DEFINICION DE UN MODELO DE IMPLEMENTACION DE GOBIERNO DE TECNOLOGIA PARA LA BANCA CENTRAL

De La Ossa Vélez Oscar José
06/10/2015

Contenido

Introducción

Ante el escenario actual, en el que la tecnología aporta todo el soporte a la toma de decisiones y se vuelve repositorio y medio de administración de la información, la cual se constituye en el activo más valioso para las organizaciones; toma cada vez más relevancia la aplicación de prácticas que van más allá de la simple gestión adecuada de recursos. El gobierno corporativo y su aplicación puntual a la tecnología, denominado gobierno de TI, está orientado a proveer un marco normativo de buenas prácticas dentro de la organización con el fin de garantizar que toda la administración se ejecute bajo los mismos criterios estratégicos.

Dentro de este marco y centrándonos en la actividad de la banca central, los factores de riesgo a los cuales dicha actividad se ve expuesta, obligan a realizar un manejo prudente de las amenazas y oportunidades y a su vez diseñar modelos de control de riesgo operativo y tecnológico, perfectamente acoplados en un esquema de gobierno de TI, de manera tal que pueda mitigarse el impacto de cualquier evento negativo que pudiera llegar a materializarse, afectando el desempeño de una organización (1).

Cabe mencionar que, en este contexto, el riesgo operativo se entiende como el resultado de factores de riesgo endógenos y exógenos, que pueden ser tan diversos y complejos que muchas veces no se pueden medir a través de medios tradicionales. (2)

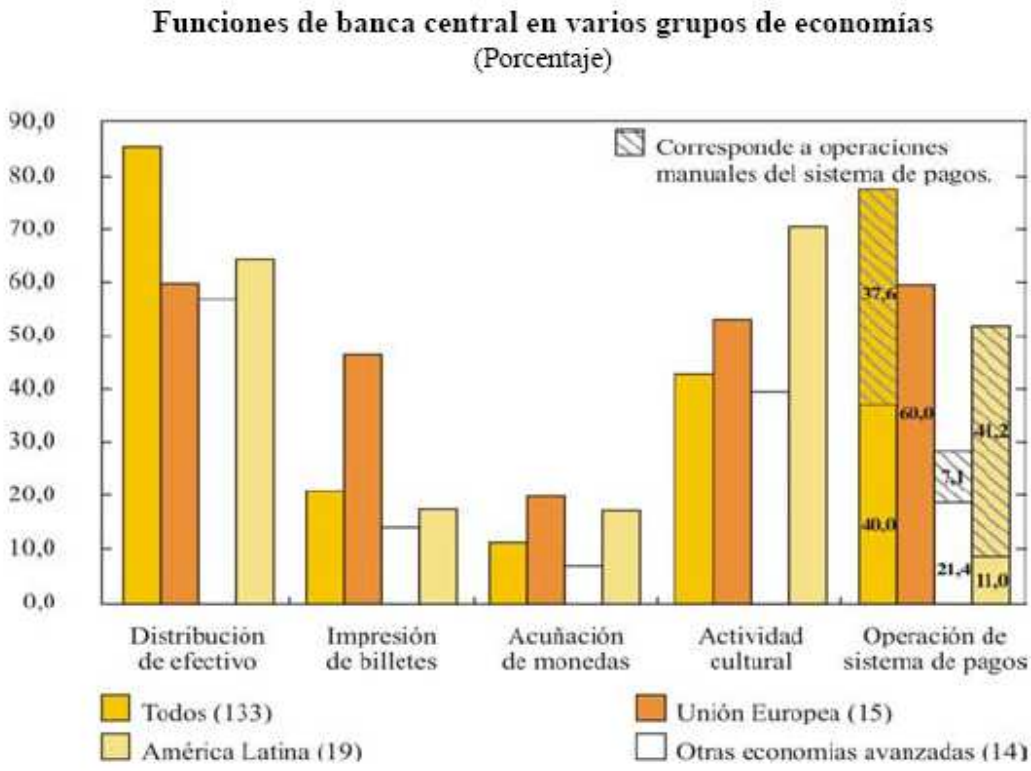
Es así como se encuentra útil considerar el riesgo de TI dentro de la actividad financiera, la que a su vez es un factor fundamental que debe considerar la banca central de un país. Esta, como responsable del manejo de la política monetaria, debe soportar sus decisiones en información que y cumplir con aspectos como: confiabilidad, integridad, confidencialidad, y auditabilidad, entre otros.

Por otra parte, las regulaciones a las que está sometida la banca central, obligan al manejo del riesgo de forma estricta con el fin de garantizar de manera contundente las condiciones que le dan estabilidad y confiabilidad a la economía de un país.

1 Formulación del Problema

1.1 Antecedentes

Típicamente las funciones de la Banca Central son: Distribución de Efectivo, Impresión de Billetes, Acuñación de Monedas, Actividad Cultural y Operaciones de sistema de pagos. En la Ilustración 1 se puede apreciar la distribución de estas funciones en varios grupos de economías (América Latina, Unión Europea, Otras Economías) (3)



Fuente: Banco de la República – Colombia

Ilustración 1. Funciones De Banca Central En Varios Grupos De Economías

La operación de cada una de estas funciones cuenta con apoyo de infraestructura, plataformas y aplicaciones de tecnología informática que son gestionadas a través de departamentos que cuentan con una misión y visión estratégica definida. Por ejemplo, algunos de estos describen su operación así:

"Proveer servicios y soluciones a las necesidades de tecnología de información del Banco, en línea con los mejores estándares internacionales y de la Banca Central, administrando los riesgos tecnológicos e incorporando las mejores prácticas de seguridad en tecnologías de la información." –Banco Central de Chile– (4)

“Proveer soluciones informáticas que generen oportunidades a las funciones del Banco y apoyen estratégicamente a sus áreas, con base en una gestión informática que integre personas, procesos y tecnología. Esta gestión debe mantener un nivel de madurez acorde con las necesidades del Banco que permita entregar productos y servicios de calidad, y administrar un nivel de excelencia en el servicio a los clientes internos y externos. “–Banco de la República de Colombia- (5)

La tecnología de información es parte integral de la infraestructura de los bancos centrales. Los sistemas informáticos son la base de numerosas funciones que van desde modelos económicos para el funcionamiento de un sistema de pagos eficiente hasta lo aplicable a las funciones de manejo de la política monetaria. En efecto, las crisis financieras han demostrado la importancia de la infraestructura financiera y su capacidad de recuperación, como el centro de grandes pagos en la economía, los bancos centrales estarán en la vanguardia de este esfuerzo para fortalecer los sistemas y sitios de respaldo.

Cada vez más, sin embargo, los expertos reconocen que la resiliencia de las redes de TI significa mucho más que los sistemas y servidores de empleados: se extiende a las personas y los procesos que operan e interactúan con ellos.

Para ello, es necesario el diálogo entre los usuarios y operadores de TI en los bancos centrales y, en un nivel más macro, la comprensión de cómo la función de TI se ajusta a los objetivos estratégicos de la organización y la forma en que contribuye a ellos. La naturaleza cambiante de la banca central impone nuevas exigencias a sus funciones, incluyendo la información, y cómo la nueva tecnología informática crea oportunidades y también riesgos tanto para los bancos centrales como los operadores y los consumidores. (6)

1.2 Planteamiento de la situación

Los cambios y la evolución de la economía están ocurriendo cada día a una velocidad más acelerada. Los desafíos asociados a los riesgos inherentes a la volatilidad de los mercados y la inestabilidad de las finanzas globales, evidencian la necesidad de tomar medidas y políticas integrales en aras de brindar las condiciones adecuadas de operación de los negocios mundiales.

La tecnología pasó de ser un área netamente de apoyo a convertirse en pieza fundamental y estratégica en la consecución de los objetivos organizacionales. Es así como hoy existe un marco denominado Gobierno de TI que busca proporcionar un esquema de principios para que la dirección de las organizaciones lo utilice para evaluar, dirigir y monitorizar el uso de las tecnologías de la información y comunicaciones (TICs). (7)

1.3 Justificación

Para hacer eficaz la función de la tecnología de la información, es esencial que la estrategia de TI esté estrechamente alineada con los objetivos institucionales. Para ello, los bancos centrales han adoptado, hasta cierto punto, procedimientos formales de gobierno. Sin embargo, estos procesos por sí solos no son suficientes para garantizar la eficacia de la inversión y el cumplimiento de objetivos. En un momento de creciente cambio en los roles de los bancos centrales y sus responsabilidades, es importante visualizar los desafíos que comprometen a las líneas de negocio en la gestión de TI de principio a fin.

Como las tecnologías de la información y la comunicación evolucionan a un ritmo rápido, es imperativo entender sus riesgos. Dadas las amenazas a las que los bancos centrales se enfrentan, es determinante contar con lineamientos normativos bien definidos para evitar errores no forzados y que la responsabilidad de la seguridad de TI está correctamente asignada y entendida.

Es importante resaltar los aspectos que garantizan la continuidad de operaciones y la recuperación en caso de desastre. Asociado al riesgo y al manejo de amenazas, el contar con un plan de continuidad de negocio es vital para la operación no solo del banco central, sino de todo el entorno económico que lo rige.

Un marco de gobierno y gestión de TI basado en las buenas prácticas y estándares de la industria, brinda soporte a la operación y permite atender de manera sistemática los desafíos económicos actuales.

2 Objetivos

2.1 General

Definir un modelo de implementación de gobierno de tecnología informática aplicable a la Banca Central, con énfasis en la gestión de riesgos operativos y la continuidad del negocio.

2.2 Específicos

Exponer de manera conceptual el marco de gobierno de TI que puede ser referente para diversas áreas de la organización: alta gerencia, gerencia de TI, auditoria, control interno, etc.

Establecer por separado las actividades de los marcos de gobierno y de gestión de TI aplicables al entorno de la banca central.

Proponer un modelo de madurez que permita medir el estado actual vs el estado deseado de gobierno y gestión de TI para un banco central.

Aplicar el marco definido hasta una de sus fases (la fase IV) y comparar contra el estado actual del desarrollo del gobierno de TI en un banco central, guardando la confidencialidad que ello requiere para el banco seleccionado por lo que en este documento se hablará de éste de manera genérica como el Banco Central[1].

[1] Este documento se prepara con el único propósito que haga parte de los requisitos para obtener el grado de Maestría en Gobierno de TI por parte de su autor, por lo que tiene fines meramente académicos y de consulta y revisión por parte de los jurados, profesores, estudiantes y asesores que de alguna forma deban consultarlo y/o comentarlo como aporte a dicho fin. En el evento que alguno de sus lectores asocie su contenido con alguna institución bancaria en particular, será producto de su libre entender, por lo que su autor no se hace responsable de ello.

3 Alcances y Limitaciones

El alcance del proyecto está determinado por los siguientes entregables:

1. Definir un modelo de implementación de Gobierno de Tecnología Informática para la Banca Central.
2. Aplicar la guía parcialmente (hasta la fase IV), partiendo de un paralelo entre dicha guía propuesta y lo que reporta un subconjunto de Bancos Centrales en sus sites públicos, seleccionados para tal fin, para llegar a una propuesta afinada a partir de ello.
3. Definir una línea de madurez como fase final de la guía.

El resultado del proyecto tendrá especial énfasis en el análisis de control de riesgo operativo y continuidad del negocio.

Se tomarán como puntos de referencia, entre otros, las siguientes prácticas y estándares: PMBOK, COBIT 5, ITIL v3, ISO 38500, BASILEA.

Los procesos clave para lograr el objetivo propuesto son: Investigación, levantamiento de información, alineación de modelos, elaboración de modelo, construcción de guía de implementación, aplicación y cierre.

La limitantes fundamentales que no será posible aplicar en su totalidad la guía en un Banco Central específico por las limitantes de privacidad que ello implica (incluso hasta alguna de sus fases por lo que se propone, en caso que ello suceda, lo mencionado al comienzo de este numeral); no obstante, el tiempo y alcance del que se dispone y que se requiere a nivel de este posgrado se considera adecuado para lo que se propone como alcance de este trabajo.

Es importante, además, hacer la salvedad que los conceptos y opiniones tratados y consignados en este trabajo no comprometen a ningún funcionario de un Banco Central ni a un Banco Central específico, son de total autoría del creador de este documento y tienen como único objetivo el consolidar un trabajo académico, para cumplir con el requerimiento final de grado del programa de Maestría que se encuentra cursando.

4 Metodología

La elaboración de este trabajo de grado se realizó siguiendo el estándar de gerencia de proyectos del Project Management Institute (8). Se siguieron las etapas del ciclo de vida tanto de la gerencia del proyecto, como del producto del proyecto en sí mismo. La estructura del proyecto se define por entregables generados en las etapas a cumplir para alcanzar el resultado esperado.

Cada componente del proyecto constituye la guía propuesta para que un Banco Central implante un Modelo de Gobierno de TI.

Para los fines correspondientes a este trabajo de grado, dadas las limitantes de tiempo y de confidencialidad de la información, el proyecto se construye a partir de procesos, en dónde para cada uno se describen las actividades a realizar, sus entradas y las salidas esperadas.

El modelo definido en este trabajo puede ser utilizado como guía para emprender un proyecto de implementación de gobierno de tecnología en un Banco Central teniendo en cuenta las características propias de este tipo de organizaciones y la importancia de este trabajo integrando los aspectos de los marcos metodológicos existentes y los requerimientos propios y particulares del negocio. Y a partir de esto último y tomando como base los lineamientos de BASILEA se establecen cuáles son los elementos de entrada, las técnicas/herramientas y las salidas que se deben considerar en el desarrollo de la implementación de un marco de gobierno de TI.

Si bien es cierto que los bancos centrales no son homogéneos en sus funciones, las funciones tradicionales de los bancos centrales se pueden clasificar en dos grupos: primarias y secundarias. Las funciones primarias incluyen conducir la política monetaria, emitir billetes y monedas, administrar las reservas internacionales, regular y supervisar el sistema financiero, ser banquero de bancos y prestamista de última instancia, velar por la existencia de sistemas de pagos seguros y eficientes, ser banquero del Gobierno y realizar investigaciones económicas. Las funciones secundarias incluyen actuar como agente fiscal del Gobierno, producir y distribuir billetes y monedas, manejar los cambios internacionales, asesorar al Gobierno en materia económica, publicar estadísticas y mantener relaciones con las instituciones financieras internacionales. (3)

Una las funciones principales con la que nacieron buena parte de los banco centrales en el mundo son la regulación y la supervisión. Esto permitía dar solidez a las operaciones entre los bancos comerciales. En años recientes tras varias crisis financieras mundiales un grupo de bancos centrales creo el Comité de Basilea. Las funciones de dicho comité han ido

evolucionado hasta definir estándares orientados a prevenir crisis en los sistemas financieros de los países que adoptan sus principios.

Según Carlos Gustavo Cano (9) En suma, la razón de ser de la regulación y la supervisión es la estabilidad financiera. Y para el logro del tal propósito, es indispensable concentrarse en los siguientes cinco cometidos:

- La minimización de los riesgos y de los costos de las crisis bancarias.
- El aseguramiento del buen funcionamiento de los sistemas de pagos.
- La protección de los depositantes, sin caer en riesgos morales.
- La eficiencia y la competitividad del sistema financiero, fomentando la competencia entre sus agentes y evitando posiciones dominantes en el mercado.
- La plena credibilidad en la institucionalidad reguladora y supervisora por parte de los ahorradores, los clientes y el público en general.

En este sentido y partiendo de que el manejo de la política monetaria y la función de regulación y supervisión del sistema financiero son funciones que desempeñan muchos bancos centrales en el mundo, es importante la aplicación de un modelo de gobierno de TI que contemple los principios de Basilea para efectos de su gestión efectiva de riesgo operativo y auditabilidad de sus procesos

Lo aquí definido se implementará hasta la fase IV del proyecto propuesto y se compara contra lo existente y publicado por entidades de este tipo y que está disponible en sus sitios web y es información de libre distribución y no viola ningún aspecto de reserva o confidencialidad sobre dicha información.

A continuación se presenta el marco y estructura del proyecto y se detallan cada uno de los elementos claves del modelo de implementación que se propone.

5 Propuesta de Definición de un Modelo de Implementación de Gobierno de Tecnología para la Banca Central

Este proyecto está dividido en 5 fases principales a través de las cuales se define un ciclo de vida, las cuales se integran a través de sus actividades siguiendo una secuencia lógica que permite cubrir los aspectos a tener en cuenta al implementar un modelo de gobierno de tecnología en un Banco Central.

Cada fase del proyecto cuenta con unas entradas que son procesadas a través de unas técnicas y herramientas bien definidas y se generan unas salidas que alimentan otras fases del proyecto y/o son entregables finales del mismo.

Las fases del ciclo de vida del proyecto son:

I. Definir y Levantar Requerimientos del Proyecto
II. Investigar y Seleccionar Marcos de Trabajo
III. Alinear los Marcos Seleccionados
IV. Construir Modelo de Gobierno de TI
V. Implementar Modelo

El siguiente gráfico ilustra las fases del ciclo de vida del proyecto en lo que podría ser un círculo virtuoso de mejoramiento continuo que en la medida en que se defina una interacción periódica de dichas fases se implementan los ajustes a la implementación, bien sea por necesidades del negocio o requerimientos del entorno

Ilustración 2. Ciclo de Vida del Proyecto

En la siguiente figura se presentan las fases del proyecto en forma secuencial. Aunque estas fases se presentaran para su explicación de esta forma su implementación práctica puede realizarse de forma paralela en algunas de sus actividades de acuerdo con la programación y definición del proyecto puntual en cada Banco Central.

Cada fase alimenta el proyecto de manera progresiva de tal forma que se llega a un mayor nivel de detalle en la medida en que se avanza

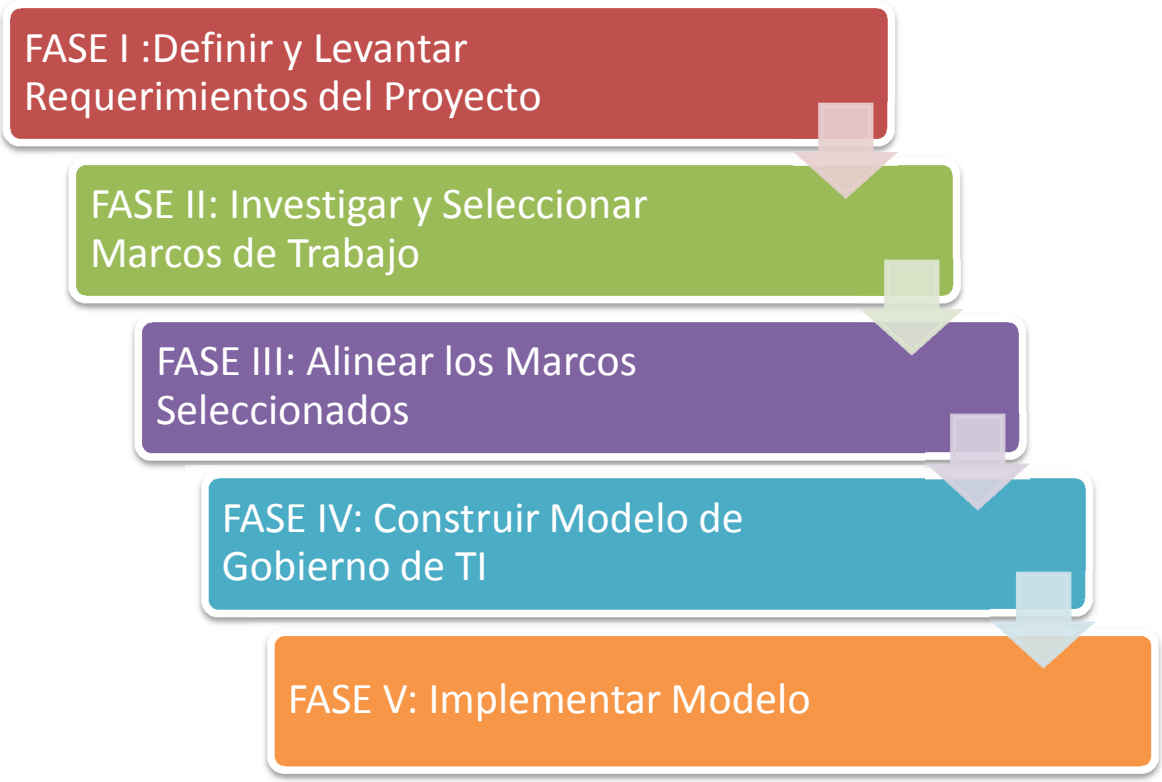


Ilustración 3. Fases del proyecto en forma secuencial

Tal y como se planteó en el alcance, este trabajo se implementará hasta la fase IV en la cual construiremos un modelo de Gobierno de TI aplicable de acuerdo a las necesidades levantadas en las fases previas, la investigación realizada y la alineación de los marcos de trabajos seleccionados.

A continuación se ilustra cada fase con una breve explicación del objetivo de cada una de estas.

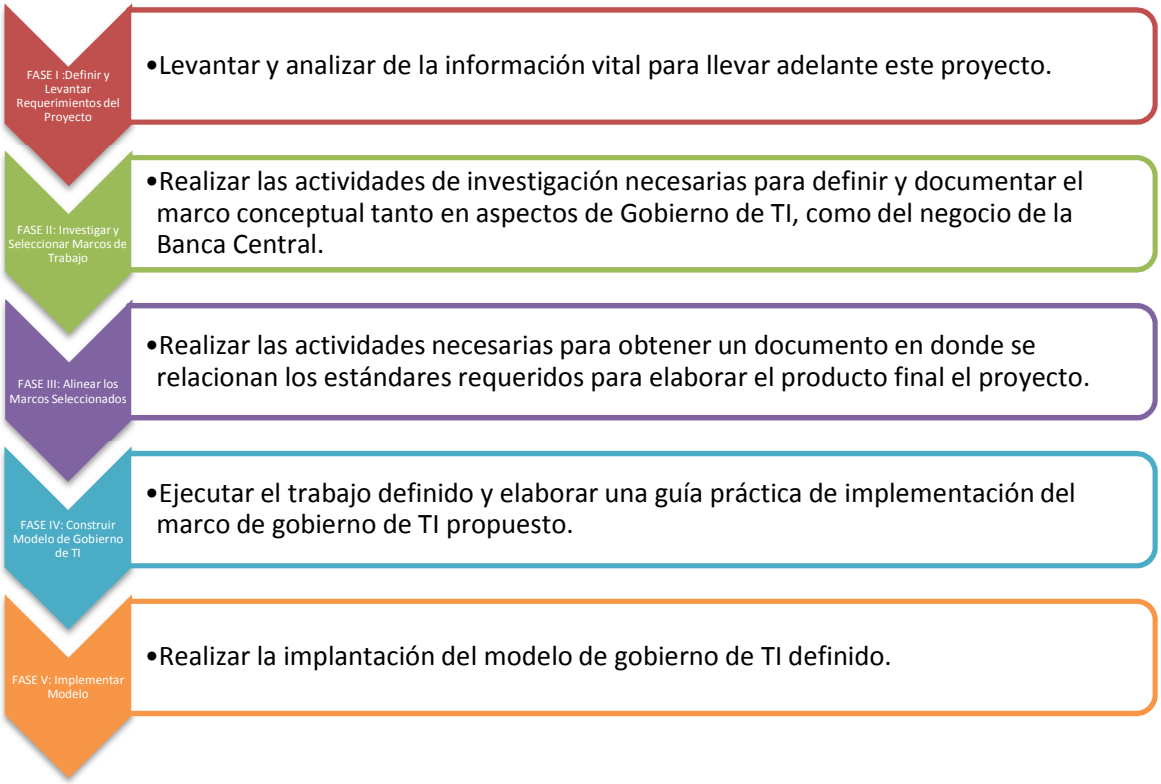


Ilustración 4. Descripción General de las Fases del Proyecto

Como se puede apreciar cada fase cumple con un objetivo puntual que ayuda a construir el proyecto gradual y progresivamente hasta lograr el objetivo planteado. La construcción del Modelo (que será nuestro objetivo de demostración en el presente trabajo) se convierte en la principal de esta herramienta.

6 DESARROLLO DEL PROYECTO

Partiendo de lo anteriormente expuesto, cada fase del proyecto se interrelaciona con las otras a través de sus entradas y salidas. Las fases definidas contienen una serie de actividades que siguen una secuencia lógica que permite la construcción sistémica del modelo de gobierno de TI

A continuación se ilustra la integración general de las fases del proyecto, teniendo en cuenta de forma las entradas y salidas globales de las actividades contenidas en cada una de ellas.

Ilustración 5. Relación de Fases del Ciclo de Vida

Durante el desarrollo de este proyecto se ejecutará cada punto como parte de la guía práctica de este trabajo (el cual de acuerdo al alcance será implementado hasta su fase IV) y cuyo resultado será confrontado contra la información disponible y publicada por un grupo seleccionado de Bancos Centrales a nivel mundial.

A continuación se describen cada una de las fases de forma detallada con sus entradas, herramientas/técnicas y salidas.

I. Definir y Levantar Requerimientos del Proyecto

Esta fase consiste realizar el levantamiento y análisis de la información vital para llevar adelante este proyecto. A través de una adecuada definición de requerimientos se puede

lograr tener un alcance claro y un plan de trabajo acorde a las necesidades de la organización.

A continuación se especifican las entradas, técnicas y salidas de esta fase del proyecto con su respectiva explicación

Entradas	Técnicas	Salidas
• Plan Estratégico Corp. • Plan Estratégico de TI • Procesos de negocio • Normatividad. • Indicadores. • Arquitectura	• Entrevistas. • Cuestionarios/Encuestas • Juicio de Expertos. • Técnicas de Gerencia de Proyecto.	• Requerimientos documentados.

Entradas

a. Plan Estratégico Corporativo.

Es el documento de más alto nivel gerencial en la organización en el cual se disponen todos los lineamientos y políticas de gobierno corporativo. En este se define la visión, misión, elementos estratégicos y culturales que rigen el día a día de la entidad. El plan estratégico establece una hoja de ruta para el logro de los objetivos del negocio. Es un documento importantísimo para establecer claramente los requerimientos del proyecto de implementación de un modelo de gobierno de TI.

b. Plan Estratégico de TI

Así como el plan estratégico corporativo define las políticas a nivel de toda la organización, el plan estratégico de TI resume el conjunto de lineamientos que tienen como propósito gestionar, monitorear, controlar y garantizar la prestación adecuada de servicios de TI que apoyan y están alineados con los objetivos del negocio. El plan estratégico de TI se constituye en una guía básica para la definición de los requerimientos del proyecto de implementación del modelo de gobierno y de hecho hace parte integral del mismo.

En el plan estratégico de TI aparte de la visión, misión y lineamientos también se define el portafolio de programas, proyectos, arquitectura, servicios, procesos, planes gestión de riesgos, contingencias, gestión humana y aspectos de cumplimiento regulatorio vitales para la prestación de servicios

c. Procesos de negocio

Los procesos de negocio son todos aquellos que son definidos y ejecutados por todas las áreas de la organización y que generan los productos y servicios que se entregan a todos

los clientes. Muchos de estos procesos pueden estar apoyados en servicios de TI que deben ser gobernados y gestionados, por lo cual también se consideran parte básica para el levantamiento de requerimientos. En relación a las funciones generales de los bancos centrales descritas en el capítulo 4, es importante destacar que los procesos de negocio de los bancos centrales están orientados a brindar solidez al sistema financiero de un país y al manejo adecuado y responsables de las políticas macroeconómicas que permitan un desarrollo sostenible de la economía de un país, aseguren el valor adquisitivo de la moneda y provea bases sólidas para en ultimas dar bienestar y mejorar la calidad de vida de los ciudadanos.

d. Normatividad.

Es importante tener presente el marco normativo y regulatorio que rige tanto el negocio de la banca central, así como las que están involucradas en el ejercicio de la gestión de tecnología. Las normas técnicas y los lineamientos gubernamentales son pieza clave a tener en cuenta en el diseño propuesto. Al estar dentro del sector financiero, uno de los marcos de referencia del cual hablaremos más adelante es el conjunto de principios del comité de BASILEA que son de cumplimiento específico para el sector. Así mismo, por ser entidades estatales regidas por normas de carácter nacional (ej: la constitución y otras leyes), es importantísimo tener presente este entorno dadas su características especiales vs empresas de otra actividad pública o privada.

Los bancos centrales son regidos por un conjunto de normar internas y externas que van desde los marcos constitucionales y las leyes de cada país hasta los acuerdos internacionales y autoridades como el Comité de Supervisión Bancaria de Basiles (BCBS), el Banco Mundial y el Fondo Monetaria Internacional.

e. Indicadores.

Los indicadores de gestión o mediciones del desempeño actual de las políticas corporativas y de TI también se consideran un elemento indispensable a la hora de definir los requerimientos del proyecto, ya que en un análisis de madurez, que miraremos más adelante, proporcionan un punto medición y de partida a partir del cual se establecerá un plan de acción para llegar a un estado deseado u obligado de madurez en la prestación de servicios que garanticen su utilidad al cumplimiento de los objetivos corporativos.

f. Arquitectura

La arquitectura empresarial contiene todos los procesos de negocio, datos/información, aplicaciones y tecnologías sobre las que se apoyan las operaciones diarias. Un modelo de arquitectura bien definido, facilitará enormemente la definición de requerimientos.

Técnicas

a. Entrevistas

Las entrevistas son un medio para hacer el levantamiento de información. Estas se realizan de forma presencial o remota con el fin de precisar aspectos relevantes para completar el proyecto. Se establece un plan para definir el número de entrevistas a realizar, las personas que harán parte de este proceso y el tiempo estimado de realización de las mismas, así como su proceso de análisis, evaluación, tabulación y resultados

b. Juicio de Expertos

Utilizar el juicio de expertos para analizar levantar información relevante. Entre estos expertos están: consultores, profesionales, expertos en temas de gobierno y gestión de TI y expertos en banca central.

c. Técnicas de gerencia de proyectos

Se refiere al uso del marco general de la gerencia definido por el PMI para estructurar, definir, ejecutar y controlar este proyecto. Se hace uso de los conceptos definidos en el PMBOK®

d. Cuestionarios/Encuestas

Las encuestas y cuestionarios a los grupos principales de interesados también son una herramienta útil para hacer el levantamiento de requerimientos. A través de estas se puede obtener un resultado cuantitativo global de las necesidades y expectativas que deberá cubrir este proyecto

Salidas

a. Requerimientos Documentados.

Este entregable contiene la definición exacta de los requerimientos del trabajo a realizar; en resumen condensa las expectativas de los interesados.

Los requerimientos del proyecto establecen la fuente base para la definición de un alcance claro, un plan de trabajo y unos mecanismos apropiados de medición de resultados

II. Investigar y Seleccionar Marcos de Trabajo

Esta fase consiste en realizar las actividades de investigación necesarias para definir y documentar el marco conceptual tanto en aspectos de Gobierno de TI, como del negocio de la Banca Central. Dadas las características particulares del negocio y de la estructura organizacional de este tipo de entidades es indispensable establecer cuáles son los marcos de trabajo que aplican específicamente para el logro de los objetivos y requerimientos definidos en la fase anterior.

La industria de TI y diversas organizaciones a nivel mundial trabajan año a año con el fin de definir las mejores prácticas de la industria en cada uno de sus múltiples aspectos, teniendo en cuenta también la complejidad cada vez mayor de los entornos de negocio y el impacto de fenómenos como la globalización y la integración política, económica, financiera y cultural del mundo.

Estos escenarios cada vez más complejos obligan a revisar cada vez con mayor detenimiento los aspectos relacionados con el riesgo y la calidad.

A continuación se especifican las entradas, técnicas y salidas de esta fase del proyecto con su respectiva explicación

Entradas	Técnicas	Salidas
• Marcos de Referencia de la Industria (TI). • Normatividad. • Requerimientos documentados. • Marcos de referencia del Negocio (Banca Central y Sector financiero)	• Juicio de Expertos • Investigación • Estimación por analogía • Análisis de Casos	• Marcos Teórico Aplicables.

Entradas

a. Marcos de Referencia de la Industria TI

Este entregable define los marcos de referencia que se utilizan para el desarrollo de este trabajo. Se contemplan tanto los estándares y regulaciones nacionales, como internacionales.

El marco de gobierno de mayor aceptación es COBIT el cual se integra con otros modelos también de reconocimiento mundial. Ver grafica siguiente:

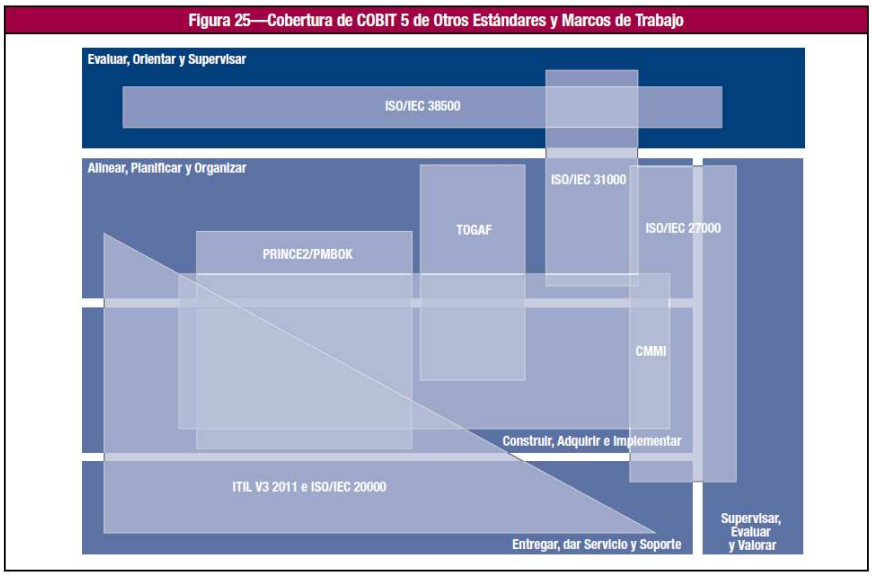


Ilustración 6~~5~~. COBIT y otros Estándares y Marcos de Trabajo

b. Normatividad

Es importante tener presente el marco normativo y regulatorio que rige tanto el negocio de la banca central, así como las que están involucradas en el ejercicio de la gestión de tecnología. Las normas técnicas y los lineamientos gubernamentales son pieza clave a tener en cuenta en el diseño propuesto. Al estar dentro del sector financiero, uno de los marcos de referencia del cual hablaremos más adelante es el conjunto de principios del comité de Basilea que son de cumplimiento específico para el sector. Así mismo, por ser entidades estatales regidas por normas de carácter nacional (ej: la constitución y otras leyes), es importantísimo tener presente este entorno dadas su características especiales vs empresas de otra actividad pública o privada

c. Requerimientos documentados.

Este entregable viene de la fase I y contiene la definición exacta de los requerimientos del trabajo a realizar; en resumen condensa las expectativas de los interesados.

Los requerimientos del proyecto establecen la fuente base para la definición de un alcance claro, un plan de trabajo y unos mecanismos apropiados de medición de resultados

d. Marcos de referencia del Negocio (Banca Central y Sector financiero)

El negocio del sector financiero a nivel mundial está cada día más enfocado en el análisis y prevención de riesgos, especialmente el riesgo operativo; es por esto que es importante tomar un punto de referencia nacional e internacional de tal manera que la implementación del modelo de gobierno contemple su impacto en el negocio y tenga presente cuales son aquellas normas de estricto cumplimiento o de deseada aceptación

para mitigar la ocurrencia y el impacto de eventos que afecten las operaciones de la organización.

Adicional a los marcos establecidos por las autoridades gubernamentales, entes de control de cobertura nacional y entidades de vigilancia del sector financiero, existe un conjunto de recomendaciones internacionales contenidas en un documento expedido por el comité de Basilea el cual fortalece los elementos clave de los principios de gobierno corporativo**.** Este modelo es aplicable a los bancos centrales ya que estos tienen en algunos casos la doble responsabilidad de ser la autoridad monetaria y la entidad reguladora del sistema financiero

Técnicas

a. Juicio de Expertos

Utilizar el juicio de expertos para analizar la información necesaria para la elaboración del proyecto. Entre estos expertos estarán: consultores, profesionales, expertos en temas de gobierno y gestión de TI y expertos en banca central

b. Investigación

Esta técnica sugiere el proceso de investigación y estudio de los marcos de trabajo y metodologías disponibles globalmente para el manejo del gobierno corporativo. A partir de las referencias de la industria y los trabajos publicados por entidades mundiales de gran reconocimiento alrededor del tema (eg: ISACA)

c. Estimación por analogía

Esta técnica constituye un complemento a la de juicio de expertos. En esta no sólo trabajan con la experiencia acumulada, sino que disponen también de datos de proyectos similares. Es posible evaluar la implementación de modelos de gobierno de tecnología en otras entidades de la banca central o incluso del sector financiero en general.

d. Análisis de Casos.

Esta herramienta permite realizar un diseño basado en casos o escenarios potenciales. Al diseñar escenarios potenciales de riesgo operativo y tecnológico se tiene la posibilidad de visualizar los riesgos, las amenazas y definir estrategias tendientes hacer un manejo adecuado de la situación.

Salidas

a. Marco Teórico del Proyecto

Se cuenta con un marco teórico definido tanto en la parte de gobierno y gestión de TI como de la operación general del negocio de la banca central. Se precisan los aspectos relevantes de las metodologías, guías, estándares, normas y frameworks estudiados.

En este punto se tienen en cuenta los marcos de referencia que se utilizan para este trabajo. Entre los que están COBIT 5, ITIL v3, ISO 38500, BASILEA.

Se definirá el siguiente marco teórico que integra las diferentes prácticas, estándares y modelos de gestión existentes de tal manera que pueda ser aplicado para gestionar los riesgos operativos y de TI a los que se ven expuestos los bancos centrales.

A continuación se presenta una extracción de los elementos más relevantes de los marcos estudiados que, acorde con el criterio del autor de este trabajo, son de utilidad para construir un modelo de implantación de Gobierno de TI en Bancos Centrales

Norma ISO 38500

Norma que fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionados con los servicios de información y comunicación. La norma ISO/IEC 38500:2008 se publicó en junio de 2008 sobre la base de la norma australiana AS8015:2005, y es la primera de una serie sobre normas de gobierno de las TIC. Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones los utilice al evaluar, dirigir y monitorizar el uso de las tecnologías de la información y Comunicaciones (TIC). Está alineada con los principios de gobierno corporativo recogidos en el Informe Cadbury y en los Principios de Gobierno Corporativo de la OCDE. (10)

La ISO/IEC 38500:2008 Corporate governance of information technology, complementa el conjunto de estándares ISO que afectan a los sistemas y tecnologías de la información: UNE-ISO/IEC 27001:2007, UNE-ISO/IEC 20000-1:2011, ISO/IEC 15504:2004, UNE-ISO/IEC 19770-1:2008, etc.

En esta norma se fijan los estándares para un buen gobierno de los procesos y decisiones empresariales relacionadas con las TIC.

La norma puede resumirse en tres propósitos:

1. Asegurar que, si la norma es seguida de manera adecuada, las partes implicadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de TIC.
2. Informar y orientar a los directores que controlan el uso de las TIC en su organización.
3. Proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TIC.

Para el inicio del siguiente estudio se parte de dos definiciones que se consideran fundamentales para el propósito del mismo y que son establecidas por la International

Organization for Standardization (ISO) en la norma ISO/IEC 38500 respecto a gobierno corporativo de tecnología de información

Gobierno Corporativo de TIC: El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información

Gestión: El sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización. Está sujeta a la guía y monitorización establecida mediante el gobierno corporativo.

El modelo de gobierno corporativo definido en la norma ISO/IEC 38500 se puede apreciar en el siguiente gráfico

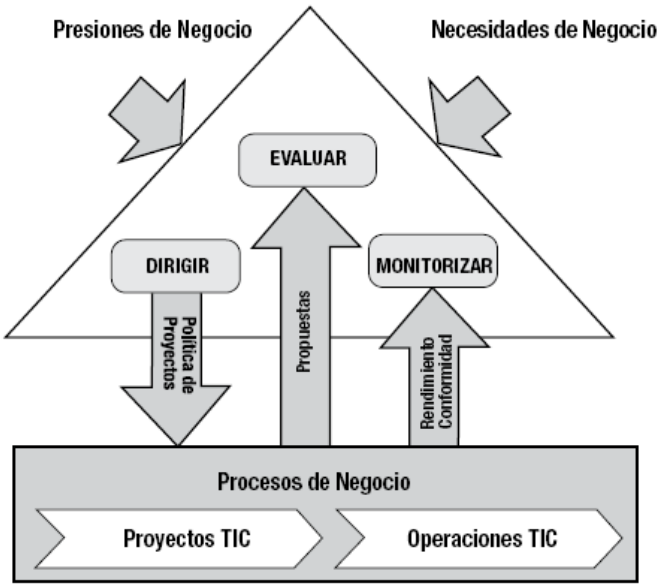


Ilustración 75. Modelo De Gobierno Corporativo De Tic

Se define mediante tres áreas principales: Evaluar, Dirigir y Monitorizar.

Evaluar: Examinar y juzgar el uso actual y futura de las TIC, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).

Dirigir: Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto. Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura. Impulsar una cultura de buen gobierno de TIC en la organización.

Monitorizar: Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado. (11)

La norma ISO 38500 se basa en 6 principios de buen gobierno:

- **Responsabilidad**: Comprender y aceptar responsabilidad sobre las acciones
- **Estrategia**: Satisfacer de necesidades actuales y futuras tanto de las TIC como del negocio
- **Adquisición**: Analizar las necesidades y buscar equilibrio entre beneficio y costos
- **Rendimiento**: Proporcionar servicios que cumplan con las necesidades actuales y futuras
- **Conformidad**: Cumplir con las normas exigidas
- **Factor Humano**: Respectar al ser humano

A continuación se comparte la guía sobre como evaluar, dirigir y monitorear la función de TIC (11)

Principios	Dirigir	Monitorizar	Evaluar
Responsabilidad	Planes con responsabilidad asignada	Mecanismos establecidos de gobierno de TIC	Asignación de responsabilidades
	Recibir información y rendir cuentas	Asignación de responsabilidades	Competencias de responsables
		Desempeño responsables	
Estrategia	Creación y uso de planes y políticas	Progreso propuestas aprobadas	Desarrollo de TIC y procesos de negocio
	Asegurar beneficios de TI en el Negocio	Alcanzar objetivos en plazos establecidos	Evaluar actividades de TIC y alineamiento
	Alentar propuestas innovadoras	Utilizar recursos asignados	Mejores prácticas
		Uso de TIC, alcanzando beneficios esperados	Satisfacción de los interesados
			Valoración y evaluación de riesgos
Adquisición	Activos deTI se adquieren manera apropiada	Inversiones y capacidades requeridas	Alternativas propuestas
	Documentos de capacidad requerida	Entendimiento interno/externo y necesidad del negocio	Propuestas aprobadas
	Acuerdos de provisión que respalden las necesidades del		Análisis de riesgo/valor

	negocio		
			Inversiones
Rendimiento	Asignación recursos suficientes	Grado TIC sustenta el negocio	TIC sustenta procesos de negocio dimensionado y capacidad
	Asignar prioridades y restricciones	Recursos e inversiones priorizados (nec. neg.)	Riesgos: continuidad de operaciones
	Satisfacer necesidades del negocio	Políticas precisión datos	Riesgos: integridad de información, protección de activos
	Datos correctos, actualizados, protegidos	Políticas uso eficiente TIC	Decisiones uso TIC apoyo al negocio
			Eficacia y desempeño gobierno de TIC
Cumplimiento	TI cumple obligaciones, normas y directrices	Cumplimiento y conformidad (auditorias/informes)	TIC cumple obligaciones, normas y directrices
	Establecer y aplicar políticas (uso TI interno)	Oportunos, completos, adecuados (nec. negocio)	Conformidad gobierno de TIC
	Personal TIC cumple directrices desarrollo y conducta	Actividades de TIC	
	Ética rija acciones relacionadas TIC		
Factor Humano	Actividades TI compatibles factor humano	Actividades de TIC, identificar, prestar atención	Actividades de TIC, identificar
	Informar cualquier individuo (riesgos, problemas)	Prácticas de trabajo consistente uso apropiado de TIC	Actividades de TIC, considera Debidamente
	Administración riesgos según políticas y procedimientos		
	Escalado a los decisores		

Tabla 1 Principios de Buen Gobierno

COBIT 5

Proporciona un marco integral que ayuda a las empresas a alcanzar sus metas y obtener valor a través de una gobernanza eficaz y la gestión de las TI corporativas. COBIT 5 ayuda a las empresas a crear valor óptimo de TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de los recursos.

En el marco de trabajo de COBIT 5 se tienen presente los principios básicos, los cuales proveen una referencia que asiste a las organizaciones en el cumplimiento de sus objetivos de gobierno y gestión de TI.

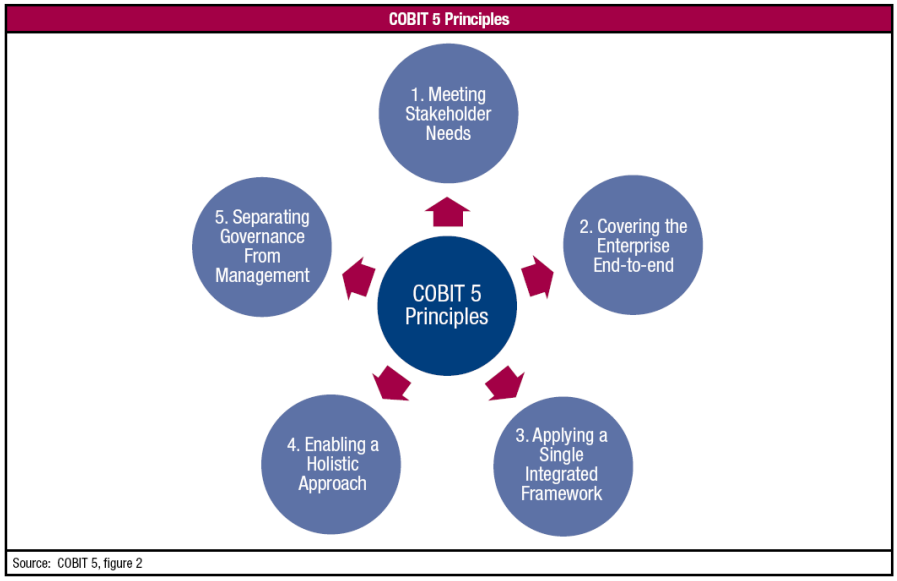


Ilustración 8~~6~~. Principios De COBIT 5

El marco COBIT 5 establece una clara distinción entre la gobernabilidad y la gestión. Estas dos disciplinas abarcan diferentes tipos de actividades, requieren diferentes estructuras organizativas y tienen objetivos diferentes. (12)

A partir de esta distinción, propone el siguiente modelo de implementación de procesos que buscan cubrir todos los objetivos de cada una de las instancias relacionadas con el gobierno de TI.

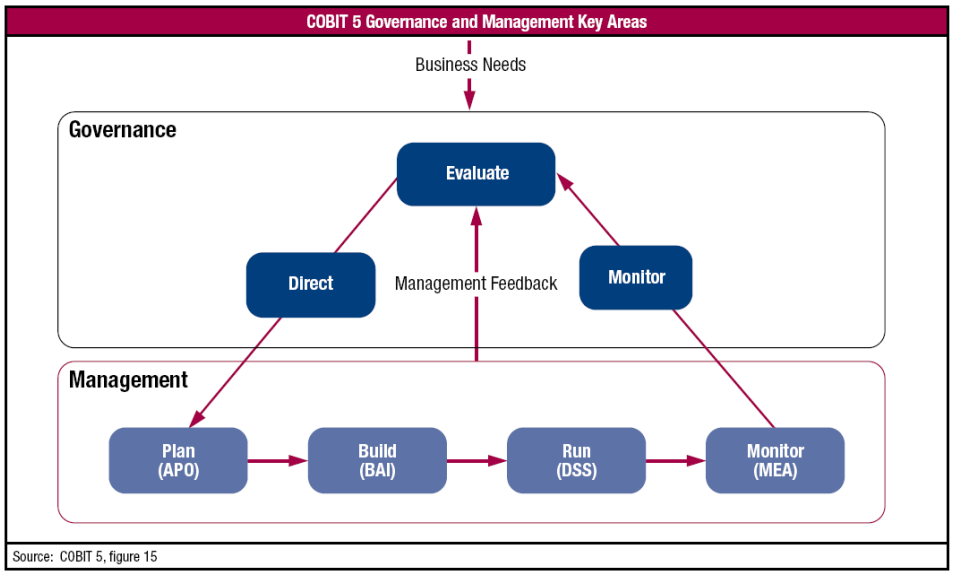


Ilustración 97. Áreas Claves De Gobierno y Gestión COBIT 5

El modelo propuesto por COBIT 5 busca cubrir todas las áreas del negocio. Es posible organizar los procesos de la manera más conveniente de acuerdo a las necesidades de cada empresa.

Como ya se había nombrado, COBIT 5 incluye en su modelo tanto la gobernabilidad como la gestión, convirtiéndose en un modelo integral, completo que debe ser aplicado a conveniencia de cada organización y basado en las necesidades propias del negocio.

COBIT 5, divide el gobierno y la gestión en dos grandes dominios de procesos:

Gobierno: Este dominio contiene cinco procesos, que se definen como Evaluar, Dirigir (dar dirección u orientar) y Monitorear (validación de la dirección correcta de la gestión)

Gestión: Contiene 4 dominios orientados a planear, construir, ejecutar y monitorear. Los dominios son: Alinear, Planear y Organizar (APO); Construir, Adquirir e Implementar (BAI); Entregar, Servir y Soportar (DSS); Supervisar, Evaluar y Medir (MEA)

Los dominios están conformados por procesos los cuales requieren ser planeados, implementados, ejecutados y monitoreados.

El modelo de referencia COBIT 5 integra el modelo de procesos COBIT 4.1, VAL IT y RISK IT.

A continuación se ilustra el modelo de referencia de COBIT 5, el cual incluye 37 procesos tanto del área de Gobierno como de Gestión

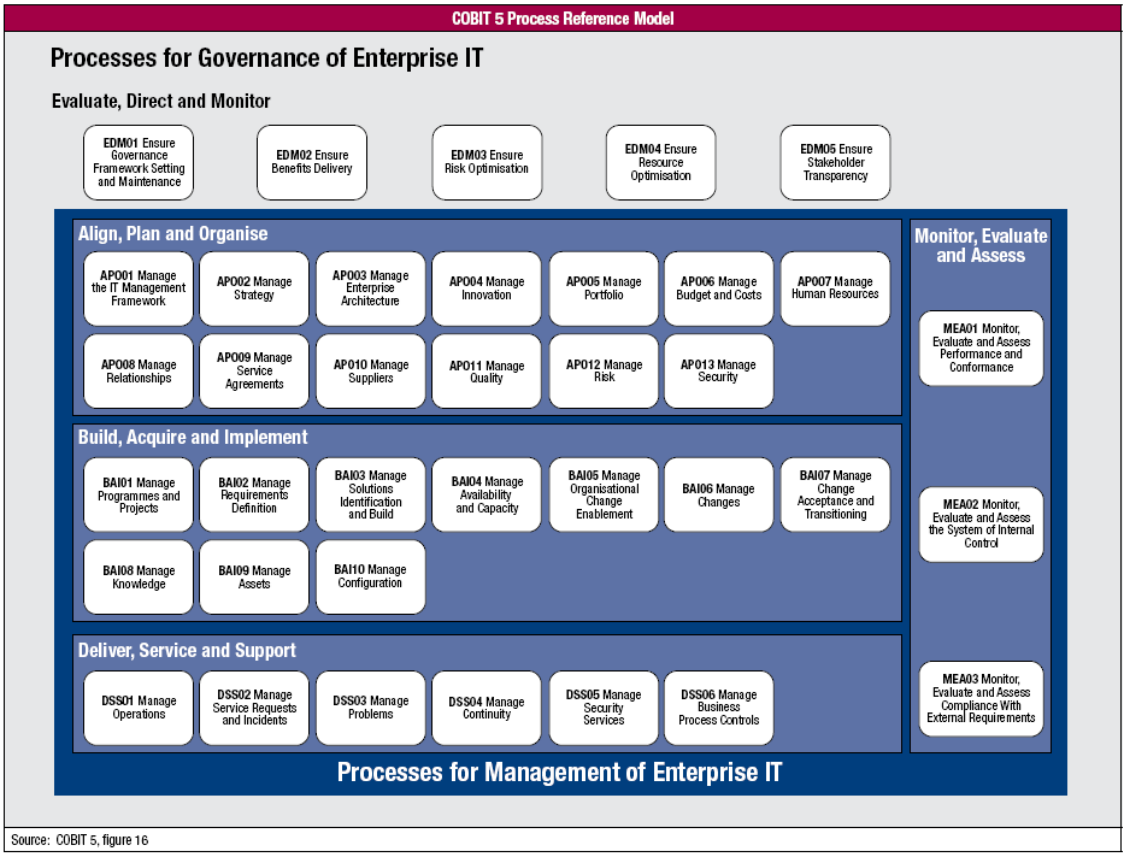


Ilustración 10~~8~~. Modelo de Referencia COBIT 5

BASILEA

Regulación Bancaria de aplicación no obligatoria, que lleva a las entidades financieras a afinar al máximo la medición y gestión de riesgos a la hora de calcular el capital que cubre dichos riesgos (13).

Basilea III fortalece los elementos clave de los principios de gobierno corporativo de la OCDE y tiene por objeto orientar la acción de los miembros del consejo, directivos y organismos reguladores de una amplia gama de bancos de varios países con diferentes sistemas legales y regulatorios (14)

Por su parte, el comité de supervisión bancaria de Basilea presenta un documento que recoge los principios para la supervisión y seguimiento del riesgo operativo en el sector financiero; esto aplica tanto para bancos, intermediarios financieros y entes reguladores. Los principios del comité de Basilea nacen de la creciente complejidad del entorno financiero mundial, el cual ha sido afectado por crisis resiente y una evidente carencia de regulación que permita prevenir los riesgos y amenazas del entorno global actual. Algunos de los riesgos operativos que se evidencian en la actualidad derivados del avance tecnológico son:

- Errores de procesamiento debido a la automatización e integración global de sistemas.
- Fraudes por crecimiento del comercio electrónico.
- Fallas debido a fusiones o adquisiciones a gran escala.
- Errores derivados de la tercerización de servicios.

"Basilea III" es un conjunto integral de reformas elaborado por el Comité de Supervisión Bancaria de Basilea para fortalecer la regulación, supervisión y gestión de riesgos del sector bancario. Estas medidas persiguen:

- mejorar la capacidad del sector bancario para afrontar perturbaciones ocasionadas por tensiones financieras o económicas de cualquier tipo
- mejorar la gestión de riesgos y el bueno gobierno en los bancos
- reforzar la transparencia y la divulgación de información de los bancos.

Las reformas se dirigen a:

- la regulación de los bancos a títulos individual (dimensión microprudencial), para aumentar la capacidad de reacción de cada institución en periodos de tensión
- los riesgos sistémicos (dimensión macroprudencial) que puedan acumularse en el sector bancario en su conjunto, así como la amplificación pro-cíclica de dichos riesgos a lo largo del tiempo.

Estas dos dimensiones son complementarias, ya que aumentando la resistencia de cada banco se reduce el riesgo de alteraciones en el conjunto del sistema.

Los siguientes son los principios acordados por el comité de Basilea: (15)

Desarrollo de un marco adecuado para la gestión del riesgo

Principio 1: El Consejo de administración deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operativo válida para toda la empresa y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.

Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control

Principio 4: los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

Principio 5: Los bancos deberán vigilar periódicamente los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

La función de los supervisores

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operativos. Además, deberán cerciorarse de que se

han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

La función de la divulgación de información

Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estratégicas de gestión del riesgo operativo.

ITIL

ITIL® fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones. (16)

Ilustración 119. Modelo de Ciclo de Vida de un Servicio

ITIL® puede ser adaptado y usado en conjunto con otras prácticas como:

- COBIT
- Seis Sigma

- TOGAF
- ISO 27000
- ISO/IEC 20000

ITIL® está organizado alrededor del ciclo de vida de un servicio el cual incluye: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del servicio y Mejora Continua del Servicio.

El ciclo de vida comienza con la Estrategia del Servicio - entendiendo quienes son los clientes de TI, las ofertas de servicios que se requieren para satisfacer las necesidades de los clientes, las capacidades de TI y los recursos que se requieren para el desarrollo de estas ofertas, y los requisitos para llevarlas a cabo con éxito. Impulsado por la estrategia a través de la entrega y soporte del servicio, el proveedor de servicios de TI siempre debe tratar de asegurarse de que el costo de la entrega sea consistente con el valor entregado al cliente.

El Diseño del Servicio garantiza que los servicios nuevos y modificados se han diseñado de manera efectiva para satisfacer las expectativas del cliente. La tecnología y la arquitectura necesaria para satisfacer las necesidades del cliente de forma rentable son una parte integral del diseño de servicios, como también lo son los procesos necesarios para gestionarlos.

A través de la fase de Transición del Servicio el diseño es construido, probado y puesto a la producción para permitir que el cliente de negocios alcance el valor deseado. En esta fase se cumple la gestión de cambios: el control de los activos y elementos de configuración (los componentes subyacentes tales como hardware, software, etc.) asociados a los servicios nuevos y/o actualizados; validación del servicio; y pruebas y planificación de la transición para asegurar que los usuarios, personal de apoyo y el entorno de producción estén preparados para la puesta en producción.

Una vez puesto en producción, la Operación del Servicio se encarga de la supervisión de la salud en general diaria del servicio. Esto incluye la gestión de las interrupciones en el servicio a través de la restauración rápida después de los incidentes; determinar la causa raíz de los problemas y detectar tendencias asociadas con temas recurrentes; tramitar las solicitudes de los usuarios finales de la rutina diaria; y gestión de acceso a los servicios.

Envolviendo el ciclo de vida del servicio se encuentra la Mejora Continua del Servicio (CSI). CSI ofrece un mecanismo para la organización de TI para medir y mejorar los niveles de servicio, la tecnología y la eficiencia y eficacia de los procesos utilizados en la gestión global de los servicios. (17)

Que Permite ITIL®?

- Alineación con las necesidades del negocio
- Los niveles de servicio alcanzables y negociados
- Procesos predecibles y consistentes
- Eficiencia en la prestación de servicios
- Servicios y procesos mejores y medibles
- Un lenguaje común

Otros Aspectos

Aspectos generales a tener en cuenta son:

El marco de gobierno corporativo y gobierno de TI deben representar la alineación que debe existir entre los objetivos organizacionales (presentes en el plan estratégico corporativo) y los lineamientos y actividades del gobierno de TI. (Ver Ilustración 7)

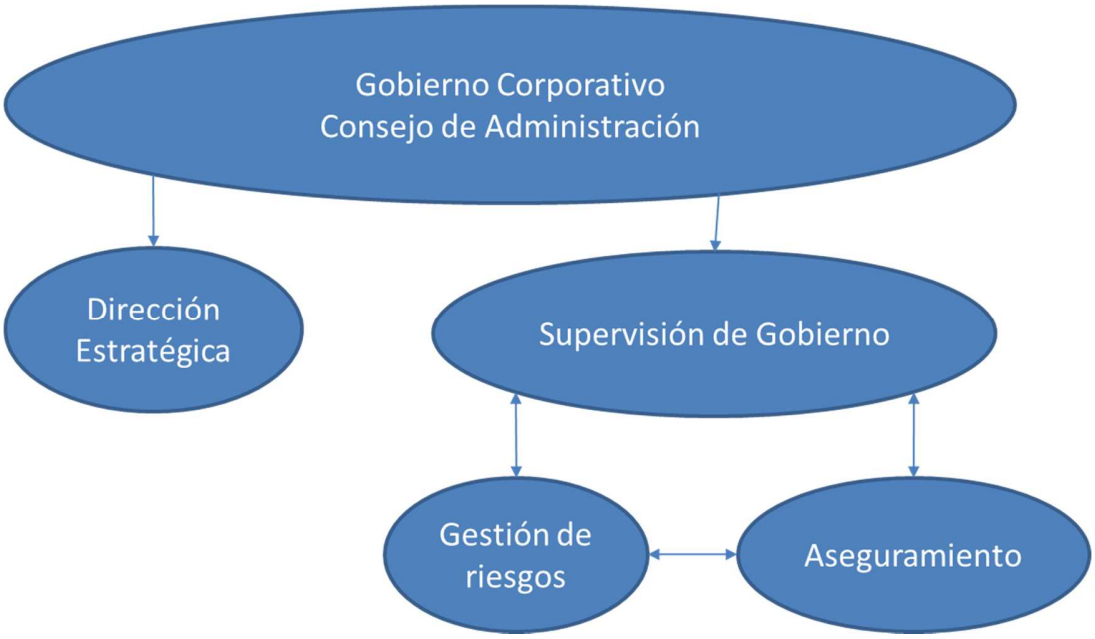


Ilustración 12~~10~~. Componente del Gobierno Corporativo – tomado del Instituto Internacional de Auditores Internos

De esta misma manera, en el siguiente grafico se ilustra cómo el Gobierno de TI involucra los aspectos de Gestión Estratégica de TI y a partir de esta la Planeación de TI (PTI), Control de Gestión de TI (CGTI) y Administración de un Portafolio de Proyecto de TI (APPTI)[2].

[2] Applegate-McFarlan-McKenney, 1996

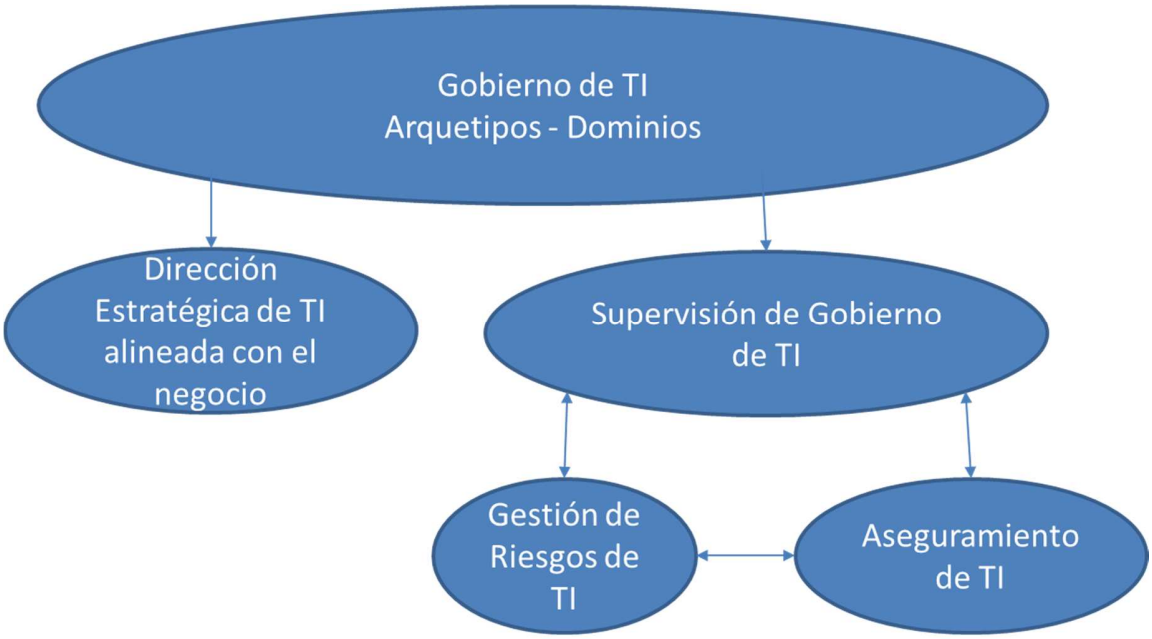


Ilustración 13~~11~~. Componentes dl Gobierno de TI (GobIT) (18)

La Gestión Estratégica de Riesgo de TI está asociada al Control de Gestión de TI y está conformada por la Administración de Riesgos y la Gestión de la Continuidad. Es aquí en donde el marco de COBIT realiza es relevante.

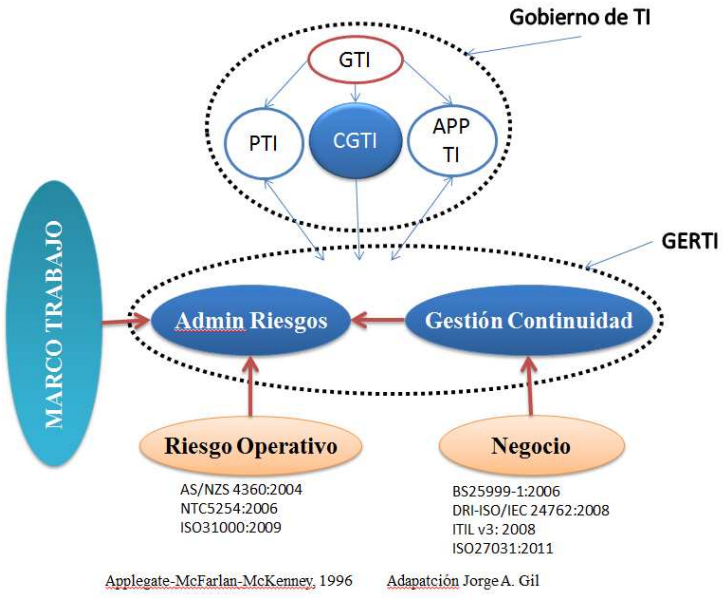


Ilustración 14~~12~~. Gestión Estratégica De Riesgos De Tecnología Informática - GERTI

III. Alinear los Marcos Seleccionados

Esta fase consiste en realizar las actividades necesarias para obtener un documento en donde se relacionan los estándares requeridos para elaborar el producto final el proyecto.

Entradas	Técnicas	Salidas
• Requerimientos documentados. • Marcos Teórico Aplicables. • Arquitectura	• Modelos Previos • Casos de Estudio. • Recomendaciones y Mejores Practicas • Juicio de expertos	• Matriz de alineación de modelos.

Entradas

a. Requerimientos documentados.

Este entregable contiene la definición exacta de los requerimientos del trabajo a realizar; en resumen condensa las expectativas de los interesados.

Los requerimientos del proyecto establecen la fuente base para la definición de un alcance claro, un plan de trabajo y unos mecanismos apropiados de medición de resultados

b. Marcos Teórico Aplicables.

En este punto se tienen en cuenta los marcos de referencia que se utilizan para este trabajo. Entre los que están COBIT 5, ITIL v3, ISO 38500, BASILEA.

c. Arquitectura

La arquitectura empresarial contiene todos los procesos de negocio, datos/información, aplicaciones y tecnologías sobre las que se apoyan las operaciones diarias. Un modelo de arquitectura bien definido, facilitará enormemente la definición de requerimientos.

Técnicas

a. Modelos Previos

Corresponde a modelos y estudios realizados con anteridad tanto en el ámbito financiero como de gobierno y gestión de tecnología. Dichos estudios pueden haber sido realizados interna o externamente, en el sectur público y tambien privado

b. Casos de Estudio.

Está técnica permite el estudio de la situación a partir del análisis de casos existentes, así mismo como la parametrización y evaluación por escenarios.

c. Recomendaciones y Mejores Prácticas

Correspode a las prácticas y recomendaciones comunmnete aceptadas por la industria

d. Juicio de expertos

Utilizar el juicio de expertos para analizar levantar información relevante. Entre estos expertos están: consultores, profesionales, expertos en temas de gobierno y gestión de TI y expertos en banca central

Salidas

a. Matriz de Alineación de Modelos

A partir de lo estudiado nuestro trabajo para la construcción e implementación del marco de gobierno consiste en alinear las mejores prácticas de gestión y seguridad de TI. Para esto se utilizó como referencia lo expuesto en C. Pardo, F. J. Pino, F. García, y M. Piattini, "Framework de armonización para múltiples marcos de referencia de proceso,"

Los modelos de referencia que se utilizaran para el presente trabajo son los ya nombrados:

- COBIT 5
- BASILEA II / III
- ITIL
- ISO 38500

Algunos trabajos previos que se tomaron como base de este documento son:

- IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance. (19)
- Mapping of BASEL III and COBIT 5 framework in Banking Sector of India: A Futuristic Approach (20)
- Towards a Model for Information Technology Governance applicable to the Banking Sector (21)
- Uruguay Central Bank adopts Cobit for entire Uruguayan Financial Market (22)

Para desarrollar el marco lo primero que se hizo es una comparación de alto nivel de los procesos de COBIT con los principios de riesgo operativo definidos por el comité de Basilea. Para esto se tomó como base análisis y estudios realizados anteriormente (23) (24) relacionados con el tema y que pueden ser considerados como referentes del presente trabajo.

Resultado del análisis de los marcos metodológicos de referencia tenemos el siguiente cuadro de resumen en el cual se tuvo en cuenta la pertinencia de los procesos COBIT con un enfoque orientado a los riesgos y los principios de BASILEA.

		Desarrollo de un marco adecuado para la gestión del riesgo			Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control				La función de los supervisores		La función de la divulgación de información
		1	2	3	4	5	6	7	8	9	10
		Conocimiento del consejo de administración	Auditoria Interna Independiente	Marco de gestión de riesgo operativo	Identificar y evaluar riesgos	Monitoreo de riesgos	Politicas, procesos y procedimientos	Planes de contingencia y de negocios	Requerimientos de supervisión bancaria	Evaluación de supervisión bancaria	Publicación de información
APO	APO02 Manage Strategy			X							
	APO11 Manage Quality			X			X		X		
	APO12 Manage Risk	X			X	X	X		X		
BAI	BAI08 Manage Knowledge						X				
DSS	DSS04 Manage Continuity							X			
MEA	MEA01 Monitor and Evaluate Performance And Conformance			X		X	X	X	X	X	
	MEA02 Monitor System of Internal Control		X			X	X		X	X	
	MEA03 Monitor and Evaluate Compliance with External Requirements		X				X		X		

Tabla 23. Relación de Procesos COBIT vs BASILEA base del modelo propuesto

IV. Construir Modelo de Gobierno de TI

Esta fase que consiste en ejecutar el trabajo definido y elaborar una guía práctica de implementación del marco de gobierno de TI propuesto y así mismo establecer una línea de madurez que nos permita medir el grado de cumplimiento del mismo.

Entradas	Técnicas	Salidas
• Matriz de alineación de modelos. • Requerimientos.	• Análisis de casos. • Juicio de Expertos. • Estimación por analogía • Investigación e innovación	• Modelo de Implementación • Línea de madurez

Entradas

a. Matriz de alineación de modelos.

Corresponde a la salida principal del proceso anterior

b. Requerimientos Documentados.

Este entregable contiene la definición exacta de los requerimientos del trabajo a realizar; en resumen condensa las expectativas de los interesados.

Los requerimientos del proyecto establecen la fuente base para la definición de un alcance claro, un plan de trabajo y unos mecanismos apropiados de medición de resultados

Técnicas

a. Análisis de casos.

Está técnica permite el estudio de la situación a partir del análisis de casos existentes, así mismo como la parametrización y evaluación por escenarios.

b. Juicio de Expertos.

Se utiliza el juicio de expertos para analizar la información necesaria para diseñar el nuevo modelo de gobierno de TI. Entre estos expertos estarán: consultores, profesionales, expertos en temas de gobierno y gestión de TI y expertos en banca central

c. Estimación por analogía

Se utiliza la comparación basada en experiencias del mismo tipo aplicado a otras industrias o de características similares a la banca central; bien sea en el ámbito nacional o internacional. Se hace uso de las lecciones aprendidas y resultados obtenidos de dichas experiencias.

d. Investigación e innovación

A partir de los conocimientos adquiridos y de la experiencia profesional y basada en los modelos mencionados, se realiza una propuesta particular sobre el caso, que refleje la posición personal del autor sobre esta temática.

Salidas

a. Modelo de Implementación

Se obtiene como resultado una guía práctica de implementación del nuevo modelo de gobierno de TI para instituciones de banca central. La guía de implementación contiene el esquema general de operación el cual es parte esencial del proceso de gobierno. Está guía resulta importante ya que permite mejorar el desempeño de la gestión de TI y dar cumplimento a las demandas de servicio a las que obliga el negocio.

A continuación se ilustra el modelo general de gobierno propuesto sobre el cual se llevará a cabo el desarrollo del objeto del presente trabajo.

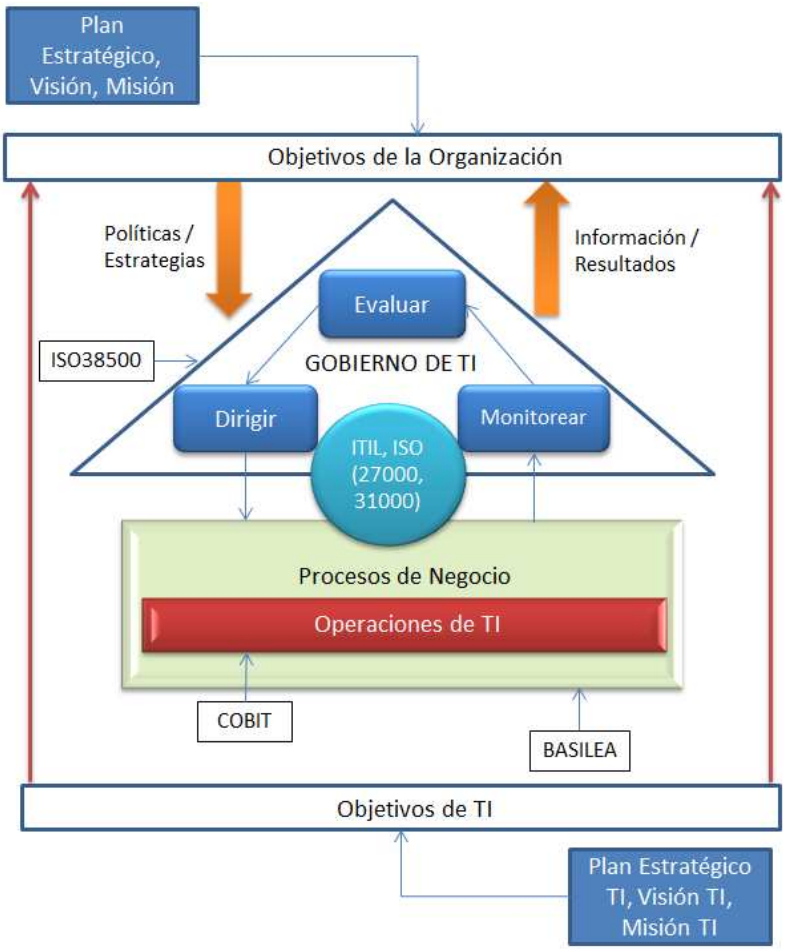


Ilustración 15~~13~~. Marco de Gobierno y Gestión de TI para la Banca Central

Definir el marco de gobierno de TI para la banca central

El marco de gobierno propuesto presenta una alineación con el gobierno corporativo desde el cual se reciben las necesidades y presiones del negocio, así como todo el ámbito regulatorio que rige la actividad de la banca central. Las políticas y estrategias de la organización son insumo en donde las tareas de Evaluar, Dirigir y Monitorear permiten a la alta dirección contar con los principios que rigen su gestión.

Este modelo presenta los factores críticos para dar solución a la gestión de la tecnología y la información. Dichos factores se definen de acuerdo a las necesidades del negocio y al marco de principios expuestos en COBIT 5 y BASILEA.

A través del gobierno de TI se dirigen esfuerzos hacia los procesos de negocio, los cuales tienen inmersas las operaciones y proyectos de TI, las cuales se realizan siguiendo un modelo de gestión basados en un numero de procesos que requieren "planeación, implementación, ejecución y monitoreo"

En el entorno de gestión se definen los procesos en una relación de cadena de valor y ciclo de mejoramiento continuo en el cual se busca garantizar que las salidas que se envían hacia el entorno de gobierno contengan los resultados refinados y con el mayor valor requerido posible.

Las fases o etapas de este ciclo son:

- Definir y Planear
- Implementar y Ejecutar
- Monitorear y Controlar
- Mantener y Mejorar

A continuación se presentará una gráfica modelo de gestión de TI (Ilustración 13) el cual se ha estructurado basado en el ciclo PHVA para asegurar que se esté realizando una gestión eficaz y un mejoramiento continuo. Cada Etapa está conformada por un grupo de actividades claves tomadas de COBIT 5 y que son extraídas de su pertinencia para el cumplimiento de lo dispuesto por ITIL y BASILEA con énfasis en la gestión del Riesgo.

A continuación se muestra se detallan las prácticas claves de cada etapa y el detalle de sus entradas, procesos y salidas

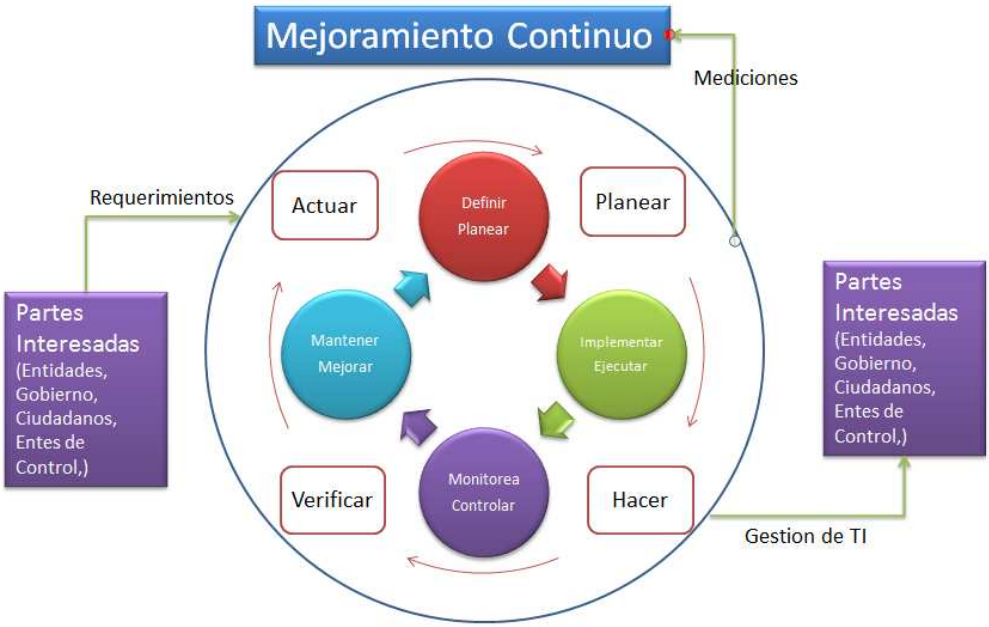


Ilustración 1614. Procesos de Gestion de TI

La siguiente tabla que relaciona los procesos de COBIT identificados con los dominios del modelo propuesto y las actividades a realizar. Para determinar tanto los procesos como las actividades se hizo un análisis con base en un enfoque orientado a los riesgos y se seleccionaron aquellos dominios o actividades que se consideran de mayor relevancia.

	Definir y Planear	Implementar y Ejecutar	Monitorear y Controlar	Mantener y Mejorar
APO				
• **APO02** • **APO11** • **APO12**	APO02.05 APO11.01 APO12.01 APO12.02 APO12.03 APO12.04	APO02.06 APO12.05 APO12.06	APO11.04	
BAI				
• **BAI08**	BAI08.01	BAI08.04		
DSS				
• **DSS04**	DSS04.01	DSS04.03 DSS04.06	DSS04.04 DSS04.06	
MEA				
• **MEA01** • **MEA02** • **MEA03**				MEA01.01 MEA02.01 MEA03.01

Como se mencionó anteriormente, el modelo está fundamentado en los 4 dominios que cubren los aspectos básicos de gestión de riesgo con base en el estudio de los marcos de referencia tenidos en cuenta en el presente trabajo (COBIT, ITIL, BASILEA) con un enfoque basado en la prevención de riesgos.

A continuación se presenta el detalle de cada uno de estos dominios con sus actividades, entradas, salidas, etc

1. Definir y Planear

En este dominio se trabajan los procesos que permiten la planeación de las actividades y proyectos de TI que serán implementados, soportados y monitoreados a futuro y que garanticen la correcta operación del negocio.

Se definen actividades como:

- Definir el plan estratégico
- Realizar análisis de riesgos
- Definir la calidad
- Definir las políticas de continuidad

Por lo tanto se seleccionaron las siguientes prácticas de COBIT 5 que se alinean con las actividades mencionadas.

PROCESO DE COBIT	PRACTICA
APO02- Gestionar la Estrategia APO11- Gestionar la Calidad APO12- Gestionar el Riesgo	APO02.05 - Definir el Plan Estratégico y Hoja de Ruta. APO11.01 - Establecer un Sistema de Gestión de la Calidad (QMS). APO12.01 – Recolectar Datos APO12.02 – Análisis de Riesgos APO12.03 - Mantener un perfil de Riesgos APO12.04 - Articular Riesgos
BAI08- Gestionar el Conocimiento	BAI08.01 - Nutrir y Facilitar una Cultura de Intercambio de Conocimientos
DSS04- Gestionar la Continuidad	DSS04.01 - Definir la política de continuidad del negocio, objetivos y alcance

A continuación se muestran los aspectos generales de los procesos y las prácticas claves con su descripción, objetivos, indicadores y sus prácticas claves que están acompañadas de sus actividades, entradas y salidas

Proceso: APO02 – Gestionar la Estrategia

Descripción: Proveer una visión holística de los negocios actuales y el ambiente de TI, la dirección futura y las iniciativas requeridas para migrar a ese ambiente deseado.
Objetivo: Alinear el plan estratégico de TI con los objetivos del negocio. Comunicar claramente los objetivos asociados alcanzados para que puedan ser entendidos por todos, con las opciones estratégicas de TI identificadas y estructuradas e integradas a los planes de negocio.
Métricas del Proceso
• Porcentaje de objetivos en la estrategia de TI que soportan la estrategia de la organización
Métricas de TI
• Porcentaje de metas estratégicas de la organización y requerimientos soportados por las metas estratégicas de TI

Practica de Gobierno		
APO02.05	Definir el Plan Estratégico y Hoja de Ruta.	Crear un plan estratégico que defina, en cooperación con los interesados principales, como las metas relacionadas con TI que contribuyen a los objetivos estratégicos de la organización.
Entradas		
• Plan estratégico corporativo • Requerimientos del negocio		
Actividades		
• Definir las iniciativas requeridas para cerrar las brechas y migrar desde el estado actual hacia un ambiente deseado, incluyendo presupuesto de inversión/operación, fuente de recursos, estrategia de abastecimiento y estrategia de compras • Convertir los objetivos en salidas medibles representadas por métricas y metas que puedan relacionarse con los beneficios empresariales. • Obtener formalmente el soporte para los interesados principales y obtener la aprobación del plan.		
Salidas		
• Plan estratégico de TI		

Proceso: APO11 – Gestionar la Calidad
Descripción: Definir y comunicar los requerimientos de calidad en todos los procesos, procedimientos y las salidas relacionadas del negocio, incluyendo controles, monitoreo y el uso de prácticas y estándares en mejoramiento continuo y esfuerzo eficiente..
Objetivo: Asegurar la entrega consistente de las soluciones y servicios para cumplir los requerimientos de calidad del negocio y satisfacer las necesidades de los stakeholders.

Métricas del Proceso
• Porcentaje de proyectos que cumplen con las metas y objetivos de calidad esperados • Numero de servicios con un plan formal de gestión de la calidad
Métricas de TI
• Porcentaje de usuarios satisfechos con la calidad de los servicios de TI • Porcentaje de cumplimiento de los niveles de acuerdo de servicio

Practica de Gobierno		
APO11.01	Establecer un Sistema de Gestión de la Calidad (QMS).	Establecer y mantener un QMS que provea un standard y un enfoque formal y continuo a la gestión de la calidad de la información, que permita que los procesos de negocio y TI estén alineados con la gestión de la calidad empresarial.
Entradas		
• Sistema de calidad de la organización		
Actividades		
• Definir las funciones, tareas, permisos de decisión y responsabilidades para la gestión de la calidad en la estructura organizativa. • Definir los planes de gestión de calidad para los procesos importantes, proyectos u objetivos alineados con los criterios y las políticas de gestión de calidad de la organización. • Comunicar eficazmente el enfoque (por ejemplo, a través de programas de formación de calidad).		
Salidas		
• Plan de Gestión de la Calidad • Roles y Responsabilidades		

Proceso: APO12 – Gestionar el Riesgo
Descripción: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
Objetivo: Integrar la gestión de los riesgos de TI con la gestión de riesgos corporativos y balancear los costos y beneficios de la gestión de riesgos de TI
Métricas del Proceso
• Porcentaje de procesos claves en la organización incluidos en el perfil de riesgo • Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados
Métricas de TI

- Costo del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de imagen.
- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen

Practica de Gobierno		
APO12.01	Recolectar Datos.	Identificar y recolectar los datos relevantes para permitir la identificación, análisis y reporte de los riesgos de TI.

Entradas

- Evaluación de las actividades de gestión de riesgo
- Políticas de gestión de riesgo

Actividades

- Establecer y mantener un método para la recogida, clasificación y análisis de los datos relacionados con los riesgos de TI, con capacidad para varios tipos de eventos, varias categorías de riesgos de TI y múltiples factores de riesgo.
- Registrar los datos relevantes sobre el entorno operativo interno y externo de la empresa que podrían desempeñar un papel importante en la gestión de riesgos de TI.
- Llevar a cabo el análisis periódico de eventos y factor de riesgo para identificar problemas de riesgos nuevos o emergentes y para obtener una comprensión de los factores de riesgo internos y externos asociados.

Salidas

- Datos del entorno de operación relacionados con los riesgos
- Datos en eventos de riesgo y factores que influyen
- Elementos y factores de riesgo emergentes

Practica de Gobierno		
APO12.02	Análisis de Riesgos.	Proveer información útil para soportar la toma de decisiones de acuerdo a los factores de riesgos relevantes

Entrada

- Análisis de impacto en el negocio
- Evaluación de amenazas potenciales

Actividades

- Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgos, teniendo en cuenta todos los factores de riesgo y la criticidad del negocio. Establecer el ámbito de análisis de riesgo después de realizar un análisis de costo-beneficio.
- Estimar la frecuencia y la magnitud de la pérdida o ganancia asociada con

escenarios de riesgo de TI. Tomar en cuenta todos los factores de riesgo aplicables, evaluar los controles operativos conocidos y estimar los niveles de riesgo residual. • Comparar riesgo residual para la tolerancia al riesgo aceptable e identificar las exposiciones que pueden requerir una respuesta al riesgo. • Análisis de costo-beneficio de las opciones de respuesta a los riesgos potenciales, tales como evitar, reducir / mitigar, transferencia / acción, y aceptar y explotar / aprovechar. Proponer la respuesta optima al riesgo. • Validar los resultados de análisis de riesgo antes de usarlos en la toma de decisiones, lo que confirma que el análisis se alinea con los requisitos de la empresa y la verificación de que las estimaciones fueron calibrados adecuadamente.
Salidas
• Resultado de análisis de riesgo

Practica de Gobierno		
APO12.03	Mantener un perfil de Riesgos.	Mantener un inventario de los riesgos conocidos (probabilidad, impacto y respuesta) y de los recursos relacionados, las capacidades y las actividades de control actuales.
Entradas		
• Evaluación de amenazas potenciales		
Actividades		
• Determinar y acordar los servicios de TI y recursos de infraestructura de TI que son esenciales para mantener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los puntos débiles. • Capturar información sobre los riesgos de TI acontecimientos que se han materializado, para su inclusión en el perfil de riesgo de TI de la organización. • Capturar información sobre el estado del plan de acción de riesgo, para su inclusión en el perfil de riesgo de TI de la organización.		
Salidas		
• Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión de riesgo		

Practica de Gobierno		
APO12.04	Articular Riesgos.	Proporcionar a todas las partes interesadas la información oportuna sobre el estado actual de las exposiciones y oportunidades relacionadas con TI necesarias para una respuesta adecuada.
Entradas		
Actividades		

• Informe de los resultados de análisis de riesgos a todos los interesados afectados en los términos y formatos útiles para apoyar las decisiones de la organización. • Informar sobre el perfil de riesgo actual para todas las partes interesadas, incluida la eficacia del proceso de gestión de riesgos, el control de eficacia, lagunas, incoherencias, redundancias, estado de remediación, y su impacto en el perfil de riesgo. • Revisar los resultados de las evaluaciones objetivas de terceros, auditoría interna y los controles de calidad, y asignarlos al perfil de riesgo.
Salidas
• Análisis de riesgos e informe del perfil de riesgos para las partes interesadas • Revisión de resultados de valuaciones de riesgos de órganos de control

Proceso: BAI08 – Gestionar el Conocimiento
Descripción: Mantener la disponibilidad del conocimiento relevenate, actual, valido y confiable para soportar todos los procesos y actividades que facilitan la toma de decisiones. Planear la identificación, obtención, organización, mantenimiento, uso y descarte del conocimiento.
Objetivo: Alienar estratégicamente el plan de TI con los objetivos del negocio. Comunicar claramente los objetivos y responsabilidades asociadas para que sean entendidas por todos.
Métricas del Proceso
• Número de usuarios entrenados en usar y compartir información • Nivel de satisfacción de los usuarios
Métricas de TI
• Nivel de satisfacción de los ejecutivos del negocio respecto a la respuesta de TI a nuevos requerimientos

Practica de Gobierno		
BAI08.01	Nutrir y Facilitar una Cultura de Intercambio de Conocimientos	Diseñar e implementar un esquema para fomentar y facilitar la cultura de intercambio de conocimiento.
Entradas		
•		
Actividades		
• Crear un ambiente, herramientas y artefactos que apoyen el intercambio y transferencia de conocimientos. • Integrar las prácticas de gestión del conocimiento en otros procesos TI.		
Salidas		
• Conocimiento de requerimientos y fuentes		

Proceso: DSS04 – Gestionar la Continuidad
Descripción: Establecer y mantener un plan que permita al negocio y a TI responder a los incidentes e interrupciones con el fin de dar continuidad a los procesos críticos del negocio y los servicios de TI y dar disponibilidad de la información en los niveles aceptables para la organización.
Objetivo: Dar continuidad a las operaciones de negocio y mantener disponible la información con los niveles aceptables para la organización ante eventos de interrupción.
Métricas del Proceso
• Frecuencia de pruebas de continuidad del servicio • Porcentaje de servicios de TI que cumplen lo requisitos del teimpos de funcionamiento
Métricas de TI
• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Nivel de satisfacción de los usuarios • Número de incidentes en los procesos de la organización causados por la indisponibilidad de la información

Practica de Gobierno		
DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance	Definir una política y alcance de continuidad del negocio alineada con los objetivos corporativos de los stakeholders
Entradas		
• Acuerdos de niveles de servicio (SLA)		
Actividades		
• Identificar los procesos de negocio internos y subcontratados y actividades de servicios que son críticos para las operaciones de la organización o que son necesarios para cumplir con las obligaciones legales y/o contractuales. • Identificar las partes interesadas y los roles y responsabilidades para definir y acordar la política de continuidad. • Definir y documentar los objetivos y el alcance mínimo acordado para la continuidad del negocio y la necesidad de integrar la planificación de la continuidad de la cultura de la organización.		
Salidas		

2. Implementar y Ejecutar

En este dominio se trabajan los procesos que permiten la implementación y ejecución de los procesos de TI que serán soportados y monitoreados a futuro y que garanticen la correcta operación del negocio.

Se definen actividades como:

- Comunicar la estrategia
- Gestionar las oportunidades para reducir el riesgo
- Responder de manera adecuada a los riesgos
- Compartir el conocimiento
- Gestionar la continuidad

Por lo tanto se seleccionaron las siguientes prácticas de COBIT 5 que se alinean con las actividades mencionadas.

PROCESO DE COBIT	PRACTICA
APO02- Gestionar la Estrategia APO12- Gestionar el Riesgo	APO02.06 - Comunicar la estrategia de TI y dirección APO12.05 - Definir Portafolio de Acción de Gestion del Riesgo APO12.06 - Responder a Riesgos
BAI08- Gestionar el Conocimiento	BAI08.04 - Usar y compartir el conocimiento
DSS04- Gestionar la Continuidad	DSS04.03 - Desarrollar e Implementar un BCP DSS04.06 - Proporcionar formación en el plan de continuidad

A continuación se muestran los aspectos generales de los procesos y las prácticas claves con su descripción, objetivos, indicadores y sus prácticas claves que están acompañadas de sus actividades, entradas y salidas

Proceso: APO02 – Gestionar la Estrategia
Descripción: Proveer una visión holística de los negocios actuales y el ambiente de TI, la dirección futura y las iniciativas requeridas para migrar a ese ambiente deseado.
Objetivo: Alinear el plan estratégico de TI con los objetivos del negocio. Comunicar claramente los objetivos asociados alcanzados para que puedan ser entendidos por todos, con las opciones estratégicas de TI identificadas y estructuradas e integradas a los planes de negocio.
Métricas del Proceso
• Porcentaje de objetivos en la estrategia de TI que soportan la estrategia de la organización
Métricas de TI
• Porcentaje de metas estratégicas de la organización y requerimientos soportados por las metas estratégicas de TI

Práctica de Gobierno		
APO02.06	Comunicar la estrategia de TI y dirección.	Crear conciencia y comprensión de los objetivos del negocio y de TI, a través de una comunicación apropiada a los stakeholders.
Entradas		
• Comunicación de estratégias		
Actividades		
• Desarrollar un plan de comunicación que maneje los mensajes requeridos, las audiencias objetivo, mecanismos de comunicación y horarios. • Preparar un paquete de comunicación con un plan de la utilización eficaz de los medios de comunicación y las tecnologías disponibles.		
Salidas		
• Plan de comunicación		

Proceso: APO12 – Gestionar el Riesgo
Descripción: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
Objetivo: Integrar la gestión de los riesgos de TI con la gestión de riesgos corporativos y balancear los costos y beneficios de la gestión de riesgos de TI
Métricas del Proceso
• Porcentaje de procesos claves en la organización incluidos en el perfil de riesgo • Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados
Métricas de TI
• Costo del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de imagen. • Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen

Prácticas de Gobierno		
APO12.05	Definir Portafolio de Acción de Gestion del Riesgo	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable
Entradas		
Actividades		
• Mantener un inventario de las actividades de control que existentes para manejar el riesgo y que permiten determinar cuáles riesgos puede asumirse de acuerdo con el apetito de riesgo y la tolerancia. Clasificar las actividades de control y mapearlas		

a las categorías específicas de riesgos de TI contempladas. • Determinar si cada entidad organizativa monitorea el riesgo y acepta la rendición de cuentas para operar dentro de sus niveles de tolerancia individual como sectorial. • Definir un conjunto equilibrado de propuestas de proyectos diseñados para reducir el riesgo y/o proyectos que aprovechen oportunidades empresariales estratégicas, considerando el costo/beneficio, el efecto sobre el perfil de riesgo actual y las regulaciones existentes.
Salidas
• Propuestas de proyecto para reducir el riesgo

Prácticas de Gobierno		
APO12.06	Responder a Riesgos	Responder de manera adecuada y a tiempo para limitar las pérdidas por eventos relacionados con TI.
Entradas		
• Acciones correctivas para tratar las desviaciones de gestión de riesgos		
Actividades		
• Preparar, mantener y ensayar planes que documentan los pasos específicos a seguir cuando un evento de riesgo puede provocar un incidente operacional o hecho significativo con impacto serio en el negocio. • Aplicar el plan de respuesta adecuada para minimizar el impacto cuando se producen incidentes de riesgo.		
Salidas		
• Planes de respuesta para incidentes relacionados con el riesgo • Comunicaciones del impacto del riesgo		

Proceso: BAI08 – Gestionar el Conocimiento
Descripción: Mantener la disponibilidad del conocimiento relevenate, actual, valido y confiable para soportar todos los procesos y actividades que facilitan la toma de decisions. Planear la identificación, obtención, organización, mantenimiento, uso y descarte del conocimiento.
Objetivo: Alienar estratégicamente el plan de TI con los objetivos del negocio. Comunicar claramente los objetivos y responsabilidades asociadas para que sean entendidas por todos.
Métricas del Proceso
• Número de usuarios entrenados en usar y compartir información • Nivel de satisfacción de los usuarios
Métricas de TI
• Nivel de satisfacción de los ejecutivos del negocio respecto a la respuesta de TI a

nuevos requerimientos

Práctica de Gobierno		
BAI08.04	Usar y compartir el conocimiento	Propagar los recursos de conocimientos disponibles para los interesados y comunicar como estos recursos pueden ser utilizados para diferentes necesidades
Entradas		
• Documentos de soluciones • Planes de uso y operacion		
Actividades		
• Identificar los usuarios potenciales y clasificarlos • Transferir el conocimiento basado en las necesidades y en un análisis de brechas • Educar y entrenar a los usuarios sobre las bases de conocmiento disponibles, su acceso y uso		
Salidas		
• Base de datos de conocimiento		

Proceso: DSS04 – Gestionar la Continuidad
Descripción: Establecer y mantener un plan que permita al negocio y a TI responder a los incidentes e interrupciones con el fin de dar continuidad a los procesos críticos del negocio y los servicios de TI y dar disponibilidad de la información en los niveles aceptables para la organización.
Objetivo: Dar continuidad a las operaciones de negocio y mantener disponible la información con los niveles aceptables para la organización ante eventos de interrupción.
Métricas del Proceso
• Frecuencia de pruebas de continuidad del servicio • Porcentaje de servicios de TI que cumplen lo requisitos del teimpos de funcionamiento
Métricas de TI
• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Nivel de satisfacción de los usuarios • Número de incidentes en los procesos de la organización causados por la indisponibilidad de la información

Práctica de gobierno		
DSS04.03	Desarrollar e Implementar un BCP	Desarrollar un plan de continuidad del negocio basado sobre la estrategia que documenta los procedimientos y la información que existe para

		que la empresa continúe sus actividades críticas.
Entradas		
Actividades		
• Definir las acciones de respuesta a incidentes y comunicaciones que deben adoptarse en caso de perturbación. Definir las funciones y responsabilidades relacionadas, incluyendo la responsabilidad para la política y la implementación. • Definir las condiciones y los procedimientos de recuperación que permitan la reanudación del proceso de negocio, incluida la actualización y la reconciliación de las bases de datos de información para preservar la integridad de la información. • Definir y documentar los recursos necesarios para apoyar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.		
Salidas		
• Acciones de respuesta a incidentes • Plan de continuidad del negocio		

Práctica de gobierno		
DSS04.06	Proporcionar formación en el plan de continuidad	
Entradas		
• Lista de personal que requiere formación		
Actividades		
• Definir y mantener los planes y requerimiento de formación para quienes planifiquen la continuidad y realicen análisis de impacto, evaluaciones de riesgo, comunicación con los medios y respuesta a incidentes. • Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación		
Salidas		
• Requerimientos de formación • Planes de formación		

3. Monitorear y Controlar

En este dominio se trabajan los procesos que permiten el monitoreo y control de los procesos de TI de tal forma que se garantice la correcta operación del negocio.

Se definen actividades como:

- Monitorear la calidad
- Entrenar en continuidad del negocio

Por lo tanto se seleccionaron las siguientes prácticas de COBIT 5 que se alinean con las actividades mencionadas.

PROCESO DE COBIT	PRACTICA
APO11 – Gestionar la Calidad	APO11.04 - Realizar Monitoreo y Control de la Calidad
DSS04 - Gestionar la Continuidad	DSS04.04 - Probar y Revisar el BCP DSS04.08 - Ejecutar revisiones post-reanudación

A continuación se muestran los aspectos generales de los procesos y las prácticas claves con su descripción, objetivos, indicadores y sus prácticas claves que están acompañadas de sus actividades, entradas y salidas

Proceso: APO11 – Gestionar la Calidad
Descripción: Definir y comunicar los requerimientos de calidad en todos los procesos, procedimientos y las salidas relacionadas del negocio, incluyendo controles, monitoreo y el uso de prácticas y estándares en mejoramiento continuo y esfuerzo eficiente..
Objetivo: Asegurar la entrega consistente de las soluciones y servicios para cumplir los requerimientos de calidad del negocio y satisfacer las necesidades de los stakeholders.
Métricas del Proceso
• Porcentaje de proyectos que cumplen con las metas y objetivos de calidad esperados • Numero de servicios con un plan formal de gestión de la calidad
Métricas de TI
• Porcentaje de usuarios satisfechos con la calidad de los servicios de TI • Porcentaje de cumplimiento de los niveles de acuerdo de servicio

Práctica de Gobierno		
APO11.04	Realizar Monitoreo y Control de la Calidad.	Monitorear la calidad de los procesos y servicios y las salidas básicas como están definidas en el QMS.
Entradas		
• Plan de aseguramiento de Calidad • Reportes y estado de incidentes		
Actividades		
• Supervisar la calidad de los procesos y servicios de manera continua y sistemática para describir, medir, analizar, mejorar el control de los procesos. • Controlar la calidad de los procesos, así como el valor de la calidad. Asegurar que la medición, control y registro de información es utilizada por el propietario del proceso para tomar las acciones correctivas y preventivas apropiadas.		

• Monitorear las métricas orientadas a objetivos alineados a las metas generales de calidad que cubran la calidad de los proyectos y servicios individuales.
Salidas
• Resultados de revisiones y auditorias • Proceso de calidad de servicios

Proceso: BAI08 – Gestionar el Conocimiento
Descripción: Mantener la disponibilidad del conocimiento relevenate, actual, valido y confiable para soportar todos los procesos y actividades que facilitan la toma de decisions. Planear la identificación, obtención, organización, mantenimiento, uso y descarte del conocimiento.
Objetivo: Alienar estratégicamente el plan de TI con los objetivos del negocio. Comunicar claramente los objetivos y responsabilidades asociadas para que sean entendidas por todos.
Métricas del Proceso
• Número de usuarios entrenados en usar y compartir información • Nivel de satisfacción de los usuarios
Métricas de TI
• Nivel de satisfacción de los ejecutivos del negocio respecto a la respuesta de TI a nuevos requerimientos

Proceso: DSS04 – Gestionar la Continuidad
Descripción: Establecer y mantener un plan que permita al negocio y a TI responder a los incidentes e interrupciones con el fin de dar continuidad a los procesos críticos del negocio y los servicios de TI y dar disponibilidad de la información en los niveles aceptables para la organización.
Objetivo: Dar continuidad a las operaciones de negocio y mantener disponible la información con los niveles aceptables para la organización ante eventos de interrupción.
Métricas del Proceso
• Frecuencia de pruebas de continuidad del servicio • Porcentaje de servicios de TI que cumplen lo requisitos del teimpos de funcionamiento
Métricas de TI
• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Nivel de satisfacción de los usuarios • Número de incidentes en los procesos de la organización causados por la indisponibilidad de la información

Práctica de Gobierno

DSS04.04	Probar y Revisar el BCP	Probar los planes de continuidad de forma regular para ejercitar los planes de recuperación contra resultados predeterminados y permitir soluciones innovadoras que deban desarrollarse y así contribuir a que el plan funcione como se espera.
Entradas		
Actividades.		
• Definir los objetivos para probar los sistemas de negocio, técnico, logístico, administrativo, procedimental y operacional del plan para verificar la integridad del BCP. • Programar ejercicios y actividades de prueba tal como se define en el plan de continuidad. • Desarrollar recomendaciones para mejorar el plan de continuidad, basado en los resultados de la revisión.		
Salidas		
• Pruebas y ejercicios • Resultados y recomendaciones		

Práctica de Gobierno		
DSS04.08	Ejecutar revisiones post-reanudación	Proveer a las partes internas y externe sesiones regulares de entrenamiento de los procedimientos, roles y responsabilidades en caso de una interrupción de servicios
Entradas		
•		
Actividades.		
• Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia e incidentes, infraestructura técnica y estructuras organizativas y relaciones • Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la organización		
Salidas		
• Informe de revisión post-reanudación • Cambios aprobados a los planes		

4. Mantener y Mejorar

En este dominio se trabajan los procesos que permiten el mantenimiento y mejor de los procesos de TI de tal forma que se garantice la correcta operación del negocio.

Se definen actividades como:

- Monitorear la calidad
- Entrenar en continuidad del negocio

Por lo tanto se seleccionaron las siguientes prácticas de COBIT 5 que se alinean con las actividades mencionadas.

PROCESO DE COBIT	PRACTICA
MEA01 - Supervisar, Evaluar y Valorar Rendimiento y Conformidad MEA02 - Supervisar, Evaluar y Valorar el Sistema de Control Interno MEA03 - Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA01.01 - Establecer un enfoque de supervisión MEA02.01 - Monitorear Controles Internos MEA03.01 - Identificar los requisitos de cumplimiento externos

A continuación se muestran los aspectos generales de los procesos y las prácticas claves con su descripción, objetivos, indicadores y sus prácticas claves que están acompañadas de sus actividades, entradas y salidas

Proceso: MEA01 – Supervisar, Evaluar y Valorar Rendimiento y Conformidad
Descripción: Recolectar, validar y evaluar el negocio, IT, las metas de los procesos y las métricas. Monitorear que los procesos se están realizando de acuerdo a los objetivos y con las métricas de rendimiento de conformidad con lo acordado y proporcionan información de manera sistemática y oportuna.
Objetivo: Proveer transparencia en el desarrollo y conformidad y dirigir el complimiento de metas.
Métricas del Proceso
• Porcentaje de procesos críticos revisados • Porcentaje de objetivos y métircas alineadas al sistema de supervisión empresarial
Métricas de TI
• Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Frecuencia de revisión y actualización de políticas

Práctica de Gobierno		
MEA01.01	Establecer un enfoque de supervisión	Participar con las partes interesadas para establecer y mantener un enfoque de supervisión para definir los objetivos, el alcance y el método para la medición de solución de negocio y la prestación de servicios y la

		contribución a los objetivos de la empresa. Integrar este enfoque con el sistema de gestión del rendimiento corporativo.
Entradas		
Actividades		
1. Identificar las partes interesadas (por ejemplo, gestión de procesos, propietarios y usuarios). 2. Comprometerse con las partes interesadas y comunicar los requisitos y objetivos de la empresa para el seguimiento, la agregación y la presentación de informes, utilizando definiciones comunes. 3. Alinear y mantener continuamente el enfoque de seguimiento y evaluación con el enfoque de la empresa y las herramientas que se utilizarán para la recopilación de datos y generación de informes empresariales. 4. Acordar los objetivos y métricas (por ejemplo, la conformidad, rendimiento, valor, riesgo), taxonomía (clasificación y las relaciones entre los objetivos y métricas) y datos (pruebas) de retención. 5. Acordar una gestión del ciclo de vida y cambiar el proceso de control para la supervisión y presentación de informes. 6. Solicitar, priorizar y asignar recursos para el monitoreo. 7. Validar periódicamente el enfoque utilizado e identificar nuevos interesados, los requisitos y los recursos.		
Salidas		

Proceso: MEA02 – Supervisar, Evaluar y Valorar el Sistema de Control Interno
Descripcion: Monitorear Continuamente y evaluar el ambiente de control incluyendo auto evaluaciones revisiones independientes de aseguramiento. Habilitar la gestión para identificar las deficiencias de control e iniciar planes de mejora.
Objetivo: Obtener transparencia para los stakeholders clave sobre la adecuación del sistema de control interno y proveer certeza en operaciones, confidencialidad en el logro de los objetivos empresariales y un adecuado entendimiento de los riesgos residuales.
Métricas del Proceso
Métricas de TI

Práctica de Gobierno		
MEA02.01	Monitorear Controles Internos.	Continuamente controlar, comparar y mejorar el ambiente de control de TI y el marco de control para cumplir con los objetivos

		organizacionales.
Entradas		
Actividades		
1. Realizar las actividades internas de control y evaluación de control basado en normas de gobierno de la organización y los marcos aceptados por la industria. 2. Considerar las evaluaciones independientes del sistema de control interno. 3. Identificar los límites del sistema de control interno de TI. 4. Asegurar que las actividades de control están en su lugar y las excepciones sean notificadas rápidamente, seguidas y analizadas, y las acciones correctivas apropiadas son priorizados y ejecutadas de acuerdo con el perfil de la gestión de riesgos. 5. Mantener el sistema de control interno de TI, teniendo en cuenta los cambios en curso en los negocios y los riesgos de TI, el ambiente de control organizacional, empresarial relevante y los procesos de TI y los riesgos de TI. Si existen lagunas, evaluar y recomendar cambios. 6. Evaluar periódicamente el desempeño del marco de control de TI, la evaluación comparativa contra la industria de acuerdo a las normas y buenas prácticas. 7. Evaluar el estado de los controles internos de los proveedores de servicios externos y confirmar que los proveedores de servicios cumplan con los requisitos legales y reglamentarios y obligaciones contractuales.		
Salidas		

Proceso: MEA03 – Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
Descripción: Evaluar que los procesos de negocios soportados en TI cumplen con la ley, las regulaciones y los requerimientos contractuales. Obtener garantías de que los requisitos se han identificado y respetado, y la integran el cumplimiento de cumplimiento global de la empresa.
Objetivo: Asegurar que la empresa cumple con todos los requerimientos externos que le aplican.
Métricas del Proceso
• Frecuencia de revisiones de cumplimiento • Número anual de incidentes críticos por incumplimiento
Métricas de TI
• Costo de la no conformidad de TI, incluidos arreglos y multas, e impactos de la pérdida de reputación • Porcentaje de procesos de negocio crítico, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgo

Práctica de Gobierno

MEA03.01	Identificar los requisitos de cumplimiento externos.	Periódicamente, identificar y monitorear los cambios en las leyes, reglamentos y otros requerimientos externos locales e internacionales que deben cumplirse a partir de una perspectiva de TI.
Entradas		
Actividades		
1. Asignar la responsabilidad de identificación y seguimiento de los cambios de los requisitos contractuales externos legales, reglamentarios y otros relativos a la utilización de los recursos de TI y el procesamiento de la información dentro de la empresa. 2. Identificar y evaluar todos los requisitos de cumplimiento potenciales y el impacto en las actividades de TI en áreas tales como el flujo de datos, la privacidad, los controles internos, los informes financieros, las regulaciones específicas de la industria, la propiedad intelectual, salud y seguridad. 3. Evaluar el impacto de los requisitos legales y reglamentarios relacionados con TI en contratos con terceros en relación con operaciones de TI, proveedores de servicios y socios comerciales de negocios. 4. Obtener un abogado independiente, en su caso, sobre los cambios en las leyes, reglamentos y normas. 5. Mantener un registro de puesta al día de todos los requisitos legales, reglamentarios y contractuales pertinentes, su impacto y acciones requeridas. 6. Mantener un registro global armonizado e integrado de los requisitos de cumplimiento externos para la empresa.		
Salidas		

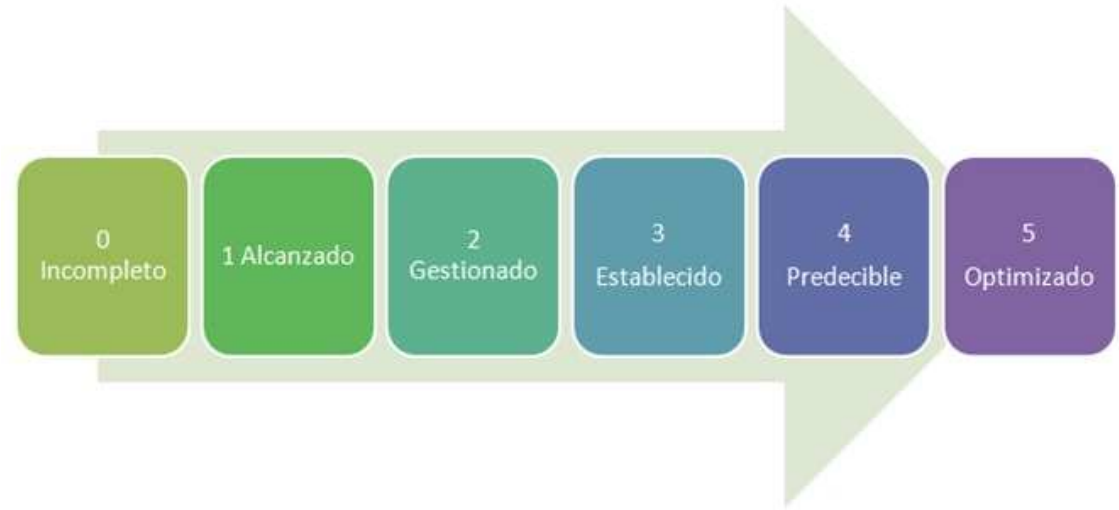
g. Línea de madurez

Corresponde a la fase final de la guía con el propósito de definir el estado actual de cumplimiento de la guía propuesta

La información relacionada con los riesgos requiere documentación alineada con los requerimientos de los procesos de supervisión con el propósito de habilitar y suportar dichos procesos.

La organización debe adoptar un modelo holístico de evaluación de la madurez de la capacidad, donde se entiende capacidad como que tan bien funcionan los procesos y madurez es una medida de que tanto esa capacidad se ha desarrollado.

Los procesos examinados deben estar por lo menos en el nivel 4 el cual indica que se encuentran en un estado de Predecible.



Una breve descripción de los niveles es la siguiente:

Nivel 0: Proceso Incompleto: El proceso no está implantado o no alcanza sus objetivos

Nivel 1: Proceso Alcanzado: El proceso implementado alcanza su objetivo

Nivel 2: Proceso Gestionado: El proceso ejecutado del nivel 1 es implementado de forma gestionada (planificado, supervisado y ajustado) y sus resultados son debidamente establecidos, controlados y mantenidos)

Nivel 3: Procesos establecidos: el proceso gestionado del nivel 2 se implementa usando un proceso definido que es capaz de alcanzar sus objetivos

Nivel 4: Proceso establecido: el proceso establecido del nivel 3 es operado ahora dentro de unos límites definidos para alcanzar sus resultados

Nivel 5: Proceso optimizado: el proceso del nivel 4 es mejorado continuamente para alcanzar metas de negocio actuales y futuros.

V. Implementación del marco de trabajo propuesto

Esta fase consiste en elaborar una guía práctica de implantación del modelo de gobierno de TI.

Entradas	Técnicas	Salidas
• Modelo de Implementación • Línea de madurez	• Juicio de Expertos. • Simulación • Prototipo	• Proyecto de implementación

Entradas

a. Modelo de Implementación

Se obtiene como resultado una guía práctica de implementación del el nuevo modelo de gobierno de TI para instituciones de banca central. La guía de implementación contiene el esquema general de operación el cual es parte esencial del proceso de gobierno. Está guía resulta importante ya que permite mejorar el desempeño de la gestión de TI y dar cumplimento a las demandas de servicio a las que obliga el negocio

b. Linea de madurez

Corresponde a la fase final de la guía con el propósito de definir el estado actual de cumplimiento de la guía propuesta

Técnicas

a. Juicio de Expertos.

Utilizar el juicio de expertos para analizar levantar información relevante. Entre estos expertos están: consultores, profesionales, expertos en temas de gobierno y gestión de TI y expertos en banca central

b. Simulación

Esta herramienta nos permite crear escenarios supuestos con el fin de afinar la estrategia de respuesta

c. Prototipo

Los prototipos son una herramienta de gran utilidad porque permiten diseñar a escala los posibles resultados esperados y funcionalidad deseada

Salidas

a. Proyecto de implementación

El modelo definido para la implementación sigue un esquema similar al propuesto por COBIT 5.

La Guía de Implementación COBIT 5 cubre los siguientes temas:

- Posicionar al Gobierno de IT dentro de la organización
- Tomar los primeros pasos hacia un Gobierno de IT superador
- Desafíos de implementación y factores de éxitos
- Facilitar la gestión del cambio
- Implementar la mejora continua
- La utilización del COBIT 5 y sus componentes

- Reconociendo los puntos débiles
    - Frustración del negocio por iniciativas fallidas, escalada de costos y baja percepción de valor
    - Incremento de incidentes de TI
    - Problemas con servicios tercerizados
    - Regulaciones o requerimientos contractuales incumplidos
    - Limitaciones a la innovación, poca agilidad del negocio
    - Observaciones recurrentes de auditoría
    - Baja performance o calidad
    - Costos ocultos o inflexibles
    - Pérdida de recursos, duplicación de esfuerzos
    - Modelos complejos de operación
    - Falta de sponsors o reacios a participar de iniciativas de TI

A continuación se ilustran las fases del ciclo de vida de la implementación del modelo de gobierno de TI. Se parte de la implementación inicial de un ambiente empresarial apropiado para su desarrollo.

Ilustración 17~~15~~ Fases del Ciclo de vida de Implementación de COBIT 5

Fase 1: comienza con el reconocimiento y el acuerdo de implementar una iniciativa de implementación o mejora. Se identifican las debilidades y se establece una necesidad de cambio desde los niveles de gestión administrativa o ejecutiva.

Fase 2: se centra en definir el alcance de la iniciativa de implementación utilizando el mapeo de objetivos empresariales a objetivos relacionados con TI a procesos asociados de TI y considerando escenarios de riesgo que pueden tener una incidencia en los procesos claves.

Fase 3: se establece un objetivo de mejoramiento, seguido por un análisis detallado aprovechando la guía de implementación de COBIT, con el objeto de identificar las deficiencias y las posibles soluciones.

Fase 4: se establecen planes de soluciones prácticas mediante la definición de los proyectos apoyados por casos de negocios justificables. Un plan de cambio para la implementación también se desarrolla.

Fase 5: las medidas pueden ser definidas y el seguimiento se establece, utilizando los objetivos de COBIT y las métricas para asegurar que la alineación del negocio se logra y se mantiene; y el rendimiento puede medirse.

Fase 6: se centra en un funcionamiento sostenible de los facilitadores nuevos o mejorados y en el seguimiento y obtención de los beneficios esperados.

Fase 7: se revisa el éxito global de la iniciativa, los requisitos adicionales para el gobierno y la gestión corporativa de TI se identifican, y la necesidad de mejora continua se refuerza.

7 Conclusiones

7.1 Resultados obtenidos en la aplicación del Marco de Gobierno de Tecnología para la Banca Central propuesto.

En este capítulo se lleva a cabo la tarea de validar el modelo propuesto frente a lo encontrado en los sitios públicos de información de diversos Bancos Centrales en el mundo. Se inicia con la toma de una muestra aleatoria de Bancos a nivel mundial a partir de los cuales se revisa la información y planes de gobierno corporativo y de TI que estos aplican.

1. **Bancos Centrales estudiados (sitios web) y marcos de referencia que han adoptado**

Los Bancos centrales seleccionados para este estudio son:

Banco de la Republica de Colombia (www.banrep.gov.co)
Banco Central de Chile (www.bcentral.cl)
Reserve Bank of India
Bank of Canada
Banco Central de Uruguay (www.bcu.gub.uy)
Banco Central de la República de Argentina (www.bcra.gov.ar)

La evidencia recolectada a través de un estudio de los sitios web de los Bancos seleccionados y otras fuentes disponibles sumado a la experiencia de campo muestran que estas organizaciones hacen la implementación de sus modelos de gobierno de TI a partir de la combinación de modelos y marcos tales como COBIT, ITIL, ISO 38500 y estándares como ISO 20000 e ISO 27002.

De acuerdo con un informe de ISACA (25), COBIT ha sido adoptado mundialmente como el marco regulatorio del sector público y gobiernos de varios países

A nivel de la banca central, COBIT es reconocido entre otros por: el Reserve Bank of india, Banco Central de la República de Argentina, Banco Central do Brasil, Banco Central de Paraguay, Banco Central de Uruguay, Federal Reserve en Estados Unidos. En Colombia La Superintendencia Financiera lo utiliza como un modelo de referencia para sus evaluaciones (26).

El Banco Central de Uruguay en su Plan Estratégico 2015-2020[3] expresa que unas de sus capacidades a desarrollar es la Gestión tecnológica efectiva, la cual tiene una iniciativa llamada: Continuar desarrollando un modelo de Gobierno y Gestión de TI a través de acciones que reduzcan las brechas identificadas en relación al modelo de capacidades de COBIT5. Igualmente uno de sus procesos estratégicos es Gestionar riesgos y continuidad del negocio.

Dentro de la planeación estratégica del Banco Central de Chile se encuentra un capitulo orientado a Informática que indica como objetivo Proveer servicios y soluciones a las necesidades de tecnología de información del Banco, en línea con los mejores estándares internacionales y de la Banca Central, administrando los riesgos tecnológicos e incorporando las mejores prácticas de seguridad en tecnologías de la información.[4]

El Banco de la Republica de Colombia en sus lineamientos estratégicos (Plan estratégico "El Banco somos todos 2013-2016"[5] define iniciativas alrededor de proveer una infraestructura tecnológica de excelente desempeño y ofrecer soluciones tecnológicas modernas que agreguen valor. En cuanto a riesgos, existen iniciativas para evaluar y asegurar el riesgo operativo.

A partir de la información recopilada en la investigación previa, el desarrollo del modelo de implementación y la validación de la información disponible en los sitios web de los Banco centrales, se propone la aplicación de un camino, como el planteado en este trabajo, para la definición más apropiada del modelo del gobierno de TI que se desee implementar.

Aunque existe información disponible en la mayoría de los sitios web consultados, esta es de carácter general y orientada sobre todo a marcos de gobierno corporativo. En general, se asume que no hay acceso a información detallada, dado el carácter de reserva de gran parte de la información que estos manejan. Se hace necesario, a la hora de implementar este modelo, realizar un trabajo de campo específico para desarrollar el marco propuesto.

Esta guía cumple con el objetivo de brindar un método a través del cual cada Banco Central puede realizar una aproximación más detalladas de los elementos a contemplar a la hora de implementar un marco de gobierno de TI, además de establecer un modelo para hacerlo realidad.

[3] http://www.bcu.gub.uy/Acerca-de-BCU/Transparencia/Plan%202015-2020%20para%20web.pdf
[4] http://www.bcentral.cl/acerca/planificacion-estrategica/index.htm
[5] http://www.banrep.gov.co/sites/default/files/publicaciones/archivos/bst_2013-2016.pdf

Lista de Ilustraciones

Lista de Tablas

Bibliografía

1. *El Gobierno de TI.* **ACIS.** Enero / Marzo 2011, Revista Sistemas.

2. *Operational Risk Management using a Fuzzy Logic Inference System.* **Reveiz Herault, Alejandro y Leon Rincon, Carlos Eduardo.** 574, Bogota : Banco de la Republica, 2009, Vol. Borradores de Economía.

3. **http://www.banrep.gov.co/documentos/el-banco/pdf/Bancos-centrales-tendencias.pdf. [En línea]**

4. http://www.bcentral.cl/acerca/planificacion-estrategica/index.htm. [En línea]

5. http://www.banrep.gov.co/documentos/el-banco/doctos-relativos/nuestro_norte.pdf. [En línea]

6. IT Governance for Central Bank. ***Training course/seminar series.*** **2011.**

7. Journal Online – Gobierno de las TIC ISO/IEC 38500.

8. Project Management Institute. ***PMBOK.***

9. Cano, Carlos Gustavo. Borradores de Economía. ***Sitio web Banco de la Republica.*** **[En línea] 2008. http://www.banrep.gov.co/sites/default/files/publicaciones/pdfs/borra501.pdf.**

10. Manuel Piattini Velthuis, Mario y Fernández Sánchez, Carlos. ***Modelo para el gobierno de las TIC basado en las normas ISO.***

11. ***Gobierno de las TIC ISO/IEC 38500.*** **Manuel, Ballestero. s.l. : ISACA, 2010, Vol. 1.**

12. ISACA. ***COBIT 5. A Business Framework for the Governance and Management of Enterprise IT.*** **2012.**

13. BASILEA II. Covergencia Internacional de Medidas y Normas de Capital. [En línea] 2004. www.bis.org.

14. ***El Gobierno Corporativo y las Mejores Prácticas en el Sector Bancario.*** **DELOITTE. 2011.**

15. COMITE DE SUPERVISIÓN BANCARIA DE BASILEA. ***Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo.*** **2004.**

16. OSIATIS. OSIATIS. [En línea] [Citado el: 14 de 01 de 2015.] http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php.

17. *ITIL-the-basics-White-Paper.*

18. *El Gobierno de TI.* Peñaloza Gil, Jorge Alberto. 118, Bogota : ACIS, 2011, Sistemas.

19. IT Governance Institute (ITGI). *IT Control Objetives for BASEL II.* 2007.

20. *Mapping of BASEL III and COBIT 5 framework in Banking Sector of India: A Futuristic Approach.* Kushwaha, Deepti y Vasant Gadankush, Ashwini. 8, 2013, Vol. 4.

21. Lemus, Sandra Patricia, Pino, Francisco y Piattini, Mario. Towards a Model for Information Technology Governance applicable to the Banking Sector. [En línea] 2010. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5556638&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5548153%2F5556594%2F05556638.pdf%3Farnumber%3D5556638.

22. Cantera, Juan Pedro. ISACA. [En línea] 2011. http://www.isaca.org/Knowledge-Center/cobit/Pages/Uruguay-Central-Bank-adopts-COBIT-for-entire-Uruguayan-Financial-Market.aspx.

23. Lemus, Sandra María, Pinto, Francisco y Piattini, Mario. *Towards a Model for Information Technology Governance applicable to the Banking Sector.*

24. *Mapping of BASEL III and COBIT 5 framework in Banking Sector of India.* Kushwaha, Deepti y Vasant Gadankush, Ashwini. 8, 5 de 2013, Vol. 4.

25. ISACA. *COBIT® Global Regulatory an Legislative Recognition.* 2014.

26. isaca.org. ISACA. [En línea] https://www.isaca.org/COBIT/Documents/Recognition-table.pdf.

27. *The IT Dimension of Basell II.* Guldentops, Erick. 2004, Information System Control Journal, Vol. 6.