del curso sobre esta incidencia para tomar las acciones correctivas alterando lo menos posible el cronograma. Según
R08	Retiro del asesor de la universidad.	ALTO	Cambiar de asesor notificándole al profesor y coordinador del curso.
			En caso se dé esta situación durante la ejecución del proyecto coordinar con el profesor del curso para la ampliación del cronograma

			Realizar los cambios sugeridos por el nuevo asesor.
R09	Poca experiencia en el tema de tesis y en las herramientas empleadas	ALTO	Capacitación constante en las herramientas empleadas. Asistir a charlas informativas, como también optar por mayor documentación bibliográfica sobre estos temas.

Tabla 1.6.1 - Identificación de riesgos del proyecto

1.7 Viabilidad y Justificativa

Haciendo una breve revisión del contexto del proyecto, las empresas prestadoras de servicios de salud elaboran planes estratégicos para tratar de alcanzar sus objetivos de negocio. No obstante no siempre están alineados con los planes estratégicos de TI y la infraestructura existente, además de considerar las regulaciones que los obliga a proteger información personal y garantizar la calidad de sus servicios.

Para lograr estos objetivos, tal como se menciona en la problemática se debe garantizar la existencia del alineamiento estratégico entre objetivos de negocio y las tecnologías de información asegurando también el retorno de valor de las inversiones de TI realizadas en conjunto con los proyectos. Así mismo, gestionar los riesgos, los recursos tecnológicos y medir el desempeño de las Tecnologías asegurarán que se cumpla un ciclo que permita entregar a los stakeholders y a la organización una mejora dentro de los procesos para alcanzar sus objetivos de la mano de la dirección estratégica de TI.

Dado a que se requiere una solución que entregue mejoras dentro de un espacio de tiempo continuo, se recomienda que las empresas prestadoras de servicio de salud opten por un Gobierno de Tecnologías de Información, pues este permite que se pueda dimensionar un problema existente y particular de una empresa y sustentando por medio de un caso de negocio, el alcance para la empresa según sus recursos, el cual puede ir incrementándose a medida el gobierno tome mayor madurez. COBIT 5.0 permite acotar este alcance por medio de procesos habilitadores que aplican de acuerdo al enfoque seleccionado, garantizando siempre alineamiento estratégico y teniendo como meta alcanzar los objetivos de negocio.

A partir de COBIT 5.0, se podrá tener un enfoque general de todos los aspectos relacionados a la empresa, lo cual a futuro, resultaría conveniente, pues progresivamente podría aplicarse esta solución a más enfoques y procesos, lo cual dependerá también de la adaptación del cambio dentro de tal organización. Por último a lo largo de la implementación de este sistema de gobierno bajo ciertos lineamientos de COBIT se podrá evaluar el nivel de madurez de los procesos como parte de la mejora continua y ciclo de vida de gobierno.

El sector empresarial seleccionado para ese proyecto se justifica porque tal como se señala posteriormente en el estado del arte existen casos de éxito empleando COBIT 4.1 y es una oportunidad de mejora bajo las regulaciones recientes en nuestro país. No obstante, se comprometerá a la alta dirección para velar de forma transversal por el desempeño organizacional en conjunto.

En cuanto a la viabilidad del proyecto, se verifica que existe la disponibilidad de elementos técnicos, entiéndase por esto, información referente al tema y a la solución. Así mismo, por el lado del aspecto económico es viable, pues se tiene acceso al marco de gobierno a utilizar, y en caso se requiera adquirir alguna licencia adicional para algún otro documento el costo sigue siendo viable y no exceden los límites esperados.

Finalmente, respecto a la viabilidad temporal, tal como se indica en el alcance y las limitaciones del proyecto, se limita una solución para empresas prestadoras de servicios de salud tomando en cuenta dos enfoques de gobierno de TI, seguridad de información y gestión de operaciones de TI. Además, considerando que los métodos y procedimientos utilizados consisten en su mayoría la aplicación del marco COBIT 5.0, es posible culminar el proyecto en el tiempo esperado. No obstante, se toma en cuenta la gestión de cambios en caso el proyecto se llegue a implementar, debido a la resistencia al cambio, o sufra alguna modificación del contexto.

1.8 Plan de actividades

A continuación se detalla las actividades relacionadas al proyecto dentro del cual se realiza la planificación, ejecución y cierre del proyecto incluyendo el control, dentro del cual se realizan los ajustes para la entrega del producto final.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	DISEÑO DE UN MODELO DE GOBIERNO DE TI BAJO LA ÓPTICA DE COBIT 5.0 PARA EMPRESAS PRESTADORAS DE SERVICIOS DE SALUD	364 días?	lun 20/08/12	sáb 30/11/13
2	1. Inicio	7 días	lun 20/08/12	lun 27/08/12
3	Definición del área del proyecto.	2 días	lun 20/08/12	mar 21/08/12
4	Definición del tema	2 días	mié 22/08/12	jue 23/08/12
5	Elaboración del primer entregable: Elección y justificación del tema y área	3 días	vie 24/08/12	dom 26/08/12
6	Entregable 1	0 días	lun 27/08/12	lun 27/08/12
7	2. Planificacion	92 días?	lun 27/08/12	lun 26/11/12
8	Levantamiento bibliográfico	75 días	lun 27/08/12	vie 09/11/12
9	Revisión bibliográfica	42 días	lun 27/08/12	dom 07/10/12
10	Fichamiento	84 días	lun 27/08/12	dom 18/11/12
11	Elaboración del Segundo entregable: Problemática, Marco Conceptual y Estado del Arte.	21 días?	lun 03/09/12	lun 24/09/12
12	Elaboración del borrador previo	18 días?	lun 03/09/12	jue 20/09/12
13	Entrega del entregable 2 previo	0 días	jue 20/09/12	jue 20/09/12
14	Levantamiento de correcciones del asesor	3 días	vie 21/09/12	dom 23/09/12
15	Entregable 2 Completo	0 días	lun 24/09/12	lun 24/09/12
16	Elaborar Tercer entregable: Objetivo General	7 días	lun 24/09/12	lun 01/10/12
17	Elaboración del borrador previo	4 días	lun 24/09/12	jue 27/09/12
18	Entrega del entregable 3 previo	0 días	jue 27/09/12	jue 27/09/12
19	Levantamiento de correcciones del asesor y profesores del curso.	3 días	vie 28/09/12	dom 30/09/12
20	Entregable 3 Completo	0 días	lun 01/10/12	lun 01/10/12
21	Elaborar Cuarto entregable: Objetivos específicos	7 días	lun 01/10/12	lun 08/10/12
22	Elaboración del borrador previo	4 días	lun 01/10/12	jue 04/10/12
23	Entrega del entregable 4 previo	0 días	jue 04/10/12	jue 04/10/12
24	Levantamiento de correcciones del asesor y profesores del curso.	3 días	vie 05/10/12	dom 07/10/12
25	Entregable 4 Completo	0 días	lun 08/10/12	lun 08/10/12
26	Elaborar Quinto entregable: Resultados esperados.	9 días	sáb 20/10/12	lun 29/10/12
27	Elaboración del borrador previo	6 días	sáb 20/10/12	jue 25/10/12
28	Entrega del entregable 5 previo	0 días	jue 25/10/12	jue 25/10/12
29	Levantamiento de correcciones del asesor y profesores del curso.	3 días	vie 26/10/12	dom 28/10/12
30	Entregable 5 Completo	0 días	lun 29/10/12	lun 29/10/12
31	Elaborar Sexto entregable: Correcciones de entregable 2, 3, 4, 5	7 días	lun 29/10/12	lun 05/11/12
32	Elaboración del borrador previo	4 días	lun 29/10/12	jue 01/11/12
33	Entrega del entregable 6 previo	0 días	jue 01/11/12	jue 01/11/12
34	Levantamiento de correcciones del asesor y profesores del curso.	3 días	vie 02/11/12	dom 04/11/12
35	Entregable 6 Completo	0 días	lun 05/11/12	lun 05/11/12
36	Elaborar Séptimo entregable: Métodos y procedimientos. Alcances y Limitaciones.	7 días	lun 05/11/12	lun 12/11/12
37	Elaboración del borrador previo	4 días	lun 05/11/12	jue 08/11/12
38	Entrega del entregable 7 previo	0 días	jue 08/11/12	jue 08/11/12
39	Levantamiento de correcciones del asesor y profesores del curso.	3 días	vie 09/11/12	dom 11/11/12
40	Entregable 7 Completo	0 días	lun 12/11/12	lun 12/11/12
41	Elaborar Entregable final: Capítulo 1 y planificación	15 días	lun 12/11/12	lun 26/11/12
42	Elaboración del borrador previo	8 días	lun 12/11/12	lun 19/11/12
43	Entrega del entregable 8 previo	0 días	lun 19/11/12	lun 19/11/12
44	Levantamiento de correcciones del asesor y profesores del curso.	3 días	mar 20/11/12	jue 22/11/12
45	Entregable 8 Completo	0 días	lun 26/11/12	lun 26/11/12
46	Sustentación Parcial	1 día	lun 26/11/12	lun 26/11/12
47	3. Ejecucion (Proyecto Tesis 2)	101 días?	lun 12/08/13	mié 20/11/13
48	E1 - Verificar la documentación de la tesis y revisar nuevas referencias o actualizaciones	10 días?	lun 12/08/13	mié 21/08/13
49	E1 - Elaborar el entregable 1 para tesis 2: Correcciones capítulo 1. Revisión del nuevo contexto por cambio de empresa	9 días	lun 12/08/13	mar 20/08/13
50	E1 - Modificar el documento según las correcciones u observaciones del asesor.	1 día?	mié 21/08/13	mié 21/08/13
51	Entregable 1 - Revisado y firmado. Semana 1	0 días	mié 21/08/13	mié 21/08/13
52	E2- Elaborar el segundo entregable correspondiente al capítulo 2	7 días	jue 22/08/13	mié 28/08/13
53	E2- Elaborar el segundo entregable preliminar	2 días	jue 22/08/13	vie 23/08/13
54	E2 - Modificar el documento según las correcciones u observaciones del asesor	5 días	sáb 24/08/13	mié 28/08/13
55	Entregable 2 - Revisado y firmado. Semana 2	0 días	mié 28/08/13	mié 28/08/13
56	OBJ-E1: Elaborar el Business Case de la empresa	13 días	jue 22/08/13	mié 04/09/13
57	Elaborar el documento que corresponde al resultado esperado 1.	5 días	jue 22/08/13	lun 26/08/13
58	Entrega de borrador previo	0 días	lun 26/08/13	lun 26/08/13
59	Levantamiento de correcciones	5 días	mar 27/08/13	sáb 31/08/13
60	Entrega del documento que corresponde al resultado esperado 1 - Revisado y Firmado. Semana 3	0 días	mié 04/09/13	mié 04/09/13

Figura 1.8.1 - Actividades programadas para el desarrollo del proyecto (1)

Id	Nombre de tarea	Duración	Comienzo	Fin
61	**OBJ-E2: Mapear las fases el ciclo de vida del gobierno de TI.**	**80 días**	**vie 23/08/13**	**dom 10/11/13**
62	Mapeo de fases - fase 1 - 4	8 días	vie 23/08/13	vie 30/08/13
63	Entrega de borrador previo	0 días	vie 30/08/13	vie 30/08/13
64	Levantamiento de correcciones	5 días	sáb 31/08/13	mié 04/09/13
65	Entrega del documento que corresponde al resultado esperado 2 parte 1- Revisado y firmado. Semana 3	0 días	mié 04/09/13	mié 04/09/13
66	Mapeo de fases - Fase 5	8 días	vie 13/09/13	vie 20/09/13
67	Entrega de borrador previo	0 días	vie 20/09/13	vie 20/09/13
68	Levantamiento de correcciones	5 días	sáb 21/09/13	mié 25/09/13
69	Entrega del documento que corresponde al resultado esperado 2 parte 2- Revisado y firmado. Semana 6	0 días	mié 25/09/13	mié 25/09/13
70	Mapeo de fases - Fase 6 y 7	8 días	vie 01/11/13	vie 08/11/13
71	Entrega de borrador previo	0 días	vie 08/11/13	vie 08/11/13
72	Levantamiento de correcciones	2 días	sáb 09/11/13	dom 10/11/13
73	**E4 - Elaborar el documento que contenga las correciones anteriores. (Capítulos: 1, 2 , 3, 4)**	**12 días**	**sáb 31/08/13**	**mié 11/09/13**
74	E4- Elaborar el documento preliminar	7 días	sáb 31/08/13	vie 06/09/13
75	Entrega de borrador previo	0 días	vie 06/09/13	vie 06/09/13
76	Realizar el levantamiento de correcciones	5 días	sáb 07/09/13	mié 11/09/13
77	Entregable 4 - Revisado y firmado. Semana 4	0 días	mié 11/09/13	mié 11/09/13
78	**OBJ-E3: Elaborar el balance scorecard de TI de la empresa**	**20 días**	**vie 30/08/13**	**mié 18/09/13**
79	Elaborar el documento que corresponde al resultado esperado 3.	15 días	vie 30/08/13	vie 13/09/13
80	Entrega de borrador previo	0 días	vie 13/09/13	vie 13/09/13
81	Levantamiento de correcciones	5 días	sáb 14/09/13	mié 18/09/13
82	Entrega del documento que corresponde al resultado esperado 3. Semana 5	0 días	mié 18/09/13	mié 18/09/13
83	**OBJ-E4: Elaborar la declaración de aplicabilidad de cobit 5.0 según los enfoques que aplican en la empresa.**	**14 días**	**jue 12/09/13**	**mié 25/09/13**
84	Elaborar el documento que corresponde al resultado esperado 4.	9 días	jue 12/09/13	vie 20/09/13
85	Entrega de borrador previo	0 días	vie 20/09/13	vie 20/09/13
86	Levantamiento de correcciones	5 días	sáb 21/09/13	mié 25/09/13
87	Entrega del documento que corresponde al resultado esperado 4. Semana 6	0 días	mié 25/09/13	mié 25/09/13
88	**OBJ-E5: Modelar los procesos de negocio.**	**21 días**	**jue 26/09/13**	**mié 16/10/13**
89	Elaborar el documento que corresponde al resultado esperado 5. Parte 1	12 días	jue 26/09/13	lun 07/10/13
90	Entrega avance 1. Semana 8	0 días	lun 07/10/13	lun 07/10/13
91	Elaborar el documento que corresponde al resultado esperado 5. Parte 2	4 días	mar 08/10/13	vie 11/10/13
92	Entrega avance 2	0 días	vie 11/10/13	vie 11/10/13
93	Levantamiento de correcciones	5 días	sáb 12/10/13	mié 16/10/13
94	Entrega del documento que corresponde al resultado esperado 5. Semana 10 - EXPOSICIÓN PARCIAL	0 días	mié 16/10/13	mié 16/10/13
95	Exposición - Sustentación parcial	1 día?	lun 28/10/13	lun 28/10/13
96	**OBJ-E6: Elaborar políticas de gobierno de TI dentro de la empresa. TO-BE**	**32 días**	**mar 08/10/13**	**vie 08/11/13**
97	Elaborar el documento que corresponde al resultado esperado 6.	27 días	mar 08/10/13	dom 03/11/13
98	Entrega de borrador previo	0 días	dom 03/11/13	dom 03/11/13
99	Levantamiento de correcciones	5 días	lun 04/11/13	vie 08/11/13
100	Entrega de políticas validadas y alineadas a norma ISO	0 días	mié 06/11/13	mié 06/11/13
101	**OBJ-E7: Evaluar el estado de los procesos habilitadores correspondientes a los enfoques de gobierno de TI.**	**24 días**	**mié 16/10/13**	**vie 08/11/13**
102	Elaborar el documento que corresponde al resultado esperado 7.	19 días	mié 16/10/13	dom 03/11/13
103	Entrega de borrador previo	0 días	dom 03/11/13	dom 03/11/13
104	Levantamiento de correcciones y completar evaluación de la empresa	5 días	lun 04/11/13	vie 08/11/13
105	Entrega del documento que corresponde al resultado esperado 7	0 días	vie 08/11/13	vie 08/11/13
106	**Elaboración de correcciones Finales**	**17 días**	**lun 04/11/13**	**mié 20/11/13**
107	Revisión y Levantamiento de correcciones	7 días	lun 04/11/13	dom 10/11/13
108	Entrega Documento de Tesis completo . Semana 12	0 días	lun 11/11/13	lun 11/11/13
109	Revisión y Levantamiento de correcciones	10 días	lun 11/11/13	mié 20/11/13
110	Documento de proyecto de tesis corregido. Semana 13	0 días	mié 20/11/13	mié 20/11/13
111	**4. Control**	**325 días**	**lun 03/09/12**	**mar 05/11/13**
112	**Reuniones de asesoría tesis 1**	**77 días**	**lun 03/09/12**	**dom 18/11/12**
121	**Reuniones de asesoría tesis 2**	**70 días**	**mié 28/08/13**	**mar 05/11/13**
122	Reunión de asesoría Tesis 2 - 1	1 hora	mié 28/08/13	mié 28/08/13
123	Reunión de asesoría Tesis 2 - 2	1 hora	mié 04/09/13	mié 04/09/13
124	Reunión de asesoría Tesis 2 - 3	1 hora	mié 11/09/13	mié 11/09/13
125	Reunión de asesoría Tesis 2 - 4	1 hora	mié 18/09/13	mié 18/09/13
126	Reunión de asesoría Tesis 2 - 5	1 hora	mié 25/09/13	mié 25/09/13
127	Reunión de asesoría Tesis 2 - 6	1 hora	mié 02/10/13	mié 02/10/13
128	Reunión de asesoría Tesis 2 - 7	1 hora	mié 09/10/13	mié 09/10/13
129	Reunión de asesoría Tesis 2 - 8	1 hora	mié 23/10/13	mié 23/10/13
130	Reunión de asesoría Tesis 2 - 9	1 hora	mié 30/10/13	mié 30/10/13
131	Reunión de asesoría Tesis 2 - 10	1 hora	mié 06/11/13	mié 06/11/13
132	**5. Cierre**	**1 día?**	**sáb 30/11/13**	**sáb 30/11/13**
133	Sustentación Final	1 día?	sáb 30/11/13	sáb 30/11/13
134	Documento de proyecto de tesis completo y Modelo de Gobierno de TI	0 días	mié 20/11/13	mié 20/11/13

Figura 1.8.2 - Actividades programadas para el desarrollo del proyecto (2)

Capítulo 2. Marco Teórico y Revisión de estado del arte.

En el presente capítulo, definen conceptos básicos que forman parte de la solución propuesta para la problemática y también sobre términos relacionados y de negocio que se toman en cuenta al hablar de gobierno de TI, así como el marco legal a considerar dentro del contexto. Por último, se describe el estado del arte y se concluye a partir de este la viabilidad y oportunidad de la solución.

2.1 Marco teórico

2.1.1 Conceptos relacionados al problema

Se definen los siguientes conceptos como parte del problema y solución.

- **CIO (*Chief Information office)*:**
  Es el Director General de las Tecnologías de Información cuya responsabilidad, junto con el CEO, es el monitoreo de las actividades relacionadas a los proyectos de TI y la concordancia con las necesidades de negocio con la finalidad de verificar su utilidad y aporte a los objetivos de negocio. [Tupia, 2011].

  "Debe tener un conocimiento profundo de la organización, ser más un líder que un especialista en tecnología y tener la competencia de estructurar las TI para que puedan alcanzar sus objetivos estratégicos". [Fernández y Llorens, 2010].

- **CEO (*Chief Executive Office)*:**
  "Es la máxima autoridad en temas de gestión y dirección administrativa en una organización o institución y por ende, el gobierno y la dirección de las tecnologías de información que impulsen los objetivos de negocio caen dentro de su responsabilidad." [Tupia, 2011].
- **Riesgo:**
  Combinación de la probabilidad de un evento con su consecuencia. Entiéndase por consecuencia el impacto dentro de la organización que puede ser negativo o una oportunidad según el punto de vista. [ISO/IEC Guide 73. Citado por ISO/IEC 38500].

2.1.2 Conceptos directamente relacionados

2.1.2.1 Gobierno Corporativo

Hablar acerca de Gobierno de TI invita a discutir conceptos relacionados sobre gobierno corporativo debido a que existe una confusión respecto a ambos tema. Por esta razón se toma como referencia algunas definiciones:

Se define gobierno como la responsabilidad de la alta dirección y está centrado a la creación de mecanismos que utiliza una organización para asegurar que el personal siga los procesos y políticas establecidas. Entonces, Gobierno corporativo es un conjunto de responsabilidades y practicas ejercidas por la junta y dirección ejecutiva con el objetivo de proporcionar dirección estratégica, asegurar que se logren los objetivos, determinar que los riesgos se gestionan adecuadamente y verificar que los recursos de la empresa sean utilizados con responsabilidad. [ISACA, 2012d].

No obstante, desde otra perspectiva se define como un comportamiento ético por parte de los directores u otros encargados del gobierno corporativo en la creación y presentación del valor para los stakeholders. [ISACA, 2009a].

Gobierno Corporativo es el sistema por el cual las sociedades son dirigidas y controladas. La estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la sociedad, tales como el directorio, los gerentes, los accionistas y otros agentes económicos que mantengan interés en la empresa. [ODCE, 2004. Citado por Muñoz y Ulloa, 2011].

Gobierno corporativo es un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva y gerencia ejecutiva teniendo como objetivos [Carrillo, 2009. Citado por Fernández y Llorens, 2010]:

- Proveer dirección estratégica.
- Asegurar el logro de los objetivos.
- Establecer que los riesgos se administran adecuadamente.
- Verificar que los recursos de la empresa se utilizan responsablemente.

En resumen, el gobierno corporativo es un conjunto de prácticas y responsabilidades ejecutadas por la gerencia con la finalidad de cumplir objetivos para conllevar a la empresa al éxito deseado.

Así mismo, ha adquirido mayor importancia. Se reconoce que la tecnología tiene un papel fundamental que desempeñar para mejorar las prácticas de gobierno corporativo, ya que los procesos de negocio críticos son automatizados y por lo general confiados a sistemas y tecnologías de información para tomar decisiones. Por esta razón los directivos se centran en como las tecnologías de información pueden ser utilizadas para agregar valor a la estrategia empresarial. [National Computing Centre, 2005].

2.1.2.2 Gobierno de Tecnologías de Información

Gobierno de tecnología de información hace referencia a la suma de los conceptos “Gobierno”, “Tecnología” e “Información”. A continuación se muestran algunas definiciones:

Gobierno de TI es responsabilidad del consejo de administración y la dirección ejecutiva. Es parte integral del gobierno de la empresa. Consiste en el liderazgo, las estructuras organizativas y procesos que aseguren que las tecnologías de las organizaciones sostengan los objetivos y estrategias de negocio. [ITGI, 2003].

“El gobierno de las TI especifica los procedimientos de toma de decisiones y los esquemas de responsabilidad para alcanzar el comportamiento deseado en el uso de las TI” [Weill y Ross, 2004. Citado por Fernández y Llorens, 2010].

La norma ISO/IEC 38500 Gobierno de TI como el sistema por medio del cual de dirige y controla el uso actual y futuro de las Tecnologías de información. Supone la

dirección y evaluación de los planes de uso de las TI que dan soporte a la organización y al monitoreo de dicho uso para alcanzar lo establecido en los planes. Incluye estrategias y políticas de uso de TI dentro de la organización. [ISO/IEC, 2008].

Gobierno de TI forma parte integral de la gestión empresarial o Gobierno Corporativo. La necesidad de la gobernanza a nivel de empresa se debe a la entrega de valor para los accionistas y la demanda de la transparencia y gestión eficaz de los riegos corporativos, las oportunidades significativas, costos y riesgos asociados con las TI, esto sugiere enfocarse en Gobierno de TI. Éste permite a la empresa sacar el máximo provecho de las TI maximizando los beneficios, capitalizando oportunidades y ganando ventajas competitivas. [ISACA, 2012a].

Tal como se puede observar, no existen definiciones definitivas para gobierno de TI, pero tiene en común el concepto de gobernar tecnologías de información para lograr los objetivos de la organización. No obstante, sus objetivos son [ITGI, 2003]:

- Alinear las TI con la empresa y la realización de los beneficios esperados.
- Permitir que la empresa tenga las oportunidades de explotar y maximizar beneficios a través del uso de tecnologías de información.
- Usar responsablemente los recursos de tecnologías de información.
- Gestionar de forma adecuada los riesgos relacionados con las tecnologías de información.

Los objetivos mencionados tienen relación e interacción con actividades propias de gobierno de TI los cuales se visualizan en la siguiente figura:

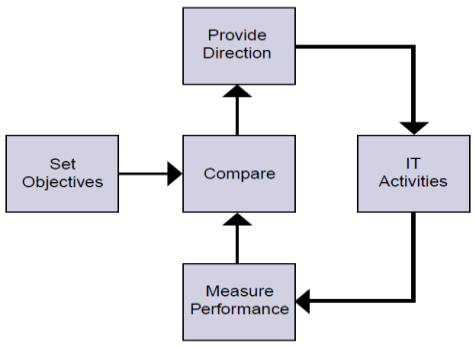


Figura 2.1.1 - Interacción entre los objetivos y las actividades de TI. [ITGI, 2003].

Entonces, tal como se muestra el proceso de gobernanza empieza cuando se establecen los objetivos de las tecnologías de información de la empresa dando así la

dirección inicial. Luego continuamente ingresan a un ciclo de medición de rendimiento comparando los objetivos y dando como resultado el re-direccionamiento de las actividades donde sea necesario y cambiar objetivos cuando es apropiado.

Gobierno de TI ofrece los siguientes beneficios [National Computing Centre, 2005]:

- Transparencia y rendición de cuentas: Aclara la toma de decisiones y la redención de cuentas y definir las relaciones existentes entre los usuarios y proveedores.
- Retorno de valor para los stakeholders: Se permite conocer los riesgos de las tecnologías de información y se mejora la contribución a la rentabilidad de los stakeholders mejorando y protegiendo la reputación de la organización.
- Oportunidades y Asociaciones: Posiciona las tecnologías de información como un socio de negocio y facilita a las empresas a relacionarse con otras empresas y compañeros o socios en TI. Así mismo permite que las tecnologías participen en la estrategia del negocio.
- Mejoras en el rendimiento: Ofrece una mayor transparencia que aumentará el nivel de rendimiento constantemente al incrementar la valla de aceptación, conduciendo al logro de mejores prácticas.
- Cumplimiento externo: Permite tener un enfoque integrado para satisfacer los requerimientos legales y regulatorios.

Esto conduce a cinco pilares para gobierno de TI impulsados por el valor de los stakeholders. Dos son los resultados: Entrega de valor y administración de riesgos y los otros tres son conductores: Alineamiento estratégico, administración de recursos y la medición de desempeño.

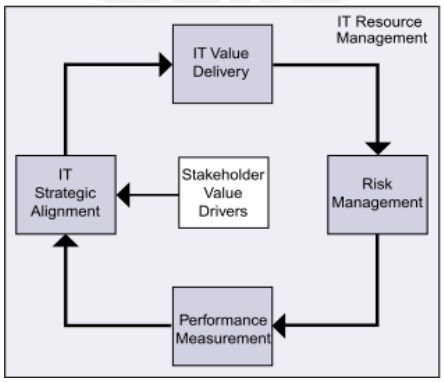


Figura 2.1.2 - Ciclo de vida de los pilares de gobierno de TI. Estructura de relaciones. [ITGI, 2003].

El ciclo señalado muestra que el retorno de valor a los stakeholders influye en el alineamiento estratégico de las tecnologías de información, el cual debe garantizar el

valor de retorno de TI y administrar los riesgos asociadas a éstas, midiendo constantemente el desempeño, cuya respuesta influirá en las estrategias de negocio y verificar el alineamiento de las tecnologías. Todo este ciclo constituye la administración de los recursos de tecnologías de información.

Entonces teniendo en cuenta esta definición de gobierno de TI, se da a conocer su importancia y las áreas principales que abarca formando así el pentágono por el cual es reconocido en diversas organizaciones.

Figura 2.1.3 – Gobierno de TI y sus cinco pilares. [ITGI, 2007. Citado por Muñoz y Ulloa, 2011].

2.1.2.3 Alineación Estratégica

Enfocado en la alineación con los negocios y las soluciones corporativas.
Tiene como objetivo asegurar el enlace entre las TI y los planes de negocio, en definir, mantener y validar la proposición de valor de TI y alinear las operaciones de TI con las de la empresa.
La alineación de las TI ha sido sinónimo de las estrategias de TI. La pregunta es ¿La estrategia de TI soporta a la estrategia de la empresa? Para el ITGI alineamiento abarca más que la integración entre las TI de la organización y la empresa. Se trata sobre la alineación de las operaciones de TI con las de la empresa. [ITGI, 2003].

Su importancia radica en la estrategia de ejecución. De no existir la alineación entre la estrategia de TI y la empresarial conduce a problemas de negocio que incluyen [ITGI, 2005a]:

- Incapacidad de la empresa para alcanzar su máximo potencial.
- No identificar y aprovechar las oportunidades de negocio que brindan las TI.
- Mayores costos de operación, lo cual trae desventaja competitiva debido a la falta de mano de obra para automatizar procesos.

- Incorrecta e ineficaz enfoque de los recursos relacionados con las TI.
- Incapacidad para contratar y retener a alta calidad de TI y de negocio personal.
- Mayores costos generales.
- Erosión de valor para los accionistas a través del tiempo.

2.1.2.4 Entrega del valor

El principio básico del valor de TI es la entrega a tiempo y dentro del presupuesto con la calidad adecuada que permita aplicar los beneficios prometidos.
En términos de negocio se pretende tener ventaja competitiva, dentro del tiempo transcurrido para la realización de pedidos, satisfacción del cliente, el tiempo de espera del cliente, la productividad de los empleados y la rentabilidad. Algunos de estos elementos pueden resultar subjetivos o difíciles de medir, pero los stakeholders necesitan entender. [ITGI, 2003].

Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega asegurando que las tecnologías de información otorguen los beneficios acordado alineados con la estrategia, concentrándose en la optimización de costos y demostrando el valor de las TI. [Muñoz y Ulloa, 2011].

Desde el aspecto de la seguridad de información, el manual del CISM[10] sostiene que la entrega de valor se produce cuando las inversiones en seguridad están optimizadas para apoyar a los objetivos de la organización. La entrega de valor es una función de alineación estratégica entre las estrategias de seguridad y los objetivos de negocio. Es decir, cuando un caso de negocio puede ser realizado para todas las actividades de seguridad. Los niveles óptimos de inversión se producen cuando los objetivos estratégicos de seguridad se consiguen y se logra una postura de riesgo aceptable al menor costo posible. [ISACA, 2012d].

2.1.2.5 Administración de Riesgos

Se direcciona a salvaguardar los activos de TI y la recuperación de desastres.
La administración de riesgos tiene como motor la necesidad de mostrar una buena gobernanza empresarial a los accionistas y clientes.

[10] CISM: *Certified Information Security Manager.*

El riesgo empresarial no es solo a nivel financiero, también existen preocupaciones por el lado operacional y el riesgo sistémico, en el que la tecnología de riesgos y la seguridad de información se vuelven prominentes. El BIS[11] apoya este punto de vista porque los principales problemas de riesgos estudiados dentro de una industria financiera fueron causados por fallas en el control interno, supervisión y TI. [ITGI, 2003].

Por ello se recomienda que la directiva ponga esfuerzo en la administración de los riesgos de la organización. Una correcta administración de riesgos requiere [Muñoz y Ulloa, 2011]:

- "Conciencia de riesgo por parte de los directores superiores de la empresa."
- "Un claro entendimiento del apetito de riesgo de la empresa."
- "Un entendimiento de los requerimientos de cumplimiento."
- "Transparencia sobre los riesgos significativos de la empresa."
- "Implementar las responsabilidades de la administración de riesgos dentro de la organización."

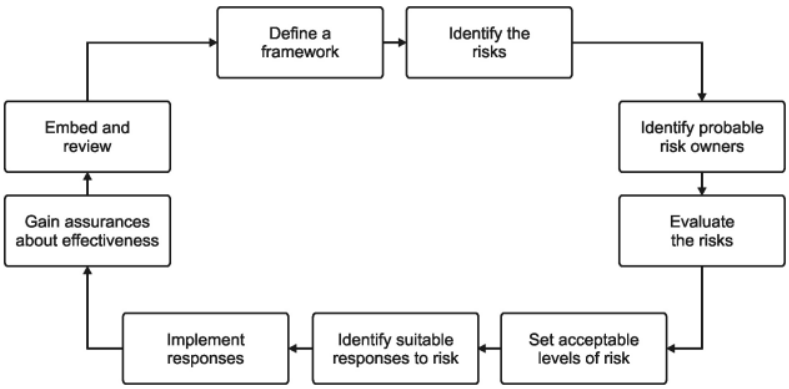


Figura 2.1.4 - Como identificar y administrar riesgos según la OGC. [National Computing Centre, 2005].

Respecto al plan de riesgos a seguir, según los tipos identificados y la importancia para el negocio, administración y la junta directiva se puede elegir [ITGI, 2003]:

- Mitigar: Implementar controles.
- Transferir: Compartir riesgos con socios o transferirlos a la cobertura del seguro.
- Aceptar: Reconocer la existencia del riesgo y monitorearlo.

[11] BIS: *Bank for International Settlements.*

2.1.2.6 Administración de Recursos

Se refiere a optimizar el conocimiento y la infraestructura. Para un satisfactorio desempeño de las TI es clave la inversión óptima, uso y administración de recursos de TI, que puede incluir personas, aplicaciones, tecnología, instalaciones, datos), de manera que se atiendan necesidades de la empresa [ITGI, 2003].

La junta de directivos debe abordar inversiones adecuadas en infraestructura y capacidades garantizando [ITGI, 2003]:

- Responsabilidades con respecto a sistemas informáticos y los servicios procurando que sean utilizados y comprendidos.
- Métodos apropiados y habilidades adecuadas para gestionar proyectos y sistemas de TI.
- Mejora en la planificación de la plantilla y de inversión existentes para asegurar la contratación y retención del experto personal de TI
- Educación, formación y desarrollo identificados y tratados para todo el personal.
- Instalaciones adecuadas y procurar el tiempo disponible para que el personal desarrolle las habilidades necesarias.

Así mismo, deben garantizar el correcto uso de las TI asegurando:

- Métodos y habilidades adecuadas dentro de la organización para la administración de proyectos de TI.
- Ventajas obtenidas de alguna eventual contratación de servicios.

Es importante tomar en cuenta que el personal es parte de la organización forma parte de los recursos de la organización y debe representar la mayor parte del costo base de la organización, por ello deben identificarse las competencias del personal y gestionar constantemente que ellos también cumplan los objetivos y estrategias señaladas por la dirección.

2.1.2.7 Medición del desempeño

Consiste en dar seguimiento y supervisar la estrategia de la implementación, cierre de proyectos, el desempeño de los procesos y la entrega de servicios con la finalidad de medir y evaluar las actividades de TI, de no ser posible esta medición, no se puede

asegurar el alineamiento estratégico, la entrega de valor, la administración de riesgos y la administración de los recursos. [Muñoz y Ulloa, 2011].

La medición del desempeño, involucra como se mencionó anteriormente de medir algunas pautas subjetivas, pues no todo se refleja en balances o perspectivas financieras tradicionales.

Cada una de las perspectivas de la medición de desempeño se ha diseñado para responder a una pregunta relacionada a la empresa [ITGI, 2003]:

- Perspectiva financiera: Para satisfacer a los stakeholders, ¿Qué objetivos financieros debemos perseguir y conseguir?
- Perspectiva del cliente: Para lograr los objetivos financieros, ¿Qué necesidades de los clientes debemos satisfacer?
- Perspectiva del proceso interno: para satisfacer a nuestros clientes y a los stakeholders, ¿Qué procesos internos de negocio debemos mejorar y destacar?
- Aprender de la perspectiva: Para lograr nuestros objetivos ¿Cómo debe la organización realizar el aprendizaje e innovación?

2.1.2.8 Balance Scorecard de Tecnologías de información

“Técnica monitoreo de desempeño empresarial que actualmente es muy empleada para medir la competencia de las iniciativas de TI, es la elaboración de un tablero de comando balanceado o *balance scorecard* (BSC) y en donde se va más allá de la simple evaluación financiera, para calificar aspectos tales como la satisfacción del cliente (usuario de las TICs), procesos internos y la capacidad de innovación alineada, nuevamente, al logro de los objetivos organizacionales. Se usa comúnmente una estructura de tres capas para su aplicación”. [Tupia, 2011].

El balance scorecard, fue desarrollado inicialmente por Kaplan y Norton como un sistema de administración de desempeño que las empresas deben seguir para llevar y seguir la medición de desempeño. Recientemente, está técnica ha sido aplicada a las TI y por primera vez en la vida real las aplicaciones de TI han empezado a emerger. [Van Grembergen, 2000].

Las dimensiones del balance scorecard se muestran en la siguiente figura. Estas son: Financiera, Cliente, Procesos y Aprendizaje, teniendo como núcleo la información.

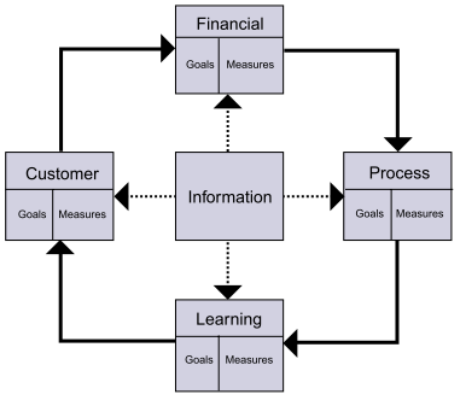


Figura 2.1.5 - Ciclo de las dimensiones del balance scorecard. [ITGI, 2003].

2.1.3 Conceptos relacionados a la propuesta de solución

2.1.3.1 Marco de Control de Tecnologías de Información

El proceso de implantación de gobierno de tecnologías de información tiene que seguir una serie de pasos y estándares. Es por esta razón que nacen los marcos de Control. Éstos deben tener los siguientes propósitos [ITGI, 2008. Citado por Muñoz y Ulloa, 2011]:

- Enlazarse con los requerimientos del negocio.
- Hacer que el desempeño sea transparente a la luz de estos requerimientos.
- Organizar las actividades de TI dentro de un modelo de procesos generalmente aceptado.
- Identificar los principales recursos a controlar.
- Definir los objetivos de control de la administración a ser considerados.

Según la definición mostrada, para implantar gobierno de TI en una organización es necesario optar por un marco de control que permita identificar “Qué” hacer y “Cómo” debe hacerse.

ISACA recomienda ciertas características que debe poseer un marco de control [ITGI, 2007. Citado por Muñoz y Ulloa, 2011]:

- Brindar un fuerte enfoque en el negocio: La medición del desempeño debe enfocarse sobre su contribución para hacer posible y expandir las estrategias de negocio.

- Definir un lenguaje común: Construye seguridad y confianza entre los participantes para sintonizar a todos al definir términos críticos o un glosario para aclarar dudas existentes.
- Ayudar a alcanzar requerimientos regulatorios: Brinda respuesta a los controles internos necesarios para evitar el manejo incorrecto de información frente a normas y estándares.
- Contar con la aceptación general de la organización: Permite ser probado y aceptado para aumentar la contribución de TI dentro de la organización.
- Asegurar la orientación a procesos: Aprovechar procesos que están definidos, asignados y aceptados, para brindar una base de control sobre estos.

Entonces los marcos de control de gobierno de TI ayudan a la gerencia a entender la importancia estratégica de TI y asegura que la empresa pueda mantener sus operaciones e implementar las estrategias requeridas para extender sus actividades en el futuro. Así mismo, garantizan que se cumplan las expectativas relacionadas a las TI y que los riesgos sean abordados. [ITGI, 2003].

Sin embargo, existen también posibilidades de que la implantación de gobierno falle y no logre beneficios dentro de las organizaciones. Estos problemas se deben a la incomprensión de la visión de los objetivos de la empresa y el marco de control elegido. Dependerá también de los recursos involucrados y la realización de una adecuada y oportuna medición de desempeño constante. Entre algunos de los marcos de control se tienen los siguientes:

- **ITIL 2011 (*Information Technology Infrastructure Library)***

  Proporciona mejores prácticas para la gestión de servicios de TI y los procesos relacionados. [ITGI, 2008d].

  Se define también como un ”Conjunto de conceptos y mejores prácticas para la administración de servicios de TI (ITSM) para el desarrollo y las operaciones de TI establecido por la Oficina de Comercio del Reino Unido (OGC).” [Muñoz y Ulloa, 2011].

  Actualmente se encuentra en la versión 2011 publicada en Julio del 2011. Ésta versión, al igual que su predecesora consta de cinco dominios: ITIL Service Strategy, ITIL Service Desing, ITIL Service Transition, ITIL Service Operation, ITIL Continual Service Improvement.

Algunos otros marcos de control para gobierno de TI, también contemplan parte de ITIL. Entre ellos tenemos: COBIT –ISACA ha elaborado un documento para realizar el mapeo de procesos entre ambos marcos [ITGI, 2008d]- y MOF[12].

- **RISK IT**

  Marco de gobierno publicado por ISACA en su última versión en el año 2010 cuyo objetivo es ayudar a las organizaciones a administrar los riesgos relacionados a las tecnologías de información. [ISACA, 2009].

  Está diseñado como un complemento para las empresas que ya usan COBIT como marco de control, aunque también puede funcionar sin él. Lo ideal es poder complementar Risk IT junto con el marco Val IT. [ISACA, 2009].

  RiskIT se encuentra dividido en tres dominios que incluyen [ISACA, 2009]: Gobierno de Riesgos, Evaluación de Riesgos, Respuesta al Riesgo.

  Según lo señalado este es un marco de control que se tiene un enfoque en particular que es parte de uno de los enfoques de gobierno de TI, no obstante al no poder cubrir todos los aspectos no podría ser considerado dentro de una implementación de gobierno de TI si es que no está acompañado por otro marco de trabajo que cubra las necesidades de la empresa y la conduzca a un buen gobierno de TI.

- **VAL IT**

  Marco de control que forma parte del ITGI. Está alineado con COBIT y lo complementa. Mientras COBIT establece las buenas prácticas para contribuir al proceso de entrega de valor, Val IT establece las buenas prácticas para proveer a las empresas las estructuras que requieren para la medición, monitoreo y optimizar la realización del valor de las inversiones en TI. [ITGI, 2008c].

  Este marco de gobierno consta de una serie de principios y procesos que se ajustan a los principios definidos como un conjunto de prácticas a manejar. Mientras Val IT siga evolucionando y creciendo abarcará mayores actividades y servicios auxiliares que apoyan al núcleo de este marco de control.

[12] MOF: *Microsoft Operations Framework*. Está basado en ITIL, pero su implementación es limitada. Este marco certifica personas y no organizaciones. [Microsoft. Citado por Muñoz y Ulloa, 2011].

Val IT 2.0 es la versión actual publicada en el año 2008. Presenta los procesos y las practicas claves de administración para tres dominios: Valor de gobierno, Administración de portafolio[13], Administración de las inversiones.

Dado que Val IT se alinea a COBIT, entonces este último podría ser el único marco de gobierno a utilizar y éste pondría en práctica algunos puntos de Val IT como una herramienta adicional. [ITGI, 2008c].

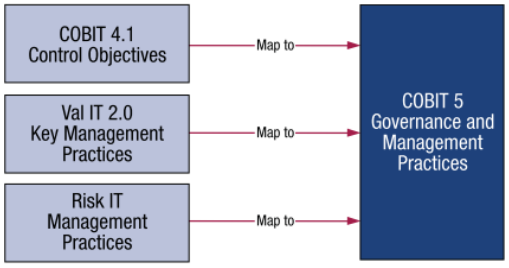


Figura 2.1.6 - Mapeo de Marcos de control a COBIT 5.0. [ISACA, 2012b].

2.1.3.2 COBIT (*Control Objectives for Information and Related Technology*)

Marco de control de gobierno de Tecnologías de Información publicado en su última versión por ISACA en junio del 2012. COBIT es un "marco de referencia globalmente aceptado para el para el gobierno de TI basado en estándares de la industria y mejores prácticas". [ITGI, 2008d].

COBIT es un Marco de control que provee una herramienta para el propietario del proceso de negocio que facilite la descarga de esta responsabilidad. El marco de control inicia con una simple y pragmática premisa: "Para proveer la información que la organización necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos naturalmente agrupados." [National Computing Centre, 2005].

COBIT 5.0 ofrece una guía sobre el gobierno empresarial y la gestión de las TI. Tiene como base 15 años de uso práctico y la aplicación de sus versiones anteriores por parte de muchas empresas, usuarios de negocios de TI, y la garantía de la comunidad ISACA. [ISACA, 2012a].

[13] Portafolio: Grupo de objetos de interés. [ITGI 2008].

COBIT está considerado como una buena práctica para el control de información y los riesgos relacionados a las TI. Este marco habilita en la empresa un gobierno de TI efectivo. En particular, la guía de administración de componentes contiene un marco de control que administra las necesidades de la empresa brindando herramientas que aseguren que las TI se alinean con la organización a través de procesos referencia que ofrece COBIT [ITGI, 2003].

En general, COBIT brinda herramientas que incluyen [ITGI, 2003]:

- Medición del desempeño de los elementos (proceso asociados con las TI).
- Lista de los factores críticos de éxito para cada proceso de TI
- Modelos de madurez para ayudar a la evaluación comparativa y la toma de decisiones para mejorar las capacidades.

Dentro de COBIT 5.0 se definen los motores de su desarrollo para cubrir ciertas necesidades. Estos son [ISACA, 2012a]:

- Proveer más partes interesadas que opinen sobre la información, la tecnología disponible y cuáles son sus prioridades para asegurar que el valor entregado sea el esperado.
- Atender el crecimiento de la empresa y su dependencia de negocios externos y en conjunto con los medios y mecanismos internos para entregar el valor esperado.
- Lidiar con las TI con mayor perspectiva y su alineación con los procesos de negocio.
- Proporcionar mayor orientación al ámbito de la información y las nuevas tecnologías para desarrollar mejores productos y/o servicios que permitan atraer nuevos clientes.
- Cubrir la empresa de extremo a extremo, sus negocios, responsabilidades de TI y cubre todos los aspectos que conducen al gobierno y gestión eficaces de las TI.
- Obtener un mejor control del incremento de las soluciones de TI.
- Integrarse con los demás marcos de ISACA, sin dejar de lado otros frameworks, de manera que COBIT 5.0 sea la base para integrar otros marcos, normas y prácticas.

COBIT 5.0 define los siguientes principios para la implementación [ISACA, 2012a]:

- Conocer las necesidades de los stakeholders
- Cubrir totalmente a la empresa.
- Aplicar un único marco de trabajo integrado.

- Habilitar una perspectiva holística.
- Separar la gobernanza de la administración

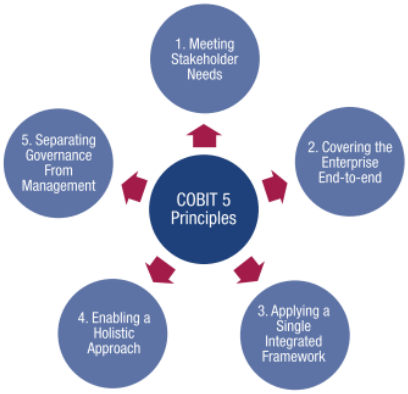


Figura 2.1.7 - Principios de COBIT 5.0 [ISACA, 2012a].

COBIT 5.0 plantea el siguiente método denominado cascada de objetivos para descender hasta los objetivos o procesos habilitadores [ISACA, 2012b]:

- Paso 1: Necesidades de los stakeholders influenciadas por su entorno
  Los stakeholders son influenciados por los factores de su entorno tales como cambios en los negocios, entorno regulatorio, entre otros.

- Paso 2: Necesidad de los stakeholders de priorizar los objetivos de la organización
  Las necesidades de los stakeholders están asociadas a alcanzar los objetivos de la empresa. Se mapean objetivos organizacionales con los objetivos de negocio de COBIT 5.0 para posteriormente identificar las métricas para el balanced scorecard de la empresa.

- Paso 3: Objetivos de la empresa relacionados con los objetivos de TI
  El logro de los objetivos de la empresa está sujeto al alcance de los objetivos de TI. Éstos últimos también se miden a través de un balanced scorecard de TI. COBIT 5.0 define objetivos genéricos de TI que se identifican a partir del mapeo con los organizacionales.

- Paso 4: Objetivos de TI relacionados con objetivos habilitadores
  El logro de objetivos de TI requiere la correcta aplicación y uso de habilitadores. Se realiza el mapeo de estos objetivos identificados con los habilitadores de COBIT 5.0 y se prioriza su selección según los drivers o necesidades del entorno.

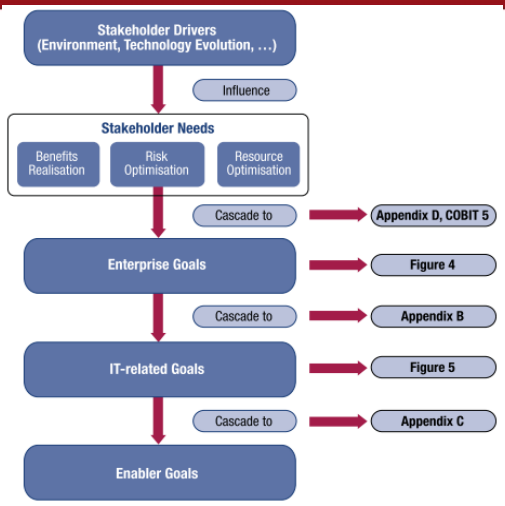


Figura 2.1.8 - Diagrama de objetivos en cascada de COBIT 5.0. [ISACA, 2012b].

COBIT 5.0 proporciona un método para hacer frente a la complejidad y desafíos en la ejecución del Gobierno de TI. Existen tres componentes relacionados al ciclo de vida: El núcleo es la mejora continua del ciclo, la habilitación del cambio y la gestión del programa. Este modelo enfatiza que las actividades no son tratadas una sola vez, sino son parte de un proceso continuo de implementación y mejora. [ISACA, 2012c].

El ciclo de vida propuesto por COBIT 5.0 comprende de siete fases, descritas en el **anexo B**. El programa de Gobierno es continuo e iterativo. Durante la última fase, las nuevas metas serán identificados y comenzará un nuevo ciclo. [ISACA, 2012c].

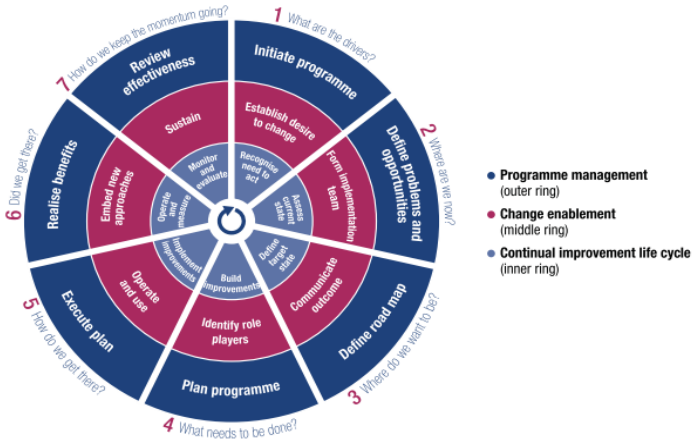


Figura 2.1.9 - Siete fases del ciclo de vida de COBIT 5.0. [ISACA, 2012c].

Sobre los procesos habilitadores mencionados, COBIT 5.0 subdivide los procesos de las prácticas relacionadas con TI y las actividades de la empresa en dos áreas: gobernanza y gestión junto con la administración. Estos procesos pueden consultarse en el **anexo B**.

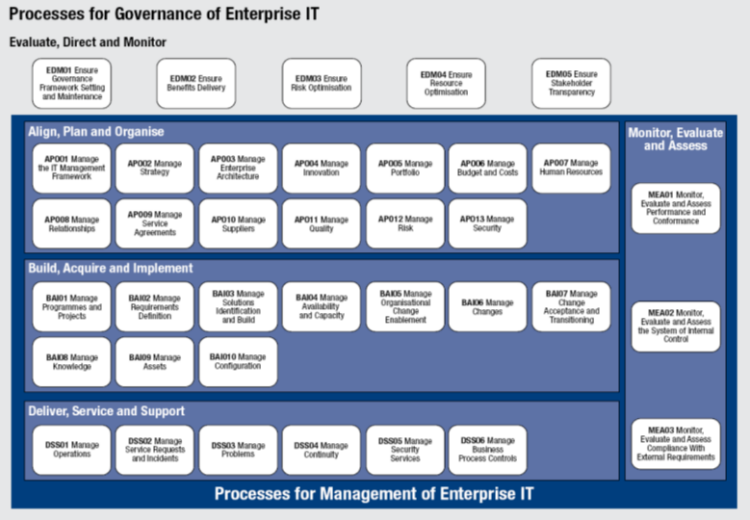


Figura 2.1.10 – COBIT 5.0. Procesos habilitadores. [ISACA, 2012b]

Los procesos habilitadores tienen una serie de actividades a controlar, así mismo, COBIT 5.0 brinda una guía de matriz de responsabilidades del personal identificados por sus roles dentro de la organización, para cada uno de éstos como parte de la implementación del marco de control. Esta matriz es conocida como RACI[14]. [ISACA, 2012c].

Finalmente, cabe destacar que como el marco tiene un año en vigencia, no se tiene referencias directas de aplicación en organizaciones a nivel nacional e internacional, pero se otorgan certificaciones sobre este marco a nivel foundation e Implementation.

COBIT 5.0 define nuevos modelos de madurez, los cuales se basan en una norma exigente como lo es la ISO/IEC 15504. Estos se especifican en el **anexo B** [ISACA 2012a]:

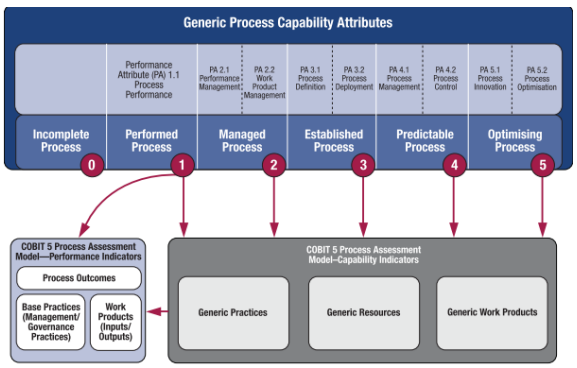


Figura 2.1.11 - Modelos de Madurez según ISO/IEC 15504. [ISACA, 2012a].

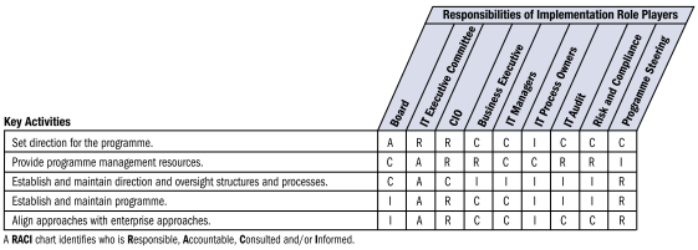
[14] RACI: *Responsible, Accountable, Consulted and/or Informated*.

2.1.3.3 Matriz RACI

Es una matriz de asignación de responsabilidades que ilustra quien es el responsable, aprobador, consultado e informado dentro del marco de trabajo organizacional. [ISACA, 2012e].

Es una herramienta excelente para definir los diferentes roles asociados al desarrollo de un programa de gobierno de TI, seguridad de información u otro ámbito relacionado. Es necesario designar los roles de forma clara para garantizar una implementación eficaz. [ISACA, 2012d].

Dentro de la organización pueden existir distintas funciones de trabajo que respaldan las funciones dentro de un gobierno de TI y la capacidad de asignar autorizaciones de acceso en base a roles simplifican la administración. [ISACA, 2012d].



Key Activities	Board	IT Executive Committee	CIO	Business Executive	IT Managers	IT Process Owners	IT Audit	Risk and Compliance	Programme Steering
	Responsibilities of Implementation Role Players								
Set direction for the programme.	A	R	R	C	C	I	C	C	C
Provide programme management resources.	C	A	R	R	C	C	R	R	I
Establish and maintain direction and oversight structures and processes.	C	A	C	I	I	I	I	I	R
Establish and maintain programme.	I	A	R	C	C	I	I	I	R
Align approaches with enterprise approaches.	I	A	R	C	C	I	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Figura 2.1.12 - Modelo de Matriz RACI. [ISACA, 2012c].

La matriz RACI muestra los siguientes cuatro roles que serán asignados a los miembros del equipo o proyecto [Figuerola, 2012]:

- **Responsable**: recursos que hacen el trabajo para lograr la tarea.
- **Accountable**: Encargado de rendir cuentas sobre la autoridad o autoridad final de aprobación.
- **Consulted**: Aquellos a los que se les solicita opiniones y con quien existe comunicación bidireccional. No están directamente implicados en el desarrollo de las actividades.
- **Informated**: Encargados de mantenerse al día con los progresos o quienes reciben las salidas de un proceso y con el qué solo hay una vía de comunicación.

2.1.3.4 ISO 38500

Fue publicada en el mes de junio del año 2008 y está basada en la norma australiana AS8015:2005. Tiene como objetivo proporcionar un marco de principios para que la dirección de las organizaciones lo utilicen al evaluar, dirigir y monitorear el uso de las tecnologías de información [Bosch, 2008. citado por Muñoz y Ulloa, 2011].

Ésta norma define seis principios para un buen gobierno de tecnologías de información [ISO/IEC, 2008]:

- Responsabilidad: Los grupos e individuos de la organización comprenden y aceptan sus responsabilidades en relación con la oferta y la demanda de tecnologías de información. Las partes interesadas, es decir accionistas e inversionistas tienen también autoridad para llevar a cabo estas acciones.
- Estrategia: Las estrategias de negocio de la organización toman en cuenta las capacidades actuales y futuras de las TI. Los planes estratégicos de TI satisfacen las necesidades actuales y en curso de las estrategias de la organización.
- Adquisición: Las adquisiciones de tecnologías de información se efectúan tras razones válidas teniendo como base un análisis continuo y una decisión clara y transparente. Existe equilibrio entre los beneficios, oportunidades, costos y riesgos a corto y largo plazo.
- Rendimiento: Es apto para propósito de organización, prestar servicios de nivel y calidad necesaria para la satisfacción de los requerimientos de negocio actuales y futuros.
- Conformidad: Las tecnologías de información cumplen con todas las legislaciones y regulaciones. Las políticas y prácticas están claramente definidas, implementadas y aplicadas.
- Conducta humana: Las políticas, prácticas y decisiones respecto a las TI demuestran respeto por el comportamiento humano, incluidas las necesidades actuales y futuras de todas las personas involucradas en el proceso.

El modelo de gobierno de TI presentado en la norma presenta tres tareas [ISO/IEC, 2008]:

- Evaluar el uso actual y futuro de las tecnologías de información.
- Dirigir la preparación e implementación de planes y políticas que aseguren que el uso de TI se alinean a los objetivos de negocio.
- Monitorear el cumplimiento de las políticas y el rendimiento de los planes.

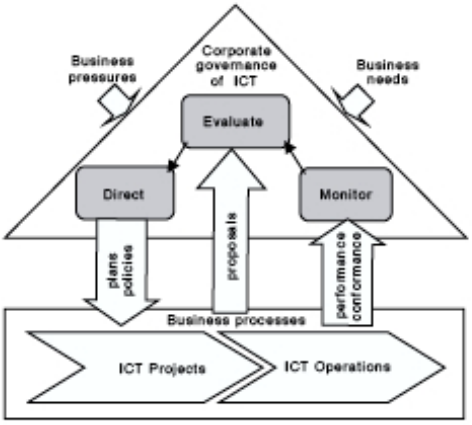


Figura 2.1.13 - Modelo de gobierno de TI según ISO 38500. [ISO/IEC 38500, 2008].

2.1.4 Marco regulatorio / legal

2.1.4.1 NORMA ISO/IEC 27001: TECNOLOGÍAS DE INFORMACIÓN, SISTEMAS DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN. REQUERIMIENTOS.

La presente norma se toma en cuenta dentro del marco regulatorio porque la seguridad de información es el enfoque del gobierno de TI.
Es una norma cuya última versión fue publicada en octubre del 2013. Forma parte de la familia 27000 y cubre todo tipo de organizaciones.

Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema documentado de Gestión de Seguridad de Información en el contexto de los riesgos de negocio que presenta la organización. Indica los requisitos para la aplicación de controles de seguridad según las necesidades de la organización. [ISO/IEC, 2013a].

Está diseñada para garantizar la selección de controles de seguridad adecuados y proporcionales para proteger los activos de información y brindar la confianza necesaria para los stakeholders. [ISO/IEC, 2013a].

La ISO 27001 no se encarga de definir lo que es riesgo u otros aspectos relacionados, sino definir las actividades que guardan relación con el riesgo y mostrar como alinear las políticas de gestión de seguridad de información con el contexto de gestión estratégica de riesgos. [Calder y Watkins, 2010].

2.1.4.2 NORMA ISO/IEC 27002: TECNOLOGÍA DE INFORMACIÓN, SEGURIDAD DE INFORMACIÓN. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE SEGURIDAD DE INFORMACIÓN.

La presente norma se toma en cuenta dentro del marco regulatorio debido a que está relacionada con la norma ISO 27001, pues esta indica cómo debe de aplicarse.
Su fecha de publicación data también de octubre del 2013 y se basa en la anterior norma ISO/IEC 27002:2005.

Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de información en una organización. Los objetivos señalados es el de proporcionar una orientación general sobre las metas comúnmente aceptadas de gestión de seguridad de información. [ISO/IEC, 2013b].

Contiene las mejores prácticas de objetivos de control y controles en las siguientes áreas de gestión de la información de seguridad [ISO/IEC, 2013b]: Política de seguridad, Organización de la seguridad de información, Seguridad de recursos humanos, Gestión de activos, Control de acceso, Criptografía, Seguridad física y ambiental, Seguridad de las operaciones, Seguridad de comunicaciones, Relaciones con los proveedores, Adquisición de sistemas de información, desarrollo y mantenimiento, Gestión de incidentes de seguridad de información, Gestión de la continuidad de negocio, Cumplimiento.

Los objetivos de control y controles de la norma están destinados a ser implementados para cumplir los requerimientos señalados por la evaluación del riesgo. La norma pretende ser una base común y orientación práctica para la elaboración de estándares organizacionales de seguridad y prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en actividades interinstitucionales. [ISO/IEC, 2013b].

En cuanto a la gestión de activos, la norma indica que en sistemas de información complejos puede ser útil designar grupos de activos, los cuales actúan juntos para proveer una función particular, como “servicios”. En este caso, el propietario del servicio es responsable de la entrega del activo. [Calder y Watkins, 2010].

2.1.4.3 LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY N° 29733)

La presente ley tiene como objeto garantizar el derecho fundamental a la protección de los datos personales. Se considera dentro del marco regulatorio porque involucra al área de seguridad de información que también forma parte del gobierno de tecnologías de información. De tomar encuentra está área para el gobierno de TI, se tendría que ceñir a ésta ley.

Definiciones [Congreso de la República 2011]:

- Nivel suficiente de protección para los datos personales: Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.
- Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

La ley señala artículos importantes para evitar la violación de los datos y otorga derechos al titular de los datos. Entre éstos se señalan los siguientes:

- Artículo 18. Derecho de información del titular de datos personales.
- Artículo 23. Derecho al tratamiento objetivo.
- Artículo 35. Derecho a la Confidencialidad.

Entre las infracciones señaladas la ley menciona [Congreso de la República, 2011]:

- “Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales”.
- “No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales, cuando legalmente proceda”.
- “Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales”.
- “Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la presente Ley o su reglamento”.

2.1.4.4 NORMA TÉCNICA DE LA HISTORIA CLÍNICA

La presente norma es aplicada solo en el caso de empresas prestadoras de servicios de salud, pues manejan ciertos documentos de vital importancia para sus clientes o en este caso pacientes. Esta norma puede complementarse con la reciente ley de protección de datos personales y brindar mayor seguridad sobre los datos que éstas historias contienen.

Definiciones [MINSA, 2005]:

- **Historia clínica**:

  Es el documento médico legal, que registra los datos, de identificación y de los procesos relacionados con la atención del paciente, en forma ordenada, integrada, secuencial e inmediata de la atención que el médico u otros profesionales brindan al paciente. A su vez poseen un alto valor y su correcta gestión mejora la calidad de atención de los clientes y protege interés de ambas partes.

Disposiciones generales [MINSA, 2005]:

- Todo acto médico brindado a los usuarios en los establecimientos será registrado en la historia clínica, registro primario de cada atención.
- Las historias clínicas deberán estar accesibles al personal autorizado durante el horario de atención del establecimiento.
- Para la elaboración de la historia clínica de debe tener en cuenta el nivel de atención y el tipo de prestación: Nivel I con población y sin población asignada, Nivel II y Nivel III.

Estructura [MINSA, 2005]:

1) **Identificación del paciente**: Contiene datos de identificación incluyendo su número de historia clínica y datos del establecimiento de salud.
2) **Registro de atención de salud**: Registro de atención de salud. Se emplean los formatos para consignar la información de la atención según la naturaleza el servicio que presta.
3) **Información complementaria**: Contiene resultados de exámenes auxiliares, documentos que sirven como sustento legal, técnico, científico y/o administrativo de las acciones realizadas al paciente en el proceso de atención.

Dentro de la ley se describen los formatos a seguir y se presentan como anexo algunas fichas y modelos que el Ministerio de Salud recomienda. No obstante se debe

de considerar que el cumplimiento de esta norma es responsabilidad de autoridades competentes y dependencias del Ministerio.

La implementación de la norma debe estar acompañada de las actividades de capacitación e información al personal y todo incumplimiento será sancionado de acuerdo a las disposiciones administrativas existentes a la Ley General de Salud y al Código de Ética y Deontologías Profesional, sin perjuicio de las acciones civiles o penales a que hubiere lugar. [MINSA, 2005].

2.1.4.5 HIPAA: ACTA DE CONTABILIDAD, PORTABILIDAD Y SEGUROS DE SALUD.

Esta acta es una regulación dada por el gobierno norteamericano para regular los servicios de salud y los datos electrónicos que manejan. Consta de 2 partes [OCR, 2003]:

Parte 1: Acceso a servicios de salud, potabilidad y rentabilidad
Esta parte regula que beneficios se deben transferir al cambiar de seguro y que beneficios permanecen cuando una persona pierde su empleo.

Parte 2: Prevención de fraude y abuso en el sistema de salud; simplificación administrativa; reforma de confianza medica
Esta parte define políticas, procedimientos y guías para mantener la privacidad y seguridad de la información médica de cada individuo. Además crea varios programas de control para prevenir fraudes y abusos en el sistema médico. Aparte, crea regulaciones sobre estándares de diseminación de información médica.

La regla de privacidad que define entre otras cosas que los individuos tienen derecho a pedir a las entidades de salud que corrijan cualquier información incorrecta que tengan. Además, regula las comunicaciones entre entidades de salud y con los individuos, para que todo tenga la más alta confidencialidad [OCR, 2003].

La regla de seguridad define los estándares mínimos de protección de información electrónica y física. Incluye regulaciones en el ámbito administrativo, físico y técnico. [OCR, 2003].

2.2 Estado del arte

2.2.1 Formas aproximadas de resolver el problema

A continuación se presentan casos en los cuales las implantaciones de gobierno de Tecnología de Información han sido las soluciones aproximadas para resolver la problemática descrita.

2.2.1.1 CASO DE ESTUDIO: SUNNYBROOK HEALTH SCIENCES CENTRE

Basado en los casos de estudio de ISACA Internacional [ISACA, 2013a].

Sunnybrook es uno de los centros de salud más importantes de Canadá. Con aproximadamente 60 años de experiencia y convenios con universidades del país para recibir dentro de su staff a los alumnos. Al ser uno de los hospitales veteranos se han dedicado a atender en su mayoría al adulto mayor, atender embarazos de alto riesgo, prevención del cáncer, entre otros.

Dicho centro reconoce el Gobierno de TI como parte integral del Gobierno Corporativo y consiste de un líder, estructuras organizacionales y procesos que aseguren que sus servicios de información conlleven a alcanzar los objetivos estratégicos. Por esta razón, el CIO expresa la necesidad de incrementar el enfoque en el lado técnico y gestión de riesgos de TI tras el incremento de operaciones e incidentes e interrupciones en los servicios u otros proyectos.
Para iniciar el programa de gobierno, se definen los objetivos estratégicos de Sunnybrook, mencionados en su plan estratégico del año 2012:

- Ser líder nacional en el desarrollo de programas de salud por medio de la expansión de su programa MyChart.
- Ser líder en el diseño y construcción de soluciones innovadoras para el cuidado de la salud.
- Emplear sistemas de información y tecnologías para mejorar la integración con sus proveedores y canales de atención.
- Ser líder en el desarrollo herramientas de gestión de la información en tiempo real e implementar almacenes de datos clínicos para la investigación de servicios de salud.
- Implementar un marco de gobierno de tecnologías de Información.

Sunnybrook gestiona su programa de gobierno de TI basado en COBIT 4.1 en combinación con otros marcos de gobierno complementarios como RISK IT y VAL IT. Esto se debe a que manejan las buenas prácticas para entregar servicios de TI y gestión estratégica para lograr el cumplimiento de los programas ya mencionados.

Los enfoques optados para el gobierno de TI es la entrega de valor de TI y la mitigación de los riesgos de TI. Estos serán habilitados bajo el aseguramiento del alineamiento estratégico de las tecnologías de TI con los objetivos de negocio de Sunnybrook, disponibilidad y gestión de recursos apropiados de TI y la medición del desempeño y gestión de TI.

Las áreas de enfoque seleccionadas son trasladadas hacia un cuadro de mando, en este caso en balanced scorecard que será el reporte entregado a la alta dirección y que parte a partir de los objetivos y procesos asociados. Para esto, se requiere encontrar los indicadores y métricas para cada una de las dimensiones del cuadro. Se logran finalmente aplicar unos para la medición de sus dimensiones del balanced scorecard según los resultados en SunnyCare.

- **Acceso**: reducir la espera, número de usuarios únicos, número de programas clínicos con programas clínicos.
- **Eficiencia**: Minimizar residuos, incluidos los de tiempo, equipos, suministros, entre otros.
- **Eficacia**: Prestación de servicios con los que todos puedan beneficiarse
- **Centrarse en el cliente**: Responder a las preferencias del cliente, necesidades y valores.
- **Seguridad**: Evitar lesiones a los pacientes, atención que se destina a ayudar a ellos.

Sunnybrook está comprometida con el desarrollo y medición de estos indicadores para el próximo año ejecutar su plan de Gobierno de TI con la finalidad de evaluar la viabilidad de construir a futuro mayor cantidad de programas de TI de forma estratégica. Como se señala, se ha llevado a discusión la necesidad de entregar valor y la gestión de los riesgos, por ello se deben de refinar y tratar a través de un cuadro integral. El comité de auditoría ha elogiado al grupo de TI por la introducción del marco COBIT y con lo que pone en la pista de medición para garantizar el valor y el riesgo responsabilizando al directorio y la gerencia.

2.2.1.2 CASO DE ESTUDIO: NHS Fife.

Basado en los casos de estudio de ISACA. [ISACA, 2012f].

El NHS es un centro de servicios de salud en el Reino Unido. NHS Fife es proveedor de servicios de salud pública en Escocia y cubriendo una amplia gama de servicios con la participación de hospitales de toda la región. Empieza a trabajar con COBIT 4.0 en el año 2007 tras la necesidad de garantizar que sus servicios de salud se alinearan con estrategias nacionales y locales de NHS y mejorar la seguridad, resultados de auditorías y cumplir con las normas reconocidas.

Hasta el 2007 NHS Fife empleaba ITIL v2 como estándar de mejores prácticas para la gestión de servicios, no obstante carecía de una visión global de mejora continua incorporando todos los procesos relevantes de estrategia de servicio a las operaciones, estableciendo el ciclo de mejora en términos de nivel de madurez y el cómo medir el progreso. Todo esto encontrado en COBIT.

Tras entender que COBIT es un marco de alto nivel, apoyó su implementación con Meycor COBIT Suite, útil para establecer una línea base, desarrollo de planes de mejora, selección de indicadores y seguimiento de los ciclos de mejora para cada uno de los procesos.

Los objetivos para la aplicación de COBIT desde la perspectiva de NHS Fife son:

- Entender las prioridades para establecer un proceso maduro para involucrar y alinearse con la estrategia de NHS Fife.
- Reducir el riesgo y mejorar la seguridad
- Mejorar los resultados de la auditoría interna y externa
- Establecer un modelo de mejora continua que sea sostenible y permita mostrar resultados.
- Lograr tener procesos clave en nivel 3 de Madurez según COBIT en un año

Se definen dos fases para la implementación: la de capacitación, en la cual participan los propietarios de los procesos y se capacita en COBIT 4.0 y herramientas Meycor COBIT, y la segunda fase que contiene lo siguiente:

- Sensibilización sobre el gobierno de TI con todo el equipo
- Formación continua en el marco y herramientas Meycor COBIT

- Identificación de los procesos pertinentes con sus propietarios y responsabilidades.
- Revisión de todos los procesos existentes y establecer una línea base de la situación actual.
- Seleccionar procesos experimentales según la necesidad de la organización.
- Desarrollo de planes de mejora.
- Aplicar encuesta de satisfacción de los usuarios del departamento de TI para demostrar los cambios a través de ciclos de mejora.

En el año 2010 el proceso de gestión de cambio fue auditado mostrando un logro de alto nivel de madurez (calificación 3) la cual fue una de las calificaciones más altas y rápidas obtenidas en mejoras de procesos.

A partir de ese año la infraestructura de NHS Fife logró la certificación ISO 27001 (Enero 2012) y desarrolló un marco institucional para el gobierno de TI, lo cual implica el reconocimiento de su importancia, independientemente de los servicios que ofrece.

Actualmente el equipo de infraestructura se centra en los indicadores y establecimiento de cuadros de mando para necesidades específicas, en particular el apoyo a la gestión de activos y gestión de procesos, SLA's y seguridad. Con la publicación de COBIT 5, la organización, por su parte, se centra en satisfacer las expectativas de los stakeholders y la revisión de la estructura de gobierno para determinar cómo hacer mejor uso de características adicionales.

2.2.2 Productos comerciales para resolver el problema

2.2.2.1 MEYCOR COBIT SUITE

Meycor Cobit Suite es una herramienta software desarrollada por Datasec. Ésta solución cubre [Meycor, 2010]:

- Requerimientos de los CIOs y CTOs para implantar el gobierno de TI.
- Necesidades de los asesores y auditores para implantar el aseguramiento de las TI.
- Necesidades de los CSOs[15] para implantar procesos de seguridad de TI y desarrollar Sistemas de Gestión de la seguridad de información

[15] CSO (*Chief Security Office):* Director de la seguridad de la organización.

Incluye los servicios de capacitación y consultoría de desarrollo e implantación. Ésta herramienta como su nombre lo indica es utilizada para implantar COBIT como una herramienta de Buen Gobierno de TI, Seguridad de TI o aseguramiento de las TI según COBIT 4.1. Incluye los siguientes módulos:

- **Meycor COBIT CSA (Control Self – Assessment)**

  Herramienta de autoevaluación que posibilita la participación de la auditoría. Permite diagnosticar el estado de la organización respecto al nivel de seguridad, calidad, eficacia y eficiencia en TI de acuerdo al Marco de control COBIT. Así mismo, permite integrar cuestionarios de normas y marcos de mejores prácticas constituyéndose en una herramienta de evaluación de la conformidad. Incluye los riesgos asociados a los objetivos de control de COBIT 4.1 y realiza las evaluaciones de riesgos.

- **Meycor COBIT MG (Management Guidelines)**

  Permite definir los logros gerenciales de una organización de acuerdo al modelo de madurez[16] de las guías de gerenciamiento de COBIT 4.1. También permite realizar un diagnóstico de la situación actual de madurez para cada proceso de COBIT, generar recomendaciones e implementar proyectos de mejora.

  Determina la relación entre las metas del negocio, metas de TI y correspondientes procesos de COBIT 4.1. Posibilita realizar la evaluación de desempeño de las actividades que comprenden sus procesos.

- **Meycor COBIT AG (Audit Guidelines)**

  Permite crear y gestionar proyectos de auditoría de TI basado en COBIT. La estructura del producto permite que se puedan definir los objetivos de éste marco de control a ser evaluados, los centros auditados, procedimientos usados y auditores asignados. Se incluye también las guías de auditoría de COBIT 3 y guías de aseguramiento de COBIT 4.1.

- **Meycor COBIT KP (Knowledge Provider)**

  Permite el desarrollo, residencia, distribución y mantenimiento de sistemas de gestión que siguen el Ciclo de Deming[17], así como todo tipo de contenidos generados durante un proyecto de implantación del gobierno de TI o gobierno corporativo. Básicamente es útil para el tratamiento de documentación de procesos, análisis de riesgos e implementación de un Sistema de Gestión de Seguridad de la Información. Así mismo gestiona distintos eventos y realiza la autoevaluación contra marcos regulatorios. Se incluye también el proceso DS4,

[16] Modelo de Madurez (CMMI): Es un modelo de evaluación de procesos de una organización.
[17] Ciclo de Deming: Columna vertebral de los procesos de mejora continua. (ITIL V3 Guide)

Aseguramiento de la Continuidad de Servicio, útil para implantación de la norma ISO 27001.

- **Meycor COBIT Delphos**
  Administrador de indicadores de gestión estratégica conocido como Cuadro de Mando Integral (CMI). Se usan sus facilidades para crear un CMI que pueda ser integrado con otros existentes en la organización.

Ésta Suite incorpora un Módulo central (Meycor COBIT Route Finder) que incluye una guía metodológica para implantar gobierno de TI pasado en el Roadmap de la segunda edición del IT Governance Implementation Guide.

2.2.2.2 ERA KAIROS

Herramienta Software desarrollada por la empresa Methodware que se presenta como una solución integrada para los riesgos, cumplimiento y auditoría.

Era Kairos permite a los usuarios sus vistas personales de *Governance Risk Management and Compliance (*Gobierno, Administración de riesgos y Cumplimiento), en base a necesidades específicas y requisitos de la organización. Llevando al usuario a una experiencia intuitiva.

Entre sus principales ventajas ofrece:

- Usabilidad intuitiva: Es personalizable permitiendo así que los usuarios trabajen de forma más productiva evitando largos cursos de actualización.
- Reducción en apoyo.
- Aumento de eficiencia: La reducción del tiempo de capacitación para el uso del software hace que los usuarios finales aprovechen ese tiempo en ocuparse de sus labores diarias de trabajo.
- Flexibilidad mejorada: Según la evolución del negocio, Era muestra las nuevas circunstancias sin cambios en la programación o bases de datos.
- Mejorar la alineación entre GRC y el Negocio: Reduce prioridades conflictivas asegurando que los riesgos y métricas sean valiosas.
- Mayor comprensión de la cartera de riesgos: Obtiene un panorama más claro de la situación actual y futura. Es capaz de identificar oportunidades correctas a seguir.

Otras características de apoyo:

- Elaboración de informes: Más de 3550 informes estándar. Asegura la provisión de datos a herramientas de reporte.
- Incidentes: Registro, rastreo y análisis de incidentes.
- Medición del desempeño: Vincula las actividades del GRC a sus objetivos de negocio y seguir el progreso individual en función de parámetros definidos.
- Estándares internacionales: Soporta ISO 31000 y AS5. También COBIT, Basel II, SOX, PCI y Solvency II.
- Planificación y Programación: Estructura de las auditorías y evaluaciones de acuerdo a prioridades, recursos disponibles y conjunto de habilidades.
- Integración de datos: Los elemento comparten n almacén de datos central como estándar.
- Lógica de negocio: permite establecer las reglas para ayudar a administrar los usuarios finales.
- Notificaciones: Se puede configurar alertas dentro de la aplicación así como a través de correo electrónico.

2.2.2.3 COBIT ONLINE

Herramienta software en línea, basada en el marco de control COBIT 4.1 útil para consultores y auditores para verificar el cumplimiento de la actividad de TI.

Características [ISACA, 2010]:

- Construir resultados personalizados de la organización y ver online o descargar en formato MyCOBIT.
- Acceso a la base de conocimientos de COBIT.
- Buscar mejores prácticas de COBIT.
- Realizar retroalimentación en línea.
- Acceso a los foros de discusión.

Como es de conocimiento, el marco de control COBIT 4.1 ha sido reemplazado por COBIT 5.0. ISACA menciona que se realizará la actualización de COBIT online a la versión 5.0. Aún no se tiene la fecha exacta de publicación, sin embargo ISACA continuará apoyando el uso en línea en de ambas versiones para minimizar el tiempo de transición.

Para tener acceso a esta herramienta cabe resaltar que se tiene como requisito ser miembro permanente o estudiantil de ISACA

MyCOBIT, comprendido dentro de COBIT Online, permite crear y descargar una versión personalizada de COBIT que se adapte a las necesidades especiales de la empresa. Permite la selección de componentes lo cual permite que se personalizar a la medida del cliente y realizar el benchmarking.

2.2.3 Problemas relacionados

En el presente apartado se hablará de los problemas relacionados respecto al gobierno de TI.
Tras haber identificado los pilares del gobierno y la problemática, no se puede dejar de mencionar problemas en cuanto a la seguridad de información, gestión de servicios de TI e incluso la continuidad de negocios.

Se priorizan estos tres problemas por lo siguiente:

- Seguridad de Información:
  "En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. Una efectiva administración sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

  A esto se suman las nuevas leyes y/o normas que van surgiendo **(Basilea II, Sarbanes Oxley)**, las cuales en un futuro cercano, impartirán lineamientos obligatorios sobre cómo las instituciones financieras del Perú deberán manejar su información, los controles internos que deberán asignarse e implementarse y el presupuesto que deberán destinar a la administración de los riesgos." [Villena, 2006]

  El autor menciona una problemática relacionada a los problemas dentro del área. El gobierno de TI tiene como enfoque la Administración de Riesgos, asociados también con las TI y a la seguridad de información. Debido a las regulaciones, consideradas también en el marco regulatorio para las empresas prestadoras de salud, se vuelve un objetivo para las estas mantener salvaguardados los datos

que maneja la empresa. En nuestro país, con la nueva Ley de Protección de Datos Personales y la norma técnica para historias clínicas, se hace notar la importancia de este tema.

- Gestión de Servicios de TI:

  "En la actualidad, muchas áreas de sistemas de las empresas no tienen una adecuada gestión de incidentes o de problemas de los sistemas de información empresariales en sus ambientes productivos, es por ello que, muchas veces el personal de soporte de sistemas que atiende estos eventos, no tiene definido el proceso de escalamiento o los tiempos de atención en que deben ser atendidos según la prioridad del mismo.

  Muchas veces el servicio de Tecnologías de Información llega a recuperarse, pero no se logra investigar y descubrir las causas raíz de los problemas o peor aún, se tienen incidentes que no son resueltos en realidad. Todo esto repercute en la imagen y la capacidad del personal de TI así como en la continuidad del negocio." [Gómez, 2012].

  El autor señala un problema dentro del área de los servicios de TI y los errores comunes de la gestión de los mismos. El gobierno de TI muestra también la importancia de este tema en el área de Administración de Recursos, que contempla también la parte de servicios. COBIT 5.0 presenta controles que permiten realizar un seguimiento a estos servicios y poder priorizar sus objetivos a través del balance scorecard de TI, por lo cual las empresas implantando esta solución pueden ocuparse también de ésta problemática. A esto se suma, la importancia de entregar servicios de calidad lo cual se complementa con buenas prácticas que pueden gestionarse desde COBIT 5.0 tales como las que sugiere ITIL V3.

- Plan de Continuidad de Negocios:

  Gobierno de TI señala la importancia de la continuidad de los negocios, razón por la cual se considera este tema como parte de un problema relacionado.

  En la actualidad existen normas y marcos de control que permiten diseñar planes de continuidad, entre ellas la más actual es la ISO/IEC 22301.

COBIT 5.0 contempla en sus procesos el monitoreo y mantenimiento de un plan de continuidad, por ende las organizaciones podrían ocuparse de este tema también importante para su crecimiento y cumplimiento de objetivos.

2.2.4 Conclusiones sobre el estado del arte

- Dada la publicación de COBIT 5.0, no se encuentran referencias sobre implantaciones de gobierno TI utilizando esta versión del conocido marco de control. No obstante, ya se pueden acceder a guías complementarias e incluso certificaciones en dicho marco.

- Las soluciones, implantación de gobierno de TI, respecto a la problemática de las empresas prestadoras de servicios de salud y las tecnologías de información no son comerciales en nuestro país. Esto se ve reflejado en que no se cuenta con referencias exactas dentro de nuestro entorno. No obstante, si existen casos de éxito en otros lugares del mundo tal como se muestra en este apartado.

- La solución de la problemática, implantando gobierno de TI o controles adicionales, según otros marcos de control como ISO 38500, Val IT y Risk IT, no es una práctica comercial. Se brinda esta conclusión tras realizar la investigación respecto a los productos comerciales que brindan solución al problema. Los productos software mencionados en el estado del arte se localizan en marcos de control COBIT o la integración de diversos marcos para mayor versatilidad.

- Los casos mencionados en el estado del arte, ambos presentan como solución implantar un gobierno de TI o sus buenas prácticas empleando COBIT. Aunque el problema no sea netamente económico o de inversión en tecnologías, si reconocen la necesidad de inversión, gestión de servicios y manejo de riesgos y seguridad para cumplir con regulación externa.

- La implantación de gobierno de TI en una empresa, si bien es cierto puede realizarse con otro marco de control como ISO/IEC 38500, Val IT, ITIL V3, se debe tomar en cuenta las limitaciones de éstos marcos pues resultan también limitantes en algunos aspectos ya que dan énfasis a algunas áreas de enfoque en particular, razón por la cual no brinda una solución íntegra y versátil como se espera.

- COBIT 5.0 integra marcos de control como Val IT, Risk IT y además toma en cuenta las tareas sugeridas por la ISO/IEC 38500 y se alinea con aspectos de ITIL V3, siendo entonces una versión mejorada de COBIT 4.1 y que a la vez puede ser apoyada por una o varias herramientas software comerciales, lo cual hace que tenga ventaja frente a los marcos mencionados.

- Respecto a los problemas relacionados, para cada uno de ellos se muestra que el gobierno de TI y su implantación son también una posible solución adicional a las existentes y que COBIT 5.0 y sus procesos habilitadores contemplan también las actividades para evaluar, diseñar y monitorear los controles a aplicar tras su nuevo enfoque integrador.

- COBIT se presenta como una buena alternativa de solución a la problemática planteada inicialmente a pesar de no tener referencias actuales de esta última versión. Además, en tesis y documentos elaborados por ex alumnos de otras universidades recomiendan el uso de este marco de control por la integridad con todos los elementos de gobierno de TI. Así mismo, por características descritas como la integración y alineación con otros marcos de control, es posible y conveniente tomarlo como referencia única para diseñar la solución. [Arteaga, 2012] [Baldeón y Pinoargote, 2007].

Capítulo 3. Análisis del Negocio

En el presente capítulo, se elabora el primer resultado esperado propuesto, en este caso el Business Case de la clínica en el cual se muestra las oportunidades viables para las empresas prestadoras de servicios de salud. En este caso particular adoptando la realidad de una clínica de nuestro país.

Según el contexto presentado se desprenderán las oportunidades para la solución y lograr los resultados deseados por las partes interesadas, justificando su elección desde la perspectiva analítica y financiera.

3.1 Caso de Negocio

Contexto Estratégico

Las empresas prestadoras de servicio de salud, en particular con la cual se desarrolla el modelo de gobierno de TI, tiene como meta la ampliación de sus servicios hacia toda la comunidad a través de sus distintas modalidades o canales de atención.

La organización desea llegar a toda la población objetivo y brindar una mejor atención a través de nuevos recursos junto con el apoyo de una buena gestión y manejo de tecnología de vanguardia para satisfacer las necesidades de sus clientes.

La necesidad del negocio es encontrar los recursos y capacidades necesarias para abastecer sus sucursales y poblarlos de la infraestructura tecnológica necesaria para

brindar atención y a su vez para soportar sus sistemas organizacionales y cumplir con las regulaciones a las cuales se encuentran sujetas.

Los drivers[18] del cambio identificados son:

- Recursos: Necesidad de integrar servicios que cubran las necesidades y de acuerdo a la expansión deseada y planificada (incremento de sucursales) y que se estén alineados a los objetivos de negocio.
- Regulaciones: Se incorpora la ley 29733 para la protección de datos personales en nuestro país. No se debe dejar de lado las normas previas.
- Tecnología: Contar con tecnología de vanguardia para mejorar su servicio. (Asegurar el retorno del valor).

La inversión deseada para implementar una nueva solución tiene como base lo siguiente:

- Cumplir con la regulación actual y vigente dentro del país: Ley de protección de datos personales, norma técnica peruana de historia clínica y ley de emergencia.
- Brindar responsabilidad a la gerencia y dar una dirección correcta a los recursos técnicos y financieros para logar el cumplimiento de objetivos.

Para llevar a cabo la nueva solución, se requiere según el contexto, desarrollar el proyecto por etapas considerando los cambios que se van a implementar y evaluarlos en el espacio de tiempo necesario utilizando métricas de acuerdo a los drivers del cambio y objetivos deseados.

Análisis y Recomendaciones

Opciones viables e inversión

Tras la evaluación de los criterios que se detallan en el **anexo C** junto con las opciones preliminares propuestas, se tienen como opciones viables las siguientes:

- Opción 1: Emplear principios de ITIL para la entrega de servicio.
- Opción 2: Implementar un gobierno de TI.
- Opción 3: Implementar un SGSI.

Para la inversión se toma en cuenta los siguientes puntos:

[18] Drivers: Impulsadores del cambio

- Enfoques para gobierno de TI: Seguridad de Información como base proyectándose posteriormente a la gestión de operaciones de TI.
- Costos expresados en dólares.
- Horas laborales: 8 horas.
- Se asume un personal que cuenta con la respectiva certificación en dichos rubros.
- Beneficios Criterios: Preservar vida humana, calidad en procesos, integración con otras soluciones, trabajos futuros y tiempo de vida del proyecto.

	Costo total	Beneficios[19]	Costo efectivo[20]	Costo Beneficio	Costo beneficio Neto
Opción 1: ITIL	90000	40	80000	4000	10000
Opción 2: Gobierno	200000	25	192000	2500	5000
Opción 3: SGSI	121000	35	115000	3500	6000

Tabla 3.1.1 - Resumen de costos de proyectos

Si bien es cierto, Gobierno de TI es un proyecto de costo más elevado permite trabajos futuros que empleen la propuesta conjunta de implementación de un SGSI y buenas prácticas de ITIL según sea el enfoque.

Justificación y recomendaciones

Se sugieren estas tres opciones viables, pues a nivel general, la organización requiere acciones basadas en procesos clave para poder cumplir con las regulaciones y objetivos estratégicos planteados, lo cual implica realizar un análisis a fondo de los beneficios y cumplimiento con criterios como el alineamiento estratégico, entrega de valor, gestión del riesgo, entre otros que garanticen contrarrestar los efectos de la problemática y adaptarse al contexto descrito.

Criterios	Opción 1	Opción 2	Opción 3
Alineamiento estratégico	**No**	**Sí**	**No**
Entrega de valor	**Sí**	**Sí**	**No**
Gestión de riesgos	**No**	**Sí**	**Sí**

[19] El beneficio se considera como un factor. A mayor beneficio por ahorro de recursos, el factor es menor, por ello el costo total se incrementa a razón.
[20] Costo relacionado al trabajo neto en la consultoría.

Requerimientos definidos	**Deseable**	**Core**	**Core/Deseable**
Cumplir con la regulación	**No**	**Sí**	**Sí**
Cubrir las necesidades de negocio	**Sí**	**Sí**	**Sí**
Potenciar y mejorar el servicio entregado	**Sí**	**Sí**	**No**
Gestión óptima de recursos	**Sí**	**Sí**	**No**
Costos de implementación	**Costo menor**	**Costo elevado**	**Costo medio**
Costos de retorno (ROI)	**Válido**	**Válido/mayor**	**Válido**
Otros criterios de elección	**Sí**	**Sí**	**Sí**
Resultado		**Seleccionado**	

Tabla 3.1.2 - Análisis de criterios y justificación

Se recomienda que se realice una evaluación exhaustiva a través de cuadros de mando tales como el balance scorecard para la medición de objetivos, con lo cual se podrá tener una situación real.

Considerando la necesidad de llevar a cabo planes estratégicos y se busca una solución integral se plantea optar por un Gobierno de Tecnologías de Información, pues por medio de esta solución se puede emplear principios para diseñar un SGSI e incluso adoptar buenas prácticas de ITIL por medio de sus procesos habilitadores.

Gestión y Capacidad

Tras la elección de implementar un sistema de gobierno de tecnologías de información, se elabora el plan de supervisión de la inversión. Al ser esta una solución que compromete a la alta dirección, se debe definir el asignar un rol de supervisor y establecer mecanismos de control para velar por la inversión realizada, y a través de métricas e indicadores verificar los resultados. Es posible emplear el balanced scorecard propuesto en COBIT 5.0 y evaluar la perspectiva financiera.

Finalmente, para medir el rendimiento de la inversión realizada y del proyecto en general, se puede complementar la parte de la visualización de resultados junto con el mapeo de fases propuesto por COBIT 5.0 y aplicar métricas e indicadores para la

medición y desempeño de los procesos. Se puede optar también por emplear el cuadro de mando (balanced scorecard).

El detalle completo de esta sección se puede contemplar en el **anexo C**, en el cual se mencionan todos los aspectos que indica la guía empleada para la elaboración del presente caso de negocio que van más allá de la inversión y su gestión.

3.2 Conclusiones del capítulo

- Se concluye que este resultado muestra a nivel estratégico cómo manejar la inversión ante una serie de proyectos y posibles soluciones ante una problemática, tomando en cuenta varios aspectos, siendo uno de los más importantes la inversión y cumplimiento de las necesidades y obligaciones de una organización.

- Para el caso de las empresas prestadoras de servicios de salud, en particular la empresa modelo, existen leyes a cumplir como parte de su problemática, lo cual junto con sus objetivos y necesidades conllevan a la elección de una solución integradora como el Gobierno de Tecnologías de Información, la cual se muestra frente a las otras opciones viables como la que aplica directamente al contexto y a partir de la cual se desprenderán otras oportunidades de mejora. El marco a emplear para esta solución será COBIT 5.0, tras los beneficios señalados en la fase gestión y capacidad del business case presentado.

- Se señala que la evaluación presupuestal es una referencia de costos del mercado tentativo debido a que el trabajo con costos e inversión aceptados por la empresa de referencia debe ser previamente validado y ajustado a la realidad y capacidad de inversión, igualmente con otras empresas de este rubro.

Capítulo 4. Análisis de la Organización

En el presente capítulo, se elabora el segundo resultado esperado, en este caso el Mapeo de las fases de gobierno de TI teniendo como base lo esperado y los resultados de la Case de la clínica en el cual se muestra las oportunidades viables para las empresas prestadoras de servicios de salud. En este caso particular adoptando la realidad de una clínica de nuestro país.

Este mapeo de fases se realiza por etapas, es decir según las etapas iniciales dentro del ciclo de gobierno de TI considerando cada uno de sus anillos, la gestión del programa, habilitar el cambio dentro de la organización y la mejora continua.

4.1 Mapeo de fases de Gobierno de TI

Se realiza la identificación del estado organizacional dentro de cada una de las fases propuestas en COBIT 5.0 durante la iniciativa, ejecución y posterior al programa de gobierno de TI. Junto con el comité estratégico, del cual depende esta iniciativa, se realiza este análisis.

Se propone una estructura que represente el mapeo de cada una de las siete fases descritas en el marco teórico, la cual se observa en detalle en el **anexo D**, el cual muestra el camino y las actividades que se siguen durante el ciclo de vida de gobierno de TI para una organización específica.

4.2 Conclusiones del capítulo

- El mapeo de fases se realiza de forma conjunta con el desarrollo de cada una de las iteraciones del ciclo de vida de gobierno de TI. Inicialmente para implementaciones y consultorías reales una iteración dura entre cuatro (4) o seis (6) meses según los recursos de la organización y el trabajo conjunto con el personal y la resistencia al cambio. Para estos fines, las iteraciones duran aproximadamente entre una (1) y dos (2) semanas, acortando cada fase y limitando el alcance solo a un diseño bajo un único enfoque, más no una implementación real.

- No todos los entregables del gobierno de TI forman parte del proyecto de tesis, esto se debe a que al ser de fines académicos se deben realizar los ajustes pertinentes y tomar como escenario para el mapeo de fases del diseño, cuyo resultado final son las políticas documentadas, más no la evidencia de su implementación en la organización.

- Se verifica que las organizaciones son resistentes a los cambios organizacionales que puedan implicar una mayor responsabilidad, lo cual tiene como consecuencia no poder mapear ni materializar todos los objetivos planteados inicialmente en una única iteración y revisión del gobierno de TI.

- En este caso de la empresa referencia, se logra materializar beneficios, pero no son los ideales respecto al alcance y la necesidad de un gobierno bajo seguridad de información, debido a la falta de roles implementados y formalización de estrategias de seguridad, lo cual en efecto ser verá soportado por el programa y en las próximas iteraciones en las cuales el beneficio de acuerdo a las actividades y alcance identificado, será más substancial y alineado su entorno, producto de la gestión del marco, sus habilitadores e impulsadores de la iniciativa.

Capítulo 5. Identificación de objetivos e indicadores

En el presente capítulo se desarrolla el mapeo de los objetivos de la organización con su respectiva adaptación al marco de control COBIT 5.0, de forma que pueda aplicarse la cascada de objetivos para determinar los objetivos de TI relacionados y posteriormente los procesos habilitadores alineados al enfoque seleccionado.

El marco también propone las métricas para que se puedan medir periódicamente por medio de un cuadro de mando y sus cuatro (4) perspectivas.

5.1 Objetivos Organizacionales mapeados con objetivos de negocio COBIT 5.0

Objetivos de la empresa[21]

OBJETIVO A: Ofrecer a los pacientes seguridad y una mejor experiencia dentro de su estancia en la clínica.

OBJETIVO B: Lograr la expansión estratégica de la organización.

OBJETIVO C: Lograr ser reconocidos por la excelencia en la atención.

OBJETIVO D: Lograr la eficiencia en los procesos garantizando la seguridad al paciente.

OBJETIVO E: Contar con un equipo de calidad y altamente capacitado.

OBJETIVO F: Cumplir con las regulaciones existentes.

[21] En el **anexo A** se muestra que la empresa colaboró para la identificación de estos objetivos.

Realizando el mapeo con la lista de objetivos propuestos por COBIT 5.0 se logra la adaptación a los siguientes objetivos:

Objetivos Empresa	Objetivos de COBIT 5.0
OBJETIVO A	Operaciones y personal productivo
OBJETIVO B	Portafolio de productos y servicios competitivos.
OBJETIVO C	Cultura de servicio orientada al cliente.
OBJETIVO D	Optimización de las funcionalidades de los procesos de negocio.
OBJETIVO E	Personal motivado y capacitado
OBJETIVO F	Cumplimiento con leyes y regulaciones externas.

Tabla 5.1.1 - Correspondencia entre objetivos reales de negocio y objetivos propuestos por COBIT

5.1.1 Justificación del mapeo

La descripción y justificación de la elección del mapeo se encuentra en el **anexo E.** A continuación se muestra el cuadro resumen con los objetivos seleccionados como parte de la cascada de objetivos de COBIT 5.

Perspectiva	Objetivos	Relación con los objetivos de gobierno		
		Materialización de beneficios	Optimización de riesgos	Optimización de recursos
Financiera	Portafolio de productos y servicios competitivos	**P**	**P**	**S**
	Cumplimiento con leyes y regulaciones externas.		**P**	
Cliente	Cultura de servicio orientada al cliente.	**P**		**S**
Proceso Interno	Optimización de las funcionalidades de los procesos de negocio.	**P**		**P**
	Operaciones y personal productivo	**P**		**P**
Aprendizaje y crecimiento	Personal motivado y capacitado	**S**	**P**	**P**

Tabla 5.1.2 - Objetivos de negocio y su relación con objetivos de gobierno

5.2 Objetivos de TI identificados a partir de la cascada de objetivos

Empleando la cascada de objetivos propuesta por COBIT 5.0 se tiene por cada objetivo una relación principal (“P”) y una relación secundaria (“S”) con los siguientes objetivos de TI:

El detalle del mapeo para cada objetivo organizacional identificado se muestra en el **anexo D** del documento.

5.2.1 Justificación de Objetivos de TI identificados

Para el cumplimiento de los objetivos organizacionales planteados y alineados al marco de gobierno COBIT 5.0 en resumen se identifican los siguientes objetivos de TI, cuya justificación se muestra en detalle en el **anexo E**, la cual se ajusta a las necesidades reales de la empresa para posteriormente identificar las métricas y procesos habilitadores según el enfoque de seguridad de información.

Perspectiva	Objetivos de TI
Financiera	Alineamiento de las tecnologías y estrategia de negocio
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	Cumplimiento de TI y soporte para el cumplimiento empresarial de las leyes y regulaciones externas
	Materializar beneficios de TI habilitando la inversión y portafolios de servicio
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio
	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Proceso interno	Seguridad de Información, infraestructura de procesamiento y aplicaciones
	Optimización de activos, recursos y capacidades de las TI
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales
	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	Personal de Negocio y TI competente y motivado
	Conocimiento, experiencia e iniciativa para la innovación empresarial

Tabla 5.2.1 - Objetivos de TI de la organización

5.3 Indicadores relacionados

Se identifican para cada uno de los objetivos organizacionales y objetivos de TI las métricas o indicadores para verificar el cumplimiento y porcentaje alcanzado de cada uno de éstos. Para esto se emplea lo propuesto por el marco de gobierno COBIT 5.0.

Para mayor detalle de esta tabla identificada ver el **anexo E.**

5.4 Cuadro de mando propuesto

A continuación se presenta el balanced scorecard propuesto para la empresa en relación a los objetivos organizacionales planteados y posteriormente el balanced scorecard de TI. Ambos parten de la cascada de objetivos de COBIT 5.0. Se emplea el estándar para la presentación del cuadro de mando.

La empresa escogerá los periodos para evaluar cada una de estas métricas y establecer el porcentaje deseado en cada uno de estos periodos, incluyendo los umbrales para identificar patrones de comportamiento según cada uno de los procesos de negocio, TI y las acciones del personal involucrado en la organización según los roles propuestos. El periodo pactado es de **cuatro (4) meses** para tener un registro cuatrimestral sobre el logro y alcance de objetivos.

Balanced Scorecard Organizacional y de TI

	Objetivo	Métrica	Per. 1	Per. 2
Financiera	Portafolio de productos y servicios competitivos.	Porcentaje de productos y servicios que alcanzan o exceden los objetivos de ingreso y/o cuota de mercado		
		Porcentaje de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente.		
		Porcentaje de productos y servicios que proporcionan ventajas competitivas		
	Cumplimiento con leyes y regulaciones externas.	Costo de incumplimientos regulatorios incluyendo acuerdos y sanciones		
		Número de incumplimientos regulatorios causantes de comentarios públicos o publicidad negativa		
		Número de incumplimientos regulatorios en relación con acuerdos contractuales con socios de negocios		
Cliente	Cultura de servicio orientada al cliente.	Número de interrupciones del servicio al cliente debidos a incidentes relacionados con el servicio TI (fiabilidad)		
		Porcentaje de stakeholders que se encuentran satisfechos con que la entrega del servicio de cliente cumpla con los niveles acordados		
		Número de quejas de clientes		
Proceso Interno	Optimización de las funcionalidades de los procesos de negocio.	Frecuencia de las evaluaciones de madurez de la capacidad de los procesos de negocio		
		Niveles de satisfacción del Consejo de Administración y la alta dirección con las capacidades de los procesos de negocio		

	Operaciones y personal productivo	Número de programas/proyectos en tiempo y presupuesto		
		Niveles de costo y de personal comparados al benchmarking		
Aprendizaje y crecimiento	Personal motivado y capacitado	Nivel de satisfacción de los stakeholders con la experiencia y capacidades del personal		
		Porcentaje de personal cuya capacidad es insuficiente para la competencia requerida por su rol		
		Porcentaje de personal satisfecho		

Tabla 5.4.1 - Balanced Scorecard Organizacional

	Objetivo	Métrica	Per. 1	Per. 2
Financiera	Alineamiento de las tecnologías y estrategia de negocio	Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas estratégicas de TI		
		Nivel de satisfacción de los stakeholders con el alcance del portafolio de programas y servicios planificados		
		Porcentaje de factores de valor de TI mapeados a factores de valor del negocio		
	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Porcentaje de roles de la dirección ejecutiva con responsabilidad definida en decisiones TI		
		Frecuencia de reuniones del comité ejecutivo de estrategia de TI		
		Tasa de ejecución de decisiones TI por parte de la alta dirección.		
	Cumplimiento de TI y soporte para el cumplimiento	Costo de incumplimientos de TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación		
		Número de incumplimientos de TI reportados al Consejo de Administración o causantes de		

	empresarial de las leyes y regulaciones externas	comentarios o vergüenza pública		
		Número de incumplimientos relacionados con proveedores de servicios de TI		
	Materializar beneficios de TI habilitando la inversión y portafolios de servicio	Porcentaje de servicios de TI donde se obtienen los beneficios esperados		
		Porcentaje de inversiones de TI donde se cumplen o exceden los beneficios esperados		
Cliente	Entregar servicios de TI alineados con los requerimientos de negocio	Número de interrupciones de negocio debidas a incidentes de servicios de TI		
		Porcentaje de stakeholders satisfechos de que la entrega de servicios de TI cumpla los niveles de servicio acordados		
		Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios de TI		
	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios de TI		
		Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos		
		Valor presente neto (VPN) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas		
Proceso Interno	Seguridad de Información, infraestructura de procesamiento y aplicaciones	Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública		
		Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados		
		Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías		
	Optimización de activos,	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costos		

	recursos y capacidades de las TI	Niveles de satisfacción de la alta dirección y de la división de TI con los costos y capacidades TI		
	Capacitación y soporte de procesos de negocio a través de la integración de aplicaciones y tecnología en los procesos empresariales	Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología		
		Número de programas de negocio facilitados por TI retrasados o incurriendo en costos adicionales debido a problemas de integración de la tecnología		
		Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas		
	Cumplimiento de las políticas internas por parte de las TI	Número de incidentes relacionados con el incumplimiento de políticas		
		Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas		
		Frecuencia de revisión y actualización de políticas		
Aprendizaje y crecimiento	Personal de Negocio y TI competente y motivado	Porcentaje de personal cuyas habilidades de TI son suficientes para la competencia requerida por sus roles		
		Porcentaje de personal satisfecho con sus roles en TI		
		Número de horas de aprendizaje/formación por miembro del personal		
	Conocimiento, experiencia e iniciativa para la innovación empresarial	Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de Innovación de TI		
		Nivel de satisfacción de los stakeholders con los niveles de experiencia e ideas de innovación de TI		
		Número de iniciativas aprobadas resultantes de ideas de TI innovadoras		

Tabla 5.4.2 - Balanced Scorecard de TI

5.5 Conclusiones del capítulo

- Se concluye que todos los objetivos corporativos de la organización son mapeados en mayor grado o totalmente por los objetivos de negocio planteados en el marco COBIT 5.0 bajo el método de la cascada de objetivos, permitiendo en consecuencia la identificación de los objetivos de Tecnología de Información, lo cual garantiza el alineamiento estratégico entre objetivos de negocio y objetivos de TI.

- Se identifican las métricas o indicadores para la medición de los objetivos planteados que permitan corroborar la eficiencia y alcance de metas de la organización por medio de la entrega de valor, satisfacción de clientes y/o stakeholders, procesos internos y aprendizaje y crecimiento, descendiendo por tanto en un cuadro de mando tanto como para los objetivos organizacionales como para los objetivos de TI.

- Es viable plantear algunas otras métricas considerando las necesidades de negocio y lo que el comité estratégico considere prudente, sin olvidar las pautas del marco de gobierno en cuanto al alineamiento estratégico, pues este solo sirve de guía para crear un modelo inicial que se irá fortaleciendo a medida de cada una de sus iteraciones y la cantidad de enfoques y procesos involucrados.

- En resumen se tienen dieciséis (16) métricas para objetivos organizacionales de las cincuenta y cuatro (54) propuestas por COBIT 5.0 y treinta y cuatro (34) métricas para objetivos de TI de las cincuenta y nueve (59) propuestas, debido al número de objetivos organizacionales y de TI mapeados - seis y doce respectivamente - y a la acotación para el negocio de empresas prestadoras de servicios de salud, específicamente para la empresa modelo.

- Cada una de estos objetivos de TI serán empleados para descender a los procesos habilitadores de COBIT 5.0 según el enfoque de seguridad de información, para que este último ayude a alcanzar los mencionados objetivos y en consecuencia los objetivos de negocio, lo cual se evidenciará en los resultados de la evaluación de las métricas propuestas.

Capítulo 6. Análisis procesos de COBIT 5.0 a aplicar a la organización.

En el presente capítulo se muestra la última parte de la cascada de objetivos planteada por COBIT para descender a los procesos habilitadores.

Para esto, según la cascada de objetivos, para cada objetivo de TI se identifican los habilitadores respectivos y se analiza su aplicabilidad en la empresa. Posterior al análisis y la justificación, se aborda el enfoque de seguridad de información analizando los objetivos de TI y también los habilitadores cuya fuente es seguridad de información y gestión de riesgo para cada uno de los dominios presentados.

6.1 Aplicación de procesos habilitadores

Se procede a identificar por cada uno de los objetivos de TI planteados, empleando la cascada de objetivos, los procesos habilitadores que conllevan a su cumplimiento. Se consideran la relación principal (“P”) y secundaria (“S”). Para detalle de este mapeo consultar el **anexo F** del presente documento.

6.1.1 Justificación de procesos habilitadores

Dentro de la organización se debe tomar en cuenta únicamente aquellos procesos habilitadores que correspondan con la línea de negocio y con su situación, en otras palabras su entorno actual, regulaciones a las cuales están sujetos y hacia dónde se quiera llegar según el plan estratégico vigente y sus planes de TI. Estos procesos y su justificación se puede consultar en el **anexo F**.

6.2 COBIT 5.0 y la seguridad de información

A partir de la identificación de todos los procesos habilitadores, cuya aplicación garantizará el cumplimiento de los objetivos de TI y los organizacionales, se retoma el enfoque de seguridad de información tomando en cuenta: Ley de protección de datos personales, Norma técnica peruana de historias clínicas. No obstante, para este proyecto sigue los lineamientos del acta Hipaa a nivel internacional y lo contemplado por las normas ISO 27001 e ISO 27002, tomando en cuenta que para este caso particular, no existe alguna regulación que exija su cumplimiento y aplicación.

Para estos fines se priorizan objetivos y procesos habilitadores relacionados con la seguridad de información. En el **anexo F** se señala los objetivos de TI con relación directa a la seguridad de Información. Finalmente se realiza mapeo final según el enfoque. Esta se ve complementada con el análisis a partir de todos los procesos habilitadores con aplicación dentro de la organización teniendo como resultado:

Dominio	Proceso Habilitador – Enfoque seguridad de información
Evaluar, Dirigir y Monitorear	Garantizar el mantenimiento y configuración del marco de control de gobierno
	Garantizar la entrega de beneficios
	Garantizar la optimización de riesgos
Alinear, Planear y Organizar	Gestionar el marco de control de TI
	Gestionar la estrategia
	Gestionar los recursos humanos
	Gestionar el riesgo
	Gestionar la seguridad
Construir, adquirir e implementar	Gestionar programas y proyectos
	Gestionar el cambio
	Gestionar los activos
Entregar, dar servicio y soporte	Gestionar solicitudes de servicios e incidentes
	Gestionar la continuidad
	Gestionar los servicios de seguridad
Monitorear, evaluar y asegurar	Monitorear, evaluar y medir el rendimiento y la conformidad
	Monitorear, evaluar y medir el cumplimiento de los requerimientos externos

Tabla 6.2.1 - Aplicación de procesos habilitadores según enfoque seguridad de información

6.2.1 Justificación de los procesos habilitadores

Para cada uno de los procesos habilitadores seleccionados se plantea una justificación de su elección tomando en cuenta que se realizará la adaptación para la seguridad de información, la cual se puede verificar en su totalidad en el **anexo F** y a partir del análisis de cada uno de estos objetivos identificados previamente y sus respectivas actividades nacerán las políticas y roles a implantar en la organización tomando como base los procesos escogidos para su optimización según el enfoque.

6.3 Conclusiones del capítulo

- La evaluación de procesos habilitadores que aplican para la organización demuestra que el marco seleccionado tiene un comportamiento holístico capaz de cubrir todas las necesidades de la organización en mayor o menor medida y que a su vez puede complementarse con otros marcos. Para este particular se determina, sin tomar en cuenta el enfoque, treinta y un (31) procesos de COBIT 5.0 de los treinta y siete (37) planteados en dicho marco.

- La evaluación de procesos habilitadores puede ser realizada nuevamente en cada iteración para determinar si aplica o deja de aplicar alguno de los procesos en mayor o menor grado según las necesidades y cambios a nivel organizacional y/o del entorno de las empresas prestadoras de servicios de salud.

- Se identifican dieciséis (16) procesos habilitadores para el enfoque de seguridad de información los cuales pueden incrementarse o disminuirse según la evaluación de las respuestas a corto plazo del programa de gobierno o de lo contrario se pueden sumar nuevas métricas que refuercen la importancia y justifiquen la elección de estos procesos.

- Al incluir nuevos enfoques al programa de gobierno, por ejemplo un enfoque en gestión de recursos o servicios de TI, se incluirán nuevos procesos habilitadores y los considerados según la seguridad de información deberán ser analizados para determinar el grado de aplicación para el nuevo enfoque de manera que para la elaboración de las políticas de TI y roles organizacionales se vuelva a realizar el análisis de cada una de sus actividades con otra perspectiva que complementa a lo logrado anteriormente.

Capítulo 7. Identificación y Diseño de procesos AS-IS

En el presente capítulo se muestra el diagrama de los procesos identificados dentro de la empresa, los cuales serán la base del gobierno de TI y al cual se le aplicarán los procesos habilitadores para determinar roles y políticas de seguridad de información.

Los procesos presentados se encontraron en un nivel de madurez cero (0) y a través del levantamiento de información serán completados para poder conducirlos a un nivel superior según la ISO/IEC 15504, lo cual es lo esperado por la organización según el mapeo de fases de gobierno de TI realizado como parte de los logros a corto plazo.

7.1 Justificación de los procesos empresariales

Para este modelo de gobierno se empleará un macro-proceso hospitalario. Este incluye admisión, atención y egreso del paciente. Adicionalmente se considera el proceso de identificación. La conformidad de la empresa respecto al modelado de procesos se muestra en el **anexo H**.

La elección de estos procesos se debe a que en ellos se manejan documentos reglamentados como historias clínicas y otros relevantes como los resultados de análisis de los paciente que incluyen datos que deben ser protegidos íntegramente como parte del cumplimiento de la ley 29733 y para conseguir el logro de sus objetivos organizacionales.

7.2 Proceso: Admisión de pacientes (Indicar hospitalización)

A continuación se presenta el diagrama para el proceso de admisión, iniciado por un requerimiento externo y por medio del cual, según la necesidad y tipo de atención descenderá a otros sub-procesos hasta admitir al paciente y proceder con el internamiento y el proceso de atención.

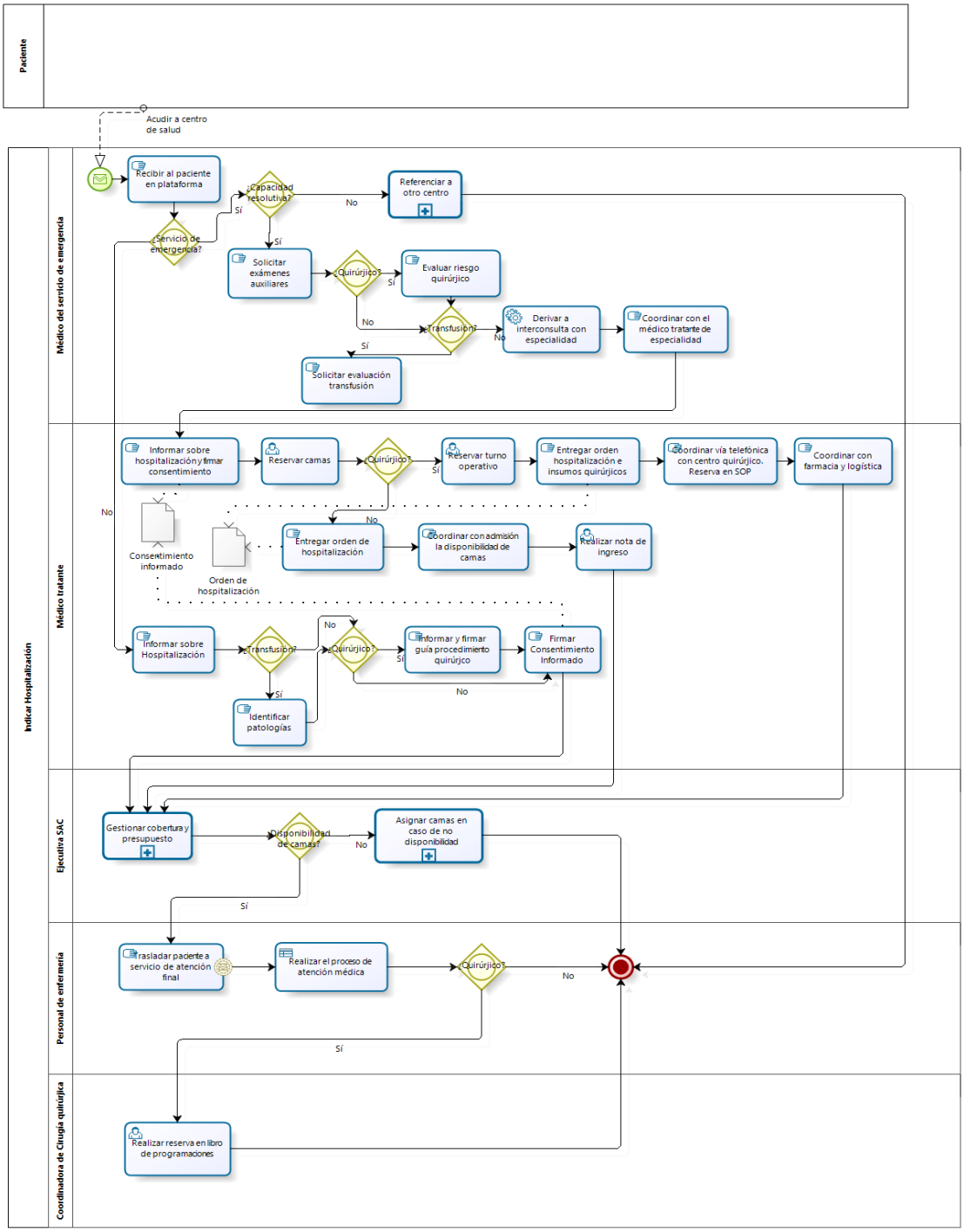


Figura 7.2.1 - Diagrama del proceso de admisión de pacientes

El detalle de sus sub-procesos relacionados se puede consultar en el **anexo G.**

7.3 Proceso: Atención del paciente hospitalizado

El presente proceso es parte del macro proceso hospitalario, en este se detalla cómo se brinda la atención al paciente y como planifican los recursos dentro de cada turno. Así mismo, se definen las condiciones de salida que determina si continúa con el proceso de alta del paciente o a otros procesos como transferencia o defunción.

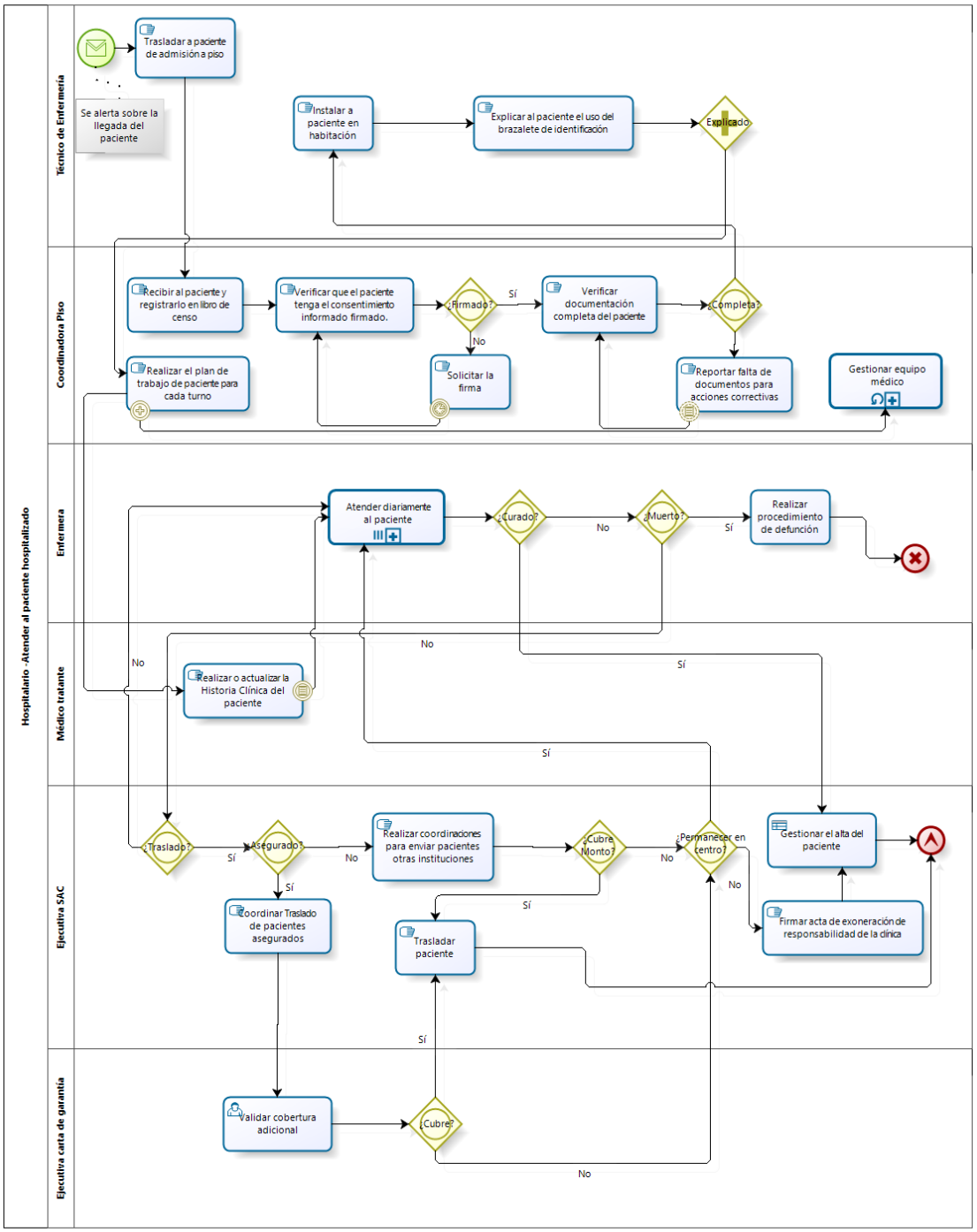


Figura 7.3.1 - Diagrama del proceso atención al paciente hospitalizado

El detalle de sus sub-procesos relacionados se puede consultar en el **anexo G.**

7.4 Proceso: Egreso del paciente hospitalizado

Este proceso detalla el alta del paciente según sus condiciones de salida, es decir, en caso este recuperado o no recuperado, incluso las condiciones bajo las cuales se realiza los trámites para la trasferencia a otro centro de referencia.

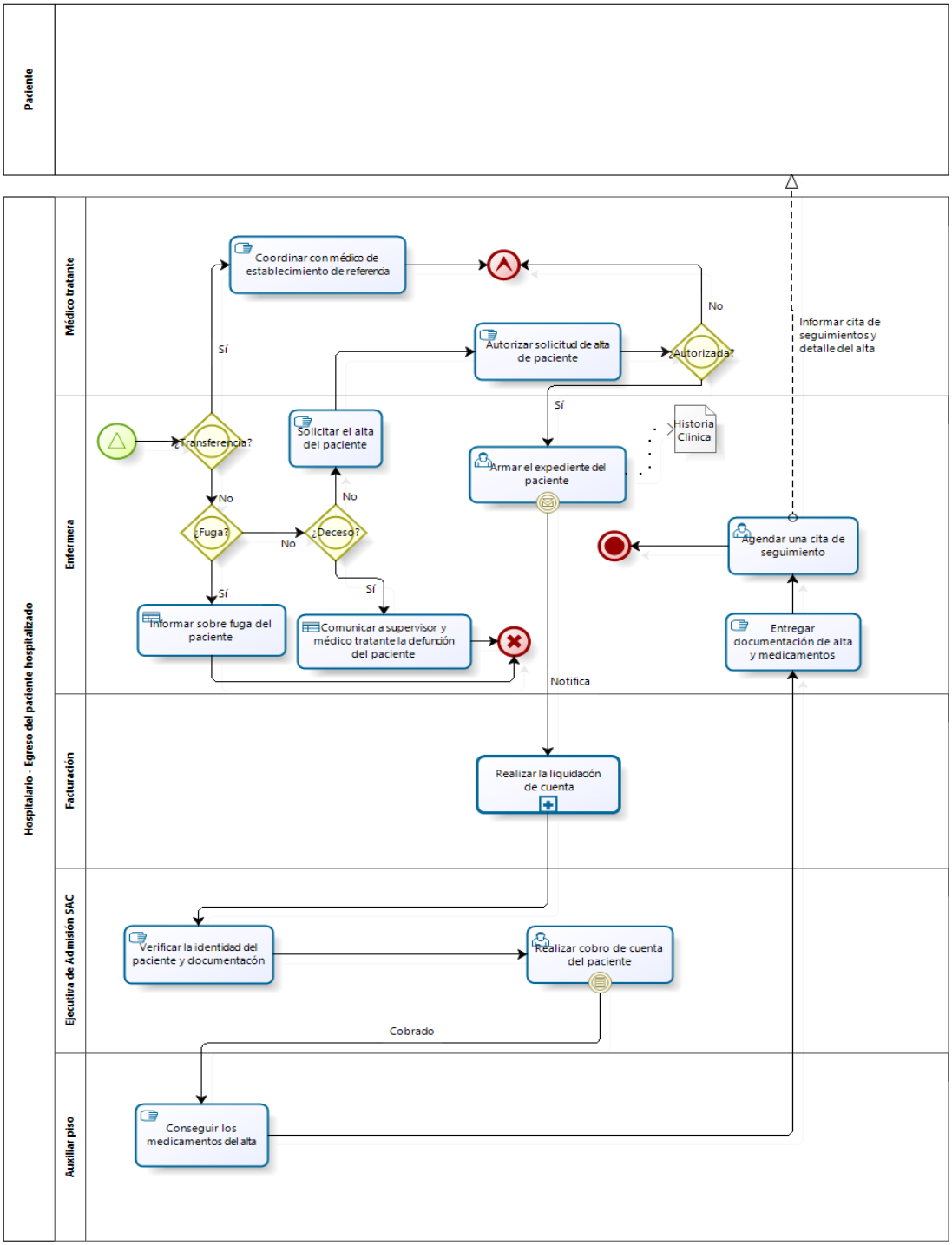


Figura 7.4.1 - Diagrama del proceso Egreso del paciente hospitalizado

El detalle de sus sub-procesos relacionados se puede consultar en el **anexo G.**

7.5 Proceso: Identificación del paciente hospitalizado

Este proceso se encuentra fuera del macro proceso hospitalario, no obstante se considera debido a que es transversal a los procesos que lo comprenden y detalla las políticas a seguir durante la estancia del paciente para verificar sus datos personales y el detalle de la historia clínica.

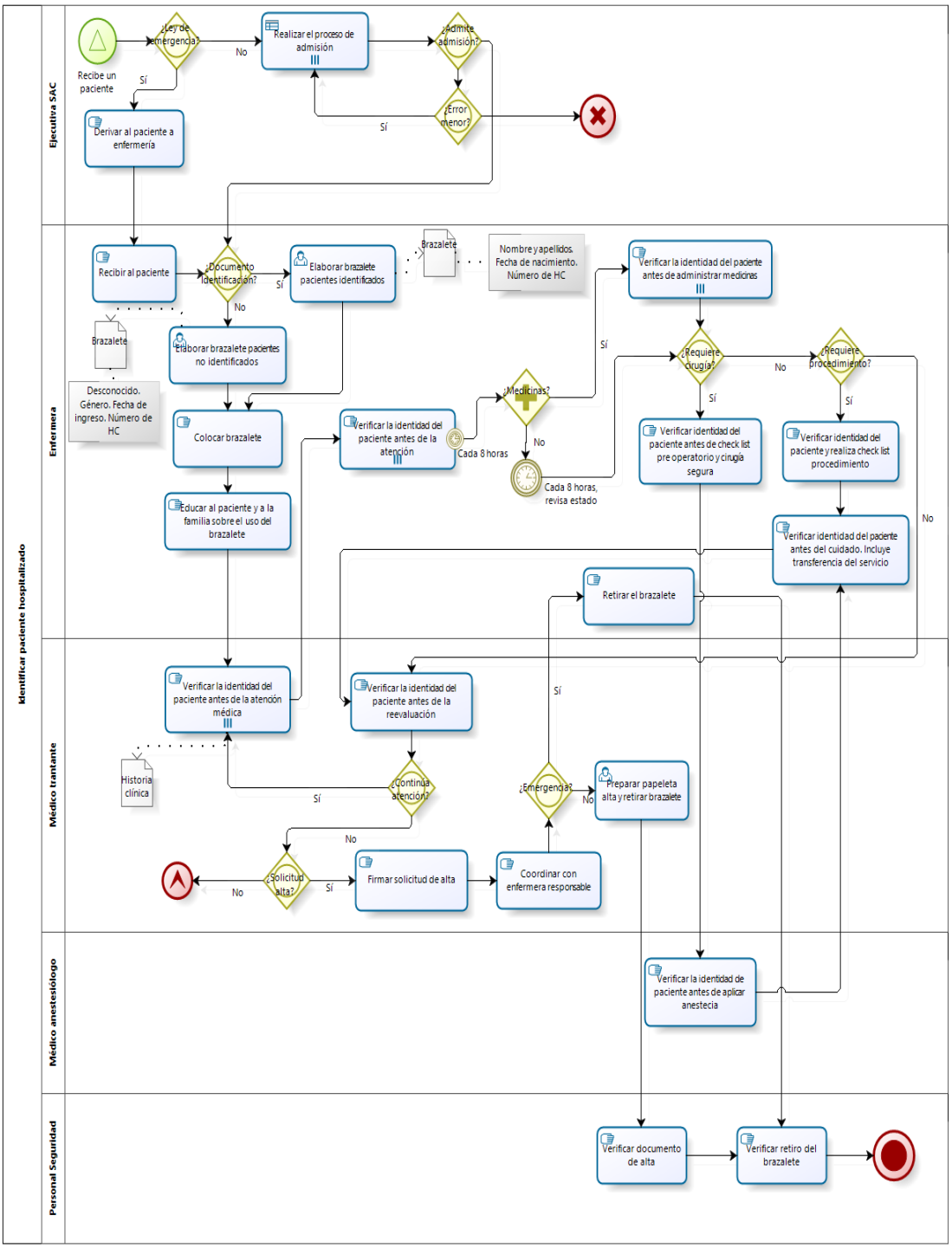


Figura 7.5.1 - Diagrama del proceso Identificación del paciente hospitalizado

7.6 Conclusiones del Capítulo

- La selección de los procesos es una de las bases del modelo de gobierno de TI, debido a que permite conocer el estado actual de la organización, para dicho enfoque, y el nivel de madurez del proceso, lo cual valida el alcance real del proyecto y se puede realizar el ajuste para cada una de las iteraciones del ciclo de vida, de manera que se puedan conseguir los logros inmediatos.

- Los procesos seleccionados, tal como se mencionó dentro del mapeo de fases, se encontraban en un nivel de madurez cero (0). No obstante, al haberlos completado se concluye que el nivel de madurez según la norma ISO/IEC 15504 es uno (1).

- Se valida el modelado de procesos en la notación BPMN 2.0 por parte de la empresa modelo para el proyecto, por lo tanto, junto con el comité estratégico, considerando que ahora el nivel de madurez es uno (1), se materializa el primer logro inmediato.

- En caso se decida ampliar el alcance del proyecto, es decir contemplar otros procesos, se deberá tener en cuenta que éstos deben ser mapeados y relacionados con el mapa actual presentado, lo cual implica que los otros procesos deben también ser adaptados a esta notación y ser validados por los dueños del proceso, para posteriormente definir su nivel de madurez.

- Respecto a considerar otros enfoques para este mismo juego de procesos, se deberá realizar el análisis previo para posteriormente realizar la identificación de políticas de TI adicionales a las del enfoque de seguridad de información.

Capítulo 8. Políticas de seguridad de información y roles para los procesos habilitadores

En el presente capítulo se presentan las políticas de seguridad de información que se desprenden del análisis realizado para los procesos que forma parte del alcance del modelo de gobierno de TI en base a los procesos habilitadores identificados. Para cada proceso habilitador propuesto por COBIT 5.0, se procederá a hallar el componente de seguridad de información con ayuda de COBIT 5.0 para seguridad de información.

Finalmente para cada uno de los procesos habilitadores y sus actividades, se propone un esquema de roles a considerarse como parte de esta iniciativa por medio de una matriz RACI especifica de acuerdo a la organización.

8.1 Actividades de gestión COBIT 5.0 bajo el enfoque de seguridad de Información

A continuación se presenta las actividades de gestión para los cuatro (4) procesos seleccionados y diseñados bajo la notación BPMN 2.0. Para su identificación, tal como se señala, se procede a analizar la viabilidad de aplicación de las actividades propuestas por COBIT 5.0 para cada proceso habilitador que aplican para el enfoque de seguridad de información.

Identificando las sub-actividades para cumplir la actividad de gestión, se elabora la matriz RACI de acuerdo al enfoque del gobierno y las capacidades y roles de la organización para que sean la base para adoptar políticas bajo la norma ISO/IEC 27002:2013.

En la siguiente tabla se muestra la leyenda que será útil para la lectura de la matriz de responsabilidades que se presentarán para cada uno de los procesos habilitadores.

Leyenda	Descripción
R	Responsable
A	Accountable
C	Consulted
I	Informated
(*)	Rol no implementado o ejercido dentro de la organización

Tabla 8.1.1 - Leyenda para lectura de matriz RACI

8.1.1 Procesos habilitadores en común para los procesos de la empresa

Para cada uno de los procesos seleccionado se ha realizado un análisis y se determina que pese a los cambios o mejoras futuras a nivel de procesos, las actividades a aplicar para el cumplimiento de los habilitadores no presentan variaciones, por lo cual se puede emplear la misma matriz y adoptar las mismas políticas de TI y seguridad de información.

Se presentan algunos de los procesos habilitadores en común:

a. <u>Proceso habilitador: Garantizar el mantenimiento y configuración del marco de control de gobierno</u>

Se verifica la aplicación de todas las actividades de gestión, no obstante se señala que no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y el nivel de madurez al cual se pretenda y sea viable llegar luego de cada iteración.
Luego se procede a elaborar la matriz de responsabilidades para gestionar el habilitador según el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar el sistema de gobierno	Analizar e identificar los factores de entorno interno y externo relacionados a la seguridad de información, los cuales afectan directamente al proceso, junto con las tendencias en el negocio que puedan influir en el diseño del gobierno.
	Evaluar el nivel de la seguridad de información dentro del negocio y el cumplimiento con regulaciones externas[22] dentro del proceso. Entre estas se tiene: Ley de protección de datos personales, Ley de emergencia y la norma técnica peruana de la historia clínica.
	Articular los principios que guiarán el diseño óptimo del modelo de toma de decisiones sobre el gobierno de TI y su enfoque a la seguridad de información.
	Considerar cómo serán aplicadas o enfocadas la ley de protección de datos personales, la ley de emergencia y la norma técnica peruana de la historia clínica en el gobierno de TI de la empresa y en los procesos base.
Dirigir el sistema de gobierno	Exigir la función de seguridad de información para toda la empresa y como esta se aplicará a los procesos.
	Contar con un comité estratégico que esté enfocado a la seguridad de información (ISSC)
	Alinear la estrategia de seguridad de información con la estrategia empresarial
	Obtener el compromiso de la alta dirección para verificar la seguridad de información y la gestión de riesgos de información.
	Asignar responsabilidad para que se apliquen principios de gobierno, modelos de toma de decisión acordados.
Monitorear el sistema de gobierno	Supervisar mecanismos para asegurar que los sistemas para medir el desempeño de seguridad de información cumplen con la ley de protección de datos personales y la norma técnica peruana de historia clínica.
	Proporcionar supervisión de la efectividad y el cumplimiento con el sistema de control de la empresa.

[22] Se consideran únicamente las regulaciones para el proceso.

	Evaluar la efectividad y rendimiento de los stakeholders en los que se ha delegado responsabilidad y autoridad para el gobierno de TI de la empresa.

Tabla 8.1.2 - Actividades de gestión para el habilitador Garantizar el mantenimiento y configuración del marco de control de gobierno

Matriz de responsabilidades (RACI)

EDM01: Garantizar el mantenimiento y configuración del marco de control de gobierno																			
	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe de proyectos	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas[23]	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar el sistema de gobierno	A	R	C	C	R	C	R			C	R	C	C	I	R		C		C	
Dirigir el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	C	I	I	C	R	I	I	I	I	I
Monitorear el sistema de gobierno	A	R	C	C	R	I	R	I	I	C	C	I	I	C	R	I	I	I	I	I

Tabla 8.1.3 - Matriz de responsabilidades para el proceso habilitador EDM01

b. Proceso habilitador: Garantizar la entrega de beneficios

Se verifica la aplicación de todas las actividades de gestión, no obstante se señala que no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y la gestión de sus inversiones. Adicionalmente se la matriz de responsabilidades destacando las acciones del oficial de seguridad de información.

[23] El administrador de plataformas en este caso realiza la gestión de tecnologías a gran nivel incluyendo los sistemas que comprende el proceso. En caso se deba de recurrir al desarrollador del sistema, lo reporta y asume la responsabilidad frente a la solución de algún incidente.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar la optimización del valor	Identificar y registrar los requisitos de los stakeholders en relación con los procesos base para la protección de sus intereses y la entrega de valor tomando en cuenta los parámetros de seguridad de información. Establecer la dirección respectiva.
	Comprender y discutir periódicamente sobre las oportunidades que pueden surgir a partir de los cambios dentro de los procesos base al emplear tecnologías actuales y optimizar el valor de estas oportunidades.
	Comprender el significado del valor en la empresa y como se ha comunicado, entendido y aplicado a través de los procesos de la organización.
	Evaluar la efectividad de la integración y alineamiento de las estrategias de TI y seguridad de información en la empresa con los objetivos para aportar valor, así como la alineación de estos últimos con el portafolio de inversiones
Dirigir la optimización del valor	Asegurar que se empleen medidas financieras y no financieras para describir el valor añadido de las iniciativas de seguridad de información en los procesos base.
	Establecer un método para demostrar el valor de la seguridad de información para garantizar el uso eficiente (considerando los niveles de seguridad) de los activos dentro de los procesos identificados.
	Dirigir los cambios necesarios en el portafolio de inversiones y servicios para realinearlos con los objetivos actuales, los esperados y/o sus limitaciones.
	Dirigir los cambios necesarios en asignación de imputaciones y responsabilidades del portafolio de inversión y entrega de valor a partir de los servicios y procesos de negocio enfocados a la seguridad de información.
Monitorear la optimización del valor	Monitorear el resultado de las iniciativas de seguridad de información frente a las expectativas para asegurar la

	entrega de valor de acuerdo a los objetivos de negocio
	Definir objetivos de desempeño, métricas, metas y puntos de referencia. Revisarlos y formalizarlo junto con los stakeholders.
	Tomar medidas de gestión para asegurar la optimización del valor. En caso sean medidas correctivas, asegurarse de que sean iniciadas y controladas.

Tabla 8.1.4 - Actividades de gestión para el habilitador Garantizar la entrega de beneficios

Matriz de responsabilidades (RACI)

EDM02: Garantizar la entrega de beneficios	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe de portafolio/proyecto de inversión (*)	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar optimización del valor	A	R	R	C	R		R		C	C	C	C		C	R		C		C	
Dirigir optimización del valor	A	R	R	C	R	C	R	I	I	I	C	I	I	I	R	I	I	I	I	I
Monitorear optimización valor	A	R	R	C	R		R		R	C	C	C	I	C	R	I	C			

Tabla 8.1.5 - Matriz de responsabilidades para el proceso habilitador EDM02

c. Proceso habilitador: Garantizar la optimización del riesgo

Se verifica la aplicación de todas las actividades de gestión, sin embargo, no pueden aplicarse todas las sub-actividades para su cumplimiento debido a la actividad realizada por la empresa y el tratamiento de riesgos y formalización del comité responsable.

Luego se elabora la matriz de responsabilidades para gestionar el habilitador según el enfoque de seguridad de información.

Actividades de gestión	Sub-actividades para el cumplimiento de actividad.
Evaluar la gestión de riesgos	Determinar junto con la directiva de la empresa el nivel de apetito por el riesgo.
	Medir el nivel de integración de la gestión de riesgos de seguridad de información con el modelo general de riesgos de la organización.
	Determinar el grado de alineamiento de la estrategia de riesgos de TI y seguridad de información con la estrategia de riesgos empresariales.
	Determinar si las tecnologías empleadas en los procesos base están sujetas a una evaluación de riesgos adecuada según lo descrito en estándares relevantes que pueda adoptar la organización.
Dirigir la gestión de riesgos	Integrar la gestión de riesgos de seguridad de información dentro del modelo general de riesgos.
	Dirigir la elaboración de planes de comunicación y acción de riesgos promoviendo una cultura consciente sobre estos y su impacto dentro del negocio.
	Dirigir la implantación de mecanismos apropiados para responder a los riesgos cambiantes y notificar a los niveles adecuados según el principio de escalamiento.
	Dirigir para que los riesgos de seguridad de información dentro de los procesos puedan ser identificados por cualquier persona en cualquier momento según las políticas y procedimientos publicados.
Monitorear la gestión del riesgos	Monitorear el perfil frente al riesgo o el apetito del riesgo de la empresa para lograr un equilibro óptimo entre riesgos y oportunidades de negocio
	Incluir las salidas de los procesos de gestión de riesgos de información como entradas las la gestión de riesgos de la organización.
	Comunicar los problemas de la gestión de riesgos al directorio.
	Monitorear las metas y métricas de gestión de los

	procesos de gobierno y gestión del riesgo respecto a los objetivos. Iniciar medidas correctivas para casos especiales

Tabla 8.1.6 - Actividades de gestión para el habilitador Garantizar la optimización de riesgos

Matriz de responsabilidades (RACI)

EDM03: Garantizar la optimización de riesgos	Directorio	Gerente Ejecutivo	Gerente de finanzas	Gerente de operaciones	Ejecutivos de negocio	Dueño de procesos de negocio	Comité ejecutivo estratégico	Comité estratégico (*)	Jefe del proyecto	Oficial de riesgos (*)	Oficial de seguridad de información (*)	Comité de riesgos (*)	Jefe de Recursos Humanos	Auditoría	Gerente de informática	Jefe/Administrador de plataformas	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de información (*)	Gestor de continuidad de negocio (*)
Evaluar la gestión de riesgos	A	R	C	C	R	C	R			R	R	I	C	C	R				C	
Dirigir la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	C	I	I	I	R	I	I	I	I	I
Monitorear la gestión de riesgos	A	R	C	C	R	C	R	I	I	R	R	I	C	C	R	I	I	I	I	I

Tabla 8.1.7 - Matriz de responsabilidades para el proceso habilitador EDM03

El detalle de la evaluación de aplicación de los otros habilitadores para los procesos de admisión, atención, egreso e identificación de pacientes se puede observar a detalle en el **anexo I**.

8.2 Políticas de seguridad de información para los procesos

Finalmente, teniendo identificadas las actividades de gestión y los roles para cada proceso habilitador dentro de los procesos de negocio, se procede a redactar las políticas de seguridad de información de acuerdo a una estructura que permita identificar responsables y objetivos de dicha política para que toda la organización pueda comprender las iniciativas y consultar al responsable o sugerir alguna modificación que se adecúe a los principios de gobierno de TI.

8.2.1 Aplicación a la norma ISO/IEC 27002:2013

Para la elaboración de las políticas de seguridad de información se toma en cuenta las actividades de COBIT 5.0 que han sido identificadas para cada uno de los procesos de negocio. Seguidamente se debe verificar, según estas actividades, la aplicación a la norma ISO/IEC 27001:2013 empleando la especificación de estos en la norma ISO/IEC 27002:2013.

Esta permitirá identificar lo que debe contemplar las políticas de seguridad de información para lograr la mejora de los procesos y alinearse a los objetivos de gobierno de TI de la empresa bajo este mismo enfoque. Para el detalle de la aplicación a la norma, consultar el **anexo J**.

8.2.2 Políticas de seguridad de información

Según el mapeo con la norma para identificar aspectos que debe tomar en cuenta las políticas de seguridad de información, se procede a la redacción. Para el detalle de todas las políticas de seguridad de información, consultar el **anexo K** que contiene toda la estructura.

Política de seguridad de información

Responsable: Oficial de seguridad de información

Propósito

Encaminar y dirigir la seguridad de información de acuerdo al enfoque de gobierno de TI y que estas estén alineadas a los requerimientos de negocio y a la ley de protección de datos personales, norma técnica peruana de la historia clínica y la ley de emergencia.

Alcance: Proceso de admisión, atención, egreso e identificación de pacientes

Fecha Inicio Vigencia: Enero 2014

---

1. Establecer las políticas de seguridad de información

La alta dirección proporciona actividades de acuerdo a la ejecución de sus procesos y dentro de ellas como se gestionan la tecnologías de información, por lo cual se

comprometen a preservar la confidencialidad, integridad y disponibilidad de los activos físicos y electrónico a través de las gerencias de la organización.

De acuerdo a las actividades realizadas para cada proceso, se identifican la información y requerimientos de seguridad, los cuales deben formar parte de un proceso continuo de gestión y estar alineados a los objetivos estratégicos de la organización para reducir riesgos de información al nivel de tolerancia escogido por la organización.

De acuerdo a los procesos y la declaración de aplicación de los dominios de seguridad de información para la empresa según la norma ISO/IEC 27001:2013, se obtienen los objetivos de control que comprenden las políticas de seguridad de información soportadas por los procesos base del proyecto gobierno de TI.

2. Revisar las políticas de seguridad de información

El responsable de velar por las políticas de la seguridad de información es el oficial de seguridad. Debe verificar la vigencia de éstas respecto a los aspectos de negocio y los procesos que quiera cubrir y en base a los requerimientos de seguridad de información que propone los stakeholders y que aquellos que son producto de la adecuación a una regulación o requerimiento externo. Todo el personal de la organización está obligado a cumplir con estas políticas de acuerdo a sus roles y responsabilidades dentro de los procesos de negocio y según su función.

Se debe por lo tanto diseñar un sistema y ejecutar procedimientos de revisión de las políticas, el cumplimiento y las brechas que indican el estado actual y el estado ideal al que se quiere llegar a partir de la implantación de éstas políticas.

8.3 Conclusiones del capítulo

- Se realiza la aplicación del marco de gobierno y la adaptación de las actividades de gestión de cada uno de los procesos habilitadores para los procesos seleccionados que forman parte de la iniciativa. La existencia de actividades en común dentro de los procesos producto de la redundancia de las actividades iniciales de cada proceso.

- Se determina la importancia de las funciones del oficial de seguridad de información, quien de acuerdo al enfoque de gobierno para este proyecto, debe encargarse del cumplimiento de los requerimientos de seguridad de los stakeholders y alinearlos a la estrategias para el cumplimiento de objetivos de negocio y de los procesos que forman la base del gobierno de TI.

- Se señala que las actividades de gestión, a medida alcancen cierto nivel de madurez pueden ser incrementadas según la necesidad de la empresa. Para esto se debe definir el tiempo en el cual debe revisarse el modelo de gobierno de TI, actualizarlo según los cambios en los procesos y lo esperado por la organización.

- Se realiza el ajuste de la matriz de responsabilidades de acuerdo al negocio de la empresa modelo y tomando en cuenta los roles que existen y que deberían de existir dentro de ella para un correcto seguimiento de los procesos habilitadores que forman parte de las iniciativas de gobierno de TI. La traducción frente a COBIT 5.0 no es literal, razón por la cual según el análisis del proceso de negocio y el habilitador, se realiza la asignación de responsabilidades.

- Se aplica la norma ISO/IEC 27001:2013 y la ISO/IEC 27002:2013 dando como resultado un alineamiento entre casi todos los dominios de la norma, doce (12) de dieciocho (18), lo cual indica que en efecto, las actividades seleccionadas para cada uno de los procesos habilitadores de COBIT 5.0 están enfocadas a la seguridad de información y que a partir de este marco es posible emplear estas norma para la gestión de esta función y la elaboración y gestión de políticas de seguridad.

- Las políticas de seguridad de información tienen como fecha de inicio de vigencia enero del 2014 debido a que estas son la propuesta que se realiza a la empresa y deben ser validadas y aplicadas de acuerdo a la madurez de la función de la seguridad de información dentro de ella, por lo cual se señala que éstas pueden ser modificadas, es decir eliminando políticas o añadir nuevas sin dejar de alinearse a la norma ISO/IEC 27001:2013.

Capítulo 9. Nivel de madurez de los procesos de COBIT 5.0

En el presente capítulo, como parte final del diseño del modelo de gobierno de TI, se identifica el nivel actual de madurez para cada uno de los procesos habilitadores de cada proceso de negocio que forma parte del alcance del gobierno. Para esto se emplea la norma ISO/IEC15504 la cual brindará los criterios para determinar en cuál de los seis (6) niveles se encuentra el proceso habilitador.

La mecánica para identificar el nivel de madurez consiste en evaluar el cumplimiento de las actividades de gestión para cada uno de los procesos de negocio y los procesos habilitadores. Finalmente, con esta evaluación se completa el ciclo de vida de gobierno, con lo cual se obtiene nuevos drivers u oportunidades de mejora a incluir en el modelo de gobierno, las cuales serán implementadas y revisadas continuamente para mantener el impulso y encaminar a la organización para el logro de sus objetivos.

9.1 Evaluación de nivel de madurez de los procesos habilitadores

Esta evaluación completa se puede contemplar en el **anexo L**. El estado de cumplimiento es determinado por la organización basándose en las actividades diarias, controles establecidos y el entorno del negocio antes de implementar las políticas de seguridad de información. Luego se determina el nivel de madurez deseado y el tiempo para la próxima revisión del gobierno de TI de la empresa..

En la siguiente tabla se muestra criterios de evaluación de la norma ISO/IEC 15504 y los criterios para identificar la escala de cumplimiento para cada nivel de madurez.

Leyenda	Descripción
N : "Not achieved"	No existe evidencia de la entrega o gestión del proceso habilitador. El cumplimiento de las actividades está entre cero (0) y quince (15) por ciento.
P: "Partially achieved"	Existe evidencia de la entrega de las actividades definidas para el proceso. Algunos aspectos deben ser no predecibles. El cumplimiento de las sub – actividades de gestión está entre quince (15) y cincuenta (50) por ciento.
L: "Largely achieved"	Existe evidencia sistemática y significativa sobre la entrega de y cumplimiento de actividades dentro del proceso. El cumplimiento está entre cincuenta (50) y ochenta y cinco (85) por ciento.
F: "Fully achieved"	Existe evidencia total y sistemática sobre el cumplimiento de las actividades de gestión definidas el proceso. El cumplimiento está entre ochenta y cinco (85) y cien (100) por ciento.

Tabla 9.1.1 - Leyenda para especificar el nivel de madurez de un proceso habilitador

9.2 Resumen de evaluación de nivel de madurez de los procesos habilitadores

Se presenta el resumen de la evaluación para cada proceso de negocio y sus respectivos procesos habilitadores de acuerdo a los criterios propuestos por la norma ISO/IEC 15504. El tiempo sugerido para la evaluación del gobierno de TI es de cuatro (4) meses, paralelo a la revisión del balanced scorecard y la medición del logro de los objetivos.

No obstante, identificando la brecha respecto al estado actual de la organización se recomienda empezar con iteraciones de mayor tiempo, por ejemplo entre seis (6) y ocho (8) meses hasta lograr una madurez mayor en el gobierno de TI bajo el enfoque de seguridad de información.

El nivel de madurez actual es determinado con el análisis y trabajo de campo realizado con la empresa referencia al igual que el objetivo, que en casi todos los casos, es poder llegar al siguiente nivel de la escala propuesta por la norma ISO/IEC 15504.

	Habilitador	Madurez actual	Madurez objetivo
Todos los procesos de negocio base	Garantizar el mantenimiento y configuración del marco de control de gobierno	Proceso incompleto – P	Proceso ejecutado
	Garantizar la entrega de beneficios	Proceso incompleto – P	Proceso ejecutado
	Garantizar la optimización de riesgos	Proceso incompleto - N	Proceso ejecutado
	Gestionar el marco de control de TI	Proceso incompleto – P	Proceso ejecutado
	Monitorear, evaluar y medir el rendimiento y la conformidad	Proceso incompleto – N	Proceso ejecutado
	Monitorear, evaluar y medir el rendimiento y la conformidad	Proceso incompleto – P	Proceso ejecutado
Admisión de pacientes	Gestionar la estrategia	Proceso incompleto – P	Proceso ejecutado
	Gestionar los recursos humanos	Proceso incompleto – L	Proceso Gestionado
	Gestionar el riesgo	Proceso incompleto - N	Proceso ejecutado
	Gestionar la seguridad	Proceso incompleto - N	Proceso incompleto – L
	Gestionar los programas y proyectos	Proceso incompleto – L	Proceso ejecutado
	Gestionar el cambio	Proceso incompleto – P	Proceso ejecutado
	Gestionar los activos	Proceso incompleto – P	Proceso ejecutado
	Gestionar las solicitudes e incidentes de servicio	Proceso incompleto - N	Proceso ejecutado
	Gestionar la continuidad	Proceso incompleto - N	Proceso ejecutado
	Gestionar los servicios de seguridad	Proceso incompleto – P	Proceso ejecutado
Hospitalización de pacientes	Gestionar la estrategia	Proceso incompleto – P	Proceso ejecutado
	Gestionar los recursos humanos	Proceso incompleto – L	Proceso Gestionado
	Gestionar el riesgo	Proceso incompleto - N	Proceso ejecutado
	Gestionar la seguridad	Proceso incompleto - N	Proceso incompleto – L

	Gestionar los programas y proyectos	Proceso incompleto – L	Proceso ejecutado
	Gestionar el cambio	Proceso incompleto - N	Proceso ejecutado
	Gestionar los activos	Proceso incompleto – P	Proceso ejecutado
	Gestionar las solicitudes e incidentes de servicio	Proceso incompleto - N	Proceso ejecutado
	Gestionar la continuidad	Proceso incompleto - N	Proceso ejecutado
	Gestionar los servicios de seguridad	Proceso incompleto – P	Proceso ejecutado
Egreso del paciente hospitalizado	Gestionar la estrategia	Proceso incompleto – P	Proceso ejecutado
	Gestionar los recursos humanos	Proceso incompleto – L	Proceso ejecutado
	Gestionar el riesgo	Proceso incompleto - N	Proceso ejecutado
	Gestionar la seguridad	Proceso incompleto - N	Proceso ejecutado
	Gestionar los programas y proyectos	Proceso incompleto – L	Proceso ejecutado
	Gestionar el cambio	Proceso incompleto – P	Proceso ejecutado
	Gestionar los activos	Proceso incompleto – P	Proceso ejecutado
	Gestionar las solicitudes e incidentes de servicio	Proceso incompleto - N	Proceso ejecutado
	Gestionar la continuidad	Proceso incompleto - N	Proceso ejecutado
	Gestionar los servicios de seguridad	Proceso incompleto – L	Proceso ejecutado
Identificación de pacientes	Gestionar la estrategia	Proceso incompleto – P	Proceso ejecutado
	Gestionar los recursos humanos	Proceso incompleto – L	Proceso ejecutado
	Gestionar el riesgo	Proceso incompleto - N	Proceso ejecutado
	Gestionar la seguridad	Proceso incompleto - N	Proceso ejecutado
	Gestionar los programas y proyectos	Proceso incompleto – P	Proceso ejecutado
	Gestionar el cambio	Proceso incompleto - N	Proceso ejecutado
	Gestionar los activos	Proceso incompleto – P	Proceso ejecutado
	Gestionar las solicitudes e incidentes de servicio	Proceso incompleto - N	Proceso ejecutado
	Gestionar la continuidad	Proceso incompleto - N	Proceso ejecutado

	Gestionar los servicios de seguridad	Proceso incompleto – L	Proceso ejecutado

Tabla 9.2.1 - Resumen de evaluación de madurez de los procesos habilitadores

9.3 Conclusiones del capítulo

- Se concluye que la organización de referencia, en efecto requiere ser gobernada bajo un enfoque de seguridad de información dado los resultados arrojados tras el trabajo de campo y la aplicación de la ley de protección de datos personales. Esto indica que existen brechas amplias a cerrar las cuales solo podrán realizarse formalizando las funciones, roles y responsabilidades discutidos en el capítulo ocho (8) del proyecto de tesis.

- Para lograr alcanzar los resultados esperados para la siguiente iteración de gobierno, verificando el alcance del gobierno de TI, se puede realizar una priorización adicional tanto sobre procesos base o sobre procesos habilitadores, de manera que al evaluar el marco de gobierno de TI y sus habilitadores se muestren avances de acuerdo al enfoque seleccionado y la necesidad producto del entorno.

- En caso empresas que hayan trabajado gobierno de TI usando COBIT 4.1, se recomienda realizar un mapeo entre la madurez definida para ambos marcos, el cual puede realizarse utilizando los anexos presentados en el marco de COBIT 5.0, de manera que se pueda validar un estado real de acuerdo a una norma exigente como lo es la ISO/IEC 15504 y a partir de esto identificar oportunidades de mejora que sean los drivers para iniciar un nuevo ciclo de vida de gobierno en el cual se realicen los ajustes de acuerdo a los resultados obtenidos y el entorno al cual se encuentra la empresa en ese instante.

- Es posible añadir nuevas actividades según el nivel de madurez al cual se requiera llegar, las cuales no necesariamente estarán señaladas en COBIT 5.0, sino que puede ser personalizadas en base a lo que estipula la norma ISO/IEC 15504 y de acuerdo a lo que la empresa pueda alcanzar con los recursos actuales, la dirección y la madurez del gobierno de TI y el modelo de toma de decisiones.

Capítulo 10. Conclusiones, observaciones y recomendaciones

Finalmente se presentan las conclusiones finales sobre el proyecto realizado, como el levantamiento de algunas observaciones referentes a este tipo de proyectos realizados, así como las recomendaciones respectivas señalando posibles trabajos futuros que se desprenden de este modelo de gobierno de TI.

10.1 Conclusiones

- Respecto al análisis del entorno, se concluye que el proyecto se justifica por medio de los drivers del cambio presentados y validados por la empresa de referencia, asumiendo que el aspecto económico incluido en el caso de negocio no es un impedimento, debido a que las empresas prestadoras de servicio de salud deben cumplir con las regulaciones y garantizar la protección de la información de sus pacientes, por lo cual este driver en particular refleja la situación de empresas del mismo rubro.

- De acuerdo la gestión de un proyecto de gobierno de TI, se concluye la necesidad de desarrollar la planificación de cada una de sus iteraciones o fases en las cuales se llevará a cabo la implementación. En este proyecto las fases se realizaron en promedio dos (2) semanas cada una, evidenciando la limitante del tiempo.

- Respecto al análisis de la organización se concluye que es importante la medición de los objetivos y emplear para esto técnicas como los cuadros de mando. No obstante, se debe de recordar que uno de los pilares de gobierno es la alineación

estratégica, por ello el marco empleado pretende garantizarlo por medio del método de la cascada de objetivos, bajo la cual se garantiza que los objetivos de TI de la organización, en efecto, contribuyen para la materialización de los objetivos organizacionales.

- Se concluye, teniendo como base el mapeo de los procesos habilitadores de COBIT 5.0, que el marco de gobierno cubre transversalmente a la empresa, pues realizando el último paso del método de la cascada de objetivos, cada proceso habilitador tiene un componente que se adapta a la necesidad y los procesos seleccionados de la empresa, los cuales se reducen al realizar el análisis de acuerdo al enfoque seleccionado, que puede variar de acuerdo a la realidad de la organización, sus procesos y prioridades.

- Respecto al modelamiento de procesos, se concluye que la información de las actividades que forman parte de estos, deben estar actualizados y diseñados en una notación actual que permita mostrar en su totalidad la lógica del proceso de una manera correcta, pues son la base del gobierno de TI pues a partir de estos se redactan y evalúan las políticas los riesgos y la aplicabilidad de procesos habilitadores según los enfoques seleccionados, como se puede verificar durante el desarrollo del modelo de gobierno.

- Respecto a la identificación de actividades de gestión para cada proceso habilitador, se concluye y justifica cambios en la estructura organizacional de la empresa para incluir un comité estratégico de TI y el rol del oficial de seguridad de información que sean los responsables de monitorear e identificar estrategias o requerimientos que retroalimenten estas actividades y sean modificadas para la siguiente iteración de acuerdo al nivel de madurez que se pretenda alcanzar.

- Se concluye que a partir del gobierno de TI bajo el enfoque de seguridad de información, la empresa necesitará adoptar políticas de seguridad de información alineadas a las actividades identificadas a cada proceso habilitador, de manera que las primeras, al ser formalizadas, comunicadas y aplicadas, garantizarán y encaminarán el cumplimiento de las actividades y logro de los objetivos de gobierno.

- Respecto a la evaluación de nivel de madurez, se concluye que se puede tener una evidencia de cómo se encuentra la organización en un determinado momento alineándolo a la ISO/IEC 15504, para que a partir de esto se inicie y tracen nuevos

objetivos que permitan mantener el impulso e iniciativa de gobierno como parte de la mejora continua identificando las brechas a cerrar para lograr estas metas.

- Finalmente, se señala que este proyecto brindará a la institución un valor agregado por el lado de gestión tecnológica, pues se garantiza el alineamiento estratégico y la entrega de beneficios a los stakeholders siguiendo actividades y estableciendo roles y responsabilidades de acuerdo un enfoque identificado y que se adapte a lo que la empresa pueda alcanzar en un determinado espacio de tiempo.

10.2 Observaciones

- El tema relacionado a la gestión de alto nivel o gobierno, en efecto, resulta ser el cuello de botella de una organización debido a la resistencia al cambio, debido a la incorporación de nuevas políticas que requieren la intervención de la alta dirección y su responsabilidad sobre las decisiones tomadas dentro cada área empresarial.

- Una de las principales observaciones sobre la empresa de referencia para el proyecto, es la falta de estandarización en los procesos organizacionales, lo cual evidencia que es probable que otras organizaciones del rubro presenten problemas similares debido a la complejidad de los procesos de hospitalización y atención, ya que existen normas de por medio que complican la lógica de los procesos, por ello notaciones simples o diagramas de flujo no pueden plasmar la realidad del proceso.

- La empresa de referencia no tiene formalizada una metodología para evaluación de riesgos y tampoco la función de seguridad de información, por lo cual este proyecto muestra la importancia de establecerlos para lograr los objetivos a largo plazo y el alineamiento con la regulación vigente que aplica a ella.

10.3 Recomendaciones

- Se recomienda la documentación y estandarización de los procesos en una notación vigente capaz de soportar todo tipo de lógica tal como es BPMN 2.0, por lo cual adicionalmente se recomienda brindar la capacitación adecuada al personal responsable de la migración y modelado del mapa de procesos en dicha notación.

- Se recomienda la actualización y gestión continua de riesgos relacionados a la seguridad de información, debido a que este es el enfoque seleccionado por la empresa y su base para el diseño de nuevas políticas o controles parte de la identificación de riesgos o identificación de nuevas actividades de gestión a cubrir.

- Así mismo, se recomienda la formalización del comité estratégico de TI que será el responsable de las decisiones para el gobierno de TI y también los responsables de llevar a cabo esta iniciativa y alinearla al plan estratégico de la empresa. Para esto se aconseja contar dentro del comité con una persona de la alta dirección, contar con el oficial o responsable de gobierno de la empresa o gobierno de TI, el jefe de proyecto, en señal de la aprobación y la gestión de la cartera de proyectos alineados y el oficial de seguridad de información encargado de mantener el enfoque del programa de gobierno.

- En caso la implementación del proyecto, se sugiere la revisión de este documento y tratar de cubrir cada una de las fases con un tiempo prudente asignado ya que las iteraciones de gobierno duran entre cuatro (4) y seis (6) meses según el nivel de complejidad. En este caso al tener 7 fases se puede estimar que un proyecto de implementación real dura alrededor de dos (2) años a tres (3), lo cual dependerá de la aceptación del proyecto y el manejo del cambio organizacional.

- Se sugiere la revisión de los objetivos resultantes de la cascada sugerida por COBIT 5.0 empleando el cuadro de mando propuesto realizando ajustes dentro de las métricas para una mayor personalización. Incluso según los resultados iniciales se puede ir agregando otras métricas o establecer valores objetivos que puedan verificar el estado o cumplimiento de objetivos según la línea base.

- Se sugiere programar revisiones periódicas al gobierno de TI para verificar si el cambio en algún proceso, organización o regulación afecta a dicho modelo y se requieran actualizar las políticas y mapa de roles y responsabilidades. En caso el cambio en el modelo sea necesario se recomienda adicionalmente, volver a realizar el mapeo de habilitadores y la aplicación de acuerdo a la priorización realizada por parte del comité estratégico.

- Se recomienda alinear la iniciativa del gobierno al plan estratégico de TI de forma que este proyecto ayude al cumplimiento de dicho plan y que tome principios de este para el análisis del entorno y la brecha entre el estado actual y la meta a alcanzar.

- Se sugiere adoptar las políticas de seguridad de información señaladas en el documento, debido a que estas se alinean a lo que estipula la norma ISO/IEC 27001:2013 que es un estándar reconocido dentro del ámbito de la seguridad de información. Estas políticas pueden ser personalizadas de acuerdo a la madurez de la organización respecto a estos temas y según se defina el alcance de aplicación en un periodo de tiempo.

- Se recomienda realizar las evaluaciones de nivel de madurez empleando la norma que integrada a COBIT 5.0, ISO/IEC 15504. En caso la empresa trabaje bajo un enfoque de COBIT 4.1 podrían mapear sus niveles hacia dicha norma más exigente, de manera que tengan un panorama claro de cómo se encuentran actualmente y a partir de esta evidencia, tomar medidas respecto a las brechas identificadas en comparación hacia donde se quiera llegar para la próxima iteración de gobierno.

- De acuerdo a los resultados de la evaluación de la organización, no se recomienda aplicar a estándares internacionales que certifiquen y garanticen la seguridad en un enfoque al negocio de empresas prestadoras de servicios de salud, como lo es HIPAA.

10.4 Trabajos Futuros

- Se recomienda como parte de los trabajos futuros llevar a cabo la implementación del diseño dentro de la empresa referencia, debido a las probabilidades de éxito y la adecuación realizada para regulaciones como la ley de protección de datos personales, lo cual garantiza la entrega de valor esperado.

- Como trabajo futuro se recomienda la adopción de otros enfoques importantes para incrementar el alcance del gobierno de TI de la empresa como parte de un trabajo futuro. Tal como se presenta en el caso de negocio, uno de los drivers del cambio sugiere la mejora e importancia de la gestión de operaciones de TI, lo cual puede ser otro enfoque a considerar e incluso desde COBIT 5.0, después de haber mapeado nuevamente la aplicación de habilitadores, llegar a adoptar las buenas prácticas de ITIL para la identificación de políticas.

Referencias bibliográficas

APOYO CONSULTORIA

2012 *Situación actual y perspectivas del mercado de la salud.* Lima.

ARTEAGA, Hernán

2012 *Desarrollo de un Gobierno de TI para la Empresa Fiduciaria Ecuador Utilizando COBIT 4.1.* Tesis para obtención del Título de Ingeniero en Sistemas Informáticos y de Computación. Quito: Escuela Politécnica Nacional.

BALDEÓN, Jorge y Juan PINOARGOTE

2007 *Modelo para Evaluación e Implementación de un Sistema de IT Governance Basado en IT BSC en la empresa ABC.* Memoria para la obtención del título de Ingeniero Informático de Gestión. Guayaquil: Universidad Santa Maria.

CALDER, Alan y Steve G. WATKINS

2010 *Information Security Risk Management for ISO 27001/ISO 27002.* Reino Unido: IT Governance Ldt 2007.

CONGRESO DE LA REPUBLICA

2011 *Ley 29733. Ley de Protección de Datos Personales.* 3 de Julio.

COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES – INDECOPI

2007 *NTP/ISO 17799. EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de información*. 22 de enero

FERNANDEZ, Antonio y Faraón LLORENS

2010 *Gobierno de las TI para universidades.* España: Conferencia de Rectores de las Universidades Españolas (CRUE).

FIGUEROLA, Norberto

2012 *Matriz de Asignación de Responsabilidades (RAM).* Consulta: 14 de noviembre del 2012. < http://articulospm.files.wordpress.com>.

GÓMEZ, Jesús

2012 "*Implantación de los procesos de gestión de incidentes y gestión de problemas según ITIL v3.0 en el área de tecnologías de información de una entidad financiera"*. Tesis para optar el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú.

HUERTAS, Yvonne

2011 "*Estrategias para la Implantación de Tecnologías de la Informática Efectivas: Marco de Trabajo de Gobierno de TI". Serie de documentos de trabajo – CICIA.* Volumen 5.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC

2013a *ISO/IEC 27001. Information technology, Security techniques, Information security management systems requirements.* Consulta: 24 de octubre del 2013 < http://www.iso.org/iso/catalogue_detail?csnumber=54534>.

2013b *ISO/IEC 27002. Information Technology, Security Techniques, Code of practice for information security management.* Octubre del 2013.

2008 *ISO/IEC 38500. Corporate governance of information technology*. 1 de Junio.

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

2013 *Comportamiento de la economía peruana en el primer trimestre del 2013*. Lima.

ITGI - IT GOVERNANCE INSTITUTE

2003 *Board Briefing Final*. Second Edition. Estados Unidos: ITGI.

2005a *IT Alignment: Who is in charge?* Estados Unidos: ITGI.

2005b *Governance of Outsourcing.* Estados Unidos: ITGI.

2005c *Information Risks: Whose Business Are They?* Estados Unidos: ITGI.

2005d *Measuring and Demonstrating the Value of IT*. Estados Unidos: ITGI.

2005e *Optimising Value Creation From IT Investments*. Estados Unidos: ITGI.

2007 *IT Governance Roundtable: IT Governance Trends.* Estados Unidos.

2008a *IT Governance Roundtable: IT Frameworks.* Estados Unidos.

2008b *IT Governance Roundtable: IT Staffing Challenges.* Estados Unidos.

2008c *The Val IT Framework 2.0.* Estados Unidos.

2008d *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.* Estados Unidos.

2009a *IT Governance Roundtable: Value Delivery.* Estados Unidos.

2009b *IT Governance Roundtable: Defining IT Governance.* Estados Unidos.

2009c *IT Governance Roundtable: Unlocking Value.* Estados Unidos.

2011 *Global Status Report on the Governance of Enterprise IT.* Estados Unidos: ITGI

ISACA - INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

2009 *The Risk IT Framework.* Estados Unidos.

2009a *Certified Information Systems Auditor Review Manual.* Estados Unidos.

2010 *COBIT Online.* Especificaciones técnicas. Consulta: 17 de septiembre del 2012 <http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Online.aspx>

2012a *COBIT 5.0: A Business Framework for the Governance and Management of Enterprise IT.* Estados Unidos.

2012b *COBIT 5.0: Enabling Process.* Estados Unidos.

2012c *COBIT 5.0: Implementation.* Estados Unidos.

2012d *Certified Information Security Manager. Manual de Preparación al Examen CISM.* Estados Unidos.

2012e *ISACA Glossary of terms*. Estados Unidos.

2012f *COBIT Case studies: COBIT Maturity Assessment and Continual e-Health Governance Improvement at NHS Fife*. Consulta: 15 de agosto del 2013 < http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-StudyCOBIT-Maturity-Assessment-and-Continual-e-Health-Governance-Improvement-at NHS-Fife.aspx >

2012g *COBIT 5.0 for Information Security.* Estados Unidos

2013a *COBIT Case studies: Sunnybrooke Health Sciences Centre*. Consulta: 15 de agosto del 2013 < http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Sunnybrook-Health-Sciences-Centre.aspx>.

2013b *COBIT Case studies: Use of COBIT 5.0 for ISACA Strategy Implementation.* Consulta: 19 de agosto del 2013 < http://www.isaca.org/COBIT/Pages/COBIT-Case-Study-Use-of-COBIT-5-for-ISACA-Strategy-Implementation.aspx>

LEECH, Tim

2003 *"A White Paper Proposing Practical, Cost Effective Compliance Strategies".* Canadá.

MEYCOR SOFTWARE

2010 *Meycor COBIT suite*. Especificaciones técnicas. Consulta: 15 de agosto de 2012 < http://www.meycor-grc.com>.

METHODWARE

2010 *Era Kairos.* Especificaciones técnicas. Consulta: 10 de septiembre de 2012 <http://www.methodware.com/kairos/>

MINISTERIO DE SALUD - MINSA

2005 *Norma Técnica de la historia clínica de los establecimientos del sector Salud.* Lima.

MUÑOZ, Ingrid y Gonzalo ULLOA

2011 *"Gobierno de TI – Estado del Arte". S&T.* Cali, 2011. Volumen 9, Número 17, pp. 23–53.

NATIONAL COMPUTING CENTRE

2005 *IT Governance: Developing a Successful Governance Strategy.* Londres: Oxford House.

OCR – OFFICE FOR CIVIL RIGHTS

2003 *Summary of the Hippa privacy rule.* Estados Unidos. Mayo 2003.

OMG - OBJECT MANAGEMENT GROUP

2011 *Business Process Model and Notation (BPMN)*. Version 2.0.

PMI - PROJECT MANAGEMENT INSTITUTE

2004 *A Guide to the Project Management Body of Knowledge (PMBOK Guide).* Fourth Edition. Pennsylvania: Project Management Institute, Inc.

TREASURY BOARD OF CANADA SECRETARIAT

2009 *Business Case Guide.* Canada.

TUPIA, Manuel

2011 *Principios de Auditoria y Control de Sistemas de Información.* Segunda Edición. Lima: Tupia Consultores y Auditores.

VAN GREMBERGEN, Wim

2000 *"The Balanced Scorecard and IT Governance"*. *Information Systems Control Journal*. 2000. Volumen 2, pp. 40-43.

VILLENA, Moisés

2006 *Sistema de Gestión de Seguridad de Información para una Institución Financiera.* Tesis para la obtención del título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú.