PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN MODELO DE GOBIERNO DE TI UTILIZANDO EL MARCO DE TRABAJO DE COBIT 5 CON ENFOQUE EN SEGURIDAD DE LA INFORMACIÓN. CASO DE ESTUDIO: UNA EMPRESA PRIVADA ADMINISTRADORA DE FONDO DE PENSIONES

Tesis para optar el Título de **Ingeniero Informático**, que presenta el bachiller:

Henry Jhonatan Beingolea Manavi

ASESOR: Mag. Moisés Antonio Villena Aguilar

Lima, Octubre de 2015

Resumen

En la actualidad la tecnología tiene un rol importante dentro de las organizaciones, independientemente del rubro y magnitud de la misma, lo cual ha ocasionado que éstas tengan una alta dependencia de las Tecnologías de Información. Lamentablemente, en muchos casos se carece de una adecuada gestión de las TI, y de esta manera se impide que las TI proporcionen un valor estratégico, y por el contrario puede llegar a ocasionar mayores complicaciones a la empresa, tal como es el incumplimiento de los objetivos de negocios, alta pérdida de dinero en las inversiones en TI, retrasos en la operatividad, entre otros.

Las empresas administradoras de fondo de pensiones, no son ajenas a esta problemática, pues para realizar sus operaciones tienen una alta dependencia de la tecnología, lo cual ha llevado a que la Superintendencia de Banca, Seguros y AFP, exija el cumplimiento de dos circulares; una referente a la Gestión de la Seguridad de la Información y otra respecto a la Gestión de la Continuidad del Negocio.

Dada la situación descrita, se ha propuesto diseñar un modelo de Gobierno de TI, utilizando el marco de trabajo COBIT 5, con enfoque en Seguridad de Información, tomando como caso de estudio una empresa de este rubro.

Para este proyecto se ha desarrollado cada uno de los cinco pilares del Gobierno de TI (Alineación estratégica, entrega de valor, gestión de riesgos, gestión de los recursos y medición del desempeño) siguiendo las buenas prácticas de gobierno de TI de COBIT 5.

FACULTAD DE
CIENCIAS E INGENIERÍA
ESPECIALIDAD DE
INGENIERÍA INFORMÁTICA

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO INFORMÁTICO

TÍTULO: DISEÑO DE UN MODELO DE GOBIERNO DE TI UTILIZANDO EL MARCO DE TRABAJO DE COBIT 5 CON ENFOQUE EN SEGURIDAD DE LA INFORMACIÓN. CASO DE ESTUDIO: UNA EMPRESA PRIVADA ADMINISTRADORA DE FONDO DE PENSIONES

ÁREA: TECNOLOGÍAS DE INFORMACIÓN

PROPONENTE: MAG. MOISES VILLENA AGUILAR

ASESOR: MAG. MOISES VILLENA AGUILAR

ALUMNO: HENRY JHONATAN BEINGOLEA MANAVI

CÓDIGO: 20087041

TEMA N°: 613

FECHA:

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Facultad de Ciencias e Ingeniería
21 JUL. 2015
MIGUEL MEJIA PUENTE
DECANO

DESCRIPCIÓN

En la actualidad, el crecimiento de la dependencia de la información y de las TI (Tecnologías de Información) en las empresas, ha hecho que estas formen parte importante para la creación de la ventaja competitiva y estratégica de las empresas. Sin embargo, se ha encontrado dentro de los principales problemas que las TI no están alineadas al negocio, lo que ocasiona que no se pueda aprovechar el potencial actual que tienen para cumplir con los objetivos empresariales.

Por lo que se presenta una alternativa de solución al problema identificado, diseñar un modelo de gobierno de TI, para una empresa privada administradora de fondo de pensiones, lo cual va permitirá otorgar valor estratégico a las necesidades del negocio desde las inversiones que se realizan en TI.

El gobierno de TI es un conjunto de políticas y mejoras prácticas que permite mejorar el uso de las tecnologías dentro de las operaciones del negocio, brindando una mayor orientación al área de tecnología para cubrir las necesidades actuales y futuras a nivel estratégico.

Dentro de los marcos de gobierno de TI se encuentra COBIT 5, el cual es un marco de mejores prácticas para el gobierno y la gestión de TI, siendo uno de los más completos al integrar otras guías y estándares de TI para realizar dicha labor.

Adicionalmente, considerando que la empresa maneja información de carácter confidencial y debido a las regulaciones que debe de cumplir respecto a la gestión de la información, el enfoque que tendrá el gobierno de TI será el de seguridad de la información.

Av. Universitaria 1801
San Miguel, Lima – Perú

Apartado Postal 1761
Lima 100 – Perú

Teléfono:
(511) 626 2000 Anexo 4801

OBJETIVO GENERAL

Diseñar un modelo de Gobierno de TI, con un enfoque en seguridad de la información para una empresa administradora de fondo de pensiones, basado en COBIT 5.

OBJETIVOS ESPECÍFICOS

- Desarrollar la alineación estratégica entre los objetivos de negocio y TI.
- Definir los procesos habilitadores del gobierno de TI para el cumplimiento de los objetivos de negocio de la empresa.
- Identificar y valorar los activos de información, analizando los riesgos de seguridad de información asociados a los procesos de negocio a los que dan soporte.
- Medir la madurez de los procesos habilitadores del gobierno de TI, que soportan los objetivos de negocio de la empresa.

ALCANCE

En el proyecto de fin de carrera se va a realizar un diseño de un modelo de gobierno de TI para una empresa de administración de fondo de pensiones. Cabe resaltar que el gobierno de TI tiene varios enfoques (como el de continuidad del negocio, seguridad de la información, proyectos, arquitectura empresarial, entre otros), pero debido a cuestiones de tiempos y en coordinación con la necesidad de los stakeholders de la empresa se va a realizar el enfoque de seguridad de la información. Adicionalmente, el alcance de los procesos que van a formar parte de este proyecto también son elegidos por los stakeholders de la empresa debido a que estos procesos forman parte de sus principales objetivos. Finalmente, el marco de referencia para la implementación del gobierno de TI es COBIT 5, debido a que es una necesidad del negocio porque junta las mejoras prácticas de otros marcos y es la última versión.

Máximo : 100 páginas

Av. Universitaria 1801
San Miguel, Lima – Perú

Apartado Postal 1761
Lima 100 – Perú

Teléfono:
(511) 626 2000 Anexo 4801

Tabla de contenido

Lista de Tablas

1 CAPÍTULO 1

1.1 PROBLEMÁTICA

En la actualidad, el mundo de los negocios es dinámico y altamente competitivo, por lo que las empresas deben de ser más creativas para innovar en la entrega de sus productos y servicios a sus clientes [HONG, 2009].

Algunas estrategias empresariales buscan desarrollar o mejorar los procesos de negocio que estén alineados a los objetivos de la organización, estos procesos pueden estar soportados en sistemas de información y/o tecnologías [LEPAGE, 2014]. En la actualidad, el crecimiento de la dependencia de la información y de las TI (Tecnologías de Información) en las empresas, han hecho que estas formen parte importante para la creación de la ventaja competitiva y estratégica de las empresas [COERTZE & VON SOLMS, 2014].

Según una encuesta realizada por la EIU (*Economist Intelligence Unit*) en el 2012, se concluye que el cambio tecnológico en las organizaciones permitirá reaccionar mucho más rápido al mercado y a los clientes [EIU, 2012]. Sin embargo según los resultados de una encuesta realizada por la asociación ISACA (*Information Systems Audit and Control Association*) que se dio en el 2012 para la región de Latinoamérica a profesiones de TI y de negocios, muestra serios problemas relacionadas a las TI que se dan en las empresas, las más recurrentes fueron [ISACA, 2012a]:

- Altos costos en TI con un bajo o nulo retorno de inversión.
- Falta de alineación entre las estrategias de TI con las del negocio.
- Proyectos tecnológicos sobregirados.

El presupuesto brindado para las inversiones en TI aumenta cada año, con el fin de que las organizaciones puedan cumplir con las necesidades del negocio [NINGSIH, 2013]. Por lo tanto es necesario asegurar que las inversiones en tecnología creen valor para la empresa y sean adecuadamente gestionadas y controladas [NINGSIH, 2013].

La falta de alineación entre el negocio y TI, se da en parte por la falta de claridad o participación del directorio con el área de TI, o por la incapacidad de TI para interpretar lo que quiere el directorio en acciones aplicables a TI [COERTZE & VON SOLMS, 2014]. Es por eso que se necesita que haya entendimiento entre TI y el negocio [COERTZE & VON SOLMS, 2014].

Los proyectos en TI siguen fallando en cumplir con los tiempos establecidos, el presupuesto asignado y la expectativa esperada en la entrega de los beneficios [ASHRAF, 2010]. Algunas de las fallas se deben a que el alcance no estaba definido, no se siguen prácticas efectivas de gestión de proyectos o no se hace el esfuerzo suficiente para realizar los beneficios del proyecto [SARUP, 2003]. Para lograr mejores resultados en los proyectos de TI es importante que el proyecto esté alineado a la estrategia de la organización y si es necesario involucrar a las gerencias que están implicadas en el proyecto [MIYAGI, 2014].

Estos problemas presentando no son problemas aislados uno del otro, pues en el fondo tratan de que las tecnologías satisfagan las necesidades del negocio adecuadamente. Por ello en este proyecto de fin de carrera el problema que será materia de estudio es la alineación estratégica entre TI y el negocio.

Lamentablemente esta alineación aparenta ser algo trivial, pero esta ha preocupado a varias organizaciones a nivel mundial en la última década y ha sido un reto para el gobierno de TI [COERTZE & VON SOLMS, 2014]. El Gobierno de TI es un conjunto de políticas y mejoras prácticas que permite mejorar las operaciones del negocio en la empresa a través de las tecnologías [MOELLER, 2013]. Además permite que las TI se vuelvan un activo estratégico debido a que permite que el negocio irrumpa en nuevos mercados, impulse estrategias competitivas, mejore en la satisfacción o retención de los clientes, entre otras ventajas [HARDY, 2006].

Según el ITGI (*IT Governance Institute*) el gobierno de TI se preocupa de dos cosas principalmente la primera es que las TI entreguen valor a la empresa a través de la

alineación estratégica y la segunda es mitigar los riesgos de TI, ambas soportadas por la gestión de los recursos y las mediciones adecuadas para asegurar que se obtengan los resultados esperados [ITGI, 2003]. Es por eso que el gobierno de TI cuenta 5 áreas principales, las cuales son: Alineación estratégica, entrega de valor, gestión de riesgos, gestión de los recursos y medición del desempeño [ITGI, 2003].

Para la implementación del gobierno de TI, se cuenta con diferentes marcos reconocidos a nivel internacional como COBIT, ISO/IEC 38500 o Calder-Moir y otros estándares que apoyan al gobierno de TI como ITIL 2011, ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 31000 y COSO [MUÑOZ & ULLOA, 2011]. Cabe resaltar que las organizaciones requieren seleccionar el marco que mejor se adapte a su organización y que el uso de un marco no excluye que se pueda usar otro, sino que se integren y permita cumplir con las cincos áreas del gobierno de TI [MUÑOZ & ULLOA, 2011].

Dada la problemática presentada de alinear las estrategias de TI con las negocio, se propone como alternativa de solución diseñar un modelo de gobierno de TI en una AFP como caso de estudio, pues estas no están ajenas a este problema, ya que son empresas que manejan gran cantidad de información asociada a clientes, inversiones, seguros, entre otros, y se soportan fuertemente en las TI para realizar sus procesos de negocio y satisfacer las necesidades de sus clientes.

Dado que la seguridad de la información es un tema importante para las AFP pues tienen que cumplir con la ley N° 29733 “Ley de protección de datos personales” [CONGRESO DE LA REPUBLICA, 2011] y la circular N° G-140-2009 “Gestión de la seguridad de la información” de la SBS (Superintendencia de Banca, Seguros y AFP) [SBS, 2009a]. El enfoque que se tendrá en el gobierno de TI será el de seguridad de la información.

1.2 Objetivo general

Diseñar un modelo de Gobierno de TI, con un enfoque en seguridad de la información para una empresa administradora de fondo de pensiones, basado en COBIT 5.

1.3 Objetivos específicos

- Objetivo específico 1: Desarrollar la alineación estratégica entre los objetivos de negocio y TI.
- Objetivo específico 2: Definir los procesos habilitadores del gobierno de TI para el cumplimiento de los objetivos de negocio de la empresa.
- Objetivo específico 3: Identificar y valorar los activos de información, analizando los riesgos de seguridad de información asociados a los procesos de negocio a los que dan soporte.
- Objetivo específico 4: Medir la madurez de los procesos habilitadores del gobierno de TI, que soportan los objetivos de negocio de la empresa.

1.4 Resultados esperados

- Resultado 1 para el objetivo 1: Documento que contenga los objetivos de TI identificados que soportan los objetivos del negocio los cuales satisfacen las necesidades del negocio del caso de estudio y el cuadro de mando integral para cada objetivo identificado.
- Resultado 2 para el objetivo 2: Identificación de los procesos habilitadores del gobierno de TI para el caso de estudio.
- Resultado 3 para el objetivo 2: Definición de las actividades, roles y responsabilidades de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.
- Resultado 4 para el objetivo 3: Identificación y valoración de los activos de TI que soportan los procesos del negocio los cuales apoyan los objetivos del negocio.

- Resultado 5 para el objetivo 3: Matriz de riesgos.
- Resultado 6 para el objetivo 4: Identificación del nivel de madurez de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.

1.5 Herramientas, métodos, metodologías y procedimientos

1.5.1 Introducción

Para poder desarrollar cada uno de los resultados esperados, se muestra a continuación las herramientas que van a ser utilizadas.

Resultados esperado	Herramientas a usarse
RE1: Documento que contenga los objetivos de TI identificados que soportan los objetivos del negocio los cuales satisfacen las necesidades del negocio del caso de estudio y el cuadro de mando integral para cada objetivo identificado.	COBIT 5: Enabling process
RE2: Identificación de los procesos habilitadores del gobierno de TI para el caso de estudio.	COBIT 5: Enabling process
RE3: Definición de las actividades, roles y responsabilidades de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.	COBIT 5: Enabling process
RE4: Identificación y valoración de los activos de TI que soportan los procesos del negocio los cuales apoyan los objetivos del negocio.	ISO/IEC 27005:2011
RE5: Matriz de riesgos	ISO 31000:2009

RE6: Identificación del nivel de madurez de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.	COBIT 5: Framework

Tabla 1.1: Herramientas, métodos, metodologías y procedimientos.

1.5.2 COBIT 5: Enabling Process

En este guía se explica el 1er principio de COBIT 5, el cual permite transformar las necesidades del negocio, en objetivos de negocio, para luego relacionarlas con un conjunto de metas de TI, las cuales van a requerir de un conjunto de habilitadores (entre ellos procesos) para poder apoyar al cumplimiento de las metas de TI y por lo tanto satisfacer las necesidades del negocio [ISACA, 2012b]. Además por cada objetivo de negocio o de TI propone un conjunto de métricas para medir el logro de cada objetivo [ISACA, 2012b].

Para cada uno de los procesos habilitadores se describen las prácticas claves de gobierno, con sus respectivas actividades que van a permitir el desarrollo del proceso habilitador en el gobierno de TI del caso de estudio, además ayuda a distribuir las responsabilidades a través de la matriz RACI [ISACA, 2012b].

Justificación:

En la publicación de COBIT 5: Enabling Process va permitir realizar la alineación estratégica para poder diseñar el gobierno de TI, siguiendo el 1er principio de COBIT 5 y desarrollar los procesos habilitadores para el caso de estudio descritos en esta publicación. [ISACA, 2012b].

1.5.3 COBIT 5: Framework

Dentro del marco de COBIT 5, presenta el modelo de madurez de procesos el cual está basado en la ISO/IEC 15504, para medir el nivel de madurez de cualquier

proceso habilitador y permite identificar las áreas de mejora. Este modelo define 6 niveles que puede alcanzar un proceso, los cuales son:

- **Nivel 0 - Proceso incompleto:** El proceso no está implementado o no alcanza su propósito.
- **Nivel 1 - Proceso ejecutado:** El proceso implementado alcanza su propósito.
- **Nivel 2 - Proceso gestionado:** El proceso ahora está implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados están establecidos, controlados y mantenidos apropiadamente.
- **Nivel 3 - Proceso establecido:** El proceso ahora está implementado usando un proceso definido que es capaz de alcanzar sus salidas del proceso.
- **Nivel 4 - Proceso predecible:** El proceso ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **Nivel 5 - Proceso optimizado:** El proceso es mejorado de forma continua para cumplir con las metas actuales y los objetivos del negocio.

Cabe resaltar que para alcanzar un nivel superior se debe de haber cumplido en su totalidad los niveles anteriores.

Justificación:

Este modelo de madurez de procesos va a permitir identificar el nivel de madurez de los procesos habilitadores definidos en al alcance del gobierno de TI del caso de estudio.

1.5.4 ISO/IEC 27005:2011

La ISO/IEC 27005 es una norma internacional para la gestión de riesgos de seguridad, como parte de la gestión de riesgos en el anexo B de esta norma brinda los lineamientos a seguir para poder identificar y valorar los activos de información y evaluar el impacto [ISO, 2011].

Justificación:

Estos lineamientos van a permitir identificar y valorar los activos de información que se utilizan en los procesos de negocio que están dentro del alcance del gobierno de TI del caso de estudio. Los cuales van a ser gestionados adecuadamente.

1.5.5 ISO 31000:2009

La ISO 31000 es una norma internacional en la cual define los principios y las directrices para la gestión de riesgos, el cual se puede aplicar a cualquier tipo de industria y sector [ISO, 2009].

El proceso de gestión de riesgos se define a través de la comunicación y consulta de los riesgos con los stakeholders, el establecimiento del contexto de la organización, la evaluación del riesgo, el tratamiento del riesgo y el seguimiento y revisión de los riesgos evaluados [ISO, 2009].

Justificación:

Dado que se va a gestionar los riesgos de información dentro del alcance del gobierno de TI del caso de estudio, se va utilizar esta norma pues se puede adaptar a las necesidades del proyecto.

1.6 Alcance

En el proyecto de fin de carrera se va a realizar un diseño de un modelo de gobierno de TI, el cual podría diseñarse para cualquier tipo de rubro empresarial, pero por fines académicos se va a realizar para una empresa de administración de fondo de pensiones. Cabe resaltar que el gobierno de TI tiene varios enfoques (como el de continuidad del negocio, seguridad de la información, proyectos, arquitectura empresarial, entre otros), pero debido a cuestiones de tiempos y en coordinación con la necesidad de los stakeholders de la empresa se va a realizar el enfoque de

seguridad de la información. Adicionalmente, el alcance de los procesos que van a formar parte de este proyecto también son elegidos por los stakeholders de la empresa debido a que estos procesos forman parte de sus principales objetivos. Finalmente, el marco de referencia para la implementación del gobierno de TI es COBIT 5, debido a que es una necesidad del negocio porque junta las mejoras prácticas de otros marcos y es la última versión.

1.6.1 Limitaciones

- **Disposición de los colaboradores por parte de la empresa**

La participación de la alta gerencia es de suma importancia debido a que son ellos dan la dirección y objetivos, y verifican que el proyecto este alineado a los objetivos del negocio. Por otro lado dueños de los procesos también son importantes, debido a que es necesario conocer como es el proceso que está entrando dentro del alcance.

- **Disponibilidad de la información**

Debido a que la empresa cuenta con políticas de información, es probable que no se pueda extraer toda la información requerida para el proyecto.

- **Regulaciones y marcos**

La empresa se encuentra sujeta a regulaciones locales las cuales pueden ser actualizadas o se puedan crear nuevas regulaciones que implicarían las cuales se tendrían que tomar en cuenta para el proyecto, así mismo el marco de COBIT 5 o ISO 27000 puede ser actualizado.

1.6.2 Riesgos

Los riesgos identificados son:

Riesgo identificado	Impacto en el proyecto	Medidas correctivas para mitigar
Cambio en la regulación	Reducir el tiempo destinado al proyecto, debido a que se debe de adecuar a la nueva regulación.	Estar al tanto de las nuevas regulaciones que podrían salir y que apliquen a la empresa.
Demora en la entrega de información de la empresa	Retraso al proyecto debido a que se cuenta con un plan de trabajo.	Solicitar la información con tiempo y dejar en claro al inicio del proyecto toda la información que se va a requerir.
Negación de entrega de información por la empresa	Se pierde la ejecución del proyecto.	Firmar un acuerdo de confidencialidad con la empresa, para asegurar que la información es de carácter confidencial y es usado solo para fines académicos. Caso contrario buscar otra empresa.

Tabla 1.2: Riesgos del proyecto.

1.7 Justificación

El contar con un modelo de Gobierno de TI es conveniente porque permite que las organizaciones puedan obtener un mayor provecho de sus tecnologías, debido a que este es un activo estratégico que le ayuda a la empresa a alcanzar sus objetivos más importantes del negocio [MUSA, 2014]. Además que la información y las tecnologías de información son activos críticos reconocidos a nivel empresarial que necesitan ser gobernados apropiadamente [COERTZE & VON SOLMS, 2014].

En este caso en particular el Gobierno de TI permitirá a la AFP, demostrar a concreta y medible la entrega de valor de las inversiones realizadas en TI optimizar sus costos, gestionando los riesgos y cumplir con las leyes [CONGRESO DE LA REPUBLICA, 2011] y la regulación [SBS, 2009a] a los que se ve expuesto la organización.

Esta entrega de valor se podrá percibir gracias a la alineación estratégica de los objetivos del negocio con los objetivos de TI y poder desarrollar hacer un indicador para medir el cumplimiento por cada objetivo específico identificado [MUSA, 2014]. Así mismo permitirá identificar cuáles serán los procesos habilitadores, actividades y responsabilidades relacionadas que permitirá cumplir con los objetivos de TI.

2 CAPITULO 2

2.1 Marco conceptual

2.1.1 Introducción

A continuación se presentaran los principales conceptos involucrados con el gobierno de TI.

2.1.2 Objetivo del marco conceptual

El objetivo de este capítulo es dar a entender cada uno de los conceptos claves, marcos de referencia y estándares asociados a la problemática del gobierno de TI.

2.1.3 Gobierno Corporativo

Para entender el gobierno de TI es importante saber que es el gobierno corporativo, pues el gobierno de TI es uno de los elementos claves del gobierno corporativo de la empresa que permite que cumplir con las estrategias y generar valor al negocio [WEILL & ROSS. 2013].

El gobierno corporativo es un conjunto de procedimientos y procesos con los que se dirige y controla una organización [ECB, 2004], lo cual contribuye a potenciar la competitividad de la empresa y defender el valor de las inversiones realizadas [OECD, 2004].

Según la OECD (*The Organisation for Economic Co-operation and Development*) no hay un modelo único de gobierno corporativo, pero dice que por lo general el directorio es responsable del gobierno corporativo y debe de proteger los derechos de los accionistas y otros stakeholders [WEILL & ROSS. 2013]. El MIT (*Massachusetts Institute of Technology*) *Sloan Center for Information Systems Research*, propone que el directorio debe de trabajar con el equipo de ejecutivos para implementar los principios del gobierno y que el equipo de ejecutivo defina las estrategias y el

ambiente organizacional las cuales van a ser logradas a través de sus elementos claves, que son: recursos humanos, financieros, físicos, propiedad intelectual, información y TI y las relaciones empresariales [WEILL & ROSS. 2013]. Por lo que es importante que el gobierno de TI que se plantee este alineado al gobierno corporativo de la empresa del caso de estudio.

2.1.4 Gobierno de TI

El gobierno de TI es un concepto que ha sido desarrollo por diferentes entidades especializadas. Por un lado el ITGI define al gobierno de TI como una parte integral de la gobierno de la corporativo que consiste de liderazgo, estructuras y procesos organizacionales, que garantice que la organización de las TI sostenga y extienda las estrategias y objetivos de la organización [ITGI, 2003]. Por otro lado la ISO define el gobierno de TI como el sistema por el cual el uso actual y futuro de las TI son dirigidas y controladas, incluyendo la evaluación y dirección de su uso para soportar a la organización y monitorear el logro de sus planes, incluyendo la estrategia y políticas para usar las tecnologías dentro de la organización [ISO, 2008]. Si bien ambos conceptos son desarrollados por distintas entidades las definiciones concuerdan en que el gobierno de TI soporte las estrategias del negocio a través desde las tecnologías.

El gobierno de TI ayuda a las empresas, sean estas privadas o públicas, a que su información y tecnologías que utilizan sean un activo estratégico mediante estos 3 principales objetivos [ISACA, 2012d]:

- **Realización de beneficios:** A través del mejor manejo de las inversiones que se realizarán en TI, las cuales tienen que generar un valor significativo a la empresa, es decir deben de ser ajustadas a los objetivos del negocio, se deben de entregar dentro del plazo y presupuesto establecido, y deben de entregar los beneficios financieros y no financieros que se propusieron.

- **Optimización de riesgos:** Los riesgos a los que el negocio estaría expuesto debido al uso de las TI, estarán integrados dentro de la gestión de riesgos de la empresa.

- **Optimización de recursos:** Se tendrá que contar con los recursos necesarios, adecuados y eficaces para cumplir con las necesidades y objetivos del negocio, por los que estos recursos solo serán mantenidos o adquiridos cuando sean necesarios para el negocio y en el nivel en que se necesiten.

El gobierno de TI cuenta con 5 principales áreas (alineación estratégica, entrega de valor, gestión de riesgos, gestión de los recursos y medición del desempeño) las cuales funcionan como un ciclo que permite gobernar adecuadamente las tecnologías [ITGI, 2003].

2.1.5 Alineación estratégica

La alineación estratégica es uno de los dominios del gobierno de TI y se encarga de que la estrategia de TI soporte la estrategia del negocio y que las operaciones en TI estén alineadas con las operaciones actuales de la empresa [ITGI, 2003]. Esta alineación no ocurre de manera casual, pues requiere de una gestión activa y enfocada, a todos los niveles y actividades dentro de la empresa [ITGI, 2005a].

Además se necesita de un liderazgo y compromiso a alto nivel para realizar esta alineación, por lo que se requiere la participación activa del gerente general y del directorio, para tomar la responsabilidad de [ITGI, 2005a]:

- Garantizar que la estrategia de TI está alineada con la estrategia del negocio.
- Garantizar que TI entregue valor a la estrategia.
- Dirigir la estrategia de TI balanceando las inversiones en los sistemas que soportan y hacer crecer la empresa.
- Tomar las decisiones sobre el enfoque y uso de los recursos de TI.

- Garantizar que las TI y los recursos del negocios están disponible para habilitar que las TI entreguen lo esperado.

Para poder lograr la alineación estratégica en el caso de estudio va a ser necesario conocer cuáles son las necesidades del negocio las cuales servirán para identificar y alinear los objetivos de TI.

2.1.6 Entrega de valor

La entrega de valor es uno de los dominios del gobierno de TI, el cual se encarga de ejecutar la propuesta de valor, garantizando que las TI entreguen los beneficios prometidos, optimizando los costos y probando el valor intrínseco de TI [ITGI, 2005b].

Los principios básicos de la entrega de valor de TI son cumplir con los tiempos y presupuesto establecidos, brindar la calidad adecuada y lograr los beneficios que se trazaron, pero esta entrega de valor necesita ser traducida en términos de negocio como: contar con ventaja competitiva, clientes satisfechos, tiempo de espera de los clientes, productividad de los empleados, entre otros [ITGI, 2003]. Es por eso que es importante que primero se haya realizado la alineación estratégica, la cual permite habilitar la entrega de valor de TI y proveer un mismo lenguaje para expresar el cumplimiento de los objetivos de TI en términos de negocio, así como establecer indicadores para medir el cumplimiento de los objetivos identificados [ITGI, 2003].

En el gobierno de TI a diseñar se realizará la entrega de valor luego de identificar y aplicar los procesos habilitadores que soportan los objetivos de TI establecidos en la alineación estrategia.

2.1.7 Gestión de riesgos

La gestión de riesgos es uno de los dominios del gobierno de TI, el cual se encarga de asegurar que el cumplimiento de los objetivos de la empresa no esté en peligro por las fallas que pueden ocurrir en TI, sean estas operacionales, de seguridad o de

proyectos fallidos, trayendo consecuencias devastadoras [ITGI, 2005c]. Por ello el gobierno de TI debe de gestionar los riesgos de los procesos que forman parte del su alcance.

2.1.8 Gestión de recursos

La gestión de recursos es uno de los dominios del gobierno de TI, que busca mejorar el rendimiento de TI, optimizando las inversiones, el uso y la asignación los recursos de TI (personas, aplicaciones, infraestructura y datos) para brindar servicios según las necesidades del negocio [ITGI, 2003]. Estos servicios deben de estar claramente definidos así como los niveles de servicios acordados, lo cual va a permitir ahorrar costos y contar con un adecuado entendimiento para introducir, reemplazar o actualizar los recursos de TI [ITGI, 2003].

2.1.9 Medición del desempeño

La medición del desempeño es uno de los dominios del gobierno de TI, que permite saber si está cumpliendo con los objetivos que se han planteado al inicio del proceso del gobierno de TI [ITGI, 2005d]. Existen métodos tradicionales para realizar la medición del desempeño como es realizar el cálculo del retorno de inversión, pero el cual solo puede ser usado para activos tangible (proyectos o sistemas de TI), por lo se opta por usar métodos más actuales como el Cuadro de Mando Integral-CMI (*Balanced Scorecard*) que permite medir tanto valores tangible como lo intangible [ITGI, 2005d].

Las medidas del desempeño de los sistemas de información y TI son de gran importancia para la estrategia de la empresa por las siguientes razones [PASTOR, 2012]:

- Una adecuada gestión es el factor dominante para la realización de la ventaja competitiva sostenible.

- Las innovaciones tecnológicas pueden cambiar la estructura actual de la industria o crear una nueva.
- Las tecnologías afecta a todas las actividades de la empresa.
- Los procesos de negocio no aceptan errores
- El éxito de los sistemas de información es un proceso vital para toda la empresa.

2.1.10 Cuadro de Mando Integral – CMI

El CMI es una herramienta que permite medir el desempeño empresarial desde 4 perspectivas diferentes [ITGI, 2003]:

- **Financiera:** Relacionada a los objetivos financieros se deben lograr para satisfacer a los stakeholders
- **Cliente:** Relacionada a las necesidades de los clientes que se están cumpliendo para cumplir con los objetivos financieros.
- **Proceso interno:** Relacionada a los proceso de negocio interno que deben de sobresalir para a satisfacer a los clientes y stakeholders.
- **Aprendizaje:** Relacionada a cómo la organización debe de aprender e innovar para cumplir con las metas.

En el caso de TI el CMI va permitir evaluar el rendimiento de TI para cumplir la alineación entre TI y el negocio [ITGI, 2003].

2.1.11 COBIT 5: Framework

COBIT 5 es un marco de negocio para el gobierno y gestión de las TI elaborada por ISACA en el 2012, en esta versión íntegra las guías de COBIT 4.1, Val IT 2.0, Risk IT y BMIS (Modelo de Negocio para la Seguridad de la Información) y se alinea con otros estándares como ISO/IEC 38500, ITIL V3 2011, ISO/IEC 20000, la serie de ISO/IEC 27000, la serie de ISO/IEC 31000, TOGAF, CMMI y PRINCE2 [ISACA, 2012c].

Este marco provee una ayuda para que las empresas de cualquier tipo y tamaño puedan alcanzar sus objetivos de gobierno y gestión de las TI, para esto se basa en 5 principios claves [ISACA, 2012c]:

- **Principio 1 - Satisfacer las necesidades de los Stakeholders:** Permite la creación de valor del negocio para satisfacer a sus stakeholders mediante el uso de las TI, para eso usa la cascada de metas la cual permite alinear las metas corporativas y relacionarlas con las metas de TI.

- **Principio 2 - Cubrir totalmente la empresa:** No se enfoca solo en la función de TI sino hace que el gobierno y la gestión de TI se integren con el gobierno corporativo, incluyendo los habilitadores del gobierno, alcance del gobierno y roles, actividades y relaciones.

- **Principio 3 - Aplicar un único marco de referencia integrado:** Debido a que COBIT 5 toma las mejores prácticas de otros estándares y se presenta como un marco principal de alto nivel que pueda cubrir un mayor aspecto de manera integrada.

- **Principio 4 - Habilitar un enfoque holístico:** A través de sus habilitadores COBIT 5 ayuda a implementar un efectivo y eficiente gobierno y gestión de las TI. Sus habilitadores son los siguientes:

    - ✓ Principios, Políticas y Marcos de Trabajo
    - ✓ Procesos
    - ✓ Estructuras Organizacional
    - ✓ Cultura, Ética y Comportamiento
    - ✓ Información
    - ✓ Servicios, Infraestructuras y Aplicaciones
    - ✓ Personas, Habilidades y Competencias

- **Principio 5 - Separar gobierno de la gestión:** Realiza una clara distinción entre el gobierno de TI y la gestión de TI, ya que cada una tiene un propósito distinto.

El gobierno se encarga de determinar que se alcancen las metas corporativas a través de la evaluación, dirección y monitoreo de sus objetivos, mientras que la gestión se encarga de la ejecución de las decisiones establecidas por el gobierno.

2.1.12 Modelo de referencia de procesos de COBIT 5

El modelo de referencia de procesos de COBIT 5, son los procesos habilitadores que van a formar parte del gobierno de TI. En este modelo presenta los 37 procesos del gobierno de TI, los cuales se dividen 5 procesos de gobierno y 32 procesos de gestión, así mismo estos procesos habilitadores se agrupan en 5 dominios los cuales son [ISACA, 2012c]:

- **Evaluar, dirigir y monitorear**: Cuenta con 5 procesos para gobernar y gestionar las inversiones en TI.
- **Alinear, planear y organizar**: Cuenta con 13 procesos para proveer orientaciones en las planificaciones de las adquisiciones en TI.
- **Construir, adquirir e implementar**: Cuenta con 10 procesos para proveer una guía en el proceso de solicitar y adquirir las implementaciones de las soluciones en TI.
- **Entregar, servicio y soporte**: Cuenta con 6 procesos para gestionar la entrega y el soporte de las soluciones en TI.
- **Monitorear, evaluar y medir**: Cuenta con 3 procesos para guiar a los gestores a monitorear y evaluar el proceso de adquisición, así como definir los controles internos para asegurar que las adquisiciones sean apropiadamente gestionadas.

Para cada uno de los procesos habilitadores se describen las prácticas claves de gobierno con su respectiva matriz RACI [ISACA, 2012c]. Así mismo, las Prácticas clave de gobierno cuentan con actividades, entradas y salidas que permiten desarrollar los procesos habilitadores del gobierno de TI del caso de estudio [ISACA, 2012c].

2.1.13 Matriz RACI

La matriz RACI permite asignar el nivel de responsabilidad que está asumiendo cada uno de los roles y estructura organizativa de la organización en cada práctica de clave de gobierno, estas responsabilidades son [ISACA, 2012c]:

- ***Responsible*** (Responsable): Es quien asegura que la actividad ha sido completada exitosamente.
- ***Accountable***: Es quien tiene la última responsabilidad sobre un tema, proceso o alcance.
- ***Consulted*** (Consultado): Son las personas brindar la información para realizar una actividad.
- ***Informed*** (Informado): Son las personas a quienes hay que informar sobre el progreso de las actividades.

2.2 Marco regulatorio / legal

2.2.1 Introducción

La AFP se encuentra regulada por la SBS (Superintendencia de Banco y Seguros), por lo cual está obligada a cumplir con toda la regulación que la SBS emita. Además debe de cumplir con todas las leyes que rigen a las empresas que operan en el Perú.

Debido a que se va implementar el gobierno de TI en una AFP y el enfoque se va realizar es el de seguridad de la información, es necesario incorporar las regulaciones y leyes a las que está sujeta la AFP y estén relacionadas con dicho enfoque para que formen parte del alcance del gobierno de TI.

2.2.2 Resolución 2116:2009 - Reglamento para la gestión del Riesgo Operacional

En esta resolución la SBS establece el Reglamento para la gestión de Riesgo Operacional, en la cual indica que dentro de la gestión de riesgos operativos se debe de gestionar los riesgos ocasionados por la tecnología de información como [SBS, 2009b]:

- Fallas en la seguridad y continuidad operativa de los sistemas informáticos
- Errores en el desarrollo e implementación de los sistemas informáticos
- Compatibilidad e integración de los sistemas informáticos
- Problemas de calidad de información
- La inadecuada inversión en tecnología
- Entre otros aspectos

Este factor de riesgo va a tener que ser identificados dentro del gobierno de TI y debe de estar alineado a la gestión de riesgos operacional del caso de estudio.

2.2.3 Circular No G-140-2009 - Gestión de la seguridad de la información

Esta circular está basada en la ISO 17799 e ISO 27001 y exige que se cumplan con ciertas actividades mínimas para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), de la estructura organizacional y los controles de seguridad [SBS, 2009a]. Se tendrá que evidenciar ante la SBS el cumplimiento de todas estas actividades mínimas exigidas, sino la empresa se verá expuesta a las sanciones que la SBS vea conveniente [SBS, 2009a]. Por lo tanto se tendrán que cumplir con esta circula en el diseño del gobierno de TI.

2.2.4 Ley N° 29733 - Ley de Protección de Datos Personales

Esta ley se encuentra vigente desde el 8 de mayo del 2013, la cual tiene como objetivo garantizar la protección de los datos personales a través de un adecuado tratamiento [CONGRESO DE LA REPUBLICA, 2011].

La ley define datos personales a "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados" [CONGRESO DE LA REPUBLICA, 2011]. Por lo que se va a tener que considerar el cumplimiento de esta Ley al momento de usar datos personales dentro de los procesos del negocio del caso de estudio.

La ley establece 9 principios rectores para resolver problemas relacionados a la aplicación de esta ley y su reglamento, los cuales son [CONGRESO DE LA REPUBLICA, 2011]:

- **Principio de legalidad:** El tratamiento de los datos personales se realizan conforme la ley
- **Principio de consentimiento:** Para el tratamiento de los datos personales se debe de contar con el consentimiento del titular
- **Principio de finalidad:** La finalidad de la recopilación de los datos debe de ser determina, explicita y licita.
- **Principio de proporcionalidad:** El tratamiento que se debe de dar a los datos personales deben de cumplir con la finalidad por la cual se recopilo.
- **Principio de calidad:** Los datos personales deben de encontrarse en las condiciones necesarias respecto a finalidad para la que fueron recopilados y solo el tiempo necesario para cumplir su fin.
- **Principio de seguridad:** Se debe de garantizar la seguridad de los datos personales, con medidas de seguridad apropiadas y acordes al tratamiento que se le va a dar
- **Principio de disposición de recurso:** Debe de haber vías administrativas o jurisdiccionales para reclamar en caso se haya vulnerado el tratamiento de los datos personales
- **Principio de nivel de protección adecuado:** Los datos personales que se vayan a trata fuera del Perú deben de cumplir como mínimo lo exigido ante la presente ley.
- **Valor de los principios:** Los personas que intervengan con relación a los datos personales, debe de ajustarse a estos principios.

2.3 Estado del arte

2.3.1 Introducción

En la actualidad, el incremento de la relación entre las tecnologías de información y el negocio ha dado pase a que las TI se conviertan en un elemento estratégico y por lo cual deban de ser gobernado adecuadamente para el cumplimiento de los objetivos del negocio. Los marcos para el gobierno de TI proponen los lineamientos generales a considerar en el diseño del gobierno de TI, pero estos deben de ser adaptados a las necesidades y la situación de cada empresa.

2.3.2 Objetivos de la revisión del estado del arte

El objetivo de la revisión del estado del arte es mostrar el proceso de implementación del gobierno de TI en otras empresas administradoras de fondo de pensiones, así como conocer la metodología que utilizaron y el resultado de dicha implementación.

2.3.3 Método usado en la revisión del estado del arte

Se utilizó el método tradicional para buscar casos de éxito de modelos de implementación del Gobierno de TI en empresas que administradoras de fondo de pensiones, durante el periodo de enero hasta junio del 2015 y la información se obtuvo en la base de datos de ISACA y ProQuest.

2.3.4 Pension-Fennia

Pension-Fennia forma parte del grupo Finnish Fennia que provee administración de pensiones, seguros generales y seguros de vida desde 1998. Pension-Fennia usaba el modelo de COSO ERM para las autoevaluaciones de control interno en sus unidades de negocio, pero luego de un tiempo el director de TI y el director de auditoría conversaron acerca del área TI con el objetivo que esta pueda obtener un mejor entendimiento de las necesidades del negocio y mejorar los servicios de TI. Como resultado identificaron la necesidad de obtener un mayor aseguramiento de los controles TI y decidieron empezar a usar el modelo de madurez de COBIT [ISACA, 2008].

Por lo que el área de TI en Pension-Fennia comenzó el proceso de autoevaluación asistiendo a una capacitación de dos días para obtener un mejor conocimiento del gobierno de TI y el marco COBIT. Luego la gerencia de TI junto con un experto externo evaluaron los 24 procesos, midiendo el nivel de madurez de los controles actuales sobre cada proceso y definieron los niveles de madurez que desean alcanzar. Para completar este vacío entre los niveles actuales y futuros, se priorizaron y agruparon acciones de mejoras en un plan de mejora del gobierno de TI, no solo incluyendo a TI sino a todas las unidades de negocio y proveedores de servicios externos [ISACA, 2008].

Además se aprovechó en usar COBIT para los aspectos de madurez que no incluye el marco de COSO ERM, por lo cual combinaron ambos marcos, obteniendo un gran beneficio de esta combinación. Como resultado del proyecto COBIT todas las áreas se beneficiaron del proyecto, así como les permito aclarar las metas, roles y responsabilidades mutuas en la empresa [ISACA, 2008].

2.3.5 Ontario Pension Board

Ontario Pension Board (OPB) administra el Plan de Pensiones del Servicio Público (PSPP) auspiciado por el gobierno de Ontario de Canadá. OPB cuenta con más de CAN$15 billones en activos, 150 empleados, 34,600 miembros activos, 36,900 pensionista y 4,800 miembros diferidos [ISACA, 2007].

El costo total de las operaciones de la PSPP en el 2006 fue CAN$41.6 millones, es por eso que OPB tiene bien definido la estructura de sus operaciones, usa altos estándares profesionales y toma un énfasis considerable en un sólido marco de gobierno. Por lo que en el 2006 OPB se trazó planes de acción como: actualizaciones de sistemas de TI, mejorar la entrega del servicio, entre otros, para garantizar que cuentan con las personas, procesos y tecnología necesarios para asegurar la pensión prometida a los pensionistas y proveer un mejor servicio personalizado a todos sus clientes y stakeholders. Los cual lo lograría mediante el aprovechamiento de las tecnologías y marcos de gestión actuales [ISACA, 2007].

Dado el objetivo del negocio que se quería cumplir era proveer un mejor, rápido e inteligente servicio orientado a sus clientes. El departamento de proyectos y de TI consideraron los mejores métodos y herramientas, junto con la mejora del Gobierno de TI y control [ISACA, 2007].

Debido a que OPB desconocía del tema de Gobierno de TI contrató un servicio de consultoría a The Manta Group, la cual era una empresa con una sólida experiencia en el uso de COBIT, el cual lo recomendó como el marco para implementar Gobierno de TI. OPB uso COBIT 4.0 para [ISACA, 2007]:

- Construir un ambiente de control usando COBIT para la estructura de TI y sus servicios para cumplir con los objetivos del negocio.
- Analizar el estado actual de los servicios entregados a OPB y su interrelación con los servicios actuales de outsourcing.
- Definir claramente la integración de los servicios de TI, proyectos y sus proveedores de outsourcing.
- Realizar un análisis de brecha para llegar del modelo actual y al deseado.

La evaluación incluyo un total de 34 objetivos de control y 215 objetivos de control detallados de COBIT, el cual se utilizó para proveer un mejor entendimiento de las mejoras prácticas de servicios de TI y gobierno de TI. Además se utilizó una metodología para realizar la autoevaluación del nivel de madurez de los objetivos de control, la cual fue todo un éxito [ISACA, 2007].

2.3.6 Ayin Banking Group

Ayin Banking Group es una empresa del sector financiero que implementó un modelo de gobierno de TI a través de la planificación estratégica, la cual consistió en 5 fases [BERMEJO, 2012]:

- **Fase 1 - Alineamiento de TI con el negocio:** En esta fase se creó la base para promover la alineación estratégica, para lo cual se empezó conociendo el contexto actual de la organización e identificando y definiendo los objetivos

de TI, los cuales se van a alinear con los objetivos del negocio [BERMEJO, 2012].

- **Fase 2 - Evaluación del rendimiento y la capacidad:** En esta fase se verificó la capacidad actual del área de TI, para lo que se identifica y evalúa la madurez de los procesos críticos de TI en base a los objetivos de negocio propuesto para TI, además se realizó un análisis FODA de los recursos de TI (información, personal, aplicaciones e infraestructura) y por último se encuesto y analizó la matriz de acordada del gobierno de TI [BERMEJO, 2012].

- **Fase 3 - Planificación estratégica de TI:** En esta fase se propuso los indicadores para medir el cumplimiento de los objetivos definidos y la eficiencia de los procesos críticos, también se definieron las acciones estratégicas que deben de cubrir la eliminación o reducción de brechas identificadas en la fase 2, y el desarrollo de mando de control integral para TI [BERMEJO, 2012].

- **Fase 4 - Planificación táctica de TI:** En esta fase se formularon los planes de acción para alcanzar las estrategias del negocio y de TI, por lo se crearon: proyectos estratégicos, estrategias para la adquisición de los recursos de TI, para la capacitación del personal y para el outsourcing de los servicios de TI [BERMEJO, 2012].

- **Fase 5 - Socialización y cierre:** En esta fase el resultado del planeamiento es validado, por lo que se revisa y valida los resultados que se acordaron para el gobierno de TI, para luego comunicar los resultados a todos los interesados de la organización y poder seguir con el compromiso de los involucrados para seguir con la ejecución del proyecto [BERMEJO, 2012].

2.3.7 Banco HDFC

El banco HDFC opera con un ambiente altamente automatizado en TI y en sistemas de comunicación, lo que le permite realizar diversas actividades a sus clientes. Dado este compromiso con sus clientes la TI es un activo clave que necesita ser gobernado que le permita posicionarse en el mercado y crear ventaja competitiva [ISACA, 2014].

En este caso el banco ya contaba con COBIT 4.1, pero al salir la nueva versión se tuvieron que implementar los 7 habilitadores para realizar el gobierno de TI, los cuales fueron:

- **Principios, políticas y marco de referencia**

Con este habilitador se transformaría el comportamiento deseado de seguridad en prácticas diarias de gestión, por lo que se crearon políticas que cubrirían los 11 dominios de la ISO 27001 y adicionalmente dada la variedad de tecnologías que tenían se crearon políticas para cada una de estas [ISACA, 2014].

- **Procesos**

En este habilitador se describieron las prácticas y actividades para cada uno de los procesos que permitirían alcanzar los objetivos relacionados a TI. En este caso se siguió un modelo de procesos de seguridad de la información basado en 21 componentes, entre los que sobresalen: La seguridad de las aplicaciones, criptografía, gestión de incidentes, seguridad de banca en línea, entre otros. Cada uno de estos componentes contribuye a la construcción de los estándares de control y procedimientos de control que satisfagan los requerimientos de las políticas previamente definidas [ISACA, 2014].

- **Estructuras organizativas**

El banco HDFC creó un grupo responsable de la identificación, evaluación y mitigación de los riesgos relacionados a la seguridad de la información, el cual estaría liderado por el oficial de seguridad de la información, quien reportaría directamente al directorio del banco. Adicionalmente debido al compromiso del banco con la seguridad de la información, se implementaron una serie de comités a

nivel gerencial para tener en cuenta los temas de seguridad de la información como parte de su agenda. Por ultimo para la definición de los roles y responsabilidad de la seguridad de la información se utilizó una matriz RACI y se involucró a todas las áreas del banco [ISACA, 2014].

- **Cultura, ética y comportamiento**

Este habilitador fue uno de los principales factores contribuyentes para el éxito del gobierno de TI para el banco HDFC, lo cual le permitió definir 8 tipos comportamientos que aportaron a la cultura de seguridad de la información. Así mismo se definieron políticas, reglas y normas claras los cuales embebieron dentro de las prácticas diarias de todos los colaboradores [ISACA, 2014].

- **Información**

La información es uno de los principales activos para que las empresas puedan operar correctamente y consciente de ello se definió dentro de la gestión de la seguridad, que la información de uso estratégico, del presupuesto, del planeamiento y las políticas contarán con requerimientos de seguridad de información los cuales serán revisadas dentro de los comités que se establecieron, a fin de que la información se encuentre adecuadamente resguardada. Adicionalmente se prepararán varios informes de las revisiones de seguridad, auditorias, análisis de amenazas, vulnerabilidad, incidentes, entre otros [ISACA, 2014].

- **Servicio, infraestructura y aplicaciones**

El banco HDFC usa más de 40 tecnologías diferentes los cuales soportan los diferentes servicios, infraestructura y aplicaciones del banco, por lo que son medidos constantemente para identificar el nivel de madurez de seguridad en el que se encuentran cada uno de ellos al brindar los servicios [ISACA, 2014].

- **Personas, habilidades y competencias**

En este habilitador el banco HDFC ha desarrollado una serie de técnicas para crear conciencia acerca de la seguridad de la información y construir las habilidades y competencias adecuadas en todo el personal. Entre las principales actividades que se

realizaron fueron: La creación de una película de seguridad de la información, cursos de seguridad, difusión de los 10 mandamientos de la seguridad, entre otros [ISACA, 2014].

2.3.8 Conclusiones sobre el estado del arte

De los casos de modelo de implementación presentados se puede concluir lo siguiente:

- No se cuenta con modelos de implementación de gobierno de TI con enfoque en seguridad de información para empresas administradoras de fondo de pensiones.
- Se debe de contar con objetivos de negocio claramente definidos que se desea que sean cubiertos por el Gobierno de TI.
- Para desarrollar el gobierno de TI, no solo es necesaria la participación del área de TI, sino que se va a requerir de un trabajo con las demás unidades del negocio e involucrar a la alta gerencia para brindar los lineamientos de negocio que se desea cubrir con el Gobierno de TI.
- El área de TI debe estar en la capacidad de satisfacer las necesidades actuales del negocio.
- Los controles en TI permiten mejorar los servicios de TI, pero es importante que se mida el nivel de madurez de estos controles.
- Capacitar al personal en temas de gobierno de TI es un aspecto clave para que la implementación de este gobierno o contratar un servicio de consultoría que cuente con el personal que tenga la experiencia adecuada en la implementación del Gobierno de TI.
- Se pueden usar más de un marco de control con la finalidad de cubrir las faltantes que se puedan encontrar.
- En caso se actualice el marco de referencia usado para el gobierno de TI, se debe de analizar los cambios que se tendrían que hacer para migrar a la versión actual.

3 CAPÍTULO 3

3.1 Objetivo específico 1: Desarrollar la alineación estratégica entre los objetivos de negocio y TI.

En este capítulo se identificará las necesidades de los stakeholders que necesitarán ser cubiertas dentro del gobierno de TI, por lo que se usará el marco de COBIT 5 para poder trasladar estas necesidades en objetivos de negocios e identificar los objetivos de TI que cubren los objetivos de negocio. Así mismo cada objetivo de negocio y de TI tendrá asociada un conjunto de métricas dentro de un cuadro de mando integral que permitirá medir el cumplimiento del objetivo de los objetivos.

3.1.1 Resultado Esperado 1: Documento que contenga los objetivos de TI identificados que soportan los objetivos del negocio los cuales satisfacen las necesidades del negocio del caso de estudio y el cuadro de mando integral para cada objetivo identificado.

3.1.1.1 Las necesidades del stakeholders son:

Según el contexto actual de la empresa se han identificado las siguientes necesidades de los stakeholders:

- Mejorar la satisfacción y atención al cliente
- Reducir la cantidad de observaciones internas y externas
- Ser eficientes al realizar las operaciones del negocio
- Realizar innovación tecnológica según las oportunidades y necesidades del negocio
- Mantener un adecuado clima laboral

3.1.1.2 Identificación y justificación de los objetivos de negocio

Cada necesidad de los stakeholders será relacionada con los objetivos de negocio COBIT 5, justificando adecuadamente su elección.

Necesidad del negocio	Mejorar la satisfacción y atención al cliente.
Objetivo de negocio	• Cultura de servicio orientada al cliente. • Continuidad y disponibilidad de los servicios del negocio.
Justificación	Para poder mejorar la satisfacción y atención al cliente es necesario que dentro de la empresa se tenga una cultura de servicio orientada al cliente para que se pueda atender adecuadamente al cliente, así como contar con los servicios disponibles para atenderlos.

Tabla 3.1 Objetivos de negocio relacionados a la 1ra necesidad del negocio.

Necesidad del negocio	Reducir la cantidad de observaciones internas y externas.
Objetivo de negocio	• Cumplir con leyes y regulaciones externas. • Cumplir con las políticas internas.
Justificación	Debido a que la empresa se encuentra en el Perú debe cumplir las leyes que se encuentre vigente tal como la Ley 29773 de Protección de datos Personales, así como cumplir con las regulaciones de la SBS. Como la circula N°140. Además de las políticas internas aprobadas por el directorio.

Tabla 3.2 Objetivos de negocio relacionados a la 2da necesidad del negocio.

Necesidad del negocio	Ser eficientes al realizar las operaciones del negocio.
Objetivo de negocio	• Optimización de los costos del proceso del negocio • Productividad operacional y del personal.
Justificación	Para lograr la eficiencia en las operaciones se debe lograr que las operaciones y el personal sean productivos al realizar sus labores

	así como optimizar los costos incurridos en los procesos del negocio.

Tabla 3.3 Objetivos de negocio relacionados a la 3ra necesidad del negocio.

Necesidad del negocio	Realizar innovación tecnológica según las oportunidades y necesidades del negocio.
Objetivo de negocio	• Portafolio de productos y servicios competitivos • Cultura de innovación de producto y negocio
Justificación	Dado el rápido avance en la tecnología se busca que las innovaciones tecnológicas permitan generar productos y servicios competitivos según las oportunidades y necesidades del negocio. Así como contar con una cultura interna de innovación que permita mejorar la operatividad en la empresa.

Tabla 3.4 Objetivos de negocio relacionados a la 4ta necesidad del negocio.

Necesidad del negocio	Mejorar el clima laboral
Objetivo de negocio	• Personal preparadas y motivado
Justificación	Como parte de mejorar el clima laboral se necesita fomentar que el personal se encuentre motivado al realizar sus labores, lo cual permite que tengan un mejor desempeño e integración en el trabajo. Además de capacitar a su personal apoyando su desarrollo profesional y desempeño laboral.

Tabla 3.5 Objetivos de negocio relacionados a la 5ta necesidad del negocio.

3.1.1.3 Métricas de los objetivos de negocio seleccionados

Por cada objetivo de negocio se ha desarrollado un conjunto de métricas adaptadas a la empresa dentro de un cuadro de mando integral, con la finalidad de medir el cumplimiento de los objetivos del negocio.

Perspectiva del cuadro de mando integral	Objetivo de negocio	Métrica
Financiera	Portafolio de productos y servicios competitivos	• Porcentaje de productos y servicios que alcanzan o exceden los objetivos de ingresos o la cuota del mercado. • Porcentaje de productos y servicios que brindan una ventaja competitiva.
	Cumplir con leyes y regulaciones externas.	• Costo de incumplimientos regulatorios externos. • Cantidad de observaciones por incumplimiento regulatorio externo. • Porcentaje de observaciones externas no resultas en el plazo establecido.
Cliente	Cultura de servicio orientada al cliente.	• Cantidad de quejas de clientes. • Porcentaje de clientes retenidos. • Porcentaje de nuevos clientes.
	Continuidad y disponibilidad de los servicios del negocio.	• Cantidad de interrupciones de servicio al cliente con daños significativos. • Cantidad de horas de información perdida por una interrupción en el negocio.
Proceso interno	Optimización de los costos del proceso del negocio	• Nivel de satisfacción del directorio por los costos de operación de los procesos. • Porcentaje del costo reducido en los procesos del negocio.
	Productividad operacional y del personal.	• Cantidad de proyectos ejecutados dentro del presupuesto y tiempo plantificado.

	Cumplir con las políticas internas.	• Cantidad de observaciones por incumplimiento de las políticas internas. • Porcentaje de observaciones internas no resultas en el plazo establecido. • Porcentaje de políticas diseñadas bajo estándares y buenas Prácticas efectivas.
Aprendizaje y crecimiento	Personal cualificado y motivado	• Nivel de satisfacción del directorio por las habilidades y conocimiento del personal. • Porcentaje del personal satisfecho con la empresa. • Porcentaje del personal retenido.
	Cultura de innovación de producto y del negocio	• Cantidad de iniciativas aprobadas para los productos debido a alguna innovación. • Cantidad de veces que se fomenta la cultura de innovación al personal de la empresa.

Tabla 3.6 Métricas de los objetivos de negocio seleccionados.

3.1.1.4 Identificación de objetivos de TI relacionados a los objetivos de negocio.

Por cada objetivo de negocio seleccionado, se tendrá un conjunto de objetivos de TI relacionados al cumplimiento del objetivo de negocio (Ir al anexo 1), esta relación puede ser primaria, cuando hay una importante relación del objetivo de TI con el objetivo del negocio, o secundaria, cuando todavía hay una relación fuerte, pero menos importante. Además cada objetivo de TI se encuentra relacionado a una perspectiva del cuadro de mando integral de TI.

3.1.1.5 Justificación de los objetivos de TI seleccionados

Objetivo de TI	Justificación
Alineamiento de TI y las estrategias del negocio.	Es necesario que las estrategias de TI se encuentren alineadas al negocio para que se pueda entregar valor a los stakeholders de las inversiones realizadas en TI.

Cumplimiento y soporte de TI para el cumplimiento de las leyes y regulaciones externas al negocio.	Dada la necesidad del negocio de reducir la cantidad de observaciones, TI debe de cumplir con las leyes y regulaciones a la que está expuesta la empresa y en cual esté involucrado.
Realización de beneficios del portafolio de inversiones y servicios de TI.	Las inversiones y servicios de TI deben de brindar los beneficios que se plantearon con la finalidad de no incurrir en pérdidas económicas y afectar directamente al presupuesto de la empresa.
Entrega de servicios de TI de acuerdo a los requisitos del negocio.	Los servicios de TI deben de cubrir las necesidades actuales de la empresa enfocándose en mejorar la atención al cliente.
Uso adecuado de aplicaciones, información y soluciones tecnológicas.	La empresa necesita ser eficiente en sus operaciones por lo que es necesario que las soluciones tecnológicas soporten los procesos del negocio adecuadamente.
Agilidad de las TI.	Se busca contar con una cultura de innovación para cubrir las oportunidades y necesidades del negocio, por lo que se necesita que las TI respondan en un tiempo adecuado.
Seguridad de la información, infraestructura de procesamiento y aplicaciones.	La información que se maneja en la empresa es de carácter confidencial, por lo tanto todo la tecnológico que la soporta debe de garantizar que la información este segura.
Optimización de los activos, recursos y capacidades de TI.	La optimización de los activos y recursos de TI ayudará a que la empresa use eficientemente sus recursos.

Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.	Los proyectos alineados a mejorar la atención del servicio al cliente deben de cumplir con los plazos establecidos y el presupuesto asignado.
Cumplimiento de las políticas internas de TI.	La empresa desea reducir la cantidad de observaciones que podría tener por incumplimiento de una política interna relacionada a TI.
Personal del negocio y de TI competente y motivado.	Como parte de mantener un adecuado clima laborar es necesario que el personal se encuentre motivado para realizar sus labores y contribuir con el avance de la empresa.

Tabla 3.7 Justificación de los objetivos de TI seleccionados.

3.1.1.6 Métricas de los objetivos de TI seleccionados

A continuación por cada objetivo de negocio se ha desarrollado un conjunto de métricas adaptadas a la empresa, con la finalidad de medir el cumplimiento de los objetivos de TI.

Perspectiva del cuadro de mando integral	Objetivo de TI	Métrica
Financiera	Alineamiento de TI y las estrategias del negocio.	• Porcentaje de objetivos de TI que soporten las estrategias del negocio. • Nivel de satisfacción del directorio con el alcance del portafolio de productos y servicios planificados.
	Cumplimiento y soporte de TI para el cumplimiento de las leyes y regulaciones externas al negocio.	• Costo por incumplimiento de las leyes y regulaciones relacionadas a TI. • Cantidad de incumplimientos de TI para las leyes y regulaciones externas.

	Realización de beneficios del portafolio de inversiones y servicios de TI.	• Porcentaje de inversiones en TI donde se cumplan los beneficios esperados. • Porcentaje de servicios de TI donde se obtienen los beneficios esperados.
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio.	• Porcentaje de stakeholders satisfechos de la entrega de los servicios de TI que cumplen con los requisitos del negocio. • Porcentaje de usuarios satisfechos de la calidad de entrega de los servicios de TI.
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	• Porcentaje de dueños de procesos satisfechos por el soporte de los productos y servicios de TI. • Nivel de entendimiento de los usuarios del negocio de como las soluciones tecnológicas soportan sus procesos.
Proceso interno	Agilidad de las TI.	• Nivel de satisfacción de la alta gerencia con la respuesta de TI ante nuevos requerimientos. • Tiempo promedio para que los objetivos estratégicos de TI sean iniciativas acordadas y aprobadas.

	Seguridad de la información, infraestructura de procesamiento y aplicaciones.	• Cantidad de incidentes de seguridad de la información que han causado pérdidas financieras, interrupción del negocio o mala reputación. • Porcentaje de cambios y eliminación de los privilegios en las cuentas realizadas en los tiempos establecidos. • Cantidad de vulnerabilidades identificadas en las pruebas de seguridad aplicadas a las aplicaciones e infraestructura que soporta la información crítica de la empresa.
	Optimización de los activos, recursos y capacidades de TI.	• Frecuencia de la evaluación de la madurez de la capacidad y de la optimización de costos de TI. • Nivel de satisfacción de la alta gerencia de los costos y capacidades de TI.
	Entrega de programas que den beneficios en tiempo, presupuesto y satisfaga los requisitos y estándares de calidad.	• Porcentaje de proyectos entregados en tiempo y dentro del presupuesto. • Porcentaje de stakeholders satisfechos por la calidad de los proyectos. • Cantidad de proyectos que necesitan rehacerse debido defectos de calidad.
	Cumplimiento de las políticas internas de TI.	• Cantidad de incidentes relacionados al no cumplimiento de las políticas. • Porcentaje de políticas soportadas por estándares y buenas Prácticas adecuados. • Frecuencia de revisión y actualización de las políticas.

Aprendizaje y crecimiento	Personal del negocio y de TI competente y motivado.	• Porcentaje del personal de TI cuyas habilidades son suficientes para la competencia requerida en sus roles. • Porcentaje de personal de TI satisfecho con sus roles. • Cantidad de horas de capacitación por cada miembro de TI.
	Conocimiento, habilidad e iniciativas para la innovación del negocio.	• Nivel de concienciación y comprensión de la alta gerencia sobre las posibilidades de Innovación de TI. • Nivel de satisfacción de los stakeholders con las experiencias e ideas de innovación de TI. • Número de iniciativas aprobadas resultantes de ideas innovadoras de TI.

Tabla 3.8 Métricas de los objetivos de TI seleccionados.

3.2 Conclusiones del capitulo

- Se concluye de que las 5 necesidades del negocio pudieron ser relacionadas con 9 objetivos de negocio definidos en COBIT 5, lo cual va a permitir realizar la alineación estratégica entre los objetivos del negocio con los objetivos de TI.
- Se pudieron identificar 11 objetivos de TI para poder soportar los 9 objetivos del negocio, tomando en cuenta el enfoque de seguridad de la información.
- Se definieron 21 métricas relacionadas al cumplimiento de los objetivos del negocio y 26 métricas relacionadas al cumplimiento de los objetivos de TI. Estas métricas se encuentran dentro de la perspectiva del cuadro de mando integral y alienadas a los objetivos.

4 CAPITULO 4

4.1 Objetivo específico 2: Definir los procesos habilitadores del gobierno de TI para el cumplimiento de los objetivos de negocio de la empresa

En este capítulo se identificará los procesos habilitadores de COBIT 5, los cuales se les dará el enfoque de seguridad de la información y soportan los objetivos de TI seleccionados para el cumplimiento de las necesidades del negocio, para luego definir las actividades y la matriz de responsabilidades (matriz RACI) de cada proceso habilitador seleccionado.

4.1.1 Resultado Esperado 2: Identificación de los procesos habilitadores del gobierno de TI para el caso de estudio.

4.1.1.1 Identificación de los procesos habilitadores relacionados a los objetivos de TI

Para cada objetivo de TI seleccionado se identificarán los procesos habilitadores (Ir al anexo 2) que lo soportan indicando si la relación entre ambos es primaria (cuando hay una importante relación ente el proceso habilitador y objetivo de TI) o secundaria (cuando todavía hay una relación fuerte, pero menos importante), para luego identificar cuales formarán parte del alcance del gobierno de TI.

4.1.1.2 Selección de procesos para el alcance del gobierno de TI

Los procesos habilitadores que formarían como parte inicial del gobierno de TI según el entorno de la empresa y la relación de los procesos habilitadores identificados se seleccionaron los siguientes:

Dominio	Proceso
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno
	Asegurar la entrega de beneficios
	Asegurar la optimización del riesgo
	Asegurar la optimización de los recursos
Alinear, planear y organizar	Gestionar el marco de gestión de TI
	Gestionar la estrategia
	Gestionar la arquitectura empresarial

	Gestionar la innovación
	Gestionar el portafolio
	Gestionar los recursos humanos
	Gestionar las relaciones
	Gestionar los acuerdos de servicios
	Gestionar los proveedores
	Gestionar la calidad
	Gestionar el riesgo
	Gestionar la seguridad
Construir, adquirir e implementar	Gestionar los programas y proyectos
	Gestionar la definición de requisitos
	Gestionar la disponibilidad y capacidad
	Gestionar la habilitación de cambio organizacional
	Gestionar el cambio
	Gestionar el conocimiento
	Gestionar los activos
	Gestionar la configuración
Entregar, dar servicio y soporte	Gestionar las operaciones
	Gestionar las respuesta e incidentes del servicio
	Gestionar los problemas
	Gestionar la continuidad
	Gestionar la servicios de seguridad
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad
	Supervisar, evaluar y medir el sistema de control interno

Tabla 4.1 Procesos para el alcance del gobierno de TI.

4.1.1.3 Selección y justificación de los procesos habilitadores para el alcance del gobierno de TI bajo el enfoque de seguridad de la información

De los procesos habilitadores para el gobierno de TI, se identificaron que los siguientes procesos son necesarios desarrollarlos para asegurar la seguridad de la información.

Dominio	Proceso	Justificación
Evaluar, dirigir y monitorear	Asegurar el establecimiento y mantenimiento del marco de gobierno	Al momento de diseñar el gobierno de TI, se debe de considerar los requerimientos y regulaciones relacionadas a la seguridad de la información que van a formar parte del alcance del gobierno de TI.
	Asegurar la entrega de beneficios	Las inversiones relacionadas a los servicios y soluciones de seguridad de la información deben brindar beneficios a las necesidades del negocio de la empresa de manera efectiva y eficiente y a costos aceptables.
	Asegurar la optimización del riesgo	Los riesgos relacionados al uso de las TI deben de ser identificados y gestionados, sin exceder el apetito ni la tolerancia del riesgo de la empresa.
Alinear, planear y organizar	Gestionar el marco de gestión de TI	Como parte de la gestión de las TI se debe de establecer mecanismos y autoridades para la gestión de la seguridad de la información necesaria para cumplir con los objetivos del gobierno.
	Gestionar los recursos humanos	La cultura de la seguridad de la información debe de ser establecida adecuadamente en los recursos humanos de la empresa, así como definir las responsabilidades, estructuras organizativas, planes de capacitación y concientización en temas de seguridad.
	Gestionar los proveedores	Debido a que se cuenta con proveedores que manejan información de la empresa del caso de estudio, es necesario establecer controles y mecanismos para asegurar la seguridad de la información y el cumplimiento normativo.
	Gestionar el riesgo	Los riesgos asociados a TI deben de ser identificados, evaluados y controlados a los

		niveles establecidos por la empresa.
	Gestionar la seguridad	Se debe de definir, operar y monitorear el sistema de seguridad de la información, debido a que es un requisito establecido por el ente regulador (SBS) y por políticas internas de la empresa.
	Gestionar el cambio	Todos los cambios realizados en TI deben de ser adecuadamente controlados y gestionados para mitigar los riesgos que podrían repercutir negativamente en el negocio.
	Gestionar los activos	Se debe de identificar todos los activos de información para poder optimizar los costos y la entrega de valor de TI así como identificar si cumplen con los controles de seguridad la información.
Entregar, dar servicio y soporte	Gestionar las respuesta e incidentes del servicio	Dado el enfoque de seguridad información se debe de contar con canales para reportar los incidentes relacionados a la seguridad de la información y gestionar la atención lo más pronto posible con la finalidad recuperar los servicios a su estado normal.
	Gestionar la servicios de seguridad	Debido al enfoque de seguridad de la información, se debe de gestionar los servicios que permitan minimizar el impacto al negocio de los incidentes de seguridad de la información.
Monitorear, evaluar y analizar	Supervisar, evaluar y medir el rendimiento y la conformidad	Se debe de evaluar el rendimiento de los procesos según los acuerdos establecidos y evaluar la conformidad de los objetivos del negocio planteados en el gobierno de TI.
	Supervisar, evaluar y medir la conformidad con	Es necesario supervisar constante que se está cumpliendo con la regulación y leyes que involucra a TI y tienen que ver con la seguridad

	los requerimientos externos	de la información, para poder dar cumplimiento y que la empresa no caiga en infracciones.

Tabla 4.2 Selección y justificación de los procesos de TI.

4.1.2 Resultado Esperado 3: Definición de las actividades, roles y responsabilidades de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.

Para cada uno de los procesos habilitadores seleccionados para el enfoque de seguridad de la información del gobierno de TI, se van a definir cuáles van a ser las a actividades que deberían de realizarse y la matriz de responsabilidades (matriz RACI) del proceso habilitador (Ir al anexo 3).

En la matriz de responsabilidades (matriz RACI) se utilizará la siguiente nomenclatura para asignar las responsabilidades en las funciones y estructuras organizativas de la empresa.

Abreviatura	Descripción
R	*Responsible* (Responsable de ejecución)
A	Accountable (Responsable de mayor dirección y jerarquía)
C	*Consulted* (Consultado)
I	*Informed* (Informado)

Tabla 4.3 Responsabilidades de la matriz RACI.

4.2 Conclusiones del capitulo

-
- Se identificaron 31 procesos habilitadores de COBIT 5 que permiten formar el gobierno de TI según las necesidades del negocio, de los cuales se escogieron 14 procesos habilitadores debido al enfoque de seguridad de la información.
- Para los 14 procesos habilitadores se definieron sus actividades que van a permitir llevar a cabo el proceso habilitador, así como una matriz RACI para

asignar las responsabilidades de todos los involucrados en el proceso habilitador.

- Cabe resalta que se tiene que revisar periódicamente las actividades de los procesos habilitadores para evaluar la posibilidad de actualizar, eliminar o incorporar nuevas actividades según la tendencia de la seguridad de la información tanto a nivel de políticas internas como regulatorias.

5 CAPÍTULO 5

5.1 Objetivo específico 3: Identificar y valorar los activos de información, analizando los riesgos de seguridad de información asociados a los procesos de negocio a los que dan soporte.

En este capítulo se identificarán y valorarán los activos de información asociados a los procesos del negocio que forman parte del gobierno de TI, así como lo riesgos de seguridad de información que se puedan encontrar en estos procesos.

5.1.1 Resultado Esperado 4: Identificación y valoración de los activos de TI que soportan los procesos del negocio los cuales apoyan los objetivos del negocio.

Para poder gestionar los activos de información, primero se tendrá que definir un método alineado a la ISO/IEC 27005:2011 que permita identificar y valorar los activos de información que se encuentra en el proceso de negocio.

5.1.1.1 Método para la Identificación y valoración de los activos de información

- **Identificación de activos**

En esta etapa se necesita identificar los activos de información de la organización por lo que primero se necesita contar con los procesos de negocios actualizados y detallados, para identificar los activos de información que están soportando las actividades que se realizan en los procesos de negocio.

Por cada activo de información identificado se tendrá que registrar en un inventario de activos (Ir al anexo 4), indicando los datos del proceso (proceso, sub-proceso, actividad) en que se usa el activo de información, la descripción del activo (nombre del activo, descripción y tipo de activo), dueño del activo y formato (físico, digital, otro).

Los tipos de activos de información pueden ser:

Tipo	Descripción	Ejemplo
Primario	Es la información que fluye en las actividades que se realizan en los procesos del negocio.	Información vital, personal y estratégica.

Soporte	Son los activos que soportan los activos primarios de la empresa.	Hardware, software, redes, personal y ambiente.

Tabla 5.1 Tipos de activo de información.

- **Valoración de activos**

Luego de realizar la identificación de activos, el dueño del activo y el oficial de seguridad de la información tendrán que asignar a cada activo un valor de confidencialidad, integridad y disponibilidad, para luego obtener el valor final del activo, el cual será el promedio de la suma de estos tres valores.

Valor	Confidencialidad	Integridad	Disponibilidad
1	Información de carácter público, que no está restringida a un proceso de negocio.	Información cuya modificación no autorizada, no afecta la operación de la empresa	La información no cuenta con carácter de urgencia de recuperación.
2	Información que está restringida a los involucrados de un proceso de negocio, pero que no contiene datos personales de los clientes, ni financieros de la empresa.	Información cuya modificación no autorizada, podría ocasionar pérdidas leves para la empresa	La información no debe de estar indisponible más de 1 días.
3	Información que está restringida a los involucrados de un proceso de negocio, pero contiene datos personales de los clientes y financieros de la empresa.	Información cuya modificación no autorizada, podría ocasionar pérdidas graves para la empresa.	La información no debe de estar indisponible más de 8 horas.

4	Información de carácter estratégico, entregada a un grupo selecto de usuarios.	Información cuya modificación no autorizada, podría ocasionar pérdidas muy graves para la empresa.	La información no debe de estar indisponible más de 1 hora.

Tabla 5.2 Tabla de valoración de activos de información.

Esta actividad tendrá que ser realizada o actualizada por lo menos una vez al año.

5.1.2 Resultado Esperado 5: Matriz de riesgos

Para poder gestionar los riesgos de seguridad de la información, primero se tendrá que definir un método alineado a la ISO 31000:2009 que permita valorar (identificar, analizar y evaluar los riesgos) y tratar los riesgos (opciones de tratamiento, tipo y modos de control) que se encuentra en el proceso de negocio.

5.1.2.1 Método para la gestión de riesgo de seguridad de la información

Valoración del riesgo

a) Identificación del riesgo

Para cada proceso de negocio se tendrá que identificar los posibles riesgos que podrían afectar la confidencialidad, integridad o la disponibilidad de la información dentro de los procesos de negocio. Para ello el Oficial de Seguridad de la Información junto con el dueño del proceso identificaran la siguiente información asociada a los posibles riesgos del proceso (la causa o fuente de riesgo, el evento, el riesgo y las posibles consecuencias del riesgo).

En esta etapa se tiene que identificar todos los riesgos, aun estos no sean evidentes, dado que si un riesgo no es identificado no se podrá realizar el análisis ni el tratamiento del riesgo.

Fuente de riesgo (causa): Es lo que tiene el potencial intrínseco para originar el riesgo, lo cual puede ser la tecnología, las personas, procesos, eventos externos, entre otros.

Evento: Acontecimiento o cambio de un conjunto particular de circunstancias.

b) Análisis de riesgo

El análisis de riesgo es responsabilidad de los dueños de procesos del negocio con asesoría del Oficial de Seguridad de la Información, para identificar la probabilidad y el nivel de impacto que puede ocasionar la materialización del riesgo.
Para identificar el nivel de probabilidad se utilizará el siguiente criterio:

Probabilidad		
Nivel	Descripción	Detalle
1	Eventual	Puede ocurrir rara vez, de manera eventual a lo largo del año.
2	Ocasional	Puede ocurrir anualmente.
3	Moderado	Puede ocurrir semestralmente.
4	Probable	Puede ocurrir bimestralmente.
5	Común	Puede ocurrir mensualmente.

Tabla 5.3 Niveles de probabilidad

Para identificar el nivel de impacto se utilizará el siguiente criterio:

Impacto		
Nivel	Descripción	Detalle
1	Muy leve	El riesgo trae un breve retraso a las operaciones de la empresa sin traer ningún impacto regulatorio. No afecta a la reputación, economía, clientes y ni al directorio de la empresa.
2	Leve	El riesgo afecta directamente al proceso y puede traer impactos regulatorios leves, sin afectar fuertemente a la

		reputación, economía, clientes y ni al directorio de la empresa.
3	Medio	El riesgo afecta a la operación de la empresa, impactos regulatorios graves, afecta económicamente a la empresa y parcialmente a un grupo pequeño de clientes.
4	Grave	El riesgo afectaría fuertemente a la economía de la empresa, a los clientes y/o directorio, así como infracciones regulatorias muy graves.
5	Muy grave	El riesgo afectaría fuertemente a la reputación y economía de la empresa, a la gran mayoría de los clientes y/o directorio, así como infracciones regulatorias muy graves.

Tabla 5.4 Niveles de impacto.

El nivel de riesgo se calcula de la suma del nivel de la probabilidad con el nivel de impacto y según el valor final se obtiene el nivel del riesgo, los cuales se categorizan de la siguiente manera:

Valor	Nivel de riesgo
2-4	Bajo
5-6	Moderado
7-8	Alto
9-10	Extremo

Tabla 5.5 Niveles de riesgos.

c) Evaluación del riesgo

El apetito del riesgo de la empresa es riesgo de nivel bajo, por lo que todos los riesgos de mayor nivel, tendrán que ser tratados.

Todos los riesgos tendrán que ser ubicados en la matriz de riesgo

Matriz de riesgo						
Impacto	5	6	7	8	9	10
	4	5	6	7	8	9
	3	4	5	6	7	8
	2	3	4	5	6	7
	1	2	3	4	5	6
		1	2	3	4	5
		Probabilidad				

Tabla 5.6 Matriz de riesgo.

Los riesgos tendrán que ser ordenados en orden descendente, para poder priorizar atender los riesgos que tengan mayor valor.

Tratamiento de riesgo

Las opciones de tratamiento de riesgos son las siguientes:

Opciones de Tratamiento	Descripción
Aceptar	El riesgo se acepta cuando: -No es posible implementar un control adecuado para tratar el riesgo -El costo de implementar el control es mayor al costo de la materialización el riesgo. -El nivel de riesgo se encuentra dentro del apetito de riesgo. Cabe mencionar que se debe de documentar y firmal los riesgos que serán aceptados indicando el motivo y el responsable de monitorear el riesgo.
Mitigar	Este tratamiento busca reducir la probabilidad o el impacto del riesgo para que en consecuencia el nivel de riesgo se reduzca hasta un nivel menor o igual al apetito del riesgo.
Transferir	Este tratamiento se utilizará cuando no se cuente con los recursos necesarios para atacar el riesgo, por lo se tendrá que compartir el riesgo buscando un proveedor o asegurador para que pueda tratar con el riesgo.

Eliminar	Este tratamiento se tiene que elegir cuando se pueda eliminar la fuente que origina el riesgo y bajo un estricto análisis de riesgo, debido a que se podría cambiar la actividad del proceso así como incurrir en altos costos.

Tabla 5.7 Opciones de tratamiento de riesgo

Los controles pueden se pueden utilizar para mitigar el riesgo, pueden ser:

Tipo de control	Descripción
Preventivo	Este tipo de control busca controlar las **causas** que pueden ocasionar el riesgo.
Detectivo	Este tipo de control busca detectar y reportar la ocurrencia de los **eventos** que pueden ocasionar un riesgo.
Correctivo	Este tipo de control busca minimizar el **impacto** del riesgo.

Tabla 5.8 Tipos de control.

Además se debe de definir por cada tipo de control, la modalidad de operación del control, los cuales pueden ser:

Modalidades de operación	Descripción
Automático	Son aquellos que se ejecutan por sí mismo una vez que son configurados o establecidos.
Semi-automático	Son aquellos que operan por sí mismo, pero con una breve o corta intervención para el control pueda seguir operando.
Manual	Son aquellos que necesitan necesariamente una intervención, de la persona responsable de ejecutar el control, para que el control funcione.

Tabla 5.9 Modos de operación de los controles

La matriz de riesgos se encuentra en el anexo 5.

5.2 Conclusiones del capitulo

- Se concluye que se pudo identificar y valorar todos los activos de información asociados a los procesos de negocio que se encuentra dentro del alcance del gobierno de TI, los cuales se encuentran dentro de un nivel alto

debido a la información que almacena o la disponibilidad con la cual se necesitan estos activos pues se deben de cumplir con los plazos establecidos en la regulación.

- Se identificaron los riesgos de seguridad de información asociados a los procesos de negocio que se encuentra dentro del alcance del gobierno de TI, de los cuales el 50% deben de ser tratados necesariamente debido a que el nivel de riesgo es mayor al apetito de riesgos de la empresa, por lo cual se recomienda seguir las recomendación que se establecieron en el tratamiento de riesgos
- Cabe resalta que tanto la identificación de activos y el análisis de riesgo son actividades que se deben de realizar constantemente o ante cualquier cambio en la operatividad de los procesos de negocios.

6 CAPÍTULO 6

6.1 Objetivo específico 4: Medir la madurez de los procesos habilitadores del gobierno de TI, que soportan los objetivos de negocio de la empresa.

Para medir el desempeño del gobierno de TI, en este capítulo se identificará el nivel de madurez de cada proceso habilitador que está enfocado en la seguridad de la información y que forma parte del gobierno TI, siguiendo el modelo de capacidad de procesos definido en COBIT5, el cual se basa en la ISO/IEC 15504.

6.1.1 Resultado Esperado 6: Identificación del nivel de madurez de los procesos habilitadores enfocados a la seguridad de la información del gobierno de TI del caso de estudio.

Para poder identificar el nivel de madurez de los procesos habilitadores, primeramente se tendrá que identificar el cumplimiento de cada una de las actividades definidas dentro las actividades y controles que se realizan en la empresa del caso de estudio, para luego poder identificar el nivel de madurez del proceso habilitador según COBIT 5.

Para identificar el nivel de cumplimiento de los procesos se utilizará la siguiente escala:

Escala de puntuación del proceso	Descripción
N (No alcanzado)	Hay poca evidencia o no hay evidencia del logro del proceso analizado. El cumplimiento de las actividades está entre el 0% hasta el 15%.
P (Parcialmente alcanzado)	Existe alguna evidencia de que el proceso tiene un enfoque y algún alcance del atributo definido en el proceso analizado. Algunos aspectos del cumplimiento del atributo pueden ser impredecibles. El cumplimiento de las actividades está entre el 15% hasta el 50%.
L (Ampliamente alcanzando)	Hay evidencia de que el proceso tiene un enfoque sistemático y significativamente a alcanzado el atributo definido en el

	proceso analizado. Algunas debilidades relacionadas con el atributo pueden existir en el proceso analizado. El cumplimiento de las actividades está entre el 50% hasta el 85%.
F (Completamente alcanzado)	Hay evidencia de un proceso completo o con un enfoque sistemático y completo el alcance del atributo definido para el proceso analizado. No hay debilidades significativas relacionadas con el atributo del proceso analizado. El cumplimiento de las actividades está entre el 85% hasta el 100%.

Tabla 6.1 Escala de puntuación de los procesos.

Cabe mencionar que la empresa del caso de estudio tiene como objetivo que todos sus procesos habilitadores se encuentren gestionados, es decir en el nivel 2, y sean completamente alcanzados.

La medición del cumplimiento de cada uno de los procesos habilitadores se encuentra en el anexo 6.

6.2 Conclusiones del capitulo

- Se concluye que la empresa del caso de estudia cuenta con un nivel de madurez adecuado para el gobierno de TI con enfoque de seguridad según el nivel que se definió en un inicio, pues en la mayoría de los caso se alcanzó dicho nivel y en algunos se superó, pues lo recomendable seria cerrar las brechas que se tienen aun en algunos procesos que no llegaron a alcanzar el objetivo establecido.
- Si bien se cumple con el objetivo definido en la actualidad, se debe de estar revisan semestralmente que nuevas actividades se deben de añadir para fortalecer el proceso así como cuales estarían dejando de ser obsoletas con la finalidad de contar con procesos de gobierno actualizados a las tendencias y requerimientos actuales de seguridad la información.

Referencias bibliográficas

ASHRAF, Javed

2010 "Why do Public Sector IT Projects Fail". *The 7th International Conference on Informatics and Systems (INFOS), 2010*. Cairo, pp 1-6

BERMEJO, Paulo

2012 "Implementation of information technology (IT) governance through IT strategic planning". *African Journal of Business Management*. pp 11179-11189

COERTZE, Jacques & VON SOLMS, Rossouw

2014 "The Board and CIO: The IT Alignment Challenge". *2014 47th Hawaii International Conference on System Science*. Waikoloa, pp 4426 - 4435

CONGRESO DE LA REPUBLICA

2011 *Ley N° 29733. Ley de protección de datos personales.* 3 de julio de 2011.

ECB - European Central Bank.

2004 *Annual Report 2004*. Alemania

EIU - Economist Intelligence Unit

2005 *El futuro de la disrupción tecnológica en las empresas.*

EY - ERNST & YOUNG

2012 *Definición del modelo de Gobierno de TI*. Consulta: 26 de febrero de 2015 <http://www.ey.com/PE/es/Services/Advisory/IT/Article-v2012-DF-definicion-del-modelo-de-gobierno-de-ti>

HARDY, Gary

2006 "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges". *Information Security Technical Report*. pp 55–61

HONG, E. K.

2009 *Information technology strategic planning.*

ISACA - INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

2007 *COBIT Case Study: Ontario Pension Board*. Consulta: 30 de enero del 2015. <http://www.isaca.org/Knowledge-Center/cobit/Pages/Ontario-Pension-Board.aspx>

2008 *COBIT Case Study: Pension-Fennia*. Consulta: 30 de enero del 2015. <http://www.isaca.org/Knowledge-Center/cobit/Pages/Pension-Fennia.aspx>

2012a *2012 GEIT Survey - Latin America*. Rolling Meadows.

2012b *COBIT 5: Enabling Processes*. Rolling Meadows.

2012c *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows.

2012d *COBIT 5: Implementation*. Rolling Meadows.

2014 *COBIT Case Study: HDFC Bank.* Consulta: 24 de junio del 2015 < http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-1-January-2014.aspx#2 >

ISO/IEC - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

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

2009 *ISO 31000. Risk management — Principles and guidelines.*

2011 *ISO/IEC 27005. Information technology — Security techniques — Information security risk management.*

ITGI - IT GOVERNANCE INSTITUTE

2003 *Board Briefing on IT Governance.* Rolling Meadows.

2005a *IT Alignment: Who is in charge?* Rolling Meadows.

2005b *Optimizing Value Creation From IT Investments*. Rolling Meadows.

2005c *Information Risks: Whose Business are They?* Rolling Meadows.

2005d *Measuring and Demonstrating Value of IT.* Rolling Meadows.

LEPAGE HOCES, Diana Estafanía

2014 *Diseño de un modelo de Gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0*. Tesis para optar el Título de Ingeniera Informática. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.

MIYAGI, Ikumi

2014 "Align Business Initiatives and IT Solutions". *ISACA JOURNAL*. Rolling Meadows, pp 22-28.

MOELLER, Robert.

2013 *Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL.* Hoboken: John Wiley & Sons, Inc.

MUÑOZ PERIÑÁN, I. L., & ULLOA VILLEGAS, G.

2011 Gobierno de TI – Estado del arte. Revista S&T, pp 23-53.

MUSA, Nadianatra

2014 "An IT governance framework for achieving the development of academic programme in higher institutions: A case of Universiti Malaysia Sarawak (UNIMAS)". *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), 2014*. Kuching, pp. 1-6

NINGSIH, Kingkin Rahayu

2013 "Developing IT Investment Management Framework of Government Institution". *Advanced Computer Science and Information Systems*. Bali, pp. 237-242.

OECD - ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

2004 *OECD Principle of Corporate Governance.* Francia

PASTOR CARRASCO, Carlos Alberto

2012 *Gobierno de tecnología de información como generador de ventajas competitivas en empresas industriales – Lima Metropolitana*. Tesis para optar el grado Académico de Doctor en Ciencias Contables y Empresariales. Lima: Universidad Nacional Mayor de San Marcos

PWC – PricewaterhouseCoopers

2015a *Formulación de Planes Estratégicos de Tecnología de Información (Tecnología y Seguridad)*. Consulta: 26 de febrero de 2015 <http://www.pwc.com/pe/es/formulacion-de-planes-estrategicos-de-tecnologia-de-informacion/index.jhtml>

2015b *Diagnóstico de la gestión de las Tecnologías de Información*. Consulta: 26 de febrero de 2015 <http://www.pwc.com/pe/es/diagnostico-de-la-gestion-de-tecnologias-de-informacion/index.jhtml>

SARUP, Deepak

2003 "To Be, or Not To Be - The Question of Runaway Projects". *ISACA JOURNAL*. Rolling Meadows, pp 22-28.

SBS - SUPERINTENDENCIA DE BANCA, SEGUROS Y ADMINISTRADORAS PRIVADAS DE FONDOS

2009a *Circular N° G-140-2009 Ref.: Gestión de la seguridad de la información*. Consulta: 12 de enero de 2015 <http://intranet1.sbs.gob.pe/IDXALL/FINANCIERO/DOC/CIRCULAR/PDF/G-140-2009.C.PDF>

2009b *Resolución 2116:2009 - Reglamento para la gestión del Riesgo Operacional*

WEILL, Peter, & ROSS, Jeanne.
2013 *IT Governance: How top performers manage IT decision rights for superior results*. USA: Harvard Business Press.