Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia

PROYECTO DE GRADO

María Helena Correa Correa
Breyner Alexander Parra Rojas

Asesor
Ing. Hernando Peña Villamil
Magister en Teleinformática
Certificado PMP, ITIL, COBIT, ISO27001

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia

María Helena Correa Correa
Breyner Alexander Parra Rojas

Trabajo de grado para optar al título de
Máster en Gestión de Informática y Telecomunicaciones
Énfasis en Gerencia de TI

Asesor
Ing. Hernando Peña Villamil
Magister en Teleinformática
Certificado PMP, ITIL, COBIT, ISO27001

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, Fecha

TABLA DE CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

Desde la fundación del primer banco privado en Colombia en 1870 (el Banco de Bogotá)[1], el sector bancario colombiano ha tenido un crecimiento importante, no solo financieramente, sino desde el punto de vista tecnológico. En la actualidad, este sector está regido por diferentes leyes y decretos. El principal, el decreto 663 de 1993[2], por medio del cual reglamenta y define que son Establecimientos Bancarios y regula el tipo de operaciones autorizadas; además marca una diferencia entre entidades bancarias y otros tipos de entidades y/o corporaciones financieras. De igual forma, el decreto 4327 de 2005[3] faculta a la Superintendencia Financiera como ente de control del sector bancario, con el fin de hacer preservar la estabilidad, seguridad y confianza, apoyado en el cumplimiento de la ley y sancionando a aquellas entidades que incurran en faltas.

Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo, y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros, sin embargo, el problema es que hasta ahora, no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

A nivel Latinoamérica, el Banco Supervielle S. A. uno de los principales Bancos privados de la Republica Argentina lanzó en el año 2009 un proyecto denominado "Gobierno de TI", donde la Gerencia General del Banco era el patrocinador "Sponsor" y la Gerencia Coordinadora de TI y sus Gerentes los líderes del mismo[4] Sin embargo, no es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.

Por tal motivo, el propósito del presente documento es proponer un modelo de Gobierno de TI, con su respectiva guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector.

---

[1] **Orígenes de la banca comercial en Colombia**. Banco de la Republica. http://www.banrepcultural.org/blaavirtual/revistas/credencial/marzo2001/135origenes.htm

[2] **Decreto 633 de 1993**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

[3] **Decreto 4327 de 2005**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/dec4327-05.doc

[4] **Caso de Estudio: Banco Supervielle S.A.**, Argentina. ISACA. http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/COBIT-Caso-de-Estudio-Banco-Supervielle-SA-Argentina.aspx

1. INTRODUCCIÓN

Son establecimientos bancarios las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito.

Los establecimientos bancarios se dividen en dos tipos:

Banco comercial: Las palabras banco comercial significan un establecimiento que hace el negocio de recibir fondos de otros en depósito general y de usar éstos, junto con su propio capital, para prestarlo y comprar o descontar pagarés, giros o letras de cambio.

Banco hipotecario: Las palabras banco hipotecario significan un establecimiento que hace el negocio de prestar dinero garantizado con propiedades raíces, que debe cubrirse por medio de pagos periódicos y para emitir cédulas de inversión[5].

Es importante saber que todas las entidades que hacen parte del sistema financiero están sujetas a la regulación y supervisión por parte de las autoridades de intervención: el Congreso de la República, el Ministerio de Hacienda y Crédito Público y la Superintendencia Financiera. Así mismo, estas son las encargadas de crear los marcos normativos y de velar porque los recursos de las personas, empresas y el gobierno se encuentren seguros en manos de las diferentes instituciones. Además, la Superintendencia Financiera también tiene funciones de inspección, vigilancia y control sobre las entidades[6].

1.1 Gobierno de TI

Gobierno de TI (Tecnologías de Información) es la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, agregando valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre inversiones en TI. El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas. Muchas organizaciones cuentan con diferentes marcos de Gestión de TI (CobiT, Itil, etc.)

---

[5] **Decreto 633 de 1993**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

[6] **Información al consumidor financiero.** ASOBANCARIA. http://www.asobancaria.com/portal/page/portal/Asobancaria/info_consumidor/sistema_financiero_y_banca/

sin embargo, cuando estos marcos de trabajo y estándares son utilizados colectivamente, se vuelven muy confusos y obstruyen el propósito principal del Gobierno de TI[7]

1.2 Planteamiento del Problema

Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo; y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros; el problema es que no existe un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

1.3 Objetivo General

Proponer un modelo de Gobierno de TI y una guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector, teniendo en cuenta que no sería útil aplicar al pie de la letra modelos de Gobierno de otros sectores colombianos, ya que la infraestructura, tecnología, modelo de negocio y sobre todo, legislación, es diferente. Tampoco es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.

1.4 Objetivos Específicos:

1. Realizar un análisis del contexto del sector bancario en Colombia, incluyendo las principales disposiciones legales que los rigen.

2. Realizar un análisis de los marcos para Gobierno de TI existentes y determinar cuáles son los más apropiados para la creación del modelo a implementar.

3. Crear una autoevaluación de nivel de madurez de Gobierno de TI

4. Desarrollar un modelo de Gobierno de TI, basado en los marcos seleccionados.

5. Crear una guía de implementación para el modelo de Gobierno de TI desarrollado.

---

[7] **Artículo: Gobierno de TI - Estado del arte**. Ingrid Lucía Muñoz Periñán MsC, Gonzalo Ulloa Villegas. Revista S&T, Universidad Icesi. http://www.icesi.edu.co/biblioteca_digital/bitstream/10906/5568/1/Gobierno_de_TI.pdf

6. Validar el modelo y la metodología por un grupo de expertos, a partir de una Rubrica que permita su evaluación.

1.5 Resumen del Modelo Propuesto

El presente modelo de Gobierno de TI propuesto recoge el espíritu de la Circular 014 de 2009, la cual tiene como objetivo primario que las entidades bancarias de Colombia creen y/o fortalezcan un sistema de control interno que permita la **evaluación continua de su eficiencia**, contribuya al **logro de sus objetivos de negocio** y fortalezca la apropiada **administración de los riesgos** a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia.

1.5.1 Requerimientos de TI relevantes para el Modelo

Las entidades bancarias de Colombia se encuentran regidas por diferentes leyes, normas y decretos. Para las áreas de TI, existe en especial la Circular 014 del 2009; en esta, se define en el capíitulo 7.6.2**. (Normas de Control Interno para la Gestión de la Tecnología),** que las entidades bancarias deberán diseñar un Sistema de Control Interno (SCI) para la gestión de la tecnología, que responda a las **políticas, necesidades y expectativas de la entidad** y a **las exigencias normativas**, con el propósito de contribuir al **logro de los objetivos institucionales**[8]

El SIC obliga a los responsables de TI de las Entidades Bancarias a contar con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir los siguientes requerimientos:

1. Plan estratégico de tecnología.
2. Infraestructura de tecnología.
3. Relaciones con proveedores.
4. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
5. Administración de proyectos de sistemas.
6. Administración de la calidad.
7. Adquisición de tecnología.
8. Adquisición y mantenimiento de software de aplicación.

---

[8] **Circular Externa 014 del 2009**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc

9. Instalación y acreditación de sistemas.
10. Administración de cambios.
11. Administración de servicios con terceros.
12. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
13. Continuidad del negocio.
14. Seguridad de los sistemas.
15. Educación y entrenamiento de usuarios.
16. Administración de los datos.
17. Administración de instalaciones.
18. Administración de operaciones de tecnología.
19. Gestión de la Documentación.

Por tal motivo y para dar cumplimiento a la ley, las entidades bancarias cuentan con un **Sistema de Control Interno para la gestión de tecnología**, el cual está encaminado a cubrir los 19 requerimientos mencionados y a contribuir al logro de los objetivos institucionales.

En razón de lo anterior, dichos requerimientos se convirtieron en los requerimientos de TI claves para el modelo de Gobierno de TI para las entidades bancarias.

Para mayor facilidad, se identificaron los 19 requerimientos de TI seleccionados con un código, tal como se muestra en la Tabla 1.

Código	Procesos
RQ01	Plan estratégico de tecnología.
RQ02	Infraestructura de tecnología.
RQ03	Relaciones con proveedores.
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
RQ05	Administración de proyectos de sistemas.
RQ06	Administración de la calidad.
RQ07	Adquisición de tecnología.
RQ08	Adquisición y mantenimiento de software de aplicación.
RQ09	Instalación y acreditación de sistemas.
RQ10	Administración de cambios.
RQ11	Administración de servicios con terceros.
RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
RQ13	Continuidad del negocio.
RQ14	Seguridad de los sistemas.

RQ15	Educación y entrenamiento de usuarios.
RQ16	Administración de los datos.
RQ17	Administración de instalaciones.
RQ18	Administración de operaciones de tecnología.
RQ19	Gestión de la Documentación.

Tabla 1: Identificación de los 19 requerimientos de TI seleccionados

1.5.2 Selección del marco de referencia del modelo de Gobierno de TI.

Para la creación del modelo de Gobierno de TI fue necesario seleccionar un marco base de referencia y otros marcos que apoyen las estrategias de Gobierno de TI.

Después de realizar un análisis de los diferentes marcos de Gobierno de TI, se escogió el ISO 38500:2008, debido a que es una Norma Internacional que provee un estándar para que la dirección de las organizaciones evalúen, dirijan y controlen el uso de las tecnologías de la información.

Los marcos de apoyo que complementan el marco base y apoyan las estrategias de Gobierno de TI son: CobiT 4.1, CMMI-DEV, ISO 27001, ISO 27002 e ISO 9001.

1.5.3 Autoevaluación de nivel de madurez de Gobierno de TI.

Si bien es cierto el sector bancario cuenta con diferentes decretos, normas y circulares las cuales no solo regulan la actividad bancaria como tal, sino que además algunas de ellas son exclusivas para controlar y garantizar la gestión de la tecnología, ello no implica que necesariamente tengan establecido un Gobierno de TI. Por tal motivo, una autoevaluación es un buen punto de partida para que los responsables de TI de las entidades bancarias determinen un estado actual y uno deseado contra un estado ideal, dentro de la escala propuesta.

1.5.4 Modelo de Gobierno de TI propuesto

Después de determinar los requerimientos de TI, el marco base y los marcos de apoyo, se procedió a definir el modelo, el cual consistió (apoyados con CobiT) en agrupar los 19 requerimientos de TI seleccionados en los 6 principios de la Norma ISO 38500:2008. Posterior a esto, se determinó cuales actividades de los marcos de apoyo ayudarían a cumplir con los objetivos de los 6 principios de ISO 38500:2008 y finalmente se determinó una serie de indicadores de gestión que permitan evaluar el cumplimiento de las metas propuestas. (ver figura 1).

El modelo de Gobierno de TI para las Entidades Bancarias planteado en este proyecto, responde a las actividades principales definidas por la norma ISO 38500:2008 de **Evaluar** la utilización actual y futura de las TI. **Dirigir** la

preparación e implementación de los planes y políticas que aseguren que la utilización de las TI de modo que alcancen los objetivos institucionales y **Controlar** el desempeño de la tecnología de la información, a través de sistemas de medición adecuados.

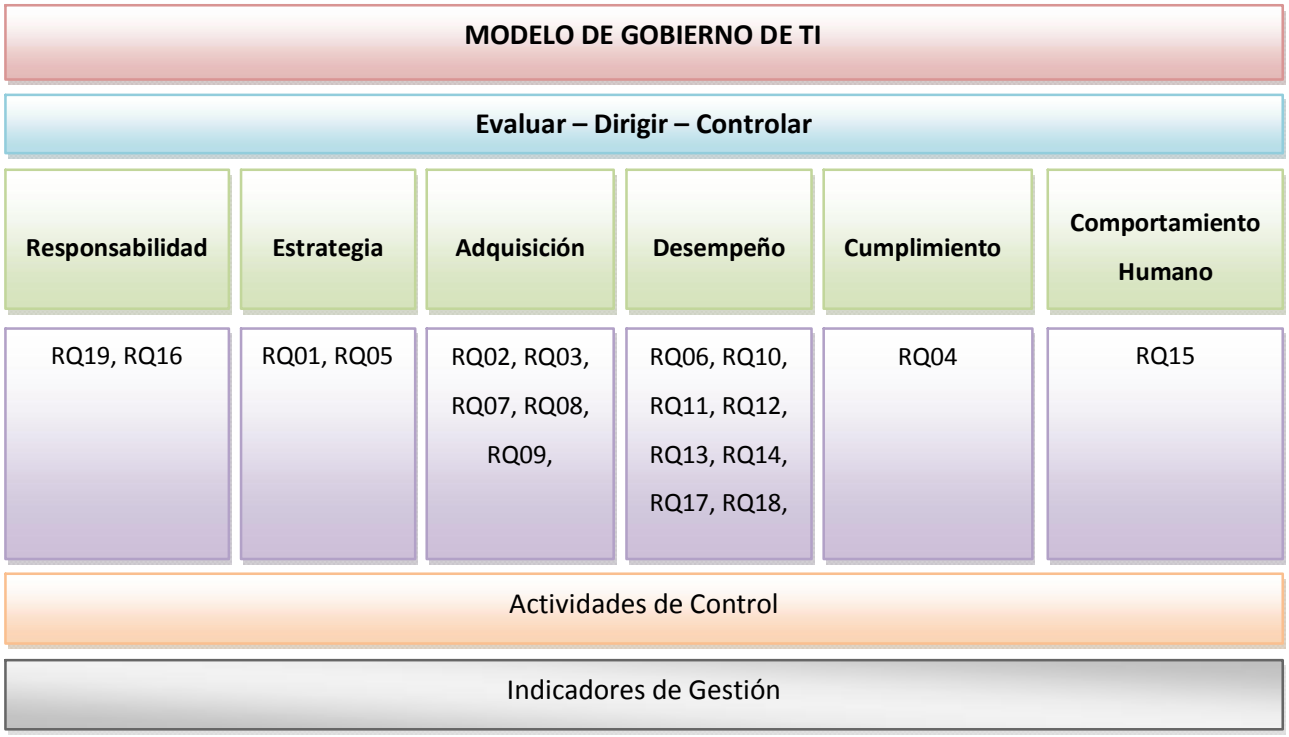


Figura 1: Modelo de Gobierno de TI Propuesto

1.5.5 Guía de Implementación del Modelo de Gobierno de TI propuesto

Con el fin de proporcionar una guía que facilite la implementación del Modelo de Gobierno de TI en las entidades bancarias de Colombia, se definieron dos actividades específicas:

1. Se documentó una guía de implementación del modelo.
2. Se documentó un ejemplo de implementación de un requerimiento de TI del modelo propuesto (ver anexo 4).

Finalmente, la base para la guía de implementación del modelo, fue la planteada por el IT Governance Institute, IT governance implementation[9].que consta de siete fases:

Fase 1: Obtener el compromiso de la alta dirección.
Fase 2: Determinar el estado actual.
Fase 3: Establecer el estado futuro deseado.
Fase 4: Identificar las brechas
Fase 5: Definir el plan de implementación
Fase 6: Desarrollar el plan de implementación
Fase 7: Monitorear y controlar el desempeño de la implementación

1.6 Resumen de Resultados Obtenidos

Los resultados más relevantes obtenidos en el desarrollo de este proyecto fueron:

- Identificación de los 19 requerimientos de TI claves para el modelo de Gobierno de TI
- Modelo de Gobierno de TI para entidades bancarias de Colombia
- Una autoevaluación de nivel de madurez de Gobierno de TI, basada en ISO 38500:2008
- Una Guía de Implementación para modelo propuesto
- Un instrumento para la validación del modelo por parte de un juicio de expertos.

Para validar la autoevaluación y conocer el estado actual de Gobierno de TI, según la escala propuesta, se pidió a 3 entidades bancarias de Colombia que la diligenciaran. El resumen de dicho resultados es el siguiente:

- Según el muestreo, el sector bancario tiene procedimientos, tareas y/o actividades, que según el modelo y la escala propuesta, ayudan al Gobierno de TI
- Se evidencia también que tienen interés de crecer a un nivel superior del actual, en todas las aristas del modelo propuesto.

[9] **IT governance implementation guide using COBIT and Val IT**. IT Governance Institute

- Se observa además, que si bien es cierto tienen expectativa de avanzar a un nivel superior, por ahora no consideran la posibilidad de estar en el nivel ideal, dentro de la escala propuesta

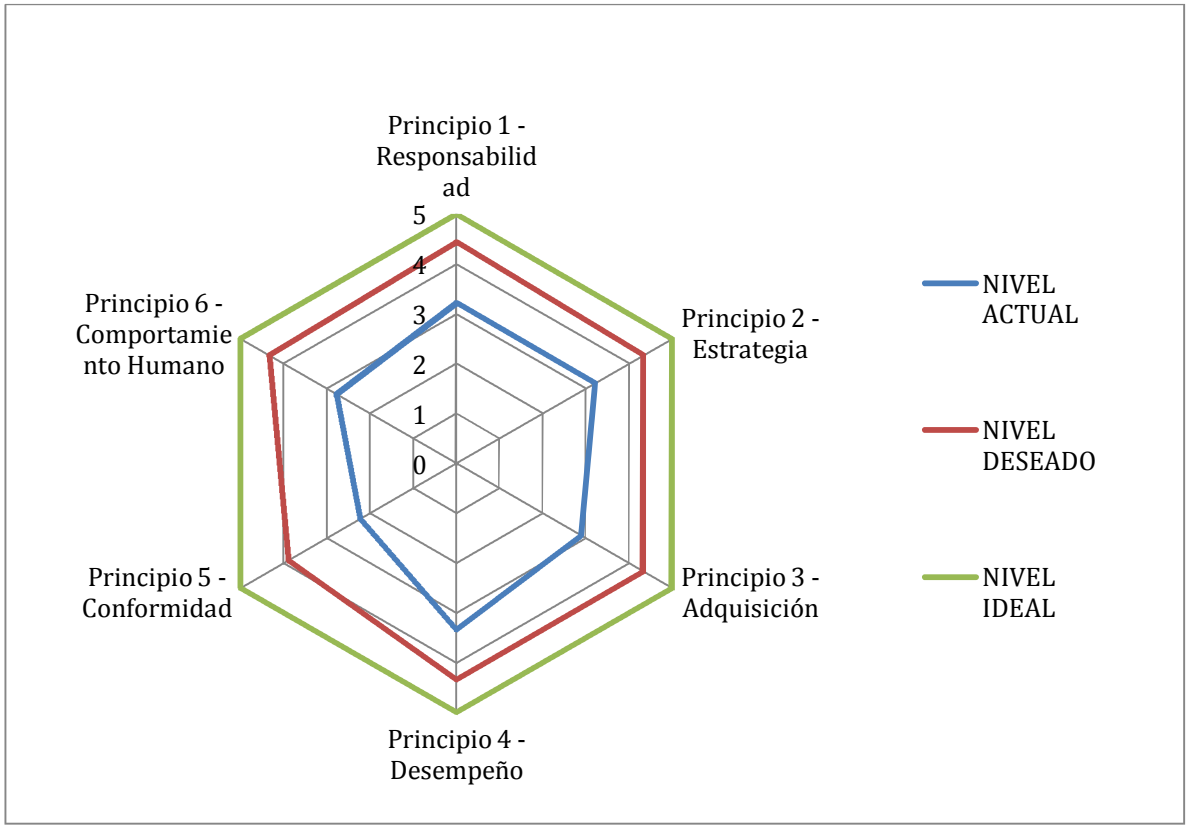


Figura 2: Promedio de nivel de madurez de 3 Entidades Bancarias de Colombia, según el modelo propuesto

Respecto al juicio de expertos y tomando como base la pregunta "*Considerando de forma global el resumen ejecutivo enviado, usted considera viable o inviable la implementación del modelo propuesto de Gobierno de TI para entidades bancarias de Colombia*" el resultado fue el siguiente:

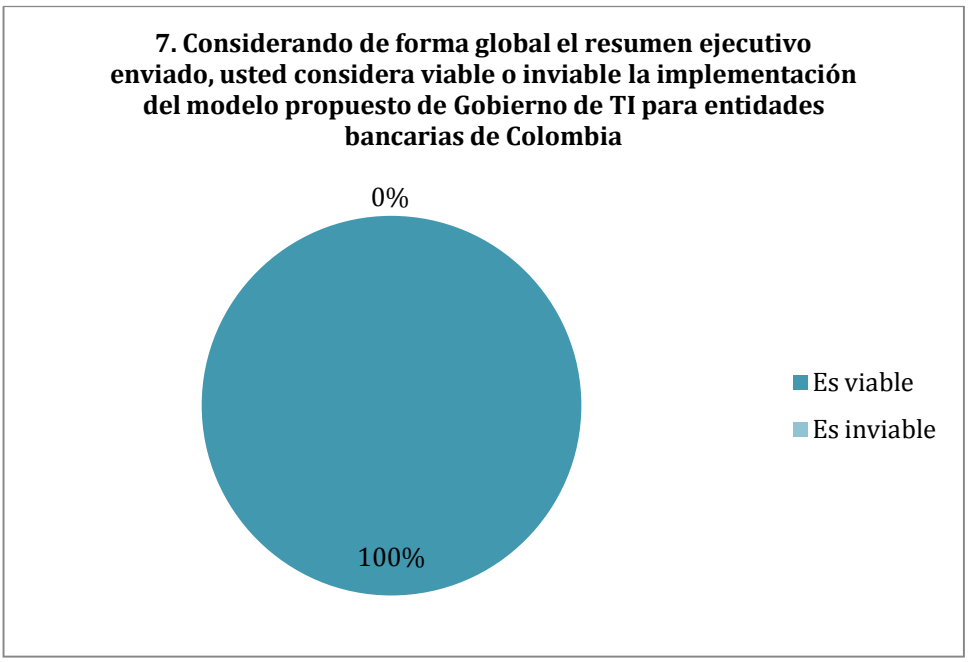


Figura 3: Resultado del juicio de expertos

Los resultados y el análisis más detallado se encuentran en el capítulo 9

1.7 Organización del Documento

Capítulo 1 **Introducción**	• Se establece el contexto del trabajo, el planteamiento del problema, los objetivos, el resumen del modelo propuesto y el resumen de los resultados obtenidos.
Capítulo 2 **Modelos de Gobierno y Gestión de TI**	• Se presenta el marco teórico, en el cual se incluyen diferentes modelos, marcos y normas iso pertinentes para la elaboración de este documento.
Capítulo 3. **Contexto del sector Bancario Colombiano**	• En este capítulo se define que son establecimientos bancarios y se presenta una actualidad del sector bancario colombiano. Además se presentan las entidades de supervisión y leyes que rigen a este sector.
Capítulo 4 **Autoevaluación de Gobierno de TI**	• Esta sección hace referencia a la forma como fue creada la autoevaluación de Gobierno de TI propuesta para el sector.
Capítulo 5 **Modelo Propuesto**	• En este capítulo se detalla el modelo de Gobierno de Ti para entidades bancarias en Colombia propuesto
Capitulo 6 **Modelo de Gobierno de TI para Entidades Bancarias de Colombia**	• Este capítulo está destinado exclusivamente para el Modelo de Gobierno de TI propuesto. En este capítulo se encuetran los principios, las actividades de control y los indicadores de gestión
Capítulo 7 **Guía de Implementación**	• En esta sección se presenta la guía para la implmentación del Modelo de Gobierno de TI propuesto
Capítulo 8 **Validación de la Propuesta**	• En este capítulo se aborda la metodología implementada para la validación del modelo propuesto, por parte de un grupo de expertos
Capítulo 9 **Resultados Obtenidos**	• Este capítulo contiene los resultados obtenidos con el presente trabajo, además de los resultados de la evaluación del modelo por parte del juicio de expertos
Capítulo 10 **Conclusiones y Futuro Trabajo**	• Esta sección contiene las conclusiones del modelo de gobierno de TI propuesto y el trabajo futuro que debería seguir

2. MODELOS DE GOBIERNO Y GESTIÓN DE TI

2.1 ISO 38500:2008

Antecedentes

Gobierno de las TIC (IT governance) ya tiene una norma ISO asociada, la ISO/IEC 38500:2008 “Corporate governance of information technology” que viene a complementar el conjunto de estándares ISO que afectan a los sistemas y tecnologías de la información (ISO/IEC 27000, ISO/IEC 20000, ISO/IEC 15504, ISO/IEC 24762, etc.). Esta nueva norma fija los estándares para un buen gobierno de los procesos y decisiones empresariales relacionadas con los servicios de información y comunicación que, suelen estar gestionados tanto por especialistas en TIC internos o ubicados en otras unidades de negocio de la organización, como por proveedores de servicios externos. En esencia, todo lo que esta norma propone puede resumirse en tres propósitos fundamentales:

- 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.

- Informar y orientar a los directores que controlan el uso de las TIC en su organización.

- Proporcionar una base para la evaluación objetiva por parte de la alta dirección en el gobierno de las TIC.

La norma ISO/IEC 38500:2008 se publicó en junio de 2008 con base en la norma australiana AS8015:2005. Es la primera de una serie sobre normas de gobierno de TIC. Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorizar el uso de las tecnologías de la información y comunicaciones (TICs). Está alineada con los principios de gobierno corporativo recogidos en el “Informe Cadbury” y en los “Principios de Gobierno Corporativo de la OCDE”

Definiciones

La norma incluye 19 definiciones de términos, entre los que se pueden destacar los siguientes:

Principios

La norma define seis principios de un buen gobierno corporativo de TIC:

1. Responsabilidad

Todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de TI. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.

2. Estrategia
La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TIC. Los planes estratégicos de TIC satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.

3. Adquisición
Las adquisiciones de TI se hacen por razones válidas, en base a un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.

4. Desempeño
La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.

5 Cumplimiento
La función de TI cumple todas las al respecto están claramente definidas, implementadas y exigidas.

6. Comportamiento humano
Las políticas de TIC, prácticas y decisiones demuestran respeto al factor humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

Modelo
La dirección ha de gobernar la TIC mediante tres tareas principales

Evaluar
Examinar y juzgar el uso actual y futuro 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.

Controlar

Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado.[10]

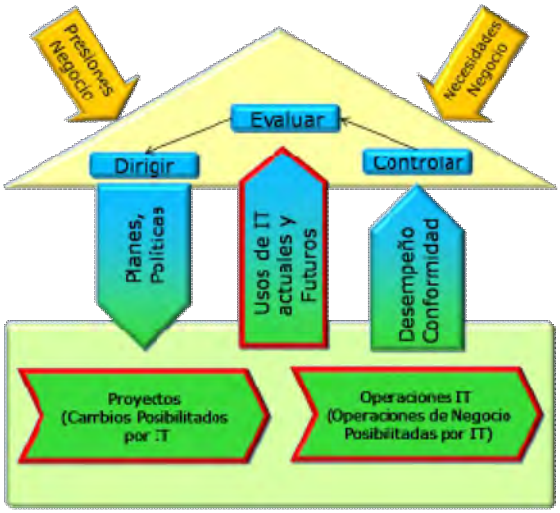


Figura 4: Modelo ISO 38500 para el gobierno de TI

2.2 COBIT 4.1

Es un producto de ISACA. Su objetivo es servir de marco de referencia para establecer un esquema de control sobre los procedimientos de gestión. COBIT ayuda a las organizaciones a reducir los riesgos de TI y aumentar el valor obtenido de las tecnologías de la información. Es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders).

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas.
Áreas de enfoque:

1. Alineamiento Estratégico.
2. Entrega de valor.
3. Manejo de riesgos.
4. Gestión de recursos.
5. Control y monitorización. Medición de rendimiento.

[10] **Gobierno de las TIC ISO/IEC 38500. The ISACA** Journal Online published by ISACA. Manuel Ballester, Ph.D.,CIS A, CIS M, CGEIT , IEEE. http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/jpdf1001-online-gobierno.pdf

2.3 CMMI DEV 1.3

Es un modelo de procesos que contiene las mejores prácticas de la industria para el desarrollo, mantenimiento, adquisición y operación de productos y servicios. Es un Modelo de Madurez de Capacidades Integrado, desarrollado por el SEI (Software Engineering Institute). Mide la madurez del desarrollo del software en una escala del 1 al 5. Describe formas efectivas y probadas de hacer las cosas, no es un enfoque radical.

La versión actual de CMMI es la versión 1.3 la cual corresponde a CMMI-SVC, liberada el 1 de noviembre de 2010. Hay tres constelaciones de CMMI:

CMMI para el Desarrollo (CMMI-DEV o CMMI for Development), En él se tratan procesos de desarrollo de productos y servicios.

CMMI para la adquisición (CMMI-ACQ o CMMI for Acquisition), En él se tratan la gestión de la cadena de suministro, adquisición y contratación externa en los procesos del gobierno y la industria.

CMMI para servicios (CMMI-SVC o CMMI for Services), está diseñado para cubrir todas las actividades que requieren gestionar, establecer y entregar Servicios.

2.4 ISO 9001:2008

Fue elaborada por la Organización Internacional para la Estandarización, y especifica los requisitos para un sistema de gestión de la calidad que pueden utilizarse para su aplicación interna por las organizaciones, para certificación o con fines contractuales. Esta norma aplica el ciclo de mejoramiento continuo de Deming "PDCA": acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Está estructurada en cuatro grandes bloques, completamente lógicos, y esto significa que con el modelo de sistema de gestión de calidad basado en ISO se puede desarrollar en su seno cualquier actividad

2.5 ISO 9004:2009

Esta norma internacional proporciona orientación para ayudar a conseguir el éxito sostenido para cualquier organización en un entorno complejo, exigente y en constante cambio, mediante un enfoque de gestión de la calidad.

La norma ISO 9004:2009 promueve la autoevaluación como una herramienta importante para la revisión del nivel de madurez de la organización

El Anexo A:

Es una herramienta para que la organización autoevalúe sus fortalezas y debilidades, para determinar su nivel de madurez y para identificar las oportunidades de mejora e innovación.

2.6 ISO 27001:2006

Es un estándar de seguridad publicado por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

2.7 ISO 27001:2006

Es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.

2.8 Modelo de Madurez de CobiT

El modelo de madurez de CobiT se basa en un método de evaluación de la organización, de tal forma que pueda valorarse a sí misma desde un nivel de no existente (0) hasta un nivel optimizado (5).
Los niveles de madurez están diseñados como perfiles de procesos de TI, donde la organización determina estados actuales y futuros. No están diseñados para ser usados como un modelo limitante, es decir, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.

El modelo de madurez de CobiT, a diferencia del CMMI, no tiene la intención de medir los niveles de forma precisa; es decir, que el objetivo no es probar que un nivel se ha conseguido con exactitud, para conseguir una certificación de cumplimiento de dicho nivel.

Las evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor en cada una de las afirmaciones individuales de las descripciones.

La ventaja de este modelo de nivel de madurez, es que es fácil para la organización ubicarse a sí misma en la escala y evaluar qué se debe hacer si se quiere avanzar hacia otro nivel superior.

La escala del modelo de madurez de CobiT se encuentra establecida entre niveles 0 y el 5 y se basa en una escala de madurez simple, donde se muestra como un proceso evoluciona desde una capacidad no existente (0) hasta una capacidad optimizada (5). (ver figura 5)

Figura 5: Modelo de Madurez de CobiT

2.9 Modelo de Madurez de CMMI

El nivel de madurez de CMMI es una plataforma evolutiva definida para la mejora de procesos de la organización, es decir, que para poder alcanzar un nivel, se debe haber cumplido con la totalidad de los requerimientos de los niveles predecesores.

Cada nivel de madurez desarrolla un subconjunto importante de procesos de la organización, preparándola para pasar al siguiente nivel de madurez.

Los niveles de madurez se miden mediante el logro de las metas específicas y genéricas asociadas con cada conjunto predefinido de áreas de procesos.

En CMM se establecen cinco niveles de madurez denominados por los números del 1 al 5 (ver figura 6)

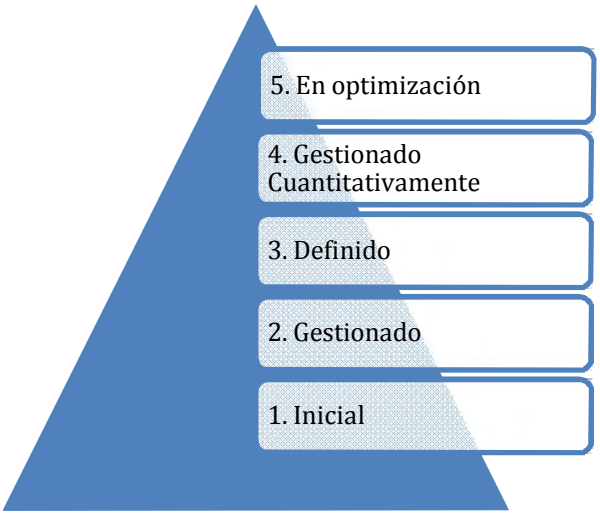


Figura 6: Niveles de madurez de CMMI

2.10 Modelo de Madurez ISO 9004:2009

Esta norma internacional proporciona orientación para ayudar a conseguir el éxito sostenido para cualquier organización en un entorno complejo, exigente y en constante cambio, mediante un enfoque de gestión de la calidad.

La norma ISO 9004:2009 promueve la autoevaluación como una herramienta importante para la revisión del nivel de madurez de la organización

La norma está compuesta por 3 anexos:

El Anexo A:

Es una herramienta para que la organización autoevalúe sus fortalezas y debilidades, para determinar su nivel de madurez y para identificar las oportunidades de mejora e innovación.

El Anexo B:

Proporciona una descripción de los principios de la gestión de la calidad que son la base de las normas sobre gestión de la calidad.

El Anexo C:

Muestra la correspondencia capítulo a capítulo entre la norma ISO 9004:2009 y la norma ISO 9001:2008

Con relación a la autoevaluación, la norma ISO 9004:2009 en su numeral 8.3.4, tiene un apartado para la autoevaluación, que la define como una revisión

exhaustiva y sistemática de las actividades de la organización y de su desempeño en relación con su grado de madurez. La autoevaluación puede ayudar a la organización a priorizar, planificar e implementar mejoras y/o innovaciones, cuando sea necesario.

En cuanto al modelo de madurez, la Norma ISO 9004:2009 define que una organización madura tiene un desempeño eficaz y eficiente y logra el éxito sostenido si logra:

- Comprender y satisfacer las necesidades y expectativas de las partes interesadas
- Realizar el seguimiento de los cambios en el entorno de la organización
- Identificar posibles áreas de mejora e innovación
- Definir y desplegar estrategias y políticas
- Establecer y desplegar objetivos pertinentes
- Gestionar sus procesos y sus recursos
- Demostrar confianza en las personas, guiándoles hacia una motivación, un compromiso y una participación mayores
- Establecer relaciones mutuamente beneficiosas con los proveedores y otros aliados.

2.11 Comparación de los modelos de niveles de madurez de CobiT, CMMI e ISO 9004

MODELOS	COMPARACION DE NIVELES DE MADUREZ					
	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
CobiT 4.1	No Existente	Inicial	Repetible	Definido	Administrado	Optimizado
CMMI-DEV	-	Inicial	Gestionado	Definido	Gestionado cuantitativamente	En Optimización
ISO 9004	-	Nivel Base				Mejor Práctica

Tabla 2: Comparación por niveles de los modelos de madurez

MODELOS	Permite avanzar sin cumplir un nivel anterior
CobiT 4.1	Si
CMMI-DEV	No
ISO 9004	No

Tabla 3: Comparación por avance entre niveles de los modelos de madurez

3. CONTEXTO DEL SECTOR BANCARIO COLOMBIANO

3.1 Establecimientos Bancarios

Son establecimientos bancarios las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito.

Banco comercial: Las palabras banco comercial significan un establecimiento que hace el negocio de recibir fondos de otros en depósito general y de usar éstos, junto con su propio capital, para prestarlo y comprar o descontar pagarés, giros o letras de cambio.

Banco hipotecario: Las palabras banco hipotecario significan un establecimiento que hace el negocio de prestar dinero garantizado con propiedades raíces, que debe cubrirse por medio de pagos periódicos y para emitir cédulas de inversión.[11]

3.2 Actualidad Bancaria

En Colombia, la industria bancaria se está transformando. La entrada de bancos latinoamericanos al mercado colombiano, la conversión de instituciones financieras locales no bancarias en establecimientos bancarios y la expansión de bancos locales hacia otros países de la región son hechos que demuestran el cambio de estructura del sector. Estos movimientos se explican en parte por las sólidas condiciones macroeconómicas, la baja profundización financiera y el mayor poder adquisitivo de la población.

A pesar de que la banca colombiana es diversa y universal, en cuanto a la cantidad y calidad de productos y servicios que se ofrecen en el mercado de crédito y captación, el segmento corporativo ha predominado. No obstante, en los últimos años el sector ha atendido más a la banca personal, situación que se evidencia tanto por el interés de la industria en implementar diferentes canales de prestación de servicio hacia personas, como por el ingreso de bancos pequeños en nichos enfocados en la modalidad de consumo. Al mismo tiempo que el segmento de microcrédito también se ha fortalecido con la incursión de nuevas entidades.

El sistema bancario ha tenido varios tipos de organización en las últimas décadas. En el período previo a la crisis doméstica de finales de los noventa (1998-2001), se observó una serie de fusiones que permitieron extender los negocios bancarios

---

[11] **Decreto 633 de 1993**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

ya vigentes hacia otras regiones y sectores de la población. En contraste, en la década pasada (2002-2006), se presentaron operaciones orientadas a la adquisición de entidades que proporcionaran nuevas sinergias a través de la diversificación de productos y servicios financieros.[12]

Recientemente, los establecimientos bancarios parecen estar viviendo un nuevo proceso de organización, pero en esta ocasión en un ambiente más regional (latinoamericano). Esta nueva dinámica se ha caracterizado por presentar dos tendencias. Por una parte, la expansión de los bancos locales hacia otros países de la región, y, por otra, la entrada de bancos latinoamericanos al mercado colombiano. También se está observando un incremento en el número de bancos locales producto de la transformación de entidades financieras no bancarias en establecimientos bancarios.

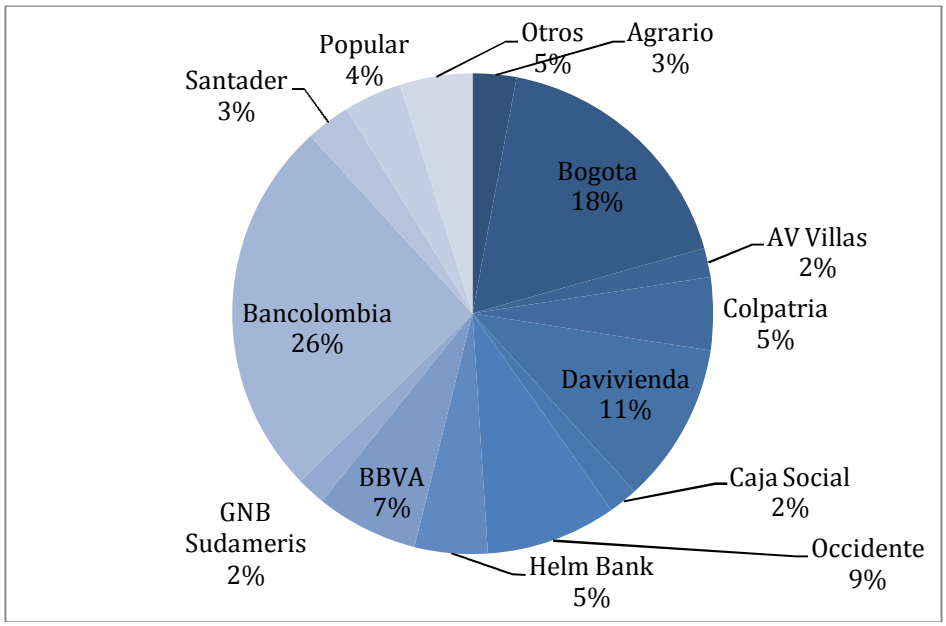
Aunque la banca colombiana es diversa, el segmento corporativo ha predominado. Sin embargo, en los últimos años el sector ha atendido más a la banca personal, situación que se evidencia tanto por el interés de la industria en implementar diferentes canales de prestación de servicio hacia personas, como por el ingreso de bancos pequeños en nichos enfocados en las modalidades de consumo y microcrédito.

A diciembre de 2011, el total de activos del sistema bancario ascendió a $302 billones (incluidas las titularizaciones), de los cuales $200 bn (66%) son cartera bruta y $58 bn (19%) son inversiones. Recientemente esta relación entre cartera e inversiones se ha mantenido estable, contrario a lo sucedido en el periodo post-crisis de los años noventa, durante el cual se presentó una sustitución de cartera por títulos valores.

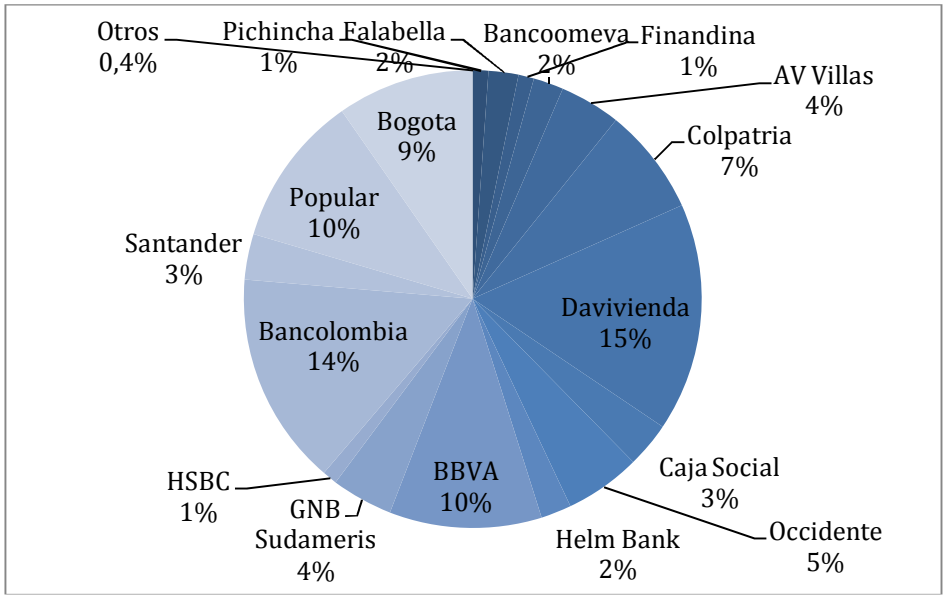
A diciembre de 2011, la cartera comercial es la más representativa del sistema con aproximadamente el 58% ($120 billones) del total de la cartera, seguida por consumo con el 27% ($56 billones), vivienda con el 12% ($24,5 billones) y microcrédito con el 3% ($5,5 billones).3 La cartera de consumo y comercial son las modalidades en las que participan la mayoría de las instituciones. Mientras que las modalidades de microcrédito y vivienda tienen una participación limitada. (ver figura 7).

[12] **Fusiones y Adquisiciones en el Sector Financiero Colombiano: Análisis y Propuestas sobre la Consolidación Bancaria**. Ministerio de Hacienda de Colombia. http://www.minhacienda.gov.co/portal/page/portal/HomeMinhacienda/regulacionfinanciera/Presentaciones/Presentaciones/7_ANIF-MULTIBAN-FINAL0606.pdf

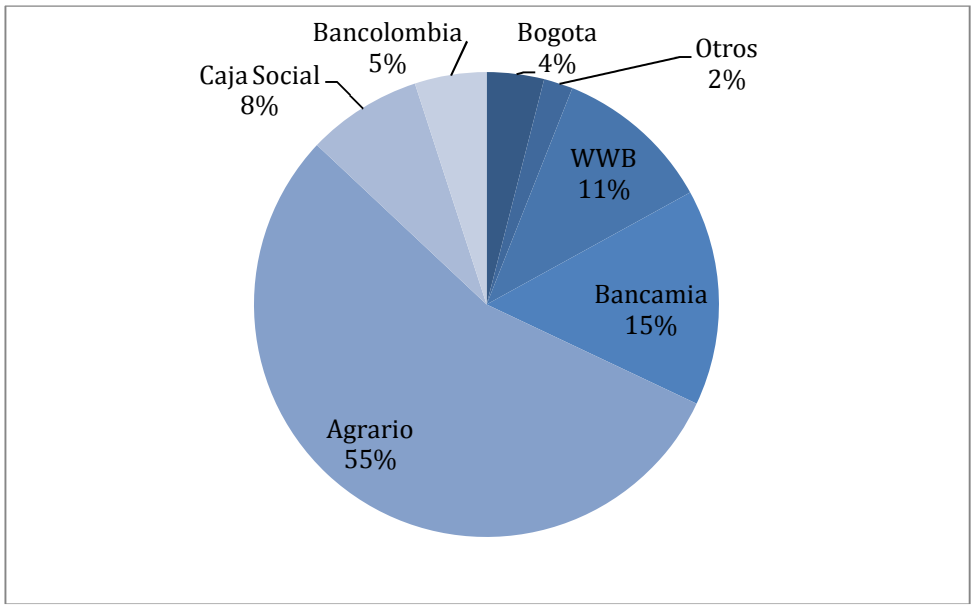
Cartera Comercial



Cartera de Consumo



Cartera de Microcredito



Cartera de Vivienda

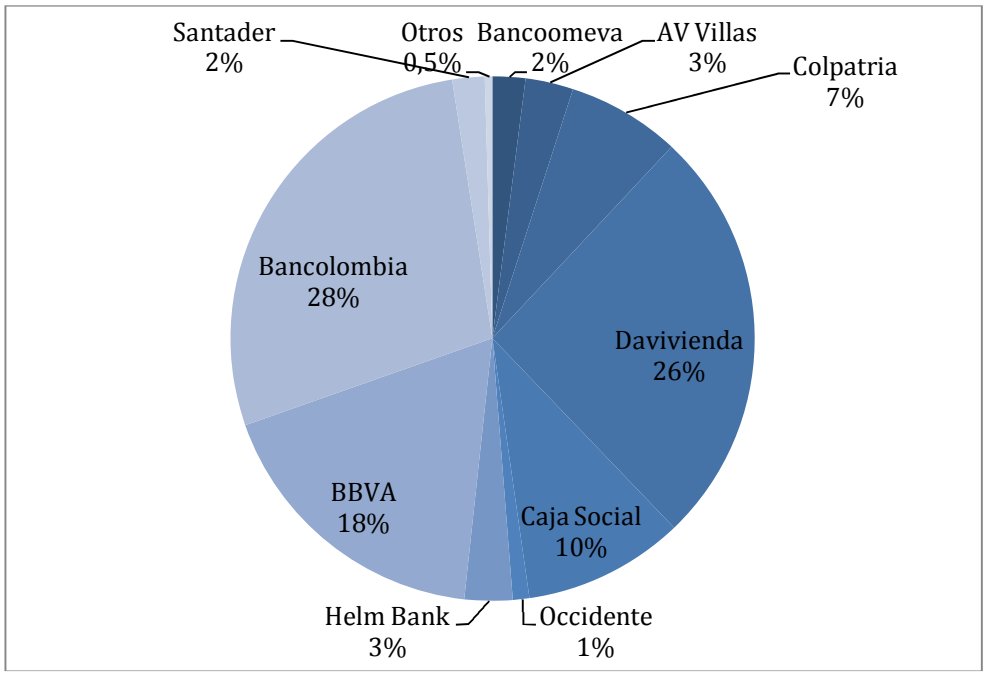


Figura 7: Distribución de carteras por Bancos

Por su importancia relativa en el sistema, Bancolombia, Bogotá, Davivienda y Occidente son los bancos con mayor participación en la cartera comercial, concentrando alrededor del 65% del total. En cuanto a la distribución de esta modalidad en sectores económicos, se tiene que la mayor parte está colocada en el campo de servicios (40%), industria (19%), comercio (18%), construcción (8%), gobierno (6%), agricultura (6%) y otros (4%). Para el mercado de servicios, las entidades que tienen la mayor proporción de su cartera en este rubro son Bancoomeva y Pichincha, con el 67% y 55%, respectivamente. En el caso del sector industrial, HSBC presenta la mayor concentración con el 31% de sus créditos. En cuanto al segmento de comercio, Citibank y Bancamía tienen un volumen considerable de la cartera, alcanzando un 50% y 43%, respectivamente. Por su parte, el Banco Agrario es la entidad que presenta la mayor concentración de su cartera en el sector agrícola con un 38%.
En el caso de la cartera de consumo, las entidades con la mayor participación son Davivienda, Bancolombia, BBVA, Popular, Bogotá, Citi y Colpatria, quienes concentran el 71% de esta cartera en el sistema bancario. El portafolio de consumo se ha concentrando principalmente en los segmentos de libranza, libre inversión y tarjetas de crédito con participaciones del 32%, 24% y 22% respectivamente. El 22% restante de la cartera de consumo corresponde a vehículos, crédito rotativo y otros.

En relación con la cartera de vivienda, Bancolombia, Davivienda, BBVA, Banco Caja Social y Colpatria concentran el 88% la cartera. Esta modalidad se divide en tres partes: vivienda propia con el 63%, leasing habitacional con el 12% y el 25% restante son créditos que se ha titularizado.

La modalidad de microcrédito está conformada principalmente por Banco Agrario, especializado en créditos destinados a pequeños productores agropecuarios, y Bancamía, WWB y Banco Caja Social, cuya cartera corresponde al 89% del sector. Este segmento presenta dos tramos: créditos menores de 25 SMMLV, con una participación del 90% en la cartera del sector, y créditos entre 25 y 120 SMMLV, con el 10% restante. Vale la pena destacar que el incremento en las tasas de interés de colocación, producto del cambio metodológico en el proceso de certificación del interés bancario corriente de esta modalidad, ha permitido que recientemente se incremente significativamente el tamaño de esta cartera.

3.3 Presencia Geográfica

Las entidades bancarias tienen presencia a lo largo de todo el territorio nacional. En 2011 el número de oficinas se incrementó en 403, de las cuales 266 fueron colocadas por los nuevos bancos, alcanzando 4.921 oficinas en todo el país. A nivel de entidad, Bancoomeva ingresó en 25 departamentos con 89 oficinas, Falabella en 14 departamentos con 36 oficinas, Finandina en 8 departamentos con 11 oficinas, Pichincha en 14 departamentos con 29 oficinas y el Banco de la Mujer

(WWB) en 24 departamentos con 101 oficinas. La región andina, una de las más activas económicamente, tiene la mayor concentración de oficinas bancarias. (ver figura 8)

Figura 8: Presencia geográfica de las entidades bancarias

3.4 Expansión de la banca

En 2011, la banca vivió un proceso de expansión en el mercado doméstico con la transformación de cinco entidades financieras en establecimientos bancarios. De esta manera, el sector quedó integrado por 23 bancos, lo que representa una mayor profundización y mayores beneficios para los clientes financieros. En especial, la cartera de consumo se expandió con la llegada de los bancos especializados en este ramo, a saber Bancoomeva, Finandina, Falabella y Pichincha. De igual forma, la cartera de microcrédito contó con la incursión del Banco de la Mujer (WWB), el cual contribuyó a fortalecer esa modalidad.

En línea con esta dinámica, las compañías de financiamiento Serfinansa, Macrofinanciera y Finamérica, enfocadas en el segmento de microcrédito y crédito de consumo, recientemente han anunciado su intención de convertirse en bancos al igual que la cooperativa Coopcentral.

El sector bancario también ha venido fortaleciendo su presencia en los mercados externos, principalmente en Latinoamérica. En 2007, Bancolombia adquirió la operación del Banco Agrícola en el Salvador por US$900 millones, seguido por el Banco de Bogotá en 2010, quien adquirió la operación del BAC Credomatic en Centroamérica por US$1.900 millones. Por su parte, en el primer semestre de 2012, Davivienda compró la operación del HSBC en Costa Rica, Honduras y El Salvador por US$801 millones y GNB Sudameris obtuvo la operación del HSBC en Colombia, Paraguay, Uruguay y Perú por cerca de US$400 millones.

Algunas entidades extranjeras también están poniendo sus ojos en el mercado colombiano. En lo corrido de 2012, Corpbanca de Chile adquirió el Banco Santander Colombia y el Scotiabank de Canadá se hizo a una importante participación accionaria en Colpatria, uno de los mayores distribuidores de tarjetas de crédito. Existen también bancos extranjeros que buscan ingresar al mercado local mediante la conformación de nuevas entidades. Por ejemplo, Itaú BBA ingresó al país a través de una corporación financiera propia, y el Banco Azteca está evaluando la incursión al mercado colombiano como banco.

Estos movimientos en la banca colombiana se explican en parte por los márgenes de rentabilidad, el limitado grado de penetración financiera y una población con un ingreso creciente. En este sentido, esperamos que esta dinámica le permita a la industria bancaria seguir avanzando en su grado de competitividad e incrementar su portafolio de productos y servicios financieros.[13]

---

[13] **Articulo: ¿Qué tipo de Banca tenemos?** Asobancaria.
http://www.asobancaria.com/portal/pls/portal/docs/1/2928048.PDF

3.5 Entidades de supervisión

Nuestro sistema financiero está conformado por las instituciones financieras y las autoridades de intervención. Las primeras captan y manejan dineros del público con la autorización del Estado. Estas entidades ofrecen una amplia gama de productos de ahorro que se ajustan a distintos requerimientos y necesidades de las personas. Para garantizar el buen funcionamiento del mercado en general, las autoridades de intervención se encargan de aportar transparencia al sistema financiero y, por lo tanto, confianza y seguridad a los ahorradores, inversionistas y deudores. Es importante saber que todas las entidades que hacen parte del sistema financiero están sujetas a la regulación y supervisión por parte de las autoridades de intervención: el Congreso de la República, el Ministerio de Hacienda y Crédito Público y la Superintendencia Financiera (ver figura 9), están encargadas de crear los marcos normativos de los demás agentes del sistema y de velar porque los recursos de las personas, empresas y el gobierno se encuentren seguros en manos de las diferentes instituciones. La Superintendencia Financiera también tiene funciones de inspección, vigilancia y control sobre las entidades. Entre las funciones del Banco de la República se encuentra el ser prestamista de última instancia y banquero de los establecimientos de crédito, en caso de que éstos tengan necesidades transitorias de liquidez. Por su parte, el Fondo de Garantías de Instituciones Financieras (Fogafin) es el asegurador de depósitos del sistema con el fin de proteger la confianza de quienes tienen productos en las instituciones financieras inscritas.[14]

Figura 9: Entidades de Supervisión

[14] **Información al consumidor financiero**. Asobancaria. www.asobancaria.com/portal/page/portal/Asobancaria/info_consumidor/sistema_financiero_y_banca/

3.5.1 La Superintendencia Financiera

La Superintendencia Financiera de Colombia surgió de la fusión de la Superintendencia Bancaria de Colombia en la Superintendencia de Valores, según lo establecido en el artículo 1 del Decreto 4327 de 2005. La entidad es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio

Misión: Preservar la confianza pública y la estabilidad del sistema financiero; mantener la integridad, la eficiencia y la transparencia del mercado de valores y demás activos financieros; y velar por el respeto a los derechos de los consumidores financieros y la debida prestación del servicio.

Funciones Generales: La Superintendencia Financiera de Colombia ejercerá las funciones establecidas en el decreto 2739 de 1991 y demás normas que la modifiquen o adicionen, el Decreto 663 de 1993 y demás normas que lo modifiquen o adicionen, la Ley 964 de 2005 y demás normas que la modifiquen o adicionen, las demás que señalen las normas vigentes y las que le delegue el Presidente de la República.[15]

Actualmente, la Superintendencia Financiera regula 23 entidades bancarías:

No	Nombre	Representante Legal		Cargo	Página Web
1	Banco de Bogotá	Alejandro Augusto	Figueroa Jaramillo	Presidente	www.bancodebogota.com
2	Banco Popular	José Hernán	Rincón Gómez	Presidente	www.bancopopular.com.co
3	Banco Santander	Jaime Francisco	Munita Valdivieso	Presidente	www.bancosantander.com.co
4	Bancolombia	Carlos Raúl	Yepes Jiménez	Presidente	www.bancolombia.com.co
5	Scotiabank	Héctor Guillermo	Quiñones Gutiérrez	Presidente	www.scotiabank.com.co
6	Citibank	Bernardo	Noreña Ocampo	Presidente	www.citibank.com.co
7	HSBC Colombia	Hans Juergen	Theilkuhl Ochoa	Presidente	www.banistmo.com.co

[15] **Nuestra Superintendencia.** Superintendencia Financiera de Colombia. www.superfinanciera.gov.co

8	Banco GNB Sudameris	Camilo	Verastegui Carvajal	Presidente	www.sudameris.com.co
9	BBVA Colombia	Oscar	Cabrera Izquierdo	Presidente Ejecutivo	www.bbvaganadero.com
10	Helm Bank	María Carmiña	Ferro Iriarte	Presidente	www.bancaext@bancodecredito.com.co
11	Banco de Occidente	Efraín	Otero Álvarez	Presidente	www.bancodeoccidente.com.co
12	BCSC	Diego Fernando	Prieto Rivera	Presidente	www.bancocajasocial.com.co
13	Davivienda	Efraín Enrique	Forero Fonseca	Presidente	www.davivienda.com
14	Colpatria Red Multibanca	Luis Santiago	Perdomo Maldonado	Presidente	www.colpatria.com
15	Banagrario	Francisco de Paula	Estupiñán Heredia	Presidente	www.bancoagrario.gov.co
16	AV Villas	Juan Camilo	Ángel Mejía	Presidente	www.avvillas.com.co
17	Procredit	Manuel Salvador	Buriticá López	Gerente General	www.bancoprocredit.com.co
18	Bancamía	Mercedes	Gómez Restrepo	Presidente	www.bancamia.com.co
19	WWB	José Alejandro	Guerrero Becerra	Presidente	www.bancowwb.com
20	Bancoomeva	José Miguel	Terreros Ospina	Presidente	www.bancoomeva.com
21	Finandina	Orlando	Forero Gómez	Gerente General	www.finandina.com
22	Banco Falabella	Jorge Alberto	Villarroel Barrera	Gerente General	www.falabella.com.co
23	Banco Pichincha	Marcel Daniel Eduardo	Fernández-Salvador Chauvet	Presidente	www.bancopichincha.com.co

Tabla 4: Listado general de entidades vigiladas por la Superintendencia Financiera [16]

[16] **Listado general de entidades vigiladas por la Superintendencia Financiera (Agosto 2012).** Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/EntidadesSupervisadas/entidades_general.xls

3.6 Legislación colombiana que rigen el sector bancario y que aportan al modelo propuesto

3.6.1 Decreto 633 de 1993

Este decreto presenta una descripción básica de las entidades sometidas a la vigilancia de la superintendencia bancaria y regula la estructura del sistema financiero.

Determina que los establecimientos bancarios son las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito.

Determina que el sistema financiero y asegurador se encuentra conformado de la siguiente manera:

a. Establecimientos de crédito.
b. Sociedades de servicios financieros.
c. Sociedades de capitalización.
d. Entidades aseguradoras.
e. Intermediarios de seguros y reaseguros

3.6.2 Circular Externa 014 del 2009

Determina que todas las entidades supervisadas, ya sean matrices o subordinadas, deberán implementar o ajustar su Sistema de Control Interno SCI a los requisitos mínimos establecidos en esta circular, en forma tal que el mismo resulte acorde con el tamaño de la organización (en términos de número de empleados, valor de los activos e ingresos, recursos captados del público, número de sucursales o agencias, entre otros.) y la naturaleza de las actividades propias de su objeto social, así como de las desarrolladas por cuenta de terceros, teniendo en cuenta la relación beneficio/costo.

3.6.3 Circular Externa 038 de 2009

Realiza unas modificaciones al numeral 7º del Capítulo IX, Título Primero - Control Interno - de la Circular Externa 014 del 2009, con el propósito de facilitar la

adecuada aplicación de las disposiciones contenidas en dicha circular expedida por la Superintendencia Financiera de Colombia [17]

3.6.4 Circular Externa 052 de 2007

Determina requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios, las cuales deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Súper Financiera de Colombia.[18]

[17] **Circular externa 038 de 2009.** Superintendencia Financiera de Colombia. www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce038_09.doc

[18] **Circular externa 052 de 2007.** Superintendencia Financiera de Colombia. www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf

4. AUTOEVALUACION DE GOBIERNO DE TI

Si bien es cierto el sector bancario cuenta con diferentes decretos, normas y circulares como las definidas anteriormente, las cuales no solo regulan la actividad bancaria como tal, sino que además algunas de ellas son exclusivas para controlar y garantizar la gestión de la tecnología (circular externa 014 de 2009), ello no implica que necesariamente tengan establecido un Gobierno de TI. Por tal motivo, una autoevaluación es un buen punto de partida para que los responsables de TI de las entidades bancarias determinen un estado actual y uno deseado contra un estado ideal, dentro de la escala propuesta.

Como punto de partida para la definición y posterior implementación de Gobierno de TI en el sector bancario colombiano, se hace pertinente realizar dos actividades:

1. **Autoevaluación de nivel de madurez de Gobierno de TI**: Esta autoevaluación tiene por objetivo que los responsables de TI de los bancos se realicen un autodiagnóstico para determinar en qué grado de nivel de madurez de Gobierno de TI se encuentran con respecto a la escala propuesta. Así mismo, se establece en qué nivel desean estar. Al ser una autoevaluación, se presume que los encargados de TI la responden de forma correcta y verídica.

2. **Comparación de procesos de TI**: Para el modelo de gobierno de TI en las entidades bancarias de Colombia, se parte de los 19 requerimientos de TI que la circular externa 014 de 2009 obliga a los bancos a cumplir. Aun así, se realizó una comparación entre dichos requerimientos y los procesos de TI del Banco de Occidente, a partir de su respectivo mapa de procesos y sus planes estratégicos de tecnología (ver Anexo 7).

4.1 Autoevaluación de nivel de madurez de Gobierno de TI

Un modelo de madurez es una forma de medir qué tan bien están desarrollados y/o implementados los procesos administrativos dentro de la Organización. En el caso de TI, esto quiere decir qué tan capaces son en realidad ó qué tan bien desarrollados o capaces deberían ser, principalmente con relación a las metas de TI.

Las escalas del modelo de madurez ayudan a explicarle a la Gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran.

La autoevaluación es una herramienta para la revisión del nivel de madurez de una organización. Una autoevaluación puede abarcar criterios como el liderazgo, estrategia, sistema de gestión, recursos y/o procesos, con fin de identificar áreas de fortalezas, debilidades y oportunidades tanto para la mejora, como para la innovación.

Para crear la estructura de la autoevaluación del nivel de madurez de Gobierno de TI en entidades bancarias, se usó la **Norma ISO 38500** como base y se apoyó en los conceptos de nivel de madurez **CobiT**, **CMMI** e **ISO 9004**, las cuales se encuentran descritas en el Capitulo 2

4.1.1 Autoevaluación de Gobierno de TI propuesto

El formato de autoevaluación toma como base la norma ISO 38500 y los principios de los modelos de madurez de CobiT, CMMI e ISO 9004 (ver figura 10)

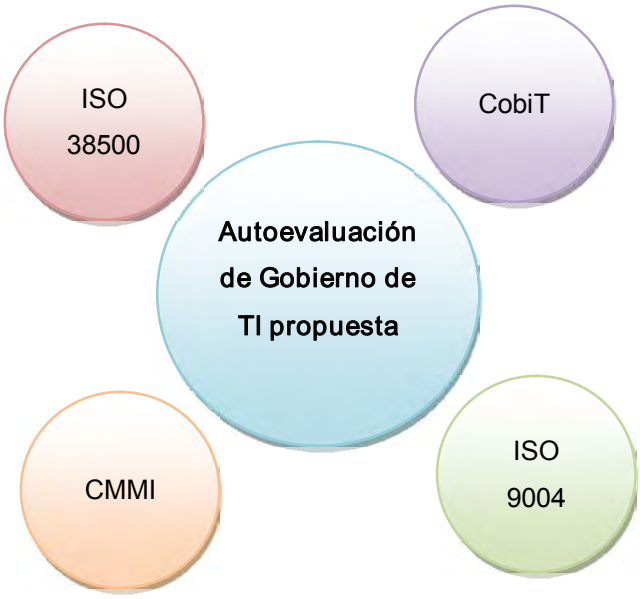


Figura 10: Autoevaluación de Gobierno de TI Propuesta

4.1.2 Realización de la Autoevaluación

Para la realización de la autoevaluación de Gobierno de TI se siguieron 3 pasos:

En el primer paso se definió como base la norma ISO 38500 y se dividieron el cumplimiento de sus 6 principios y las 3 tareas principales en niveles de madurez, utilizando como pauta los modelos de niveles de madurez de CobiT, CMMI e ISO 9004 (ver figura 11).

Posteriormente se utilizó el formato de autoevaluación de la norma ISO 9004 para presentar la propuesta y permitir que los encargados de TI que las diligencien definan su nivel actual y nivel deseado.

Por último, se adicionó a la autoevaluación una guía para su diligenciamiento, la cual incluye términos y pautas relevantes para la realización de la autoevaluación.

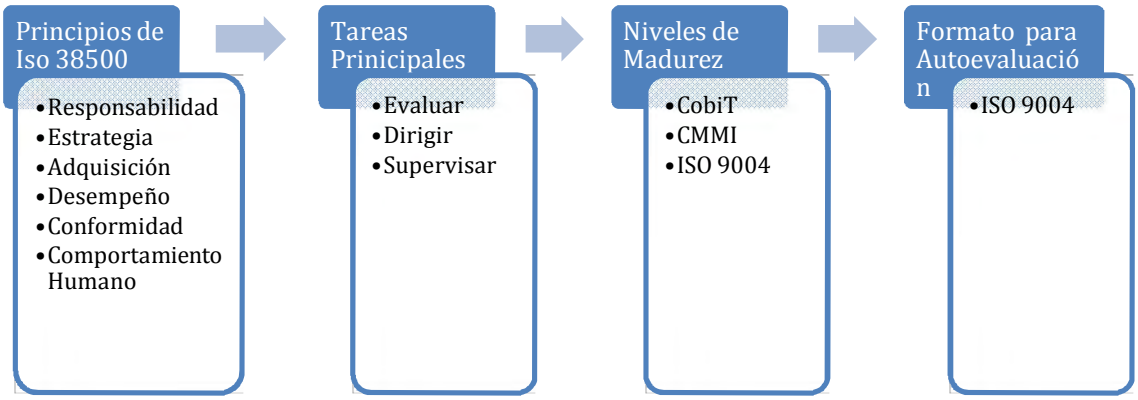


Figura 11: Esquema de la Autoevaluación propuesta

Por cada uno de los 6 principios que establece la norma ISO 38500, se plantearon actividades divididas en 3 bloques que corresponden a las tareas principales (Evaluar, Dirigir y Supervisar) (ver tabla 5)

Cada actividad cuenta con 5 niveles de madurez (preguntas). El primer nivel es el cumplimiento básico de una actividad de la norma. Para avanzar al nivel 2 se debe cumplir con el 100% de la(s) actividades del nivel 1 más la(s) actividad del nivel 2. Para alcanzar el nivel 3 de madurez se debe cumplir con las actividades de los niveles 1, 2 y 3; y así sucesivamente.

PRINCIPIOS DE ISO 38500	NIVELES DE MADUREZ					
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Evaluar					
	Dirigir					
	Supervisar					

Tabla 5: Formato de la Autoevaluación propuesta

4.1.3 Ejemplo de la Autoevaluación

A continuación se presenta un ejemplo de la autoevaluación, tomando el principio No 1 (Responsabilidad) de la Norma ISO 38500 y la tarea principal Evaluar. (ver tabla 6)

La Autoevaluación completa y su guía de diligenciamiento se encuentran en los Anexos 1 y 2 respectivamente.

Principio 1: Responsabilidad

Los individuos o grupos dentro de la organización entienden y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de Tecnología de la información. Aquellos con responsabilidad de las acciones también tienen la autoridad para ejecutar tales acciones.

Tarea Principal: Evaluar

Los directores deberían evaluar las opciones para la asignación de responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización. Al evaluar las opciones, se recomienda que los directores busquen asegurar el uso y la entrega eficaces, eficientes y aceptables de la tecnología de la información como soporte para los objetivos actuales y futuros del negocio. Los directores deberían evaluar la competencia de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a la tecnología de la información. En general, estas personas deberían ser gerentes del negocio que también sean responsables de los objetivos del negocio de la organización y del desempeño, ayudados por especialistas en TI que entiendan los valores y los procesos del negocio.

	NIVELES DE MADUREZ					
	CobiT 4.1	Inicial	Repetible	Definido	Administrado	Optimizado
	CMMI-DEV	Inicial	Gestionado	Definido	Gestionado Cuantitativamente	En optimización
	ISO 9004	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
PRINCIPIO 1: **RESPONSABILIDAD**	Tarea Principal **Evaluar**	En general, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y a la demanda de la información	Los directores de TI establecer reglas y responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización.	Con respecto al suministro y a la demanda de la información, los usuarios dentro de la organización, entienden y aceptan las reglas y responsabilidades asignadas por TI.	Los directores de TI tienen alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encuentran documentados	Los directores de TI, evalúan la competencia (capacidad, autoridad, experiencia, etc.) de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a TI. (Los resultados de estas evaluaciones se encuentran documentados)

Tabla 6: Ejemplo de la Autoevaluación, comparado con los niveles de madurez de CobiT, CMM e ISO 9004

4.1.4 Presentación de los resultados de la Autoevaluación

El objetivo de la autoevaluación es determinar el nivel de madurez actual y el deseado de Gobierno de TI para posteriormente con el modelo cerrar la brecha existente entre el nivel actual y el nivel deseado.

La presentación de los resultados de la autoevaluación se realizará a través de un gráfico radial que permita observar las brechas antes mencionadas (ver figura 12 y 13).

Para validar la autoevaluación y conocer el estado actual de Gobierno de TI, según la escala propuesta, se pidió a los responsables de TI de 3 entidades bancarias de Colombia que la diligenciaran. El análisis de los resultados de la autoevaluación se abarca en el capítulo 9

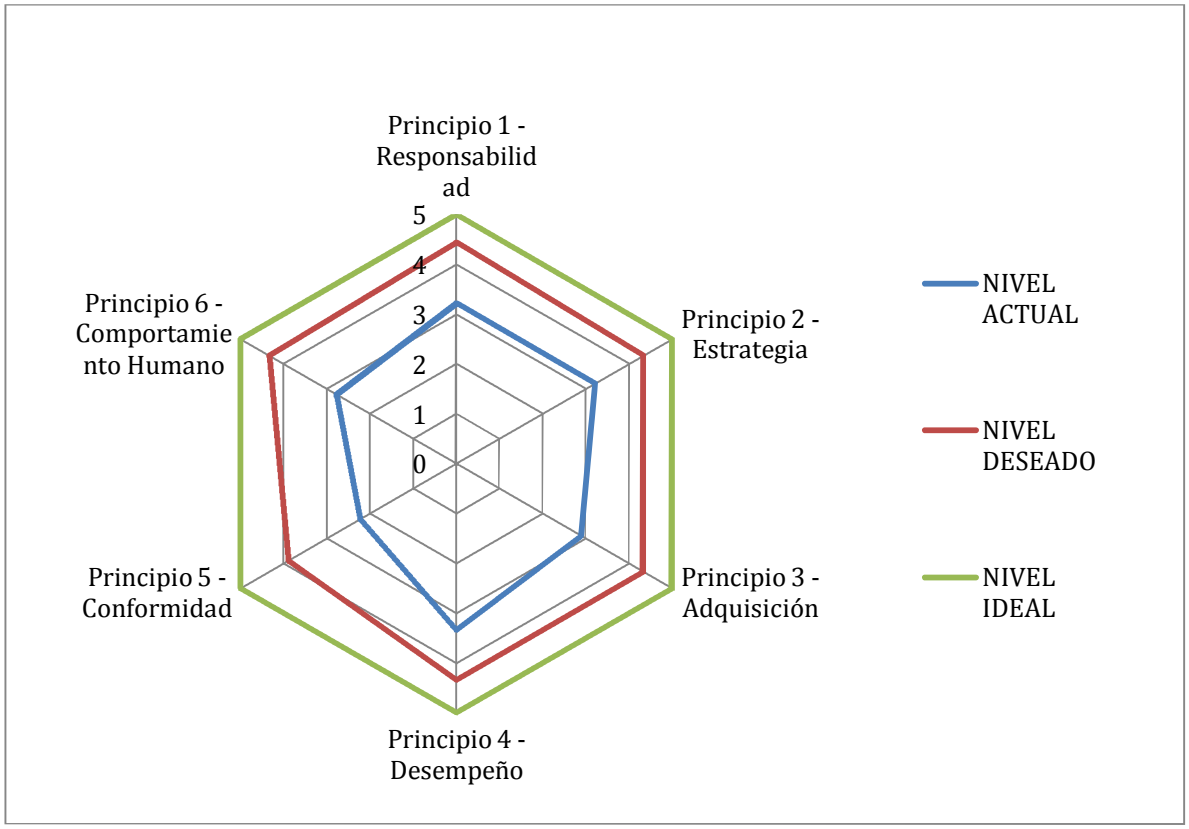


Figura 12: Ejemplo de la presentación de los resultados por los 6 principios de ISO 38500

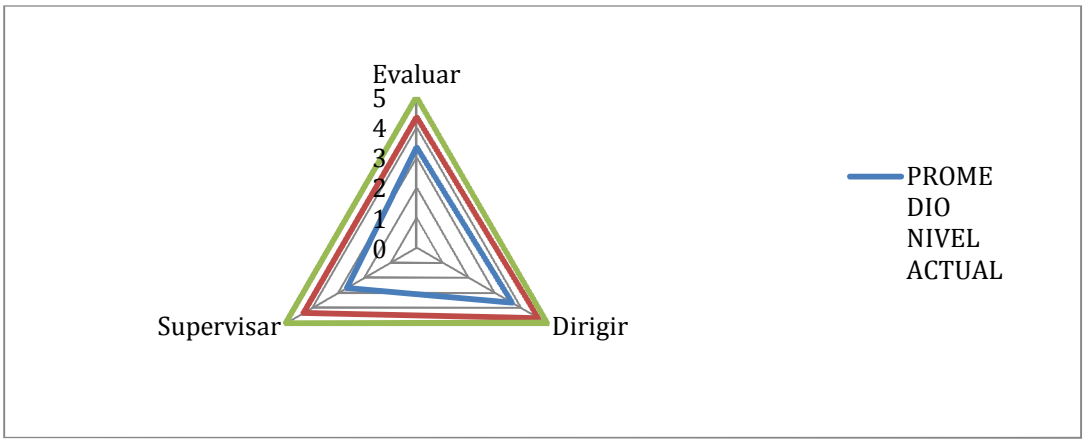


Figura 13: Ejemplo de la presentación de los resultados por las 3 tareas principales por cada principio de ISO 38500

5. MODELO PROPUESTO

El presente modelo de Gobierno de TI propuesto recoge el espíritu de la Circular 014 de 2009, la cual como tiene como objetivo primario que las entidades bancarias de Colombia creen y/o fortalezcan un sistema de control interno que permita la **evaluación continua de su eficiencia**, contribuya al **logro de sus objetivos de negocio** y fortalezca la apropiada **administración de los riesgos** a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia.

5.1 Contexto del Modelo

Las entidades bancarias de Colombia se encuentran regidas por la Circular 014 del 2009; la cual define las **Normas de Control Interno para la Gestión de la Tecnología.**

En dicha circular se establece que las entidades bancarias deberán diseñar un Sistema de Control Interno (SCI) para la gestión de la tecnología, que responda a las políticas, necesidades y expectativas de la entidad y a las exigencias normativas, **con el propósito de contribuir al logro de los objetivos institucionales**[19]

El SCI obliga a los responsables de TI de las Entidades Bancarias a contar con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir 19 requerimientos:

1. Plan estratégico de tecnología.
2. Infraestructura de tecnología.
3. Relaciones con proveedores.
4. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
5. Administración de proyectos de sistemas.
6. Administración de la calidad.
7. Adquisición de tecnología.
8. Adquisición y mantenimiento de software de aplicación.
9. Instalación y acreditación de sistemas.
10. Administración de cambios.

---

[19] **Circular Externa 014 del 2009**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc

11. Administración de servicios con terceros.
12. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
13. Continuidad del negocio.
14. Seguridad de los sistemas.
15. Educación y entrenamiento de usuarios.
16. Administración de los datos.
17. Administración de instalaciones.
18. Administración de operaciones de tecnología.
19. Gestión de la Documentación.

Por tal motivo y para dar cumplimiento a la ley, las entidades bancarias cuentan con un **Sistema de Control Interno para la gestión de tecnología**, el cual está encaminado a cubrir los 19 requerimientos mencionados y a contribuir al logro de los objetivos institucionales.

En razón de lo anterior, dichos requerimientos se convirtieron en los requerimientos de TI claves para el modelo de Gobierno de TI para las entidades bancarias. Para mayor facilidad, se identificaron los 19 requerimientos de TI seleccionados con un código, tal como se muestra en la Tabla 7.

Código	Requerimientos de TI
RQ01	Plan estratégico de tecnología.
RQ02	Infraestructura de tecnología.
RQ03	Relaciones con proveedores.
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
RQ05	Administración de proyectos de sistemas.
RQ06	Administración de la calidad.
RQ07	Adquisición de tecnología.
RQ08	Adquisición y mantenimiento de software de aplicación.
RQ09	Instalación y acreditación de sistemas.
RQ10	Administración de cambios.
RQ11	Administración de servicios con terceros.
RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
RQ13	Continuidad del negocio.
RQ14	Seguridad de los sistemas.
RQ15	Educación y entrenamiento de usuarios.
RQ16	Administración de los datos.
RQ17	Administración de instalaciones.

RQ18	Administración de operaciones de tecnología.
RQ19	Gestión de la Documentación.

Tabla 7: Identificación de los 19 requerimientos de TI seleccionados

Para la creación del modelo de Gobierno de TI fue necesario seleccionar un marco base de referencia y otros marcos que apoyen las estrategias de Gobierno de TI.

El marco de Gobierno de TI seleccionado fue el ISO 38500:2008, debido a que es una Norma Internacional que provee un estándar para que la dirección de las organizaciones evalúen, dirijan y monitoreen el uso de las tecnologías de la información.

Los marcos de apoyo que complementan el marco base y apoyan las estrategias de Gobierno de TI son: CobiT 4.1, CMMI, ISO 27002 e ISO 9001.

Para encontrar la relación entre los 19 requerimientos de la circular 014, el marco base y los marcos de apoyo, se realizó un mapeo dando los siguientes resultados.

Código	Procesos	ISO 38500	CobiT	CMMI-Dev	ISO 27002	ISO 9001
RQ01	Plan estratégico de tecnología.	Estrategia	PO1	-	-	-
RQ02	Infraestructura de tecnología.	Adquisición	AI3	-	10.2.1 10.2.2 10.2.3	6.3
RQ03	Relaciones con proveedores.	Adquisición	PO5	SAM	5.1.1 10.7.3 10.8.1 6.2.3	7.4.1
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	Cumplimiento	ME3	-	6.1.6 15.1.1 15.1.2 15.1.4	8.2.2
RQ05	Administración de proyectos de sistemas.	Estrategia	PO10	PMC, IPM, PP, QPM	-	-

RQ06	Administración de la calidad.	Desempeño	PO8	PPQA	-	4.1 4.2.2 5.1 5.3 5.4.1 5.4.2 5.5.1 5.5.2 5.6 6.1
RQ07	Adquisición de tecnología.	Adquisición	AI5	-	6.1.5 6.2.3 10.8.2 12.5.5	7.4.1 7.4.2 7.4.3
RQ08	Adquisición y mantenimiento de software de aplicación.	Adquisición	AI2	REQM, RD, PI, TS	6.1.4 7.2.1 10.3.2 11.6.2 12.1.1 12.2.3 12.3.1 12.4.3 12.5.1 12.5.2 12.5.3	-
RQ09	Instalación y acreditación de sistemas.	Adquisición	AI7	-	10.1.4 12.5.1 12.5.2 10.3.2 6.1.4	-
RQ10	Administración de cambios.	Desempeño	AI6	CM	10.1.2 12.5.3 12.5.1 12.6.1 11.5.4	7.3.7

RQ11	Administración de servicios con terceros.	Desempeño	DS2	-	6.2.1 6.2.3 8.1.3 10.2.3 10.8.2	7,4
RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	Desempeño	DS3	-	12.1.1 9.1.5 9.2.4 12.4.2 15.5.2 12.6.1	-
RQ13	Continuidad del negocio.	Desempeño	DS4	-	6.1.6 6.1.7 14.1.1 14.1.2 14.1.3 14.1.4	5.6 8.2.2
RQ14	Seguridad de los sistemas.	Desempeño	DS5	RSKM	14.1.1 14.1.2 13.1.1 13.1.2 5.1.2	8.2.2
RQ15	Educación y entrenamiento de usuarios.	Comportamiento Humano	PO7 DS7	OT	8.1.1 8.1.2 8.2.2	6.2.1 6.2.2
RQ16	Administración de los datos.	Responsabilidad	PO2 PO6 ME4 DS11	-	10.8.1 10.5.1 10.7.1 15.1.3 10.7.1 10.7.2 12.4.3	4.2.3 4.2.4
RQ17	Administración de instalaciones.	Desempeño	DS12	-	9.1.1 9.1.2 9.1.3	6.3

					9.2.5 6.2.1	
RQ18	Administración de operaciones de tecnología.	Desempeño	DS13	-	10.1.1 10.7.4	-
RQ19	Gestión de la Documentación.	Responsabilidad	PO4	-	6.1.1 6.1.2 6.1.3	4.2 4.2.1 4.2.2 4.2.3 4.2.4

Tabla 8: Relación entre los 19 requerimientos de ley y los diferentes marcos

Para llevar a cabo el mapeo anterior se realizaron los siguientes pasos:

1. Mapear los 19 requerimientos contra CobiT 4.1

2. Una vez teniendo identificados en Cobit 4.1 los 19 requerimientos, se estableció la relación entre CobiT 4.1 con ISO 38500 (ver figura 14). De esta manera se agrupó los 19 requerimientos de la circular en los 6 principios de ISO 38500.

3. Para los mapeos entre Cobit 4.1 e ISO 27002 se utilizó el documento de ISACA llamado, “Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa” y para el mapeo con ISO 9001:2008 y CMMI-Dev, utilizamos sus respectivas normas

Después de distribuir los 19 requerimientos de TI, el marco base y los marcos de apoyo, se determinó cuales actividades de los marcos de apoyo ayudarían a cumplir con los objetivos de los 6 principios de ISO 38500:2008 y finalmente se determinó una serie de indicadores de gestión que permitan evaluar el cumplimiento de las metas propuestas.

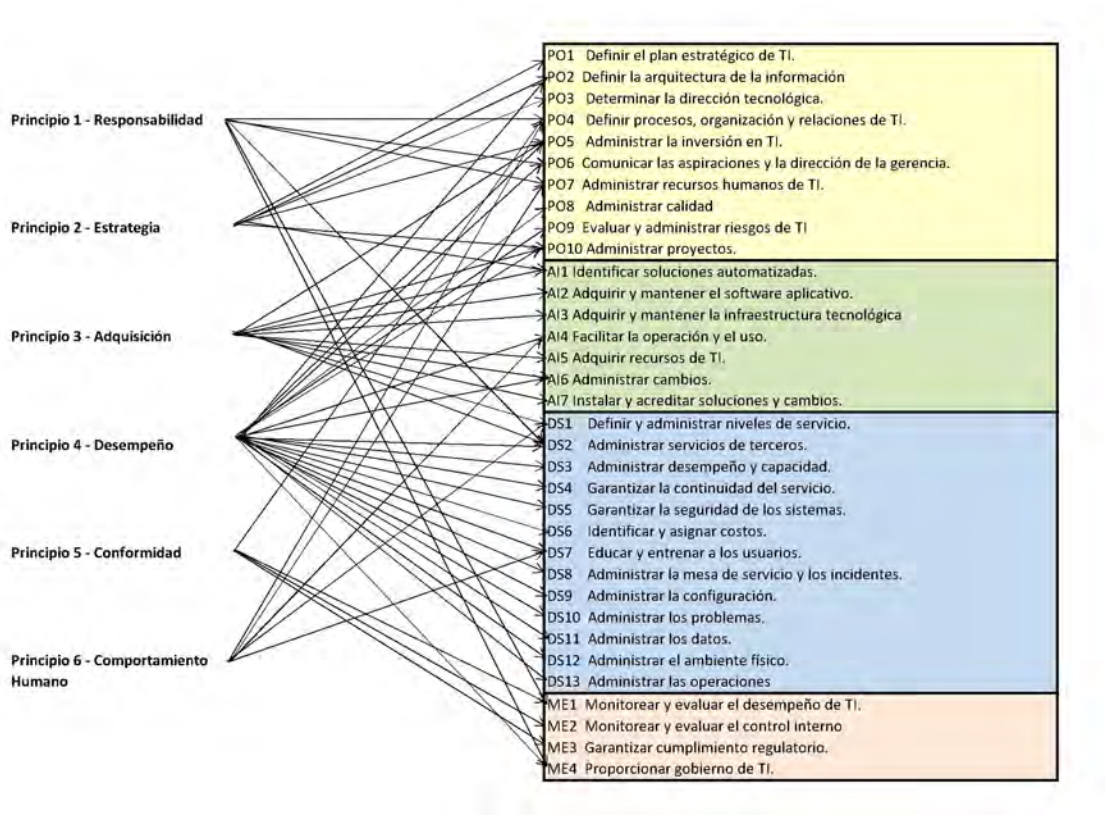


Figura 14: Relación entre principios de gobierno ISO 38500 y procesos CobiT[20]

El modelo de Gobierno de TI para las Entidades Bancarias planteado en este proyecto, responde a las actividades principales definidas por la norma ISO 38500 de **Evaluar** la utilización actual y futura de las TI. **Dirigir** la preparación e implementación de los planes y políticas que aseguren que la utilización de las TI de modo que alcancen los objetivos institucionales y **Controlar** el desempeño de la tecnología de la información, a través de sistemas de medición adecuados.

[20]"**A Foundation for Security**", IT Governance Network Netherlands, http://itgovernance.com/nl/index.php?option=com_content&view=article&id=72&Itemid=89.

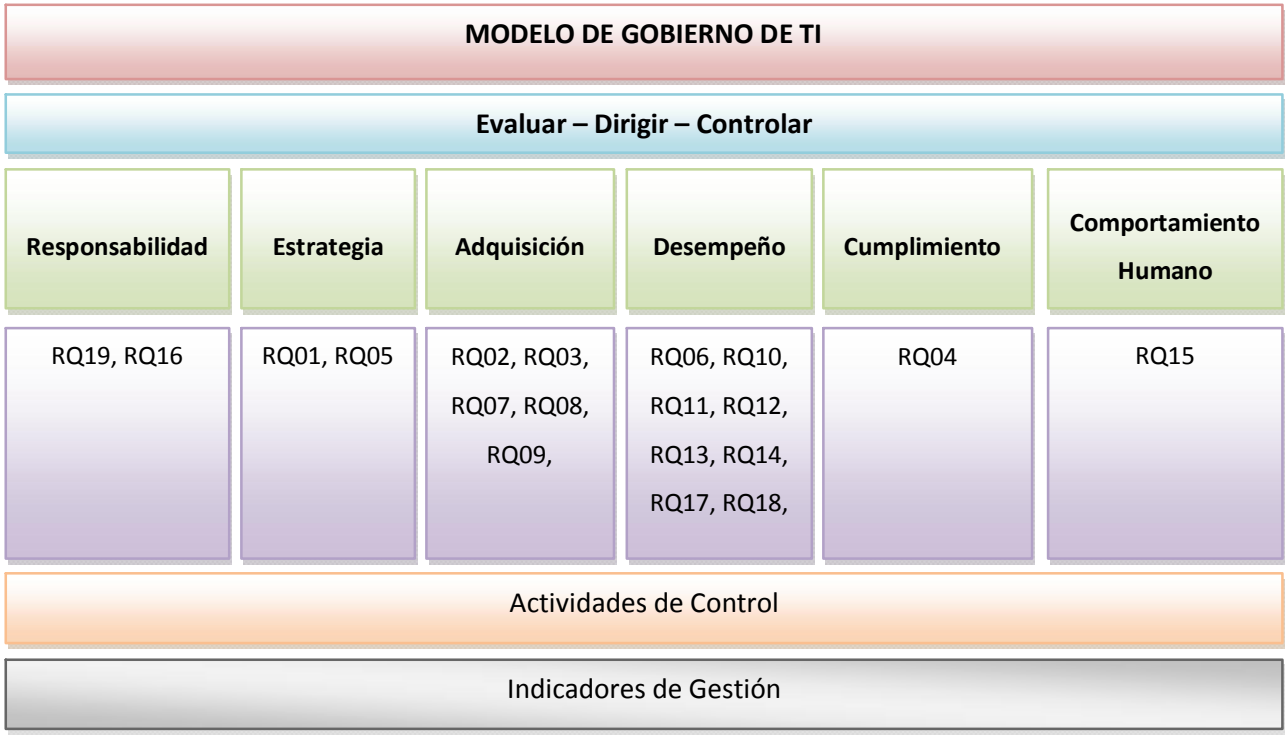


Figura 15: Modelo de Gobierno de TI Propuesto

5.2 Estructura del Modelo

El modelo de Gobierno de TI para entidades bancarias se encuentra estructurado de la siguiente manera:

- 6 principios, 19 Requerimientos de TI, 137 Actividades de control y 56 Indicadores de gestión

Principios	Requerimientos de TI		Actividades de Control	Indicadores
Responsabilidad	**RQ16**	Administración de los datos.	13	5
	RQ19	Gestión de la Documentación.	7	1
Estrategia	**RQ01**	Plan estratégico de tecnología.	6	3
	RQ05	Administración de proyectos de sistemas.	14	3
Adquisición	**RQ02**	Infraestructura de tecnología.	4	3
	RQ03	Relaciones con proveedores.	4	1

	RQ07	Adquisición de tecnología.	4	3
	RQ08	Adquisición y mantenimiento de software de aplicación.	10	2
	RQ09	Instalación y acreditación de sistemas.	9	3
Desempeño	**RQ06**	Administración de la calidad.	8	3
	RQ10	Administración de cambios.	5	3
	RQ11	Administración de servicios con terceros.	4	3
	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	6	3
	RQ13	Continuidad del negocio.	10	2
	RQ14	Seguridad de los sistemas.	12	3
	RQ17	Administración de instalaciones.	5	3
	RQ18	Administración de operaciones de tecnología.	5	3
Cumplimiento	**RQ04**	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	5	3
Comportamiento Humano	**RQ15**	Educación y entrenamiento de usuarios.	6	6

Tabla 9: Estructura del modelo de Gobierno de TI propuesto

Los 6 principios del modelo fueron obtenidos la norma ISO 38500:2008, de igual manera las **137 Actividades de Control** y los **56 Indicadores de Gestión**, fueron transcritas de CobiT 4.1, ISO 27002:2008, CMMI-DEV y/o ISO 9001:2008. Al Final de cada actividad de control aparece un superíndice con la referencia del marco utilizado en dicho control

6. MODELO DE GOBIERNO DE TI PARA ENTIDADES BANCARIAS DE COLOMBIA

Responsabilidad	•RQ16 - Administración de los datos. •RQ19 - Gestión de la Documentación.
Estrategia	•RQ01 - Plan estratégico de tecnología. •RQ05 - Administración de proyectos de sistemas.
Adquisición	•RQ02 - Infraestructura de tecnología. •RQ03 - Relaciones con proveedores. •RQ07 - Adquisición de tecnología. •RQ08 - Adquisición y mantenimiento de software de aplicación. •RQ09 - Instalación y acreditación de sistemas.
Desempeño	•RQ06 - Administración de la calidad. •RQ10 - Administración de cambios. •RQ11 - Administración de servicios con terceros. •RQ12 - Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica. •RQ13 - Continuidad del negocio. •RQ14 - Seguridad de los sistemas. •RQ17 - Administración de instalaciones. •RQ18 - Administración de operaciones de tecnología.
Cumplimiento	•RQ04 - Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
Comportamiento Humano	•RQ15 - Educación y entrenamiento de usuarios.

6.1 Responsabilidad

Los individuos o grupos dentro de la organización entienden y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de Tecnología de la información.

Los responsables TI deberían **evaluar** las opciones para la asignación de responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización. Deberían asegurar que el uso y la entrega de información se eficaz, eficiente y aceptable, de modo que la tecnología de la información ayude para alcanzar los objetivos actuales y futuros del negocio. Además deberían evaluar la competencia de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a la tecnología de la información.

Los responsables de TI deberían **dirigir** los proyectos para que se realicen de acuerdo con las responsabilidades de tecnología de la información asignadas. También deberían exigir que se les entregue la información que necesitan para cumplir sus responsabilidades, incluidas las relativas a acciones y toma de decisiones.

Los directores deberían **controlar** que se hayan establecido los mecanismos adecuados para el gobierno de la tecnología de la información. También deberían supervisar que aquellos a quienes se han asignado responsabilidad, reconozcan y entiendan sus responsabilidades.

6.1.1 RQ16 - Administración de los datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

6.1.1.1 Actividades de Control

i. Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio. Las necesidades de reinicio y reproceso están soportadas. CobiT 4.1

ii. Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios. CobiT 4.1

iii. Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad. CobiT 4.1

iv. Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware. CobiT 4.1

v. Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad. CobiT 4.1

vi. Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios. CobiT 4.1

vii. Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI El modelo debe facilitar la creación, uso y el compartir en forma óptima la información por parte del

negocio de tal manera que se mantenga su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos. CobiT 4.1

viii. Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado. CobiT 4.1

ix. Definir los elementos de un ambiente de control de información, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas y/o requerimientos respecto a la competencia del personal, la rendición de cuentas y la responsabilidad. CobiT 4.1

x. Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

xi. Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. CobiT 4.1

xii. Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización. CobiT 4.1

xiii. Definir, establecer y alinear el marco de gobierno de TI con la visión completa del entorno de control y Gobierno Corporativo. Confirmar que el marco de gobierno de TI asegura el cumplimiento con las leyes y regulaciones y que esta alineado, y confirma la entrega de, la estrategia y objetivos empresariales. Informa del estado y cuestiones de gobierno de TI. CobiT 4.1

6.1.1.2 Indicadores de Gestión

a) Satisfacción del usuario con la disponibilidad de los datos.

b) Porcentaje de restauraciones exitosas de datos.

c) Número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados.

d) El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la empresa

e) La frecuencia de actividades de validación de datos

6.1.2 RQ19 – Gestión de la Documentación

Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Los documentos y registros requeridos por la organización deben controlarse. La organización debe establecer un procedimiento documentado para definir los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, la retención y la disposición de los documentos y los registros; asimismo deben permanecer legibles, fácilmente identificables y recuperables.

6.1.2.1 Actividades de Control

i. Aprobar los documentos en cuanto a su adecuación antes de su emisión. ISO 9001:2008

ii. Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente. ISO 9001:2008

iii. Asegurarse de que se identifican los cambios y el estado de la versión vigente de los documentos. ISO 9001:2008

iv. Asegurarse de que las versiones pertinentes de los documentos aplicables se encuentran disponibles en los puntos de uso. ISO 9001:2008

v. Asegurarse de que los documentos permanecen legibles y fácilmente identificables. ISO 9001:2008

vi. Asegurarse que los documentos de origen externo, que la organización determina que son necesarios para la operación se identifican y que se controla su distribución. ISO 9001:2008

vii. Prevenir el uso no intencionado de documentos obsoletos, y aplicarles una identificación adecuada en el caso de que se mantengan por cualquier razón. ISO 9001:2008

6.1.2.2 Indicadores de Gestión

a) El porcentaje de procesos de TI documentados

6.2 Estrategia

La estrategia de negocios de la organización toma en consideración las capacidades actuales y futuras de la tecnología de la información; los planes estratégicos para la Tecnología de la Información deberían satisfacer las necesidades actuales y continuas de la estrategia de negocios de la organización.

Los responsables de TI deberían **evaluar** los desarrollos de tecnología de la información y los procesos del negocio con el fin de asegurarse de que la tecnología de la información brindará soporte a las necesidades futuras del negocio. Al considerar los planes y las políticas, los responsables de TI deberían evaluar las actividades de la tecnología de la información para asegurar que están alineadas con los objetivos de la organización para las circunstancias cambiantes, que toman en consideración las mejores prácticas y satisfacen los requisitos de otras partes clave involucradas. Es recomendable que los responsables de TI se aseguren que el uso de la tecnología de la información está sujeta a la valoración y evaluación adecuada.

Los responsables de TI también deberían fomentar y **dirigir** la presentación de propuestas para usos innovadores de la tecnología de la información que le permitan a la organización responder a oportunidades o nuevos retos emprender nuevos negocios o mejorar los procesos.

Los responsables de TI deberían **controlar** el progreso de las propuestas de tecnología de la información aprobadas para asegurar que se están cumpliendo los objetivos en los marcos temporales exigidos, utilizando los recursos asignados. Se recomienda que los responsables de TI supervisen el uso de la tecnología de la información para asegurar que ésta obtiene los beneficios previstos.

6.2.1 RQ01 - Plan estratégico de tecnología

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.

6.2.1.1 Actividades de Control

i. Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, cronograma o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar contra acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados. CobiT 4.1

ii. Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas. CobiT 4.1

iii. Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades. CobiT 4.1

iv. Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI. CobiT 4.1

v. Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones. CobiT 4.1

vi. Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y comisionar los proyectos requeridos al momento de lanzar el programa. CobiT 4.1

6.2.1.2 Indicadores de Gestión

a) El porcentaje de objetivos de TI en el plan estratégico de TI, que da soporte al plan estratégico del negocio

b) El porcentaje de proyectos TI en el portafolio de proyectos que se puede rastrear hacia el plan táctico de TI

c) El retraso entre las actualizaciones del plan estratégico de TI y las actualizaciones de los planes tácticos de TI

6.2.2 RQ05 - Administración de proyectos de sistemas

Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. El marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y post-implantación después de la instalación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. Este enfoque reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza la contribución a los programas de inversión facilitados por TI.

6.2.2.1 Actividades de Control

i. Mantener, fomentar el programa de los proyectos, relacionados con el portafolio de programas de inversiones facilitadas por TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos. CobiT 4.1

ii. Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas en cada proyecto emprendido. El marco de trabajo y los métodos de soporte se deben integrar con los procesos de administración de programas. CobiT 4.1

iii. Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores de proyectos, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global. CobiT 4.1

iv. Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversiones facilitadas por TI. CobiT 4.1

v. Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversiones facilitadas por TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de iniciar el proyecto. CobiT 4.1

vi. Aprobar el inicio de las etapas importantes del proyecto y comunicarlo a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión importante del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto. CobiT 4.1

vii. Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto. CobiT 4.1

viii. Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto. La obtención de productos y servicios requeridos para cada proyecto se debe planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de adquisición de la organización. CobiT 4.1

ix. Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central. CobiT 4.1

x. Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto. CobiT 4.1

xi. Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (Ej. costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto. CobiT 4.1

xii. Identificar las tares de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos. CobiT 4.1

xiii. Medir el desempeño del proyecto contra los criterios clave del proyecto (Ej. alcance, cronograma, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, Implementar y monitorear las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto. CobiT 4.1

xiv. Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad relevante requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas. CobiT 4.1

6.2.2.2 Indicadores de Gestión

a) Porcentaje de proyectos que satisfacen las expectativas de los interesados (a tiempo, dentro del presupuesto, y con satisfacción de los requerimientos y/o ponderados por importancia)

b) Porcentaje de proyectos con revisión post-implantación

c) Porcentaje de proyectos que siguen estándares y prácticas de administración de proyectos

6.3 Adquisición

Las adquisiciones de Tecnología de la información se hacen por razones válidas, con base en el análisis adecuado y continuo, con toma de decisiones clara y transparente. Existe el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.

Los responsables de TI deberían **evaluar** las opciones para el suministro de la tecnología de la información con el fin de realizar las propuestas aprobadas, equilibrando los riesgos y el valor del dinero de las inversiones propuestas.

Los responsables de TI deberían **dirigir** que los activos de la tecnología de la información (sistemas e infraestructura) se adquieren de la manera correcta, incluida la preparación de la documentación adecuada, a la vez que se asegura el suministra de las capacidades requeridas. Los responsables de TI deberían controlar que los acuerdos de suministro (tanto interno como externo) den soporte a las necesidades del negocio de la organización.

Los directores deberían **controlar** las inversiones en tecnología de la información para asegurar que estas proporcionan las capacidades requeridas. Se recomienda que los responsables de TI supervisen el grado en el que la organización y sus proveedores mantienen el entendimiento compartido de la intención de la organización al hacer cualquier adquisición de tecnología de la información.

6.3.1 RQ02 - Infraestructura de tecnología

Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

6.3.1.1 Actividades de Control

i. Generar un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica. CobiT 4.1

ii. Implementar medidas de control interno, seguridad y auditoría durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso. CobiT 4.1

iii. Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad. CobiT 4.1

iv. Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad. CobiT 4.1

6.3.1.2 Indicadores de Gestión

a) El porcentaje de plataformas que no se alinean con la arquitectura de TI definida y los estándares de tecnología

b) El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será)

c) El número de componentes de infraestructura que ya no se pueden soportar (o que ya no se podrán en el futuro cercano)

6.3.2 RQ03 - Relación con proveedores

Los responsables de TI deberían asegurarse de que el producto adquirido cumple los requisitos de compra especificados. El tipo y el grado del control aplicado al proveedor y al producto adquirido debe depender del impacto del producto adquirido en la posterior realización del producto o sobre el producto final.

6.3.2.1 Actividades de Control

i. La organización debería evaluar y seleccionar los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización. ISO 9001:2008

ii. Deben establecerse los criterios para la selección, la evaluación y la re-evaluación de proveedores. ISO 9001:2008

iii. Deben mantenerse los registros de los resultados de las evaluaciones y de cualquier acción necesaria que se derive de las mismas. ISO 9001:2008

iv. Cuando la organización quieran llevar a cabo la verificación en las instalaciones del proveedor, la organización debe establecer en la información de compra las disposiciones para la verificación pretendida. ISO 9001:2008

6.3.2.2 Indicadores de Gestión

a) Cantidad de proveedores evaluados y/o re-evaluados en un periodo de tiempo

6.3.3 RQ07 - Adquisición de tecnología

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

6.3.3.1 Actividades de Control

i. Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI, instalaciones, hardware, software y servicios necesarios por el negocio. CobiT 4.1

ii. Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales. CobiT 4.1

iii. Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar la mejor viable y encajable según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales. CobiT 4.1

iv. Proteger y hacer cumplir los intereses de la organización en todo los contratos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios. CobiT 4.1

6.3.3.2 Indicadores de Gestión

a) El número de controversias en relación con los contratos de adquisición

b) La reducción del costo de compra

c) El porcentaje de interesados clave satisfechos con los proveedores

6.3.4 RQ08 - Adquisición y mantenimiento de software de aplicación.

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas

6.3.4.1 Actividades de Control

i. Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para la adquisición de software, teniendo en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización. Tener aprobadas las especificaciones de diseño por gerencia para garantizar que el diseño de alto nivel responde a los requerimientos. Reevaluar cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento. CobiT 4.1

ii. Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Realizar reevaluaciones cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento. CobiT 4.1

iii. Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable. CobiT 4.1

iv. Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización. CobiT 4.1

v. Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio. CobiT 4.1

vi. En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y/o funcionalidad, seguir un proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos. CobiT 4.1

vii. Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el software aplicativo desarrollado por terceros. CobiT 4.1

viii. Desarrollar, Implementar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. CMMI-DEV

ix. Seguir el estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el diseño, desarrollo e implementación, y aprobar los cambios a los requerimientos a través de un proceso de gestión de cambios establecido. CMMI-DEV

x. Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software. CMMI-DEV

6.3.4.2 Indicadores de Gestión

a) Número de problemas en producción por aplicación, que causan tiempo perdido significativo

b) Porcentaje de usuarios satisfechos con la funcionalidad entregada

6.3.5 RQ09 - Instalación y acreditación de sistemas

Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados.

6.3.5.1 Actividades de Control

i. Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de sistemas de la información de desarrollo, implementación o modificación. CobiT 4.1

ii. Establecer un plan de pruebas basado en los estándares de la organización que define roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan esta aprobado por las partes relevantes. CobiT 4.1

iii. Establecer un plan de implantación y respaldo y vuelta atrás. Obtener aprobación de las partes relevantes. CobiT 4.1

iv. Definir y establecer un entorno seguro de pruebas representativo del entorno de operaciones planeado relativo a seguridad, controles internos, practicas operativos, calidad de los datos y requerimientos de privacidad, y cargas de trabajo. CobiT 4.1

v. Plan de conversión de datos y migración de infraestructuras como parte de los métodos de desarrollo de la organización, incluyendo pistas de auditoria, respaldo y vuelta atrás. CobiT 4.1

vi. Pruebas de cambios independientemente en acuerdo con los planes de pruebas definidos antes de la migración al entorno de operaciones. Asegurar que el plan considera la seguridad y el desempeño. CobiT 4.1

vii. Asegurar que el dueño de proceso de negocio y los interesados de TI evalúan los resultados de los procesos de pruebas como determina el plan de pruebas. Remediar los errores significativos identificados en el proceso de pruebas, habiendo completado el conjunto de pruebas identificadas en el plan de pruebas y cualquier prueba de regresión necesaria. Siguiendo la evaluación, aprobación promoción a producción. CobiT 4.1

viii. Seguimiento a pruebas, controlar la entrega de los sistemas cambiados a operaciones, manteniéndolo en línea con el plan de implantación. Obtener la aprobación de los interesados clave, tales como usuarios, dueño de sistemas y gerente de operaciones. Cuando sea apropiado, ejecutar el sistema en paralelo con el viejo sistema por un tiempo, y comparar el comportamiento y los resultados. CobiT 4.1

ix. Establecer procedimientos en línea con los estándares de gestión de cambios organizacionales para requerir una revisión posterior a la implantación como conjunto de salida en el plan de implementación. CobiT 4.1

6.3.5.2 Indicadores de Gestión

a) Tiempo perdido de la aplicación o problemas de datos provocados por pruebas inadecuadas

b) Porcentaje de sistemas que satisfacen los beneficios esperados, medidos en el proceso posterior a la implantación

c) Porcentaje de proyectos con plan de prueba documentado y aprobado

6.4 Desempeño

La tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio.

Los responsables de TI deberían **evaluar** los medios propuestos por lo gerentes para asegurar que la tecnología de la información apoye los procesos de negocio con la habilidad y capacidad requeridas. Estas propuestas deberían dirigirse hacia la continuidad de la operación normal del negocio y del tratamiento de los riesgos asociados con el uso de la tecnología de la información. Se recomienda que los responsables de TI evalúen los riesgos que se originan en las actividades de la tecnología de la información para la continuidad de la operación de los negocios. Los responsables de TI deberían evaluar los riesgos para la integridad de la información y protección de los activos de tecnología de la información, incluyendo la propiedad intelectual y memoria organizacional asociadas. También deberían evaluar las opciones para garantizar decisiones eficaces y oportunas acerca del uso de la tecnología de la información en soporte de las metas del negocio. Los responsables de TI deberían evaluar con regularidad la eficacia y el desempeño del sistema de la organización para el gobierno de la tecnología de la información.

Los responsables de TI deberían **dirigir** la asignación de los recursos suficientes de manera que tal la tecnología de la información satisfaga las necesidades de la organización, de acuerdo con las prioridades acordadas y las restricciones del presupuesto. Los directores deberían dirigir a aquellos responsables de asegurar que la tecnología de la información dé soporte al negocio, cuando se requiera por razones del negocio, con datos correctos y actualizados que estén protegidos contra pérdida o mal uso.
Supervisar

Es recomendable que los responsables de TI **controlen** en que grado la tecnología de la información da soporte al negocio. También deberían supervisar hasta donde se da prioridad a los recursos y los presupuestos asignados de acuerdo con los objetivos del negocio. De igual modo los responsables de TI deberían supervisar en que grado se cumplen adecuadamente las políticas, como aquellas para la precisión de los datos y el uso eficiente de la tecnología de la información.

6.4.1 RQ06 - Administración de la calidad

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.

6.4.1.1 Actividades de Control

i. La organización debería establecer, documentar, implementar y mantener un sistema de gestión de la calidad y mejorar continuamente su eficacia [ISO 9001:2008]

ii. La organización debería determinar los procesos necesarios para el sistema de gestión de la calidad y su aplicación a través de la organización, determinar la secuencia e interacción de estos procesos, determinar los criterios y los métodos necesarios para asegurarse de que tanto la operación como el control de estos procesos sean eficaces, asegurarse de la disponibilidad de recursos e información necesarios para apoyar la operación y el seguimiento de estos procesos, realizar el seguimiento, la medición (cuando sea aplicable) y el análisis de estos procesos, implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de estos procesos. [ISO 9001:2008]

iii. La organización debería establecer y mantener un manual de la calidad que incluya el alcance del sistema de gestión de la calidad, los procedimientos documentados establecidos para el sistema de gestión de la calidad, y una descripción de la interacción entre los procesos del sistema de gestión de la calidad. [ISO 9001:2008]

iv. La alta dirección debería crear una política de la calidad adecuada al propósito de la organización, que incluya un compromiso de cumplir con los requisitos y de mejorar continuamente la eficacia del sistema de gestión de la calidad, que proporcione un marco de referencia para establecer y revisar los objetivos de la calidad, que es comunicada y entendida dentro de la organización y que es revisada para su continua adecuación. [ISO 9001:2008]

v. Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración. CMMI Dev

vi. Enfocar la administración de calidad en los clientes, determinando sus requerimientos y alineándolos con los estándares y prácticas de TI. Definir roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI. CobiT 4.1

vii. Mantener y comunicar regularmente un plan global de calidad que promueva la mejora continua. CobiT 4.1

viii. Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del sistema de gestión de la calidad, así como el valor que el sistema de gestión de la calidad proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas. CobiT 4.1

6.4.1.2 Indicadores de Gestión

a) Porcentaje de Interesados (Stakeholders) satisfechos con la calidad (ponderado por importancia)

b) Porcentaje de procesos de TI revisados de manera formal por aseguramiento de calidad de modo periódico que satisfaga las metas y objetivos de calidad

c) Porcentaje de procesos que reciben revisiones de aseguramiento de calidad

6.4.2 RQ10 - Administración de cambios

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

6.4.2.1 Actividades de Control

i. Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales. CobiT 4.1

ii. Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios. CobiT 4.1

iii. Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia. CobiT 4.1

iv. Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales. CobiT 4.1

v. Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios. CobiT 4.1

6.4.2.2 Indicadores de Gestión

a) El número de interrupciones o errores de datos provocados por especificaciones inexactas o una evaluación de impacto incompleta

b) La repetición de aplicaciones o infraestructura debida a especificaciones de cambio inadecuadas

c) El porcentaje de cambios que siguen procesos de control de cambio formales

6.4.3 RQ11 - Administración de servicios con terceros

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

6.4.3.1 Actividades de Control

i. Identificar todos los servicios de los proveedores, y categorizar los de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados, y credenciales de los representantes de estos proveedores. CobiT 4.1

ii. Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (por ejemplo a través de los acuerdos de nivel de servicio). CobiT 4.1

iii. Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios de los estándares universales del negocio. La administración del riesgo debe considerar además acuerdos de confidencialidad, contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc. CobiT 4.1

iv. Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se adhiere continuamente a los acuerdos del contrato y los acuerdos de nivel de servicio, y que el desempeño es competitivo con proveedores alternativos y las condiciones del mercado. CobiT 4.1

v.

6.4.3.2 Indicadores de Gestión

a) El número de quejas de los usuarios debidas a los servicios contratados

b) El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio

c) El porcentaje de los principales proveedores sujetos a monitoreo

6.4.4 RQ12 - Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.

6.4.4.1 Actividades de Control

i. Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los acuerdos de nivel de servicio. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelo apropiadas para producir un modelo de desempeño, de capacidad y de desempeño de los recursos de TI, tanto actual como pronosticado. CobiT 4.1

ii. Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados. CobiT 4.1

iii. Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño. CobiT 4.1

iv. Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI. CobiT 4.1

v. Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos: Mantener y poner a punto el desempeño actual dentro de TI y atender temas como elasticidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos; y para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los acuerdo de nivel de servicio. CobiT 4.1

vi. Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas CobiT 4.1

6.4.4.2 Indicadores de Gestión

a) Número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad

b) Porcentaje de picos donde se excede la meta de utilización

c) Porcentaje de acuerdos de nivel de servicio, cuyo de tiempo de respuesta que no se satisfacen

6.4.5 RQ13 - Continuidad del negocio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

6.4.5.1 Actividades de Control

i. Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación. CobiT 4.1

ii. Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas. CobiT 4.1

iii. Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24

horas, más de 24 horas y para periodos críticos de operación del negocio. CobiT 4.1

iv. Definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna. CobiT 4.1

v. Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor. CobiT 4.1

vi. Asegurarse de que todos las partes involucradas reciban sesiones de entrenamiento de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia. CobiT 4.1

vii. Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre. CobiT 4.1

viii. Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio. CobiT 4.1

ix. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones,

debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados. CobiT 4.1

x. Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia. CobiT 4.1

6.4.5.2 Indicadores de Gestión

a) Número de horas perdidas por usuario por mes, debidas a interrupciones no planeadas

b) Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad

6.4.6 RQ14 - Seguridad de los sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

6.4.6.1 Actividades de Control

i. Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio. CobiT 4.1

ii. Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios. CobiT 4.1

iii. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso. CobiT 4.1

iv. Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios

relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados. CobiT 4.1

v. Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. CobiT 4.1

vi. Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas. ISO 27002

vii. Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria. ISO 27002

viii. Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas. CobiT 4.1

ix. Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura). CobiT 4.1

x. Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes. CobiT 4.1

xi. Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen. ISO 27002

6.4.6.2 Indicadores de Gestión

a) El número de incidentes que dañan la reputación con el público

b) El número de sistemas donde no se cumplen los requerimientos de seguridad

c) El número de violaciones en la segregación de tareas

6.4.7 RQ17 - Administración de instalaciones

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

6.4.7.1 Actividades de Control

i. Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo. CobiT 4.1

ii. Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física. CobiT 4.1

iii. Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona. CobiT 4.1

iv. Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente. CobiT 4.1

v. Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud. CobiT 4.1

6.4.7.2 Indicadores de Gestión

a) Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico

b) Número de incidentes ocasionados por fallas o brechas de seguridad física

c) Frecuencia de revisión y evaluación de riesgos físicos.

6.4.8 RQ18 - Administración de operaciones de tecnología

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

6.4.8.1 Actividades de Control

i. Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones. CobiT 4.1

ii. Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándares agendados. CobiT 4.1

iii. Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones. CobiT 4.1

iv. Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad. CobiT 4.1

v. Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño. CobiT 4.1

6.4.8.2 Indicadores de Gestión

a) Número de niveles de servicio afectados a causa de incidentes en la operación.

b) Horas no planeadas de tiempo sin servicio a causa de incidentes en la operación.

c) Porcentaje de activos de hardware incluidos en los programas de mantenimiento.

6.5 Cumplimiento

La tecnología de la Información cumple con todas las leyes y los reglamentos obligatorios. Las políticas y las prácticas están definidas, implementadas y se hacen cumplir.

Es recomendable que los responsables de TI **evalúen** con regularidad la extensión hasta la cual la tecnología de la información satisface las obligaciones (reglamentarias, legislativas, de ley, contractuales), las políticas internas, las normas y las directrices profesionales.

Los responsables de TI deberían **dirigir** a aquellos responsables de establecer mecanismos regulares y rutinarios para garantizar que el uso de la tecnología de la información cumple con las obligaciones pertinentes (reglamentarias, legislativas, de ley, contractuales), las normas y las directrices. Los responsables de TI deberían dirigir de modo que se establezcan y hagan cumplir las políticas que permiten a la organización cumplir sus obligaciones internas en el uso de la tecnología de la información. Los responsables de TI deberían dirigir de forma tal que el personal de tecnología de la información cumpla las directrices pertinentes para el comportamiento y el desarrollo profesional. Conviene que los responsables de TI dirijan de tal forma que todas las acciones relacionadas con la tecnología de la información sean éticas.

Es recomendable que los responsables de TI **controlen** la conformidad y el cumplimiento de la tecnología de la información a través de prácticas adecuadas auditoría y presentación de informes, asegurando que las revisiones sean oportunas, exhaustivas y adecuadas para la evaluación del grado de satisfacción del negocio. También deberían supervisar las actividades de tecnología de la información, incluyendo la disposición final de los activos y los datos, para asegurar el cumplimiento de obligaciones ambientales, de privacidad, de gestión de conocimiento estratégico, de preservación de la memoria organizacional y otras obligaciones pertinentes.

6.5.1 RQ04 - Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.

6.5.1.1 Actividades de Control

i. Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización. CobiT 4.1

ii. Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados. CobiT 4.1

iii. Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios. CobiT 4.1

iv. Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas o requerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna. CobiT 4.1

v. Integrar los reportes de TI sobre requerimientos legales, regulatorios y contractuales con las salidas similares provenientes de otras funciones del negocio. CobiT 4.1

6.5.1.2 Indicadores de Gestión

a) El costo del no cumplimiento de TI, incluyendo arreglos y multas

b) Tiempo promedio de demora entre la identificación de los problemas externos de cumplimiento y su resolución

c) Frecuencia de revisiones de cumplimiento

6.6 Comportamiento Humano

Las políticas, prácticas y decisiones con respecto a la Tecnología de la Información demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y evolutivas de todas las personas en el proceso

Los responsables de TI deberían **evaluar** las actividades de tecnología de la información para asegurar que los comportamientos humanos estén identificados y se consideran de manera correcta.

Los responsables de TI deberían **dirigir** de manera tal que las actividades de tecnología de la información sean consistentes con el comportamiento humano identificado. Se recomienda que los responsables de TI dirijan de manera que cualquier persona en cualquier momento pueda identificar y reportar riesgos, oportunidades, problemas y preocupaciones. Estos riesgos se deberían manejar de acuerdo con las políticas y los procedimientos publicados y escalar hasta las personas correspondientes a cargo de la toma de decisiones.

Se recomienda que los responsables de TI **controlan** las actividades de tecnología de la información para asegurar que los comportamientos humanos identificadas siguen siendo pertinentes y que se les brinda la atención adecuada. Los responsables de TI deberían supervisar las prácticas laborales con el fin de asegurar que son consistentes con el uso adecuado de la tecnología de información.

6.6.1 RQ15 - Educación y entrenamiento de usuarios.

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.

6.6.1.1 Actividades de Control

i. Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya: Estrategias y requerimientos actuales y futuros del negocio, valores corporativos (valores éticos, cultura de control y seguridad, etc.), implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones), habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias. métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo. CobiT 4.1

ii. Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño. CobiT 4.1

iii. Al finalizar el entrenamiento, evaluar el contenido del entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento. CobiT 4.1

iv. Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso. CobiT 4.1

v. Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales. ISO 9001:2008

vi. Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario. ISO 9001:2008

6.6.1.2 Indicadores de Gestión

a) Número de llamadas de soporte debido a problemas de entrenamiento

b) Porcentaje de satisfacción de los Interesados con el entrenamiento recibido

c) Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo

d) El nivel de satisfacción de los interesados respecto a la experiencia y habilidades del personal.

e) La rotación de personal de TI.

f) Porcentaje de personal de TI certificado de acuerdo a las necesidades del negocio.

7. GUÍA DE IMPLEMENTACIÓN DEL MODELO DE GOBIERNO DE TI PARA ENTIDADES BANCARIAS DE COLOMBIA

Con el fin de proporcionar una guía que facilite la implementación del Modelo de Gobierno de TI en las entidades bancarias de Colombia, se definieron dos actividades específicas:

1. Se documentó una guía de implementación del modelo
2. Se documentó un ejemplo de implementación de un requerimiento de TI del modelo propuesto (ver anexo 4).

Finalmente, la base para la guía de implementación del modelo, fue la planteada por el IT Governance Institute, IT governance implementation[21] que consta de siete fases:

Fase 1: Obtener el compromiso de la alta dirección.
Fase 2: Determinar el estado actual.
Fase 3: Establecer el estado futuro deseado.
Fase 4: Identificar las brechas
Fase 5: Definir el plan de implementación
Fase 6: Desarrollar el plan de implementación
Fase 7: Monitorear y controlar el desempeño de la implementación

7.1 Guía de implementación del modelo

7.1.1 Fase 1: Obtener el compromiso de la alta dirección.

7.1.1.1 Objetivo:

Obtener el apoyo de la alta dirección y difundir entre las partes interesadas (stakeholders) la decisión de la implementación del modelo de gobierno de TI a través de los medios habituales de divulgación interna.

7.1.1.2 Actividades

1. Presentar el modelo de gobierno de TI a la alta dirección

[21] **IT governance implementation guide using COBIT and Val IT**. IT Governance Institute

2. Explicar el alcance del proyecto

3. Definir los roles y los responsables de la implementación del proyecto

4. Definir un plan de implementación

5. Definir un cronograma de implementación

6. Informar a las partes interesadas

7.1.1.3 Entregables

a) Documento con el apoyo y compromiso de la alta dirección en la implementación del proyecto

b) Documento con el plan de implementación, los roles y responsables de cada actividad y el cronograma de implementación del proyecto

7.1.2 Fase 2: Determinar el estado actual

7.1.2.1 Objetivo:

Determinar, por medio del modelo de autoevaluación propuesto, un estado actual del nivel de madurez de Gobierno de TI que se desearía alcanzar

7.1.2.2 Actividades

1. El responsable de TI debe leer y entender la guía para el diligenciamiento de la autoevaluación descrito en el anexo 2.

2. El responsable de TI debe diligenciar la autoevaluación de nivel de madurez propuesta, la cual se encuentra en el anexo 1.

3. Trasladar los resultados numéricos de la columna “estado actual” de la autoevaluación, al formato de análisis de resultados propuesto en el anexo 3, para observar gráficamente los resultados.

7.1.2.3 Entregables

a) Diligenciamiento de la autoevaluación de nivel de madurez de gobierno de TI.

b) Diligenciamiento del formato de análisis de resultados propuesto en el anexo 3

7.1.3 Fase 3: Establecer el estado futuro deseado.

7.1.3.1 Objetivo:

Determinar, con la ayuda del modelo de autoevaluación propuesto, un estado futuro deseado, del nivel de madurez de Gobierno de TI.

7.1.3.2 Actividades

1. El responsable de TI debe leer y entender la guía para el diligenciamiento de la autoevaluación descrito en el anexo 2.

2. Teniendo especial atención en la columna de “nivel deseado”, el responsable de TI debe diligenciar la autoevaluación de nivel de madurez propuesta, la cual se encuentra en el anexo 1.

3. Trasladar los resultados numéricos de la columna “nivel deseado” de la autoevaluación, al formato de análisis de resultados propuesto en el anexo 3 para observar gráficamente los resultados.

7.1.3.3 Entregables

a) Diligenciamiento de la autoevaluación de nivel de madurez de gobierno de TI.

b) Diligenciamiento del formato de análisis de resultados propuesto en el anexo 3

7.1.4 Fase 4: Identificar las brechas

7.1.4.1 Objetivo:

Con base en el estado actual y el estado futuro deseado resultantes de la autoevaluación, identificar las brechas a ser cerradas con el fin de avanzar en la implementación del proyecto.

7.1.4.2 Actividades

1. Identificar las brechas existentes entre el estado actual y el estado deseado para cada principio.

2. Identificar en conjunto con los líderes de TI, las causas, problemas comunes, amenazas, riesgos y restricciones que dificultarían cerrar las brechas existentes.

3. Determinar en conjunto con los lideres de TI, oportunidades de mejora, fortalezas y beneficios que facilitarían cerrar las brechas.

7.1.4.3 Entregables

a) Documento con las brechas existentes que se desean cerrar

b) Documento con las acciones necesarias que ayuden a cerrar las brechas existentes

7.1.5 Fase 5: Definir el plan de implementación

7.1.5.1 Objetivo:

Establecer un plan de implementación que permita alcanzar los objetivos propuestos

7.1.5.2 Actividades

1. Definir, de acuerdo a las brechas existentes encontradas, cuales de ellas serán cerradas y cuales solo quedaran planteadas para implementar en un futuro

2. Identificar en el modelo propuesto y según las brechas a cerrar, las actividades de control necesarias para alcanzar los objetivos

3. Convertir las actividades de control, en proyectos, los cuales deberán tener sus responsables asignados, metas, recursos y cronograma a seguir.

4. Definir el orden en el cual se ejecutarán los proyectos establecidos.

7.1.5.3 Entregables

a) Documentos con las brechas que serán cerradas y cuales quedarán planteadas para un futuro

b) Documento con las actividades de control necesarias para cerrar las brechas

c) Documento con los proyectos a implementar, con sus responsables, metas, recursos y cronograma, además del orden de implementación de los proyectos

7.1.6 Fase 6: Desarrollar el plan de implementación

7.1.6.1 Objetivo:

Desarrollar el plan de implementación planteado en la fase anterior

7.1.6.2 Actividades

1. Implementar cada proyecto en el orden establecido en la fase anterior

2. Para cada proyecto, gestionar los recursos económicos, físicos y humanos necesarios; además de cualquier tipo de recurso necesario adicional para llevara cabo cada proyecto

3. Realizar las actividades necesarias en cada proyecto para dar cumplimiento al mismo en los tiempos planteados en cada cronograma

4. Una vez terminado cada proyecto, realizar pruebas y realizar el cierre del mismo.

5. Divulgar (socializar) entre las partes interesadas el fin del proyecto y realizar capacitaciones en caso de ser necesarias

7.1.6.3 Entregables

a) Listado con los recursos necesarios para la implementación de cada proyecto

b) Listado con las pruebas realizadas (ejecutadas y aceptadas) a las actividades implementadas

c) Cierre formal del proyecto, con la respectiva aprobación del responsable del proyecto y el responsable de TI del banco

7.1.7 Fase 7: Monitorear y controlar el desempeño de la implementación

7.1.7.1 Objetivo:

Establecer revisiones periódicas a los proyectos implementados para validar que cumplen con los objetivos y metas propuestos; además generar una retroalimentación con las lecciones aprendidas.

7.1.7.2 Actividades

1. Crear mecanismos que permitan validar que los proyectos implementados están cumpliendo con objetivos propuestos

2. Definir responsables para realizar el monitoreo de los proyectos implementados

3. Reportar el resultado del monitoreo al responsable de TI del Banco para que tome las medidas que considere necesarias dependiendo de los resultados obtenidos

7.1.7.3 Entregables

a) Documento con los mecanismos creados para validar los proyectos implementados y los responsables de llevar a cabo el monitoreo

b) Documento con el resultado del monitoreo efectuado

8. VALIDACIÓN DE LA PROPUESTA

8.1 Metodología de Validación

Para validar el modelo de Gobierno de TI en entidades bancarias de Colombia, se creó un resumen ejecutivo del mismo (ver anexo 5) y una encuesta en formato digital (ver anexo 6) en el cual se le solicitó a un grupo de expertos que con base en dicho resumen ejecutivo evaluaran ciertos aspectos que se describen más adelante.

Dicho formato se creó en Google Docs y se envío vía correo electrónico a los expertos para conocer su criterio.

Los aspectos a validar fueron los siguientes:

- Validación de los 19 requerimientos TI identificados como base para el desarrollo del modelo de gobierno de TI para entidades bancarias de Colombia propuesto.

- Validación del modelo de Gobierno de TI para entidades bancarias de Colombia propuesto.

- Validación de la autoevaluación de nivel de madurez de gobierno de TI propuesta

- Validación de la aplicabilidad de la guía de implementación propuesta para el modelo de Gobierno de TI en entidades bancarias de Colombia

8.2 Selección de Expertos

Para la validación de la propuesta del modelo de Gobierno de TI para entidades bancarias de Colombia, se seleccionó un grupo de expertos compuesto por personas cuyo perfil reuniera por lo menos uno de los siguientes aspectos:

- Experiencia en áreas de TI del algún banco en Colombia
- Experiencia laboral en gobierno de TI
- Experiencia en docencia de gobierno de TI
- Título universitario en ingeniería de sistemas y/o similares, con maestría en el campo de los sistemas y conocimientos de gobierno de TI
- Título universitario en ingeniería de sistemas y/o similares, dueño de empresas de tecnología las cuales tengan reconocimiento a nivel nacional ó internacional

Las personas seleccionadas fueron las siguientes:

Jesús Emilio Zabala (Respondió la encuesta)
Subgerente de Desarrollo y mantenimiento
Banco de Occidente

José Miguel López (Respondió la encuesta)
Gerente de TI
Banco WWB

Fabián Andrés Cardenas (Respondió la encuesta)
Coordinador de proyectos
Bancoomeva

Ingrid Lucia Muñoz (NO respondió la encuesta)
Docente Maestría
Universidad Icesi

Liliana del Socorro Gómez (Respondió la encuesta)
Docente Maestría
Universidad Icesi

Francisco Agray Cortés (Respondió la encuesta)
Gerente Oficina de Proyectos

Sigifredo Quintero Contreras (Respondió la encuesta)
Consultor de TI

Antonio Fernández Martínez (Respondió la encuesta)
Docente Universitario
Universidad de Almería - España

Fabián González Valencia (Respondió la encuesta)
Gerente de TI
E-com

Las observaciones realizadas por el grupo de expertos se detallan a continuación y los resultados de la encuesta se encuentran en el Capitulo 9 Resultados Obtenidos:

Observación realizada por	Detalle de la Observación	Respuesta a la Observación
Francisco Agray Cortés	No sé en qué parte del Modelo de Gobierno incorporen la necesidad de articular los Objetivos Estratégicos de TI con los Objetivos Estratégicos del Negocio.	La circular 014 de 2009 especifica textualmente en el capítulo 7.6.2. que “las entidades bancarias deberán diseñar un Sistema de Control Interno (SCI) para la gestión de la tecnología, que responda a las políticas, necesidades y expectativas de la entidad y a las exigencias normativas, con el propósito de contribuir al logro de los objetivos institucionales”
Francisco Agray Cortés	Como Modelo de Gobierno deberían proponer Mecanismos de Gobierno de TI (diferentes comités, ejecutivos a nivel del negocio, a nivel de proyectos, técnicos, operativos, entre otros)	Consideramos que puede llegar a ser prudente, sin embargo, considerando las diferentes normativas y mecanismos de control de la superintendencia, consideramos que no es necesario proponer mas comités de control
Francisco Agray Cortés	Otro aspecto que es clave en TI es la Capacitación, en el RQ15 lo veo muy focalizado a Usuarios, pero no se dónde quede la gente de TI.	El RQ15, en sus actividades de control, está orientado tanto al usuario de TI como al usuario no TI
Francisco Agray Cortés	En la propuesta de Implementación del Modelo basados en el IT Governace Institute, no se si en el punto que se refieren a Establecer el estado futuro deseado, ese sería el Modelo que están proponiendo y contra él se establecerían las brechas, de no ser así, el modelo propuesto quedaría flotando en la Implementación..	Se actualizo la guía de implementación en la Fase 7 quedando de la siguiente forma: Monitorear y controlar el desempeño de la implementación
Sigifredo Quintero Contreras	En la parte del Contexto del Trabajo, para una mayor claridad, se podría contextualizar desde el Sistema Financiero en Colombia, su composición y en este contexto, cómo se ubican los Establecimientos Bancarios en el marco general y en los establecimientos de crédito, diferenciándolos de las	Se amplió el Capitulo 3 Contexto del Sector Bancario Colombiano, para dar respuesta a la observación planteada

	corporaciones financieras, las compañías de financiamiento y las cooperativas financieras.	
Sigifredo Quintero Contreras	En el Modelo de Gobierno de TI propuesto no aparece explícito el nombre de Autoevaluación. Sugiero dejar la palabra Autoevaluación arriba de las palabras Evaluar-Dirigir-Controlar	No se incluyó dentro de la grafica del modelo, porque la Autoevaluación se quiere presentar con un complemento (anexo) a la propuesta
Sigifredo Quintero Contreras	Infraestructura de Tecnología: confirmar si ésta se refiere sólo a la Adquisición como lo plantea el Modelo (RQ02) o si es transversal (Estructura organizacional, roles, factor humano y otros) como los Indicadores de Gestión o las Actividades de Control.	El RQ02 es tranversar con los indicadres pero esta orientado a que los Bancos deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.
Sigifredo Quintero Contreras	Al Requerimiento Documentación (RQ19) quedaría más claro si se le antepone la palabra Administración o Gestión.	Se actualizó en el trabajo quedando Gestión de la Documentación
Sigifredo Quintero Contreras	En la Estructura del Modelo de Gobierno de TI Propuesto recomiendo incluir en: - Responsabilidad: Políticas y Procedimientos, Innovación. - Desempeño: Administración de servicios de Asistencia Tecnológica (ITIL). - Comportamiento Humano: Gestión del Factor Humano. Consolidar Cultura del Gobierno de TI. Se gestiona la TI, pero es clave gestionar todo lo relacionado con el factor humano.	Nuestro modelo se basa en el norma ISO 38500, la cual aborda en 3 de sus 6 principios los aspectos de Responsabilidad, Desempeño y Comportamiento Humano, sobre los cuales creamos actividades de control, tendientes a cumplir con los aspectos que se sugieren en la observación
Sigifredo Quintero Contreras	Se sugiere adicionar como principio o incluir en otro: - Gestión del Riesgo. - Investigación y Desarrollo. - Patentes y Derechos de Autor.	La norma ISO 38500 incluye un principio cumplimiento en el cual se pide cumplir con todos los aspectos legales (incluyendo los relacionados con derechos de autor). En cuanto a la Gestión del Riesgo lo cubre con su principio de Desempeño. El apartado de Investigación y Desarrollo no está incluido y lo planteamos en el Capitulo 10 Trabajo

		Futuro
Sigifredo Quintero Contreras	No sé si lo tengan en el documento, pero lo menciono: tener un glosario de términos. Es importante definir las palabras clave, incluso incluir su etimología:	En el Anexo 2 se incluye un glosario con los términos más relevantes usados en nuestra propuesta
Sigifredo Quintero Contreras	En cuanto a la Guía de Implementación del Modelo recomiendo incluir un último ítem: Fase 8: Lecciones Aprendidas y Retroalimentación.	Se actualizo la Fase 7 de la guía, quedando de la siguiente forma: “Establecer revisiones periódicas a los proyectos implementados para validar que cumplen con los objetivos y metas propuestos; además generar una retroalimentación con las lecciones aprendidas”
Antonio Fernández Martínez	Creo que entre los 19 requerimientos que habeis seleccionado cubrís bastante bien el ámbito del gobierno de las TI pero algunos de ellos están redactados de manera que son propios del nivel de Gestión o Administración de las TI y no del de Gobierno	Los 19 requerimientos de TI, los obtuvimos de la circular 014 de 2009, por tal motivo tomamos su misma redacción
Antonio Fernández Martínez	No se muy bien quién va a rellenar esta autoevaluación, pero deberían hacerlo los directivos de banca	Recibimos la observación pero no la compartimos porque pensamos que son los directivos de TI, los más indicados para responder la autoevaluación, debido a que los aspectos que se evalúan son orientados a TI

Tabla 10: Relación de observaciones del grupo de expertos

9. RESULTADOS OBTENIDOS

Los resultados más relevantes obtenidos en el desarrollo de este proyecto fueron:

- Identificación de los 19 requerimientos de TI claves para el modelo de Gobierno de TI
- Modelo de Gobierno de TI para entidades bancarias de Colombia
- Una autoevaluación de nivel de madurez de Gobierno de TI, basada en ISO 38500:2008
- Una Guía de Implementación para modelo propuesto
- Un instrumento para la validación del modelo por parte de un juicio de expertos.

Para validar la autoevaluación y conocer el estado actual de Gobierno de TI, según la escala propuesta, se pidió a 3 entidades bancarias de Colombia que la diligenciaran. El resumen de dicho resultados es el siguiente:

- Según el muestreo, el sector bancario tiene procedimientos, tareas y/o actividades, que según el modelo y la escala propuesta, ayudan al Gobierno de TI
- Se evidencia también que tienen interés de crecer a un nivel superior del actual, en todas las aristas del modelo propuesto.
- Se observa además, que si bien es cierto tienen expectativa de avanzar a un nivel superior, por ahora no consideran la posibilidad de estar en el nivel ideal, dentro de la escala propuesta

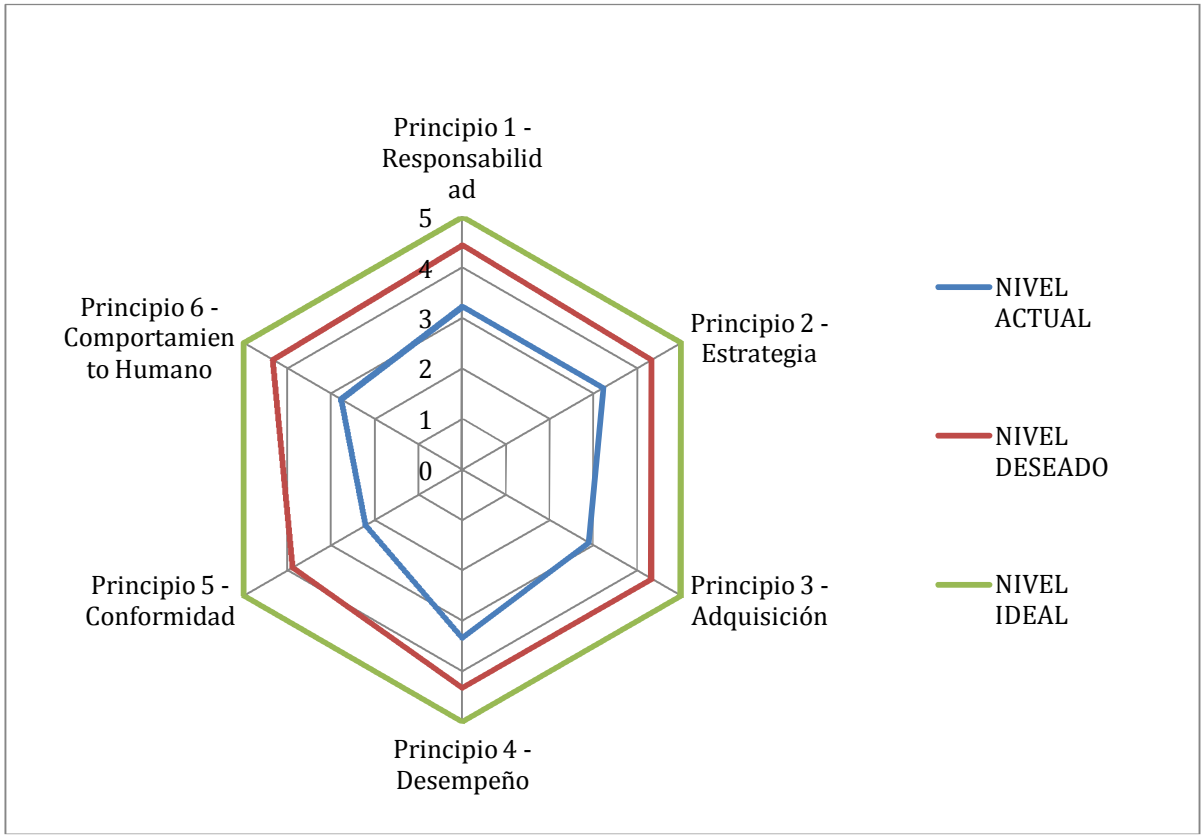


Figura 16: Promedio de nivel de madurez de 3 Entidades Bancarias de Colombia, según el modelo propuesto

Respecto a los resultados de la encuesta para el juicio de expertos (ver anexo 6), se observa que de los 19 Requerimientos de TI propuestos para hacer parte de un modelo de gobierno de TI, 3 fueron votados con 100%, 7 con 86% y 9 con el 71%; lo cual significa que en su mayoría son aceptados.

De igual forma se observa que a la pregunta de si está de acuerdo o en desacuerdo en que los 19 requerimientos de TI identificados son válidos, apropiados y sirven de base para el modelo de Gobierno de TI para entidades bancarias de Colombia, el 86% votó favorablemente a este interrogante.

Por último y ante el interrogante de si considera viable o inviable la implementación del modelo propuesto de Gobierno de TI para entidades bancarias de Colombia, el 100% de los expertos votó a favor de esta afirmación.

Los resultados del juicio de expertos fueron los siguientes:

1) Del listado de 19 requerimientos de TI que ordena la circular externa 014 de 2009, por favor seleccione los que usted considera que deben hacer parte de un modelo de gobierno de TI

RQ01	Plan estratégico de tecnología.	RQ11	Administración de servicios con terceros.
RQ02	Infraestructura de tecnología.	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
RQ03	Relaciones con proveedores.	RQ13	Continuidad del negocio.
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	RQ14	Seguridad de los sistemas.
RQ05	Administración de proyectos de sistemas.	RQ15	Educación y entrenamiento de usuarios.
RQ06	Administración de la calidad.	RQ16	Administración de los datos.
RQ07	Adquisición de tecnología.	RQ17	Administración de instalaciones.
RQ08	Adquisición y mantenimiento de software de aplicación.	RQ18	Administración de operaciones de tecnología.
RQ09	Instalación y acreditación de sistemas.	RQ19	Gestión de la Documentación.
RQ10	Administración de cambios.		

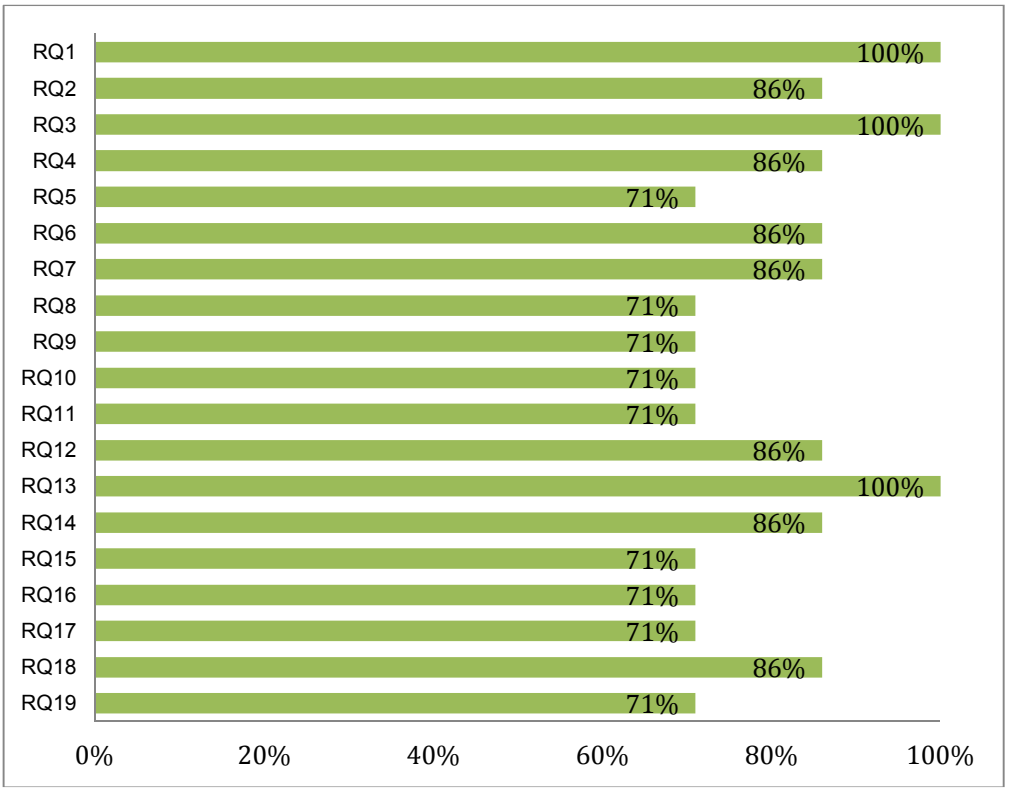


Figura 17: Resultados pregunta 1 de la encuesta

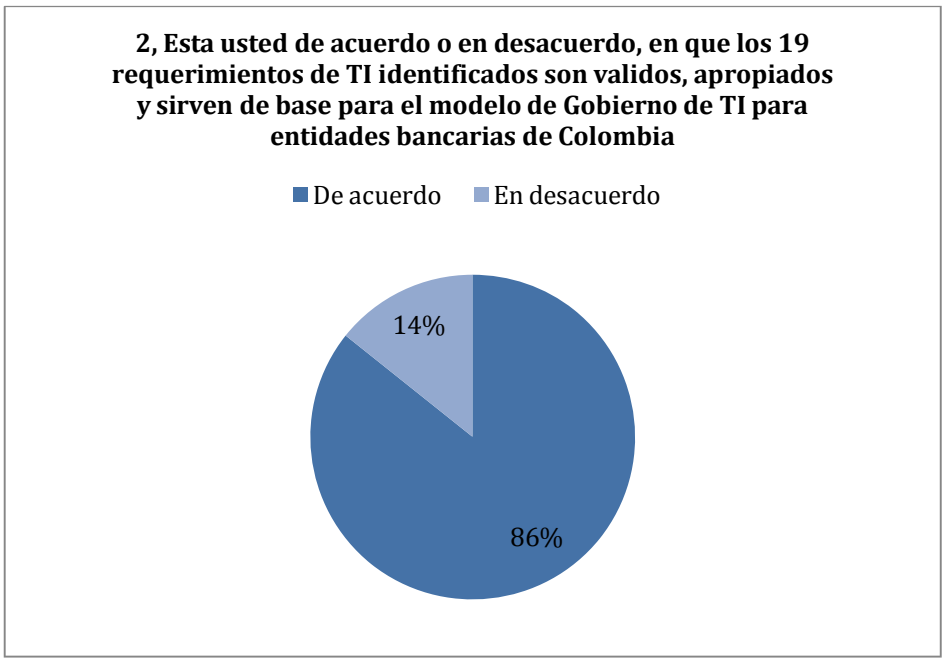


Figura 18: Resultados pregunta 2 de la encuesta

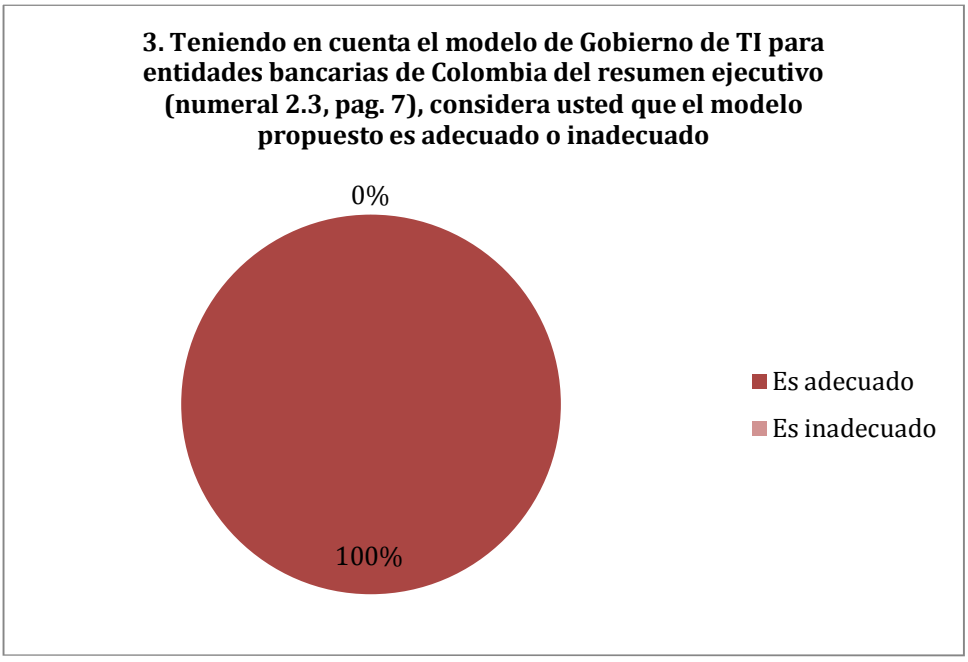


Figura 19: Resultados pregunta 3 de la encuesta

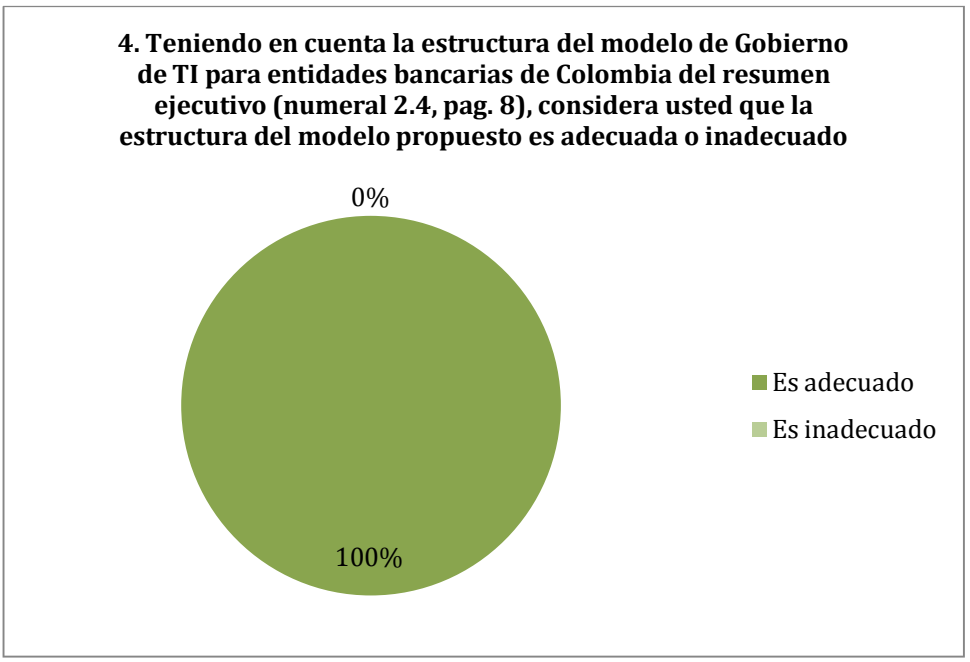


Figura 20: Resultados pregunta 4 de la encuesta

Figura 21: Resultados pregunta 5 de la encuesta

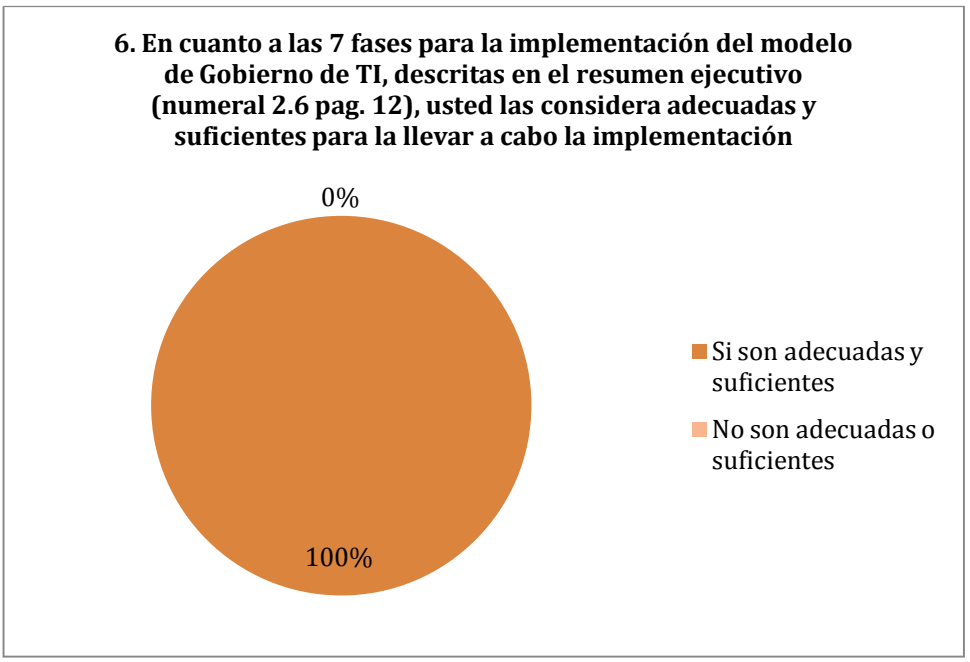


Figura 22: Resultados pregunta 6 de la encuesta

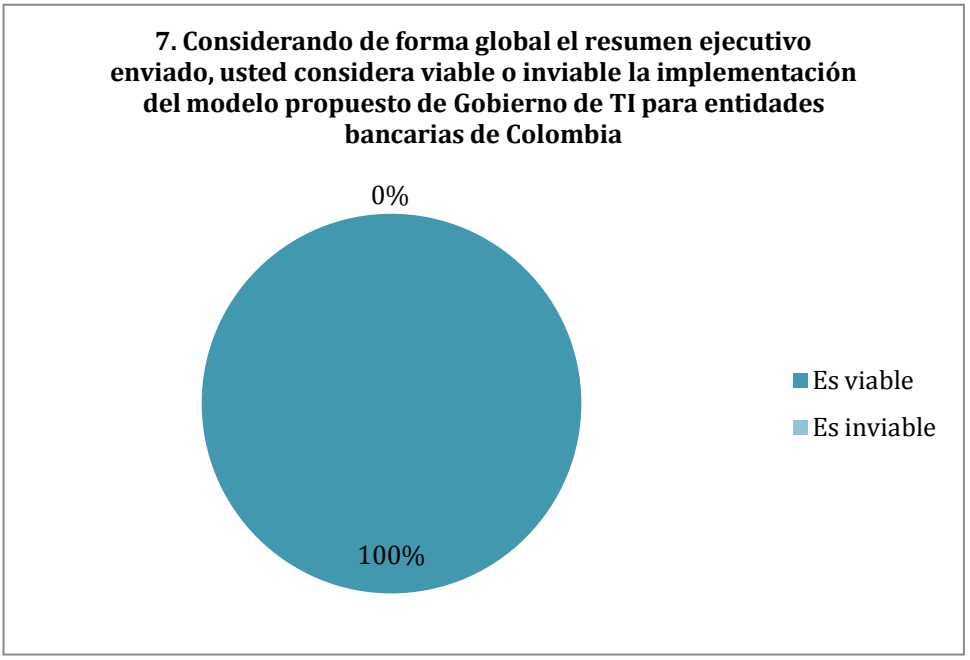


Figura 23: Resultados pregunta 7 de la encuesta

10. CONCLUSIONES Y FUTURO TRABAJO

10.1 Conclusiones

Gobierno de TI está orientado a la realidad actual de la industria, sin importar el tipo o tamaño de la organización; no se avizora algún tipo impedimento que haga que gobierno de TI no sea aplicado a las industrias. Lo que definitivamente si existe, son diferencias de tipo organizativas, culturales, económicas y legislativas dependiendo del sector de la industria, lo que implica que TI debe estar adaptada a estas necesidades propias.

Lo anterior implica que si bien es cierto gobierno de TI es un "producto genérico" que puede adaptarse a cualquier tipo de organización, sí se hace imperativo realizar un amoldamiento a la realidad de la industria particular que desea implementar.

Para la realización de este trabajo se partió de una ventaja significativa y es el hecho que el sector bancario colombiano esta agrupado y regulado por leyes, impartidas mayoritariamente por la superintendencia financiera, las cuales hacen que este sector tenga una estructura organizacional y documental muy bien establecida, lo que allana el camino para una posible implementación de Gobierno de TI. Entre estas leyes está la circular 014 de 2009, la cual obliga al sector bancario a contar con 19 requerimientos de TI, los cuales deben estar documentados y alineados con los objetivos estratégicos de la organización.

Caso contrario sucede con otros sectores comerciales del país, los cuales deben seguir un camino más complejo y extenso, debido a que se debe partir por verificar si tienen procesos claves documentados y de no ser así, se debe comenzar por conseguir esta información con las personas que lideran los diferentes procesos, con la dificultad agravada que tal vez estas personas no tienen el conocimiento necesario para entregar información clave y relevante de la organización y de TI.

Lo verdaderamente importante para llevar a cabo un proceso de implementación de Gobierno de TI en una organización, es contar con el apoyo (administrativo y financiero) por parte de la Alta Gerencia, ya que implementar cualquier modelo de Gobierno de TI requiere mínimamente de alinear los objetivos estratégicos de la organización con los objetivos de TI y en el caso de que estos no se encuentren documentados, requerirá de un esfuerzo administrativo y financiero adicional para completar en primer lugar esta actividad.

Respecto a los marcos de referencia, todos son muy valiosos y están precedidos de muchas horas de trabajo, de muchas personas con un conocimiento y experiencia indiscutible; así mismo, se observa que los marcos base de Gobierno

de TI tienen muchas cosas en común y no es difícil hacer asociaciones entre ellos, por tal motivo cualquier marco base (sabiéndolo aplicar) resultará útil para la implementación de Gobierno de TI.

10.2 Trabajo Futuro

Si bien es cierto este modelo propuesto cuenta con la aceptación en teoría de un juicio de expertos con conocimientos y experiencia en la materia, se hace determinante dar salto de la teoría a la práctica, por ende el trabajo futuro inmediato debe ser el de implementar el modelo en algún banco de país y hacer seguimiento al proceso de implementación, de modo que se pueda validar en la práctica los conceptos planteados de manera teórica y que a su vez pueda entregar aportes que permitan el mejoramiento continuo del modelo (por ejemplo incluir un principio de innovación y desarrollo) en pro de tener un modelo de gobierno de ti para el sector bancario de Colombia, cada vez más depurado.

De igual forma y teniendo en cuenta el ritmo cambiante de la tecnología, los marcos gobierno y la legislación colombiana, es prudente revisar periódicamente estas aristas, de manera que permita al modelo estar actualizado con las necesidades y tendencias que tienen incidencia en este modelo de Gobierno de TI, como por ejemplo, las tendencias cada vez más fuertes de la banca móvil y la computación en la nube, CobiT 5 y circulares externas que pueda decretar la Superintendencia Financiera de Colombia

Por último y con el ánimo de extender el alcance de este modelo de gobierno de TI, un trabajo futuro sería el de evaluar la adaptabilidad del mismo a otros sectores similares, de modo que no se aplique únicamente al sector bancario, sino todo al sector financiero dispuesto en el decreto 663 de 1993 como lo son por ejemplo las Corporaciones de Ahorro y Vivienda, las Compañías de financiamiento comercial y las Cooperativas Financieras

11. BIBLIOGRAFÍA

Superintendencia Financiera de Colombia *Circular Externa 014 del 2009*, Colombia.
http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc

Superintendencia Financiera de Colombia, *Circular externa 038 de 2009*, Colombia,
www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce038_09.doc

Superintendencia Financiera de Colombia, *Circular externa 052 de 2007,* Colombia, www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf

Superintendencia Financiera de Colombia, *Decreto 633 de 1993*, Colombia, http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

Asobancaria, *Información al consumidor financiero*. Colombia, 2012 http://www.asobancaria.com/portal/page/portal/Asobancaria/info_consumidor/sistema_financiero_y_banca/

Ministerio de Hacienda de Colombia, *Fusiones y Adquisiciones en el Sector Financiero Colombiano: Análisis y Propuestas sobre la Consolidación Bancaria.* Colombia, 2012
http://www.minhacienda.gov.co/portal/page/portal/HomeMinhacienda/regulacionfinanciera/Presentaciones/Presentaciones/7_ANIF-MULTIBAN-FINAL0606.pdf

Ingrid Lucía Muñoz Periñán MsC, Gonzalo Ulloa Villegas, *Artículo: Gobierno de TI - Estado del arte*, Revista S&T, Universidad Icesi, Cali, 2011 http://www.icesi.edu.co/biblioteca_digital/bitstream/10906/5568/1/Gobierno_de_TI.pdf

ISACA Manuel Ballester Ph D, *Gobierno de las TIC ISO/IEC 38500*. The ISACA Journal Online published, 2010, http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/jpdf1001-online-gobierno.pdf

IT Governance Institute, *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.2008,*
http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

IT Governance Institute, *Informe: Global Status Report on the Governance of Enterprise IT,* 2011,
http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf

ISACA - Centro de Conocimiento, *Caso de Estudio: Banco Supervielle S.A., Argentina*,
http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/COBIT-Caso-de-Estudio-Banco-Supervielle-SA-Argentina.aspx

ISACA - Centro de Conocimiento, Caso *de Estudio: Grupo Bancolombia Implements COBIT to Help Ensure Compliance and Improve Processes.*
http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Grupo-Bancolombia.aspx

ISACA Manuel Ballester, Ph.D, *Artículo: Gobierno de las TIC ISO/IEC 38500, Isaca Journal*, 2010,

Antonio Fernández Martínez, *Gobierno de las TI para universidades,* Universidad de Almería; Faraón Llorens Largo, Universidad de Alicante, 2011

ISACA. Steven De Haes, Ph.D., Wim Van Grembergen, Ph.D., *Artículo: Moving From IT Governance to Enterprise Governance of IT*, Isaca Journal, 2009.

12. ANEXOS

Anexo 1: Autoevaluación de nivel de madurez de Gobierno de TI propuesta. (ver archivo Anexo 1.doc)

Anexo 2: Guía para el diligenciamiento de la autoevaluación de nivel de madurez de Gobierno de TI propuesta. (ver archivo Anexo 2.doc)

Anexo 3: Formato de análisis de resultados (ver archivo Anexo 3.xls)

Anexo 4: Ejemplo de implementación de un requerimiento de TI del modelo propuesto (ver archivo Anexo 4.doc)

Anexo 5: Resumen Ejecutivo del modelo de Gobierno de TI en entidades bancarias de Colombia (ver archivo Anexo 5.doc)

Anexo 6: Encuesta en formato digital para el juicio de expertos (ver archivo Anexo 6.pdf y/o la encuesta en línea en https://docs.google.com/spreadsheet/viewform?formkey=dHJ0ZFNEcnRJeWlNRVVhV0owdHNNZGc6MQ)

Anexo 7: Verificación del cumplimiento de los 19 requerimientos en el Banco de Occidente. (Ver archivo Anexo 7.doc)

Anexo 8: Procedimiento documentado del Banco de Occidente DS01 – 01 Realizar análisis de la situación (ver archivo Anexo 8.doc)

ANEXO 1 - Autoevaluación de nivel de madurez de Gobierno de TI

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**		
3.2 Principio 1: **Responsabilidad**	Evaluar	En general, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y a la demanda de la información.	Los directores de TI establecer reglas y responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización.	Con respecto al suministro y a la demanda de la información, los usuarios dentro de la organización, entienden y aceptan las reglas y responsabilidades asignadas por TI.	Los directores de TI tienen alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encuentran documentados	Los directores de TI, evalúan la competencia (capacidad, autoridad, experiencia, etc.) de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a TI. (Los resultados de estas evaluaciones se encuentran documentados)		
	Dirigir	En la organización no se cuenta con proyectos de tecnología.	Los directores de TI, conocen pero no dirigen los proyectos de tecnología que se establecen en la alta gerencia de la organización (u otras áreas)	Los directores de TI dirigen todos los proyectos de tecnología de la organización. Los Directores de TI, cuentan con una autoridad parcial para solicitar información de otras dependencias.	Los directores de TI cuentan con un procedimiento documentado para ayudar a evaluar el cumplimiento de las metas de los proyectos de tecnología que dirigen.	Los directores de TI verifican que todos los proyectos de tecnología, estén alineadas con las responsabilidades asignadas al área de TI Los directores de TI exigen que se les entregue la información que necesitan para cumplir sus responsabilidades, incluidas las relativas a acciones y toma de decisiones.		
	Controlar	Los directores de TI tienen algún conocimiento acerca de gobierno de TI.	Los directores de TI conocen y supervisan que se hayan establecido los mecanismos adecuados para el gobierno de TI. Así mismo, cuenta con procedimientos y/o formatos que garanticen el mantenimiento de un modelo de gobierno de TI	Los directores de TI supervisan y/o auditan periódicamente el funcionamiento de los mecanismos implementados para el cumplimiento de gobierno de TI. (Dichas supervisiones se encuentran documentadas)	Los directores de TI supervisan y/o auditan periódicamente el desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI (por ejemplo, aquellas personas miembros de los comités, jefes, coordinadores, etc.)	También supervisan y/o auditan periódicamente que los individuos o grupos dentro de la organización entiendan y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de tecnología de la información.		

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**		
3.3 Principio 2: **Estrategia**	Evaluar	Los directores de TI, evalúan y brindan soporte a las necesidades actuales del negocio.	Los directores de TI estudian los avances de la tecnología de la información y los procesos del negocio con el fin de asegurarse de que TI brinda soporte a las necesidades futuras del negocio. (Los resultados de dicha evaluación se encuentran documentadas)	Los directores de TI evalúan y monitorean las actividades de TI, pero no aseguran que estas se mantengan (con el paso del tiempo) alineadas con los objetivos de la organización.	Los directores de TI cuentan con un plan estratégico de TI, el cual tiene en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización. (Los resultados de dicha evaluación y alineación con los objetivos de la organización se encuentran documentados)	Los directores de TI garantizan que sus procesos podrían ser (en cualquier momento), verificados, auditados y/o evaluados tal como se describe en normas nacionales e internacionales pertinentes.		
	Dirigir	Los usuarios conocen los procesos de TI de la Organización.	Los usuarios de la Organización están autorizados para presentar propuestas de innovación para TI	La Organización fomenta y estimula la presentación de propuestas de innovación de TI (Se tiene establecido un procedimiento, formato lineamiento, etc., que evidencie la forma como se fomenta dicha actividad)	Los directores de TI tienen establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI.	Los directores de TI fomentan y evalúan que estas propuestas permitan a la organización responder a oportunidades, nuevos retos, mejorar los procesos de la organización y/o estén alineadas con los objetivos del negocio.		
	Controlar	La Organización cuenta con una metodología para la ejecución de proyectos	Todos los proyectos de la organización (incluidos los de TI) son monitoreados para supervisar el progreso de los mismas	Los directores de TI conocen y supervisan el progreso de los proyectos de TI (Dicha supervisión se encuentra debidamente documentada)	Los directores de TI no solo supervisan el progreso del avance de los proyectos de TI, sino que se asegura que se estén cumpliendo los objetivos y beneficios planteados.	Los directores de TI, supervisan el uso de TI para asegurar que de ésta, se obtienen los beneficios previstos y que continúen alineados con los objetivos de la organización.		

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.4 Principio 3: **Adquisición**	Evaluar	Cualquier proceso dentro de la Organización puede solicitar un requerimiento para la adquisición tecnología.	Los directores de TI evalúan diferentes opciones al momento de adquirir tecnología, pero no son los únicos encargados de aprobar la propuesta.	Los directores de TI son los encargados y responsables adquirir tecnología para la organización	Los directores de TI aprueban la mejor propuesta que de cumplimiento a los requerimientos planteados, además que garantice el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.	Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento del equilibrio mencionado		
	Dirigir	Los directores de TI gestionan y mantienen los activos de TI (sistemas e infraestructura)	Los directores de TI adquieren tecnología de forma correcta, clara y transparente, teniendo en cuenta los requerimientos planteados	Los directores de TI verifican que se incluya la respectiva documentación (instructivos, manuales, etc.) de la tecnología adquirida, a la vez que aseguran que el las tecnologías adquiridas cumplen con las capacidades requeridas.	Los directores de TI verifican el cumplimiento de los acuerdos de nivel de servicio (tanto internos como externos)	Los directores de TI gestionan los acuerdos de nivel de servicio (tanto internos como externos) de modo que aseguran que estos soportan las necesidades del negocio. (Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento de los acuerdos de nivel de servicio)		
	Controlar	La organización cuenta con mecanismos para supervisar que las inversiones, en términos generales, están acordes con las requeridas.	Los directores de TI supervisan (auditan) que las inversiones en TI, proporcionan las capacidades requeridas para las cuales fueron adquiridas.	Se tienen algún tipo de procedimiento y/o formato que permita evidenciar el resultado de la supervisión realizada en las inversiones de TI	Los directores de TI tienen contacto con los proveedores de tecnología solo en ocasiones puntuales	Los directores de TI tienen contacto y/o alianzas estratégicas con los todos los proveedores de tecnología.		

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**		
3.5 Principio 4: **Desempeño**	Evaluar	Los directores de TI evalúan que la tecnología de la información apoya los procesos de negocio con la habilidad y capacidad requeridas.	Los directores de TI tienen políticas dirigidas hacia la continuidad de la operación normal del negocio y del tratamiento de los riesgos asociados con el uso de la tecnología de la información.	Los directores de TI evalúan periódicamente los riesgos que se originan en las actividades de la tecnología de la información para la continuidad de la operación de los negocios. Además evalúan los riesgos para la integridad de la información y protección de los activos de tecnología de la información, incluyendo la propiedad intelectual y memoria organizacional asociadas.	Los directores de TI garantizan que la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los acuerdos de niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio, soportando las metas del negocio.	Los directores de TI evalúan con regularidad la eficacia y el desempeño del sistema organización para el gobierno TI (Se cuenta con un procedimiento documentado y/o formatos que evidencia el cumplimiento de esta evaluación)		
	Dirigir	La Organización cuenta con un mecanismo de asignación de recursos para sus diferentes procesos.	Los directores de TI tienen asegurada la asignación de los recursos suficientes para el ejercicio de sus funciones	Los directores de TI garantizan que los recursos que le son asignados, satisfacen las necesidades de la organización.	La información que soporta al negocio, se encuentra disponible cuando se requiere, con datos correctos y actualizados y están protegidos contra pérdida o mal uso.	Los directores de Ti cuentan con mecanismos y/o procedimientos que garantizan la calidad y disponibilidad de la información		
	Controlar	Los directores de TI supervisan la “vida útil” de la tecnología de la información da soporte al negocio.	Los directores de TI cuentan con mecanismos documentados que permiten prever cuando la tecnología de la información, se acerca al final de su “vida útil”	Se tiene establecido un cronograma, el cual se encuentra supervisado, de renovación de la tecnología de la información, de igual forma se tiene asegurado los recursos para dicha renovación.	Los directores de TI poseen, controlan y supervisan el presupuesto asignado por la Organización para la inversión de TI	Los directores de TI dan prioridad a las inversiones que impacten directamente los objetivos del negocio.		

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**		
3.6 Principio 5: **Conformidad**	Evaluar	Los directores de TI garantizan que le tecnología de la Información cumple con todos lineamientos establecidos por la Organización	De igual manera, los directores de TI garantizan que la tecnología de la Información de la Organización cumple con todas las leyes y los reglamentos obligatorios.	La Organización cuenta con políticas y prácticas claras, las cuales se encuentran documentadas y detallan los requerimientos legales de TI que rigen a la Organización.	Los directores de TI supervisan periódicamente que se cumplen dichas prácticas y políticas expresadas por la Organización.	Los directores de TI evalúan periódicamente que las tecnologías de la información satisfacen las obligaciones reglamentarias, legislativas, de ley, contractuales, las políticas internas, las normas y las directrices profesionales.		
	Dirigir	La Organización garantiza que se cumple con las obligaciones legales pertinentes.	Los directores de TI colaboran con la Alta Gerencia a establecer mecanismos regulares y rutinarios para garantizar que el uso de la tecnología de la información cumple con las obligaciones pertinentes (reglamentarias, legislativas, de ley, contractuales), las normas y las directrices.	Los directores de TI supervisan periódicamente que se cumpla con las obligaciones internas y externas en el uso de la tecnología de la información.	Los resultados de estas supervisiones se encuentran documentadas y son analizadas periódicamente en busca de la mejora continua.	La organización cuenta con directrices claras que regulan el comportamiento de los usuarios con relación a las TI de la Organización.		
	Controlar	Los directores de TI supervisan la conformidad y el cumplimiento de las obligaciones de TI a través de prácticas adecuadas de auditoría.	Dichas auditorias se encuentran debidamente programadas, son oportunas, exhaustivas y adecuadas y evalúan el grado de satisfacción de las tecnologías de la información con los objetivos, políticas y/o directrices de la Organización	Las auditorias incluyen la supervisión de los activos de TI y los datos (información) de la Organización.	También se incluye la verificación del cumplimiento de todas las obligaciones legales pertinentes y las suscritas con clientes y proveedores	Las auditorias también supervisan las actividades tendientes a la preservación de la información privada de la Organización		

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.7 Principio 6: **Comportamientos Humanos**	Evaluar	Los usuarios de la Organización tienen un conocimiento básico de las tecnologías que tienen disponibles	Los directores de TI ayudan a que los usuarios entiendan y aprovechen la tecnología que tienen disponible, de modo que estos aumenten su desempeño personal y el de los sistemas de información.	Los directores de TI tienen documentadas las interacciones (relaciones) existentes entre los usuarios y las tecnologías de la información disponibles en la Organización.	La Organización conoce acerca del comportamiento humano y sabe que esto incluye: La cultura, las necesidades, y las aspiraciones de los usuarios, bien sea como individuos o como grupos. Además, los directores de TI son conscientes (y lo documentan como un riesgo) que estos comportamientos humanos pueden afectar el rendimiento las tecnologías de la información	Las políticas, prácticas y decisiones con respecto a TI demuestran respeto por el comportamiento humano.		
	Dirigir	Los directores de TI dirigen de tal manera que las actividades de TI sean consistentes con el comportamiento humano identificado.	Los directores de TI cuentan con mecanismos que permiten que cualquier persona en cualquier momento pueda identificar y reportar riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información	La Organización cuenta con políticas y/o procedimientos que permiten escalar los riegos reportados hasta las personas correspondientes a cargo de la toma de decisiones.	Todos los reportes acerca de los riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información, se encuentran debidamente documentados	Los directores de TI analizan periódicamente todos los reportes generados en busca de mejoras para la Organización		
	Controlar	La Organización supervisa periódicamente el nivel de satisfacción del comportamiento humano. (Por medio de encuestas de clima laboral, por ejemplo).	La Organización analiza los resultados de la supervisión de los comportamientos humanos y brinda la atención adecuada que se requiera para mejorar nivel de satisfacción.	Los directores de TI supervisan periódicamente cómo los comportamientos humanos afectan el rendimiento de las tecnologías de la información.	La Organización supervisa periódicamente que las políticas, prácticas y decisiones de TI demuestren respeto por el comportamiento humano	Los directores de TI supervisan las prácticas laborales de los usuarios, con el fin de asegurar que sean consistentes del uso adecuado de la tecnología de información.		

ANEXO 2

Guía para el diligenciamiento de la Encuesta

"Autoevaluación de nivel de madurez de Gobierno de TI"

La encuesta es una herramienta de diagnóstico cuyo objetivo es determinar el estado de madurez de la implementación de Gobierno de TI en los Bancos de Colombia, con el fin de generar un modelo de implementación acorde a las necesidades de las organizaciones que permita una adecuada implementación del mismo. A continuación se detalla una breve explicación de las partes que conforman la encuesta:

Principio 1 – Responsabilidad: Este apartado refiere a que los individuos o grupos dentro de la organización entienden y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de Tecnología de la información. Aquellos con responsabilidad de las acciones también tienen la autoridad para ejecutar tales acciones.

Principio 2 – Estrategia: Con este apartado la estrategia de negocios de la organización toma en consideración las capacidades actuales y futuras de la tecnología de la información; los planes estratégicos para la Tecnología de la Información satisfacen las necesidades actuales y continuas de la estrategia de negocios de la organización.

Principio 3 – Adquisición: En este apartado las adquisiciones de Tecnología de la información se hacen por razones válidas, con base en el análisis adecuado y continuo, con una toma de decisiones clara y transparente. Existe el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.

Principio 4 – Desempeño: En este apartado la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, niveles de servicio y calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio.

Principio 5 – Conformidad: En este apartado la tecnología de la Información cumple con todas las leyes y los reglamentos obligatorios. Las políticas y las prácticas están definidas, implementadas y se hacen cumplir.

Principio 6 – Comportamiento Humano: Con este apartado las políticas, prácticas y decisiones con respecto a la Tecnología de la Información demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y evolutivas de todas las "personas en el proceso".

Además, por cada principio se encuentran 3 tareas que permite a los directores controlar la Tecnología de la Información:

a. **Evaluar** el uso actual y futuro de la tecnología de la información

b. **Dirigir** la preparación e implantación de los planes y las políticas para garantizar que el uso de la TI satisface los objetivos del negocio.
c. **Controlar** la conformidad con las políticas y el desempeño frente a los planes.

A continuación se detalla el glosario que debe tenerse en cuenta al momento de realizar la encuesta:

GOBIERNO CORPORATIVO: Es el sistema mediante el cual se dirigen y controlan las organizaciones.

GOBIERNO CORPORATIVO DE TI: Es el sistema mediante el cual se dirige y controla el uso actual y futuro de la tecnología de la información. El Gobierno Corporativo de TI involucra la evaluación y dirección del uso de dicha tecnología para dar soporte a la organización y la supervisión de este uso para alcanzar los planes. Éste incluye la estrategia y políticas para utilizar la tecnología de la información dentro de una organización.

DIRECTOR: Miembro del organismo de gobierno más alto de la organización. Se incluyen dueños, miembros de la junta, socios, ejecutivos de alto nivel o similares y funcionarios autorizados por la legislación o los reglamentos.

TECNOLOGÍA DE LA INFORMACIÓN: Son aquellos recursos que se requieren para adquirir procesar, almacenar y divulgar información. Este término también incluye "Tecnología de la Comunicación (TC)" y el término combinado "Tecnología de la Información y la Comunicación (TIC)".

GESTIÓN: Es el sistema de controles y procesos que se requieren para lograr los objetivos estratégicos establecidos por el organismo de gobierno de una organización. La gestión está sujeta a las directrices y la supervisión de la política establecidas a través del gobierno corporativo.

POLITICA: Son las declaraciones claras medibles de la orientación y comportamiento preferidos para condicionar las decisiones tomadas dentro de una organización.

RECURSOS: Son las personas, procedimientos, software, información, equipo, insumos, infraestructura, capital y fondos de operación, así como el tiempo.

RIESGO: Es la combinación de la probabilidad de un evento y su consecuencia.

GESTIÓN DE RIESGOS: Son aquellas actividades coordinadas para dirigir y controlar una organización respecto a los riesgos.

ESTRATEGÍA: Plan global de desarrollo de una organización que describe el uso eficaz de los recursos que dan soporte a las actividades futuras de la organización. La estrategia implica el establecimiento de objetivos y la propuesta de iniciativas para la acción.

IMPORTANTE

- Tenga en cuenta que la encuesta es un mecanismo para identificar el nivel de madurez de Gobierno de TI en su Organización, por lo tanto recomendamos que sea muy objetivo con sus respuestas con el fin de obtener información relevante y real.
- Recuerde que para que su Organización se encuentre en nivel de madurez debe cumplir totalmente con las prácticas de los niveles inmediatamente anteriores.
- Establezca el nivel deseado al que esperaría llegar su Organización por cada uno de los principios de la encuesta.

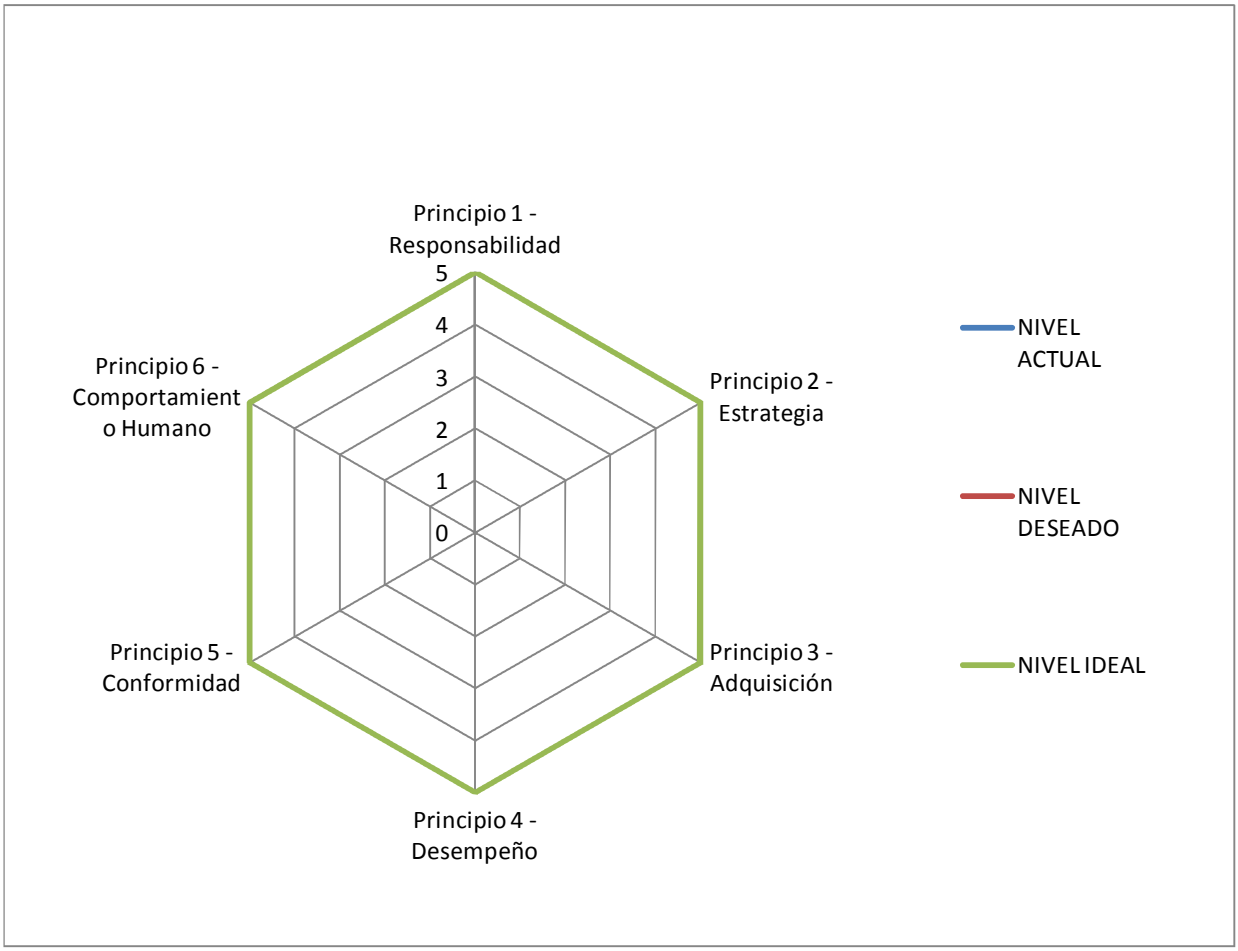
ANEXO 3

Formato de Análisis de Resultados

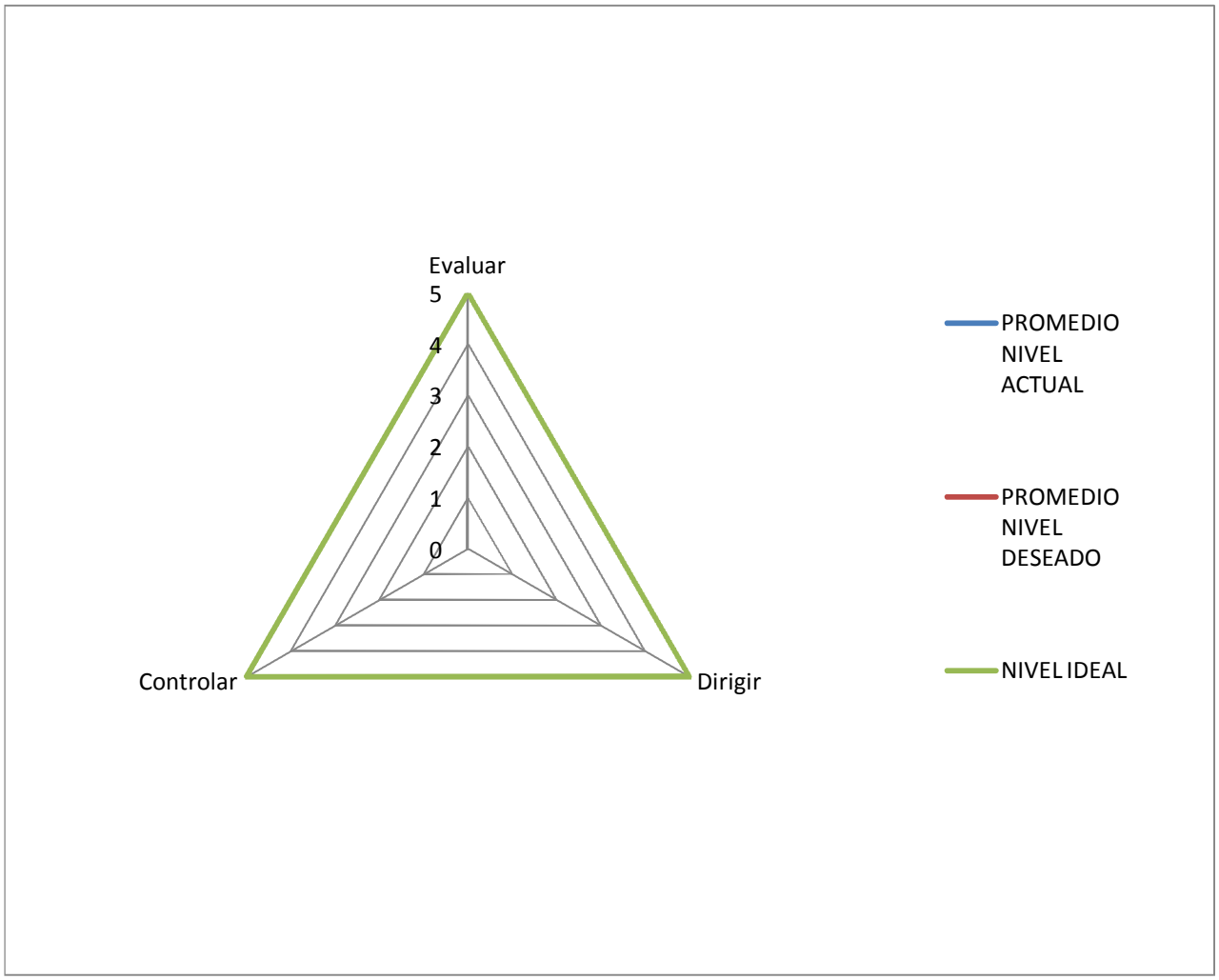
Nivel de madurez de Gobierno de TI en el sector Bancario - Nivel Actual			
Principios		**Calificación**	**Total**
Principio 1 - Responsabilidad	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 2 - Estrategia	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 3 - Adquisición	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 4 - Desempeño	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 5 - Conformidad	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 6 - Comportamiento Humano	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	

Nivel de madurez de Gobierno de TI en el sector Bancario - Nivel Deseado			
Principios		**Calificación**	**Promedio Total**
Principio 1 - Responsabilidad	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 2 - Estrategia	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 3 - Adquisición	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 4 - Desempeño	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 5 - Conformidad	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	
Principio 6 - Comportamiento Humano	Evaluar	0	0,0
	Dirigir	0	
	Controlar	0	

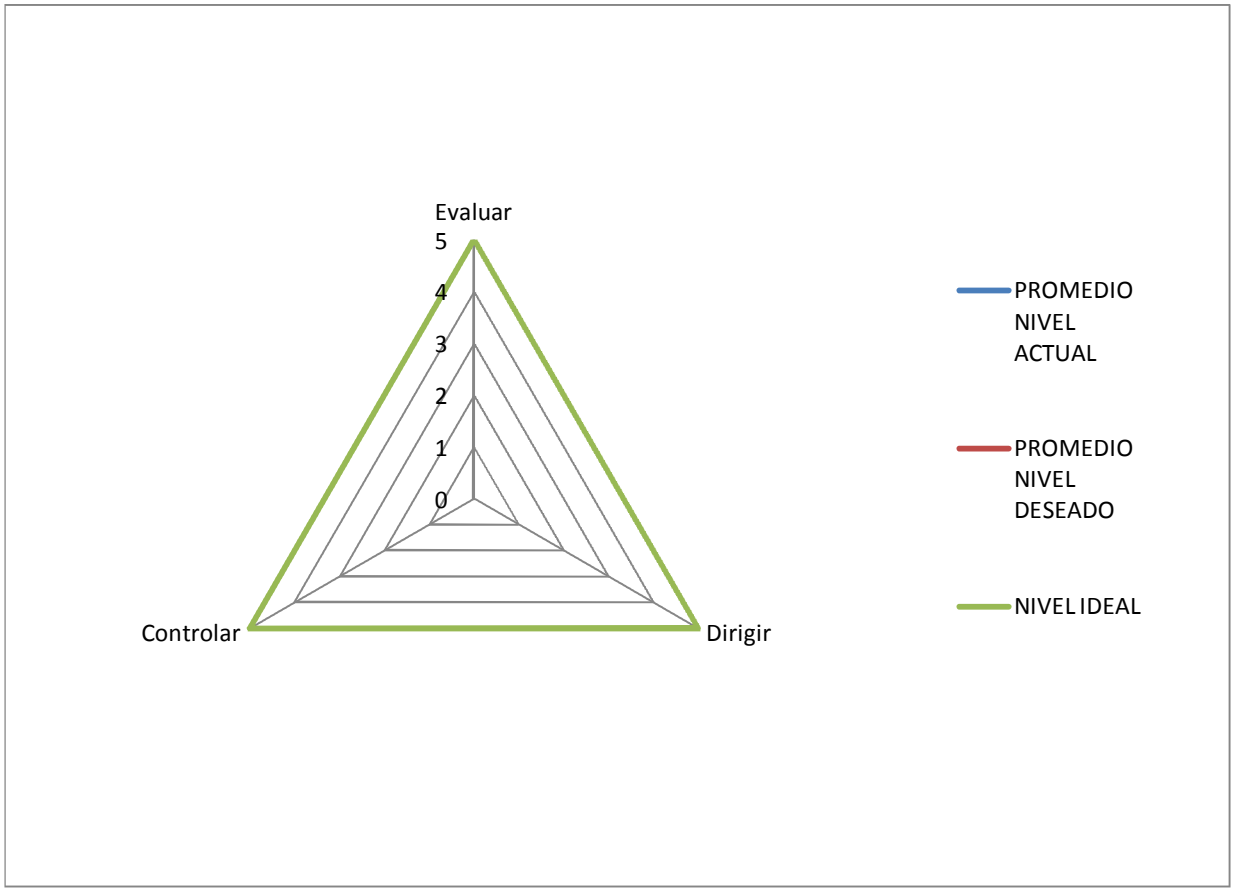
Nivel de madurez de Gobierno de TI en el sector Bancario			
PRINCIPIOS	**NIVEL ACTUAL**	**NIVEL DESEADO**	**NIVEL IDEAL**
Principio 1 - Responsabilidad	0	0	5
Principio 2 - Estrategia	0	0	5
Principio 3 - Adquisición	0	0	5
Principio 4 - Desempeño	0	0	5
Principio 5 - Conformidad	0	0	5
Principio 6 - Comportamiento Humano	0	0	5



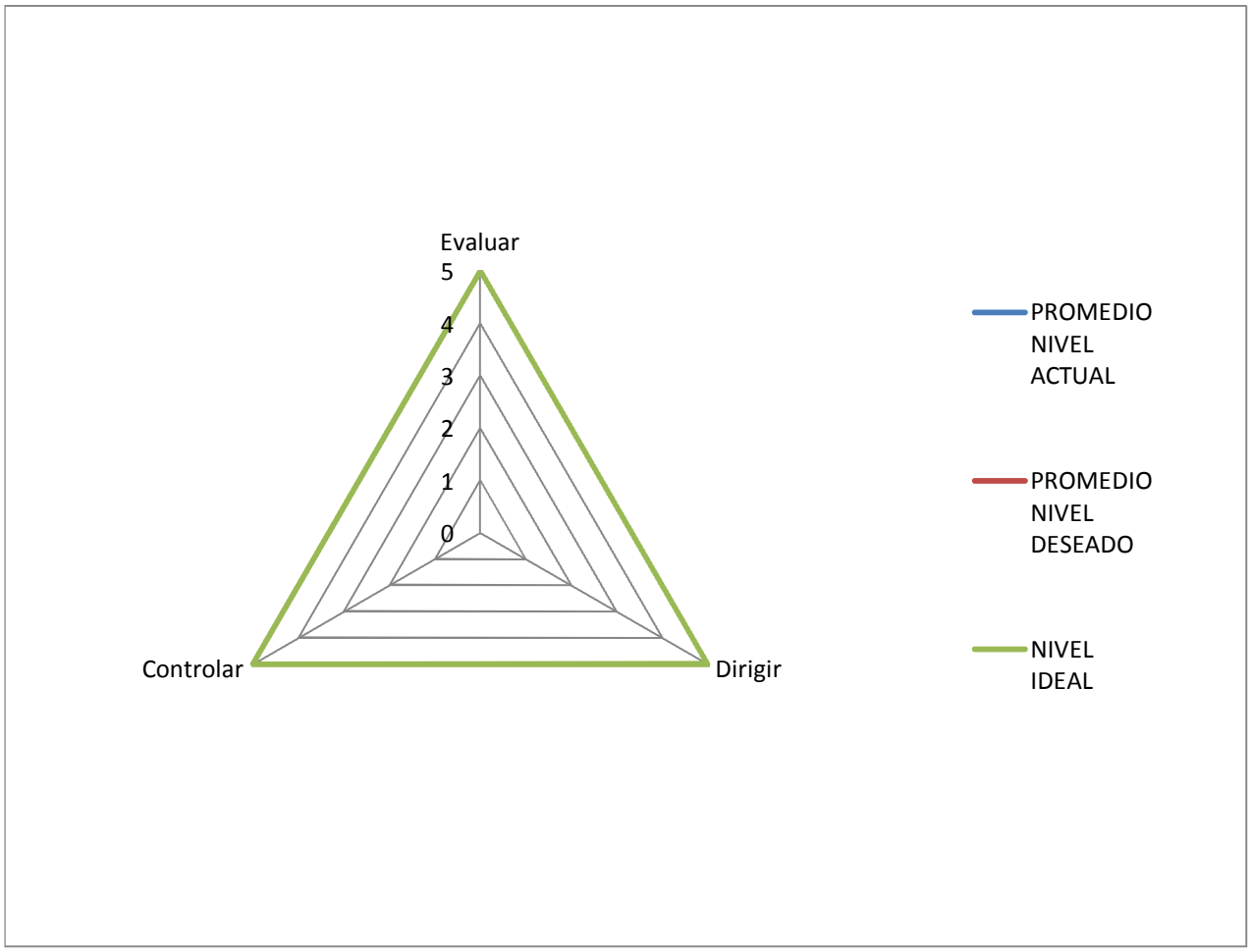
Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 1 - Responsabilidad			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



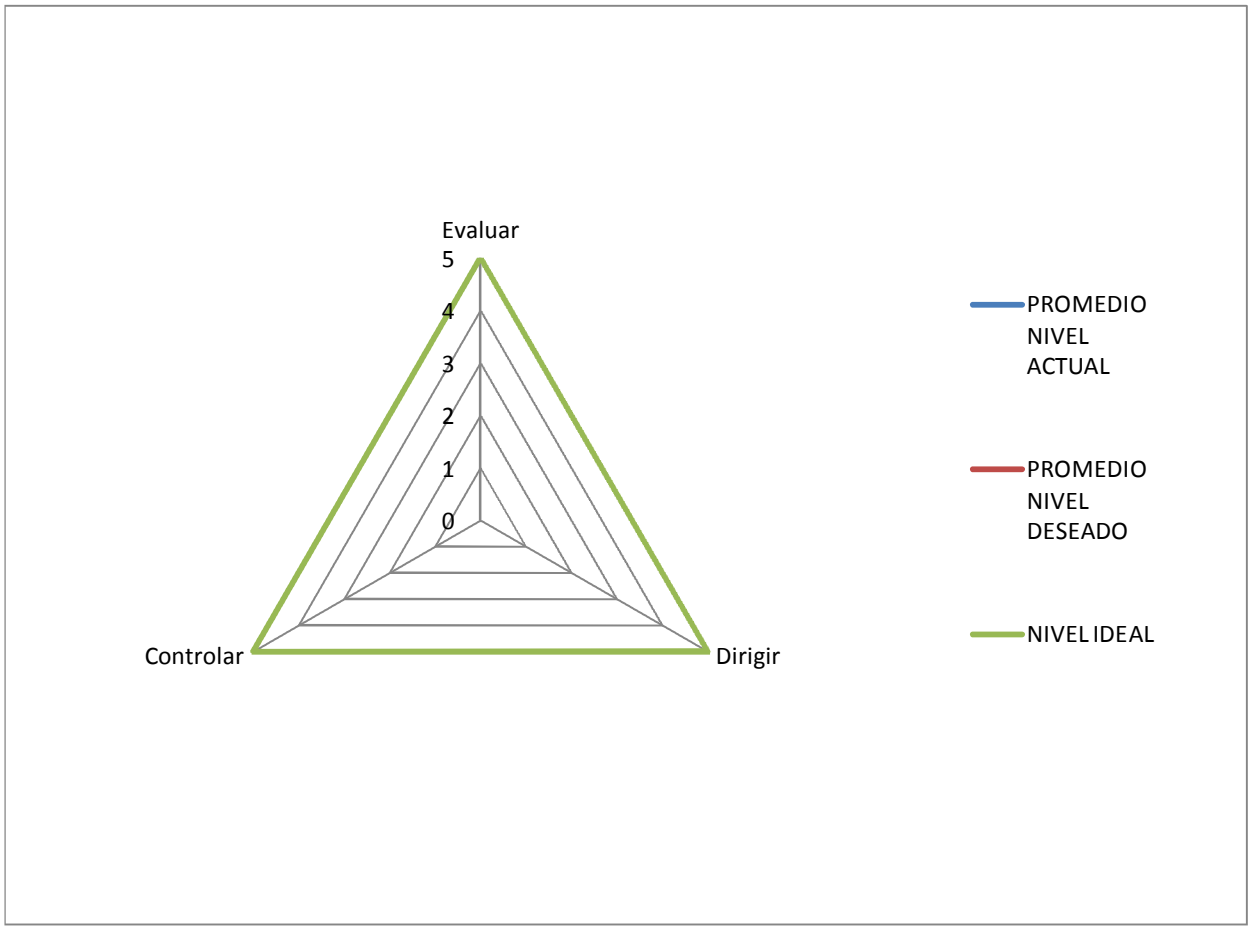
Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 2 - Estrategia			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



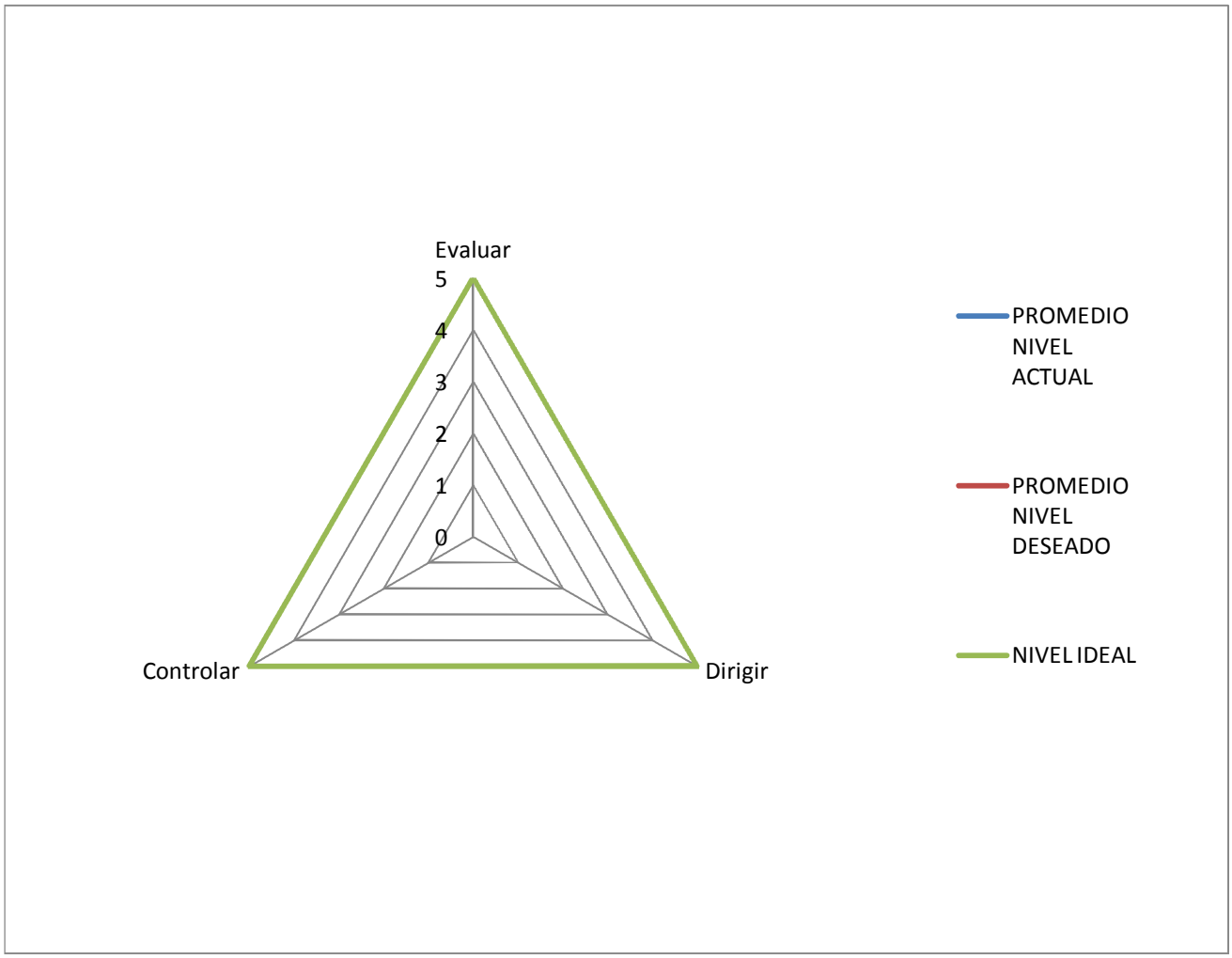
Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 3 - Adquisición			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



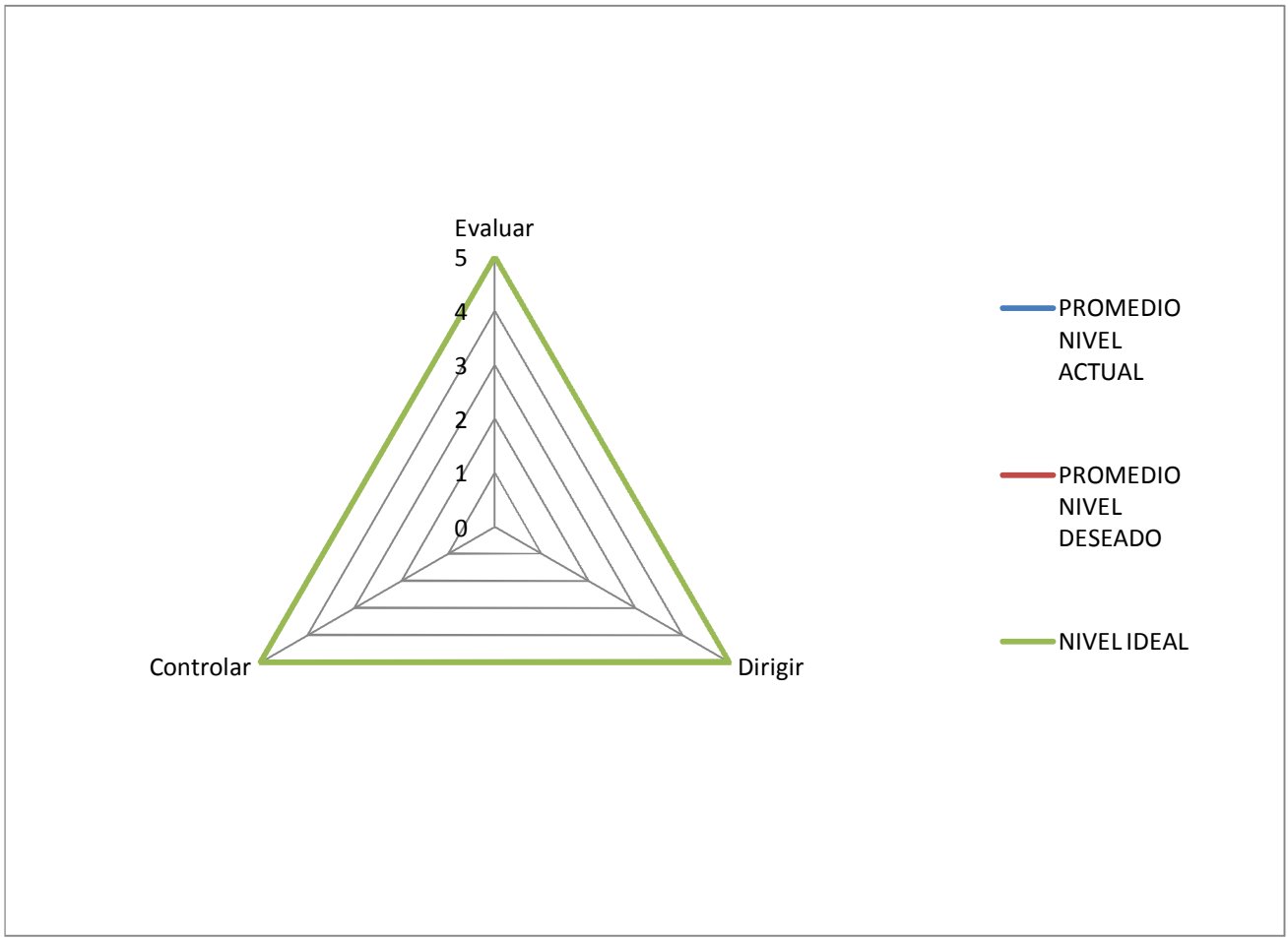
Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 4 - Desempeño			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 5 - Conformidad			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 6 - Comportamiento Humano			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	0	0	5
Dirigir	0	0	5
Controlar	0	0	5



ANEXO 4

Ejemplo de implementación de un requerimiento de TI del modelo propuesto

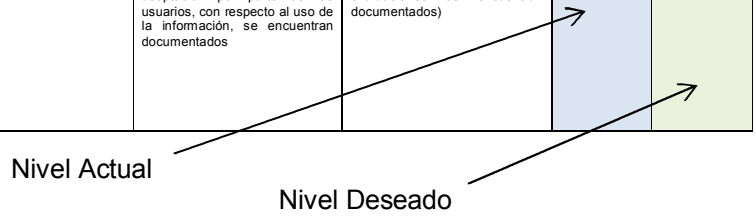
Fase 1: Obtener el compromiso de la alta dirección.

Documento con el apoyo y compromiso de la alta dirección en la implementación del proyecto	Una vez presentado el proyecto a la alta dirección, se debe crear un documento, en el cual se exprese claramente el apoyo y compromiso por parte de esta al proyecto. Debe ser un documento claro que no de espacio a malas interpretaciones
Documento con el plan de implementación, los roles y responsables de cada actividad y el cronograma de implementación del proyecto	Utilizando cualquier metodología de implementación de proyectos, se crea un documento en el cual se identifiquen claramente los objetivos a alcanzar, los roles y responsables para el proyecto, donde se identifiquen claramente sus actividades y responsabilidades; además se genera un cronograma para la implementación del proyecto

Fase 2: Determinar el estado actual
Fase 3 Establecer el estado futuro deseado.

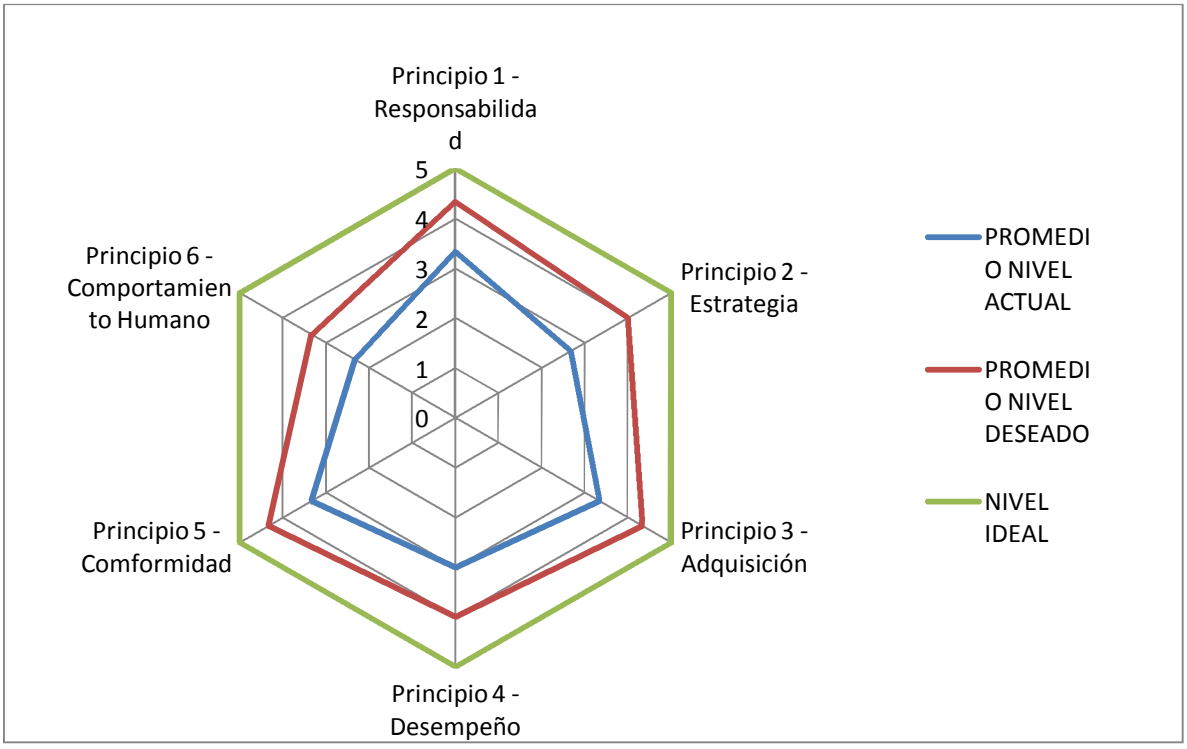
Una vez diligenciada la Autoevaluación de nivel de madurez de Gobierno de TI (anexo 1) se trasladan los resultados al Formato de Análisis de Resultados (anexo 3).

Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**		
En general, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y a la demanda de la información.	Los directores de TI establecer reglas y responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización.	Con respecto al suministro y a la demanda de la información, los usuarios dentro de la organización, entienden y aceptan las reglas y responsabilidades asignadas por TI.	Los directores de TI tienen alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encuentran documentados	Los directores de TI, evalúan la competencia (capacidad, autoridad, experiencia, etc.) de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a TI. (Los resultados de estas evaluaciones se encuentran documentados)		

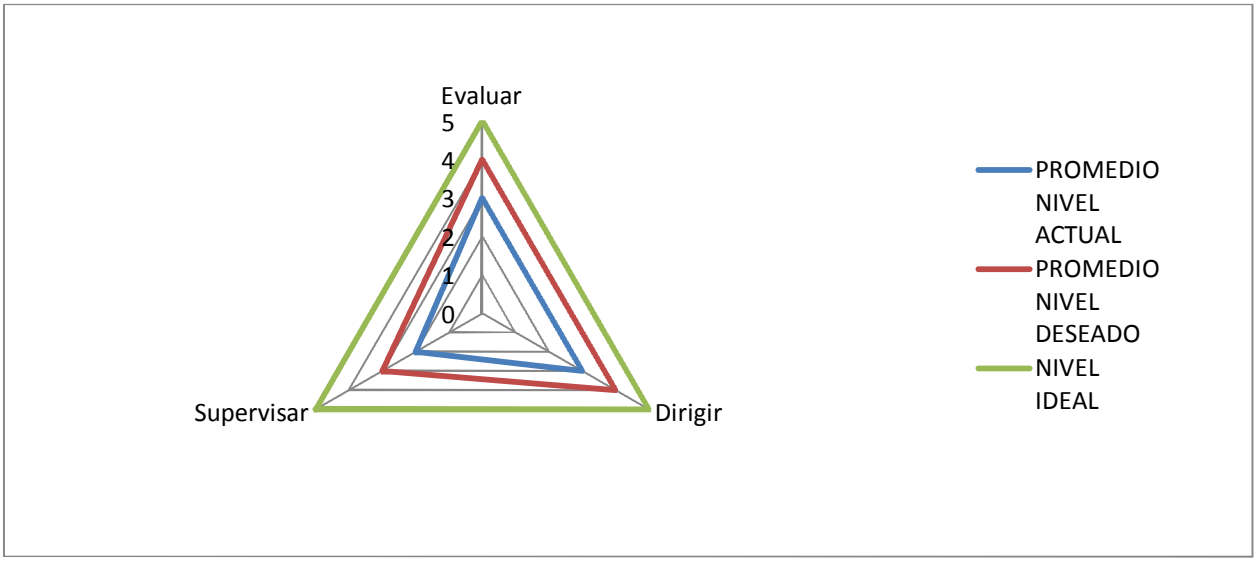


Nivel de madurez de Gobierno de TI en el sector Bancario - Nivel Actual			
Principios		**Calificación**	**Total**
Principio 1 - Responsabilidad	Evaluar	4	3,3
	Dirigir	3	
	Supervisar	3	
Principio 2 - Estrategia	Evaluar	3	2,7
	Dirigir	3	
	Supervisar	2	
Principio 3 - Adquisición	Evaluar	4	3,3
	Dirigir	3	
	Supervisar	3	
Principio 4 - Desempeño	Evaluar	3	3,0
	Dirigir	4	
	Supervisar	2	
Principio 5 - Conformidad	Evaluar	3	3,3
	Dirigir	4	
	Supervisar	3	
Principio 6 - Comportamiento Humano	Evaluar	2	2,3
	Dirigir	3	
	Supervisar	2	

Nivel de madurez de Gobierno de TI en el sector Bancario - Nivel Deseado			
Principios		**Calificación**	**Promedio Total**
Principio 1 - Responsabilidad	Evaluar	5	4,3
	Dirigir	4	
	Supervisar	4	
Principio 2 - Estrategia	Evaluar	4	3,7
	Dirigir	4	
	Supervisar	3	
Principio 3 - Adquisición	Evaluar	5	4,3
	Dirigir	4	
	Supervisar	4	
Principio 4 - Desempeño	Evaluar	4	4,0
	Dirigir	5	
	Supervisar	3	
Principio 5 - Conformidad	Evaluar	4	4,3
	Dirigir	5	
	Supervisar	4	
Principio 6 - Comportamiento Humano	Evaluar	3	3,3
	Dirigir	4	
	Supervisar	3	



Nivel de madurez de Gobierno de TI en el sector Bancario PRINCIPIO 2 - Estrategia			
PRINCIPIOS	**PROMEDIO NIVEL ACTUAL**	**PROMEDIO NIVEL DESEADO**	**NIVEL IDEAL**
Evaluar	3	4	5
Dirigir	3	4	5
Supervisar	2	3	5



Fase 4: Identificar las brechas

Documento con las brechas existentes que se desean cerrar	Para este ejemplo, la única brecha que se desea cerrar es la siguiente: **Principio 2 - Estrategia** Nivel actual: 3 Los directores de TI evalúan y monitorean las actividades de TI, pero no aseguran que estas se mantengan (con el paso del tiempo) alineadas con los objetivos de la organización. Nivel Deseado: 4 Los directores de TI cuentan con un plan estratégico de TI, el cual tiene en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización.
Documento con las acciones necesarias que ayuden a cerrar las brechas existentes	Se genera un documento con las acciones que se requieran y que sirvan de ayuda para cerrar esta brecha: Una ventaja de una planeación estratégica de

	TI es que ayuda a gestionar y dirigir todos los recursos de TI, por tal motivo sería ideal contar con un presupuesto claro para TI Otra ventaja de la planeación estratégica es que debe estar alineada con la estrategia y prioridades del negocio, por ende se hace necesario que TI cuente con las estrategias y prioridades actuales del negocio Además un plan estratégico ayuda a evaluar el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, por tal motivo se debe contar con una evaluación actualizada del desempeño, la capacidad y los recursos humanos disponibles

Fase 5: Definir el plan de implementación

Documentos con las brechas que serán cerradas y cuales quedarán planteadas para un futuro	Por motivos del ejemplo la única brecha que será cerrada es la de contar con un Plan Estratégico de TI.
Documento con las actividades de control necesarias para cerrar las brechas	Las actividades de control necesarias para cerrar esta brecha son tomadas del modelo de Gobierno de TI para entidades bancarias en Colombia, en el capítulo 7.2 Estrategia, 7.2.1 RQ01 - Plan estratégico de tecnología: Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades. Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de

	obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI. Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y comisionar los proyectos requeridos al momento de lanzar el programa.
Documento con los proyectos a implementar, con sus responsables, metas, recursos y cronograma, además del orden de implementación de los proyectos	De cada de las actividades de control detalladas en el paso anterior se debe generar uno o varios proyectos los cuales deben contar con su respectivos responsables, metas recursos y cronograma. Además se debe identificar en qué orden serán implementados

Fase 6: Desarrollar el plan de implementación

Listado con los recursos necesarios para la implementación de cada proyecto	Para cada proyecto se debe gestionar los recursos necesarios para garantizar la implementación de cada proyecto. Dichos recursos deben quedar plasmados en un documento los cuales deben contar con la aprobación de la alta gerencia
Listado con las pruebas realizadas (ejecutadas y aceptadas) a las actividades implementadas	De cada una de las actividades se les debe realizar pruebas (o indicadores) para determinar que las actividades de control (proyectos) estén dando los

	resultados esperados: El porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio El porcentaje de proyectos TI en el portafolio de proyectos que se pueden rastrear hacia el plan táctico de TI
Cierre formal del proyecto, con la respectiva aprobación del responsable del proyecto y el responsable de TI del banco	A cada proyecto terminado se le debe realizar un cierre formal, el cual debe estar en un documento y debe contar con la firmas de aprobación del responsable del proyecto y el responsable de TI del banco

Fase 7: Monitorear y controlar el desempeño de la implementación

Documento con los mecanismos creados para validar los proyectos implementados y los responsables de llevar a cabo el monitoreo	Para verificar si en el tiempo los proyectos ejecutados están dando los resultados esperados, se implementan mecanismos de control que ayuden a confirmar los resultados esperados. Uno de estos mecanismos podría ser el de realizar de nuevo la autoevaluación de nivel de madurez de gobierno de TI y validar si con los proyectos implementados se alcanzó el nivel deseado.
Documento con el resultado del monitoreo efectuado	El resultado de las verificaciones del paso anterior se deben documentar y presentar al responsable de TI y a la alta gerencia para que se tomen las medidas que se consideren necesarias.

ANEXO 5

RESUMEN EJECUTIVO

Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia

PROYECTO DE GRADO DE MAESTRÍA

Ing. María Helena Correa Correa
Ing. Breyner Alexander Parra Rojas

Asesor
Ing. Hernando Peña Villamil
Magister en Teleinformática
Certificado PMP, ITIL, COBIT, ISO27001

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

RESUMEN

Desde la fundación del primer banco privado en Colombia en 1870 (el Banco de Bogotá)[1], el sector bancario colombiano ha tenido un crecimiento importante, no solo financieramente, sino desde el punto de vista tecnológico. En la actualidad, este sector está regido por diferentes leyes y decretos. El principal, el decreto 663 de 1993[2], por medio del cual reglamenta y define que son Establecimientos Bancarios y regula el tipo de operaciones autorizadas; además marca una diferencia entre entidades bancarias y otros tipos de entidades y/o corporaciones financieras. De igual forma, el decreto 4327 de 2005[3] faculta a la Superintendencia Financiera como ente de control del sector bancario, con el fin de hacer preservar la estabilidad, seguridad y confianza, apoyado en el cumplimiento de la ley y sancionando a aquellas entidades que incurran en faltas.

Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo, y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros, sin embargo, el problema es que hasta ahora, no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

A nivel Latinoamérica, el Banco Supervielle S. A. uno de los principales Bancos privados de la Republica Argentina lanzó en el año 2009 un proyecto denominado "Gobierno de TI", donde la Gerencia General del Banco era el patrocinador "Sponsor" y la Gerencia Coordinadora de TI y sus Gerentes los líderes del mismo[4] Sin embargo, no es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.

Por tal motivo, el propósito del presente documento es proponer un modelo de Gobierno de TI, con su respectiva guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector.

---

[1] **Orígenes de la banca comercial en Colombia**. Banco de la Republica. http://www.banrepcultural.org/blaavirtual/revistas/credencial/marzo2001/135origenes.htm

[2] **Decreto 633 de 1993**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

[3] **Decreto 4327 de 2005**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/dec4327-05.doc

[4] **Caso de Estudio: Banco Supervielle S.A.**, Argentina. ISACA. http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/COBIT-Caso-de-Estudio-Banco-Supervielle-SA-Argentina.aspx

1. INTRODUCCIÓN

1.1 Contexto del Trabajo

1.1.1 Establecimientos Bancarios

Son establecimientos bancarios las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito.

Los establecimientos bancarios se dividen en dos tipos:

Banco comercial: Las palabras banco comercial significan un establecimiento que hace el negocio de recibir fondos de otros en depósito general y de usar éstos, junto con su propio capital, para prestarlo y comprar o descontar pagarés, giros o letras de cambio.

Banco hipotecario: Las palabras banco hipotecario significan un establecimiento que hace el negocio de prestar dinero garantizado con propiedades raíces, que debe cubrirse por medio de pagos periódicos y para emitir cédulas de inversión[5].

1.1.2 Entidades de Supervisión

Es importante saber que todas las entidades que hacen parte del sistema financiero están sujetas a la regulación y supervisión por parte de las autoridades de intervención: el Congreso de la República, el Ministerio de Hacienda y Crédito Público y la Superintendencia Financiera. Así mismo, estas son las encargadas de crear los marcos normativos y de velar porque los recursos de las personas, empresas y el gobierno se encuentren seguros en manos de las diferentes instituciones. Además, la Superintendencia Financiera también tiene funciones de inspección, vigilancia y control sobre las entidades[6].

1.1.3 Gobierno de TI

Gobierno de TI (Tecnologías de Información) es la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos,

---

[5] **Decreto 633 de 1993**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

[6] **Información al consumidor financiero.** ASOBANCARIA. http://www.asobancaria.com/portal/page/portal/Asobancaria/info_consumidor/sistema_financiero_y_banca/

agregando valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre inversiones en TI. El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas. Muchas organizaciones cuentan con diferentes marcos de Gestión de TI (CobiT, Itil, etc.) sin embargo, cuando estos marcos de trabajo y estándares son utilizados colectivamente, se vuelven muy confusos y obstruyen el propósito principal del Gobierno de TI[7]

1.2 Planteamiento del Problema

Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo; y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros; el problema es que no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

1.3 Objetivos

1.3.1 Objetivo General.

Proponer un modelo de Gobierno de TI y una guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector, teniendo en cuenta que no sería útil aplicar al pie de la letra modelos de Gobierno de otros sectores colombianos, ya que la infraestructura, tecnología, modelo de negocio y sobre todo, legislación, es diferente. Tampoco es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.

1.3.2 Objetivos Específicos:

1. Realizar un análisis del contexto del sector bancario en Colombia, incluyendo las principales disposiciones legales que los rigen.

---

[7] **Artículo: Gobierno de TI - Estado del arte**. Ingrid Lucía Muñoz Periñán MsC, Gonzalo Ulloa Villegas. Revista S&T, Universidad Icesi. http://www.icesi.edu.co/biblioteca_digital/bitstream/10906/5568/1/Gobierno_de_TI.pdf

2. Realizar un análisis de los marcos para Gobierno de TI existentes y determinar cuáles son los más apropiados para la creación del modelo a implementar.

3. Crear una autoevaluación de nivel de madurez de Gobierno de TI

4. Desarrollar un modelo de Gobierno de TI, basado en los marcos seleccionados.

5. Crear una guía de implementación para el modelo de Gobierno de TI desarrollado.

6. Validar el modelo y la metodología por un grupo de expertos, a partir de una rúbrica que permita su evaluación.

2. MODELO DE GOBIERNO DE TI PROPUESTO

2.1 Contexto del Modelo

Las entidades bancarias de Colombia se encuentran regidas por la Circular 014 del 2009; la cual define las **Normas de Control Interno para la Gestión de la Tecnología.**

En dicha circular se establece que las entidades bancarias deberán diseñar un Sistema de Control Interno (SCI) para la gestión de la tecnología, que responda a las políticas, necesidades y expectativas de la entidad y a las exigencias normativas, **con el propósito de contribuir al logro de los objetivos institucionales**[8]

El SIC obliga a los responsables de TI de las Entidades Bancarias a contar con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir 19 requerimientos:

1. Plan estratégico de tecnología.
2. Infraestructura de tecnología.
3. Relaciones con proveedores.
4. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
5. Administración de proyectos de sistemas.

---

[8] **Circular Externa 014 del 2009**. Superintendencia Financiera de Colombia. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc

6. Administración de la calidad.
7. Adquisición de tecnología.
8. Adquisición y mantenimiento de software de aplicación.
9. Instalación y acreditación de sistemas.
10. Administración de cambios.
11. Administración de servicios con terceros.
12. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
13. Continuidad del negocio.
14. Seguridad de los sistemas.
15. Educación y entrenamiento de usuarios.
16. Administración de los datos.
17. Administración de instalaciones.
18. Administración de operaciones de tecnología.
19. Gestión de la Documentación.

Por tal motivo y para dar cumplimiento a la ley, las entidades bancarias cuentan con un **Sistema de Control Interno para la gestión de tecnología**, el cual está encaminado a cubrir los 19 requerimientos mencionados y a contribuir al logro de los objetivos institucionales.

En razón de lo anterior, dichos requerimientos se convirtieron en los requerimientos de TI claves para el modelo de Gobierno de TI para las entidades bancarias.

Para mayor facilidad, se identificaron los 19 requerimientos de TI seleccionados con un código, tal como se muestra en la Tabla 1.

Código	Requerimientos de TI
RQ01	Plan estratégico de tecnología.
RQ02	Infraestructura de tecnología.
RQ03	Relaciones con proveedores.
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
RQ05	Administración de proyectos de sistemas.
RQ06	Administración de la calidad.
RQ07	Adquisición de tecnología.
RQ08	Adquisición y mantenimiento de software de aplicación.
RQ09	Instalación y acreditación de sistemas.
RQ10	Administración de cambios.
RQ11	Administración de servicios con terceros.
RQ12	Administración, desempeño, capacidad y disponibilidad de la

	infraestructura tecnológica.
RQ13	Continuidad del negocio.
RQ14	Seguridad de los sistemas.
RQ15	Educación y entrenamiento de usuarios.
RQ16	Administración de los datos.
RQ17	Administración de instalaciones.
RQ18	Administración de operaciones de tecnología.
RQ19	Gestión de Documentación.

Tabla 1: Identificación de los 19 requerimientos de TI seleccionados

2.2 Selección del marco de referencia del modelo de Gobierno de TI.

Para la creación del modelo de Gobierno de TI fue necesario seleccionar un marco base de referencia y otros marcos que apoyen las estrategias de Gobierno de TI.

Después de realizar un análisis de los diferentes marcos de Gobierno de TI, se escogió el ISO 38500:2008, debido a que es una Norma Internacional que provee un estándar para que la dirección de las organizaciones evalúen, dirijan y controlen el uso de las tecnologías de la información.

Los marcos de apoyo que complementan el marco base y apoyan las estrategias de Gobierno de TI son: CobiT 4.1, CMMI, ISO 27001, ISO 27002 e ISO 9001.

2.3 Modelo de Gobierno de TI para entidades bancarias de Colombia propuesto.

Después de determinar los requerimientos de TI, el marco base y los marcos de apoyo, se procedió a definir el modelo, el cual consistió en agrupar los 19 requerimientos de TI seleccionados en los 6 principios de la Norma ISO 38500:2008.

Posterior a esto, se determinó cuales actividades de los marcos de apoyo ayudarían a cumplir con los objetivos de los 6 principios de ISO 38500:2008 y finalmente se determinó una serie de indicadores de gestión que permitan evaluar el cumplimiento de las metas propuestas. (ver figura 1)

El modelo de Gobierno de TI para las Entidades Bancarias planteado en este proyecto, responde a las actividades principales definidas por la norma ISO 38500 de **Evaluar** la utilización actual y futura de las TI. **Dirigir** la preparación e implementación de los planes y políticas que aseguren que la utilización de las TI de modo que alcancen los objetivos institucionales y **Controlar** el desempeño de la tecnología de la información, a través de sistemas de medición adecuados.

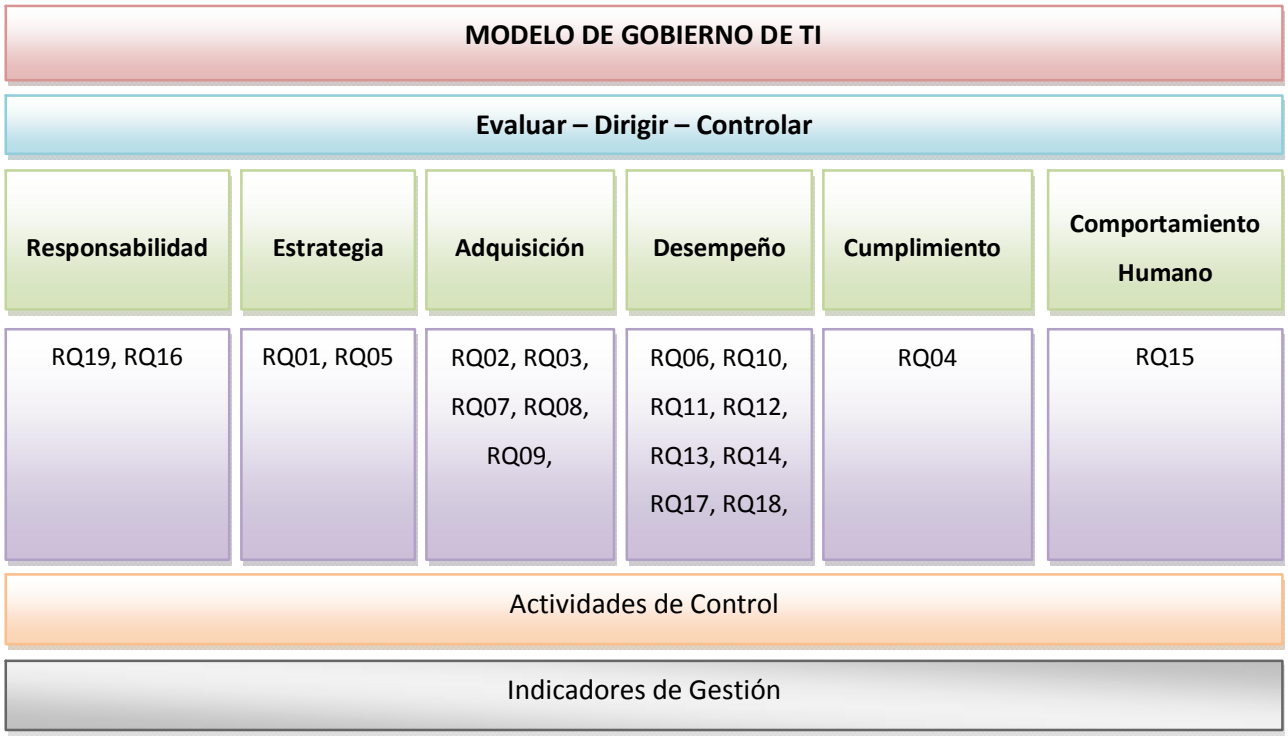


Figura 1: Modelo de Gobierno de TI para entidades bancarias de Colombia Propuesto

2.4 Estructura del Modelo

El modelo de Gobierno de TI para entidades bancarias se encuentra estructurado de la siguiente manera:

- 6 principios, 19 Requerimientos de TI, 137 Actividades de control y 56 Indicadores de gestión

Principios	Requerimientos de TI		Actividades de Control	Indicadores
Responsabilidad	RQ16	Administración de los datos.	13	5
	RQ19	Documentación.	7	1
Estrategia	RQ01	Plan estratégico de tecnología.	6	3
	RQ05	Administración de proyectos de sistemas.	14	3
Adquisición	RQ02	Infraestructura de tecnología.	4	3
	RQ03	Relaciones con proveedores.	4	1
	RQ07	Adquisición de tecnología.	4	3
	RQ08	Adquisición y mantenimiento de software de aplicación.	10	2
	RQ09	Instalación y acreditación de sistemas.	9	3
Desempeño	RQ06	Administración de la calidad.	8	3
	RQ10	Administración de cambios.	5	3
	RQ11	Administración de servicios con terceros.	4	3
	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	6	3
	RQ13	Continuidad del negocio.	10	2
	RQ14	Seguridad de los sistemas.	12	3
	RQ17	Administración de instalaciones.	5	3
	RQ18	Administración de operaciones de tecnología.	5	3
Cumplimiento	RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	5	3
Comportamiento Humano	RQ15	Educación y entrenamiento de usuarios.	6	6

Tabla 2: Estructura del modelo de Gobierno de TI propuesto

2.5 Autoevaluación de nivel de madurez de Gobierno de TI.

Si bien es cierto el sector bancario cuenta con diferentes decretos, normas y circulares como las definidas anteriormente, las cuales no solo regulan la actividad bancaria como tal, sino que además algunas de ellas son exclusivas para controlar y garantizar la gestión de la tecnología (circular externa 014 de 2009), ello no implica que necesariamente tengan establecido un Gobierno de TI. Por tal motivo, una autoevaluación es un buen punto de partida para que los responsables de TI de las entidades bancarias determinen un estado actual y uno deseado contra un estado ideal, dentro de la escala propuesta.

Para crear la estructura de la autoevaluación del nivel de madurez de Gobierno de TI en entidades bancarias, se usó la **Norma ISO 38500** como base y se apoyó en los conceptos de nivel de madurez **CobiT**, **CMMI** e **ISO 9004**.

2.5.1 Autoevaluación de Gobierno de TI propuesto

El formato de autoevaluación toma como base la norma ISO 38500 y los principios de los modelos de madurez de CobiT, CMMI e ISO 9004 (ver figura 3)

2.5.2 Realización de la Autoevaluación

Para la realización de la autoevaluación de Gobierno de TI se siguieron 3 pasos:

En el primer paso se definió como base la norma ISO 38500 y se dividieron el cumplimiento de sus 6 principios y las 3 tareas principales en niveles de madurez, utilizando como pauta los modelos de niveles de madurez de CobiT, CMMI e ISO 9004 (ver figura 6).

Posteriormente se utilizó el formato de autoevaluación de la norma ISO 9004 para presentar la propuesta y permitir que los encargados de TI que las diligencien definan su nivel actual y nivel deseado.

Por último, se adicionó a la autoevaluación una guía para su diligenciamiento, la cual incluye términos y pautas relevantes para la realización de la autoevaluación.

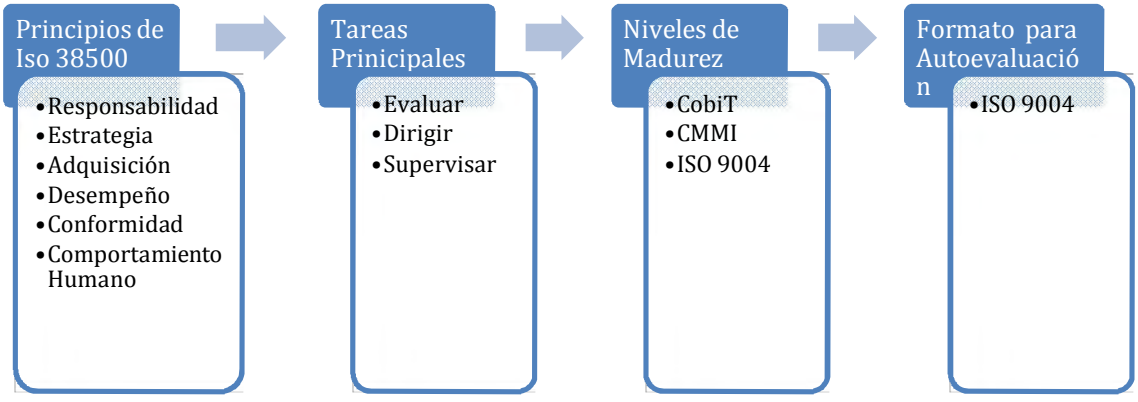


Figura 2: Esquema de la Autoevaluación propuesta

Por cada uno de los 6 principios que establece la norma ISO 38500, se plantearon actividades divididas en 3 bloques que corresponden a las tareas principales (Evaluar, Dirigir y Supervisar) (ver tabla 3)

Cada actividad cuenta con 5 niveles de madurez (preguntas). El primer nivel es el cumplimiento básico de una actividad de la norma. Para avanzar al nivel 2 se debe cumplir con el 100% de la(s) actividades del nivel 1 más la(s) actividad del nivel 2. Para alcanzar el nivel 3 de madurez se debe cumplir con las actividades de los niveles 1, 2 y 3; y así sucesivamente.

PRINCIPIOS DE ISO 38500	NIVELES DE MADUREZ					
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Evaluar					
	Dirigir					
	Supervisar					

Tabla 3: Formato de la Autoevaluación propuesta

2.6 Guía de Implementación del Modelo de Gobierno de TI propuesto

Con el fin de proporcionar una guía que facilite la implementación del Modelo de Gobierno de TI en las entidades bancarias de Colombia, se definieron dos actividades específicas:

1. Se documentó una guía de implementación del modelo
2. Se documentó un ejemplo de implementación de un requerimiento de TI del modelo propuesto

Finalmente, la base para la guía de implementación del modelo, fue la planteada por el IT Governance Institute, IT governance implementation[9].que consta de siete fases:

Fase 1: Obtener el compromiso de la alta dirección.
Fase 2: Determinar el estado actual.
Fase 3: Establecer el estado futuro deseado.
Fase 4: Identificar las brechas
Fase 5: Definir el plan de implementación
Fase 6: Desarrollar el plan de implementación

[9] **IT governance implementation guide using COBIT and Val IT**. IT Governance Institute

Fase 7: Monitorear y controlar el desempeño de la implementación

2.7 Resumen de Resultados Obtenidos

Los resultados más relevantes obtenidos en el desarrollo de este proyecto fueron:

- Identificación de los 19 requerimientos de TI claves para el modelo de Gobierno de TI
- Modelo de Gobierno de TI para entidades bancarias de Colombia
- Una autoevaluación de nivel de madurez de Gobierno de TI, basada en ISO 38500:2008
- Una Guía de Implementación para modelo propuesto

Validación Juicio de Expertos

Cordial Saludo,

El objetivo de la presente encuesta es validar la propuesta de Gobierno de TI para entidades bancarias de Colombia, a partir del resumen ejecutivo que le ha sido enviado.

Si desea aclarar algún punto en especial del resumen y/o esta encuesta, por favor no dude en hacérnosla saber a las siguientes direcciones de correo:

breyner2002@hotmail.com
maryh15@gmail.com

Muchas gracias por su valiosa colaboración

Del listado de 19 requerimientos de TI que ordena la circular externa 014 de 2009, por favor seleccione los que usted considera que deben hacer parte de un modelo de gobierno de TI

- [x] Plan estratégico de tecnología.
- [ ] Infraestructura de tecnología.
- [ ] Relaciones con proveedores.
- [ ] Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
- [ ] Administración de proyectos de sistemas.
- [ ] Administración de la calidad.
- [ ] Adquisición de tecnología.
- [ ] Adquisición y mantenimiento de software de aplicación.
- [ ] Instalación y acreditación de sistemas.
- [ ] Administración de cambios.
- [ ] Administración de servicios con terceros.
- [ ] Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
- [ ] Continuidad del negocio.
- [ ] Seguridad de los sistemas.
- [ ] Educación y entrenamiento de usuarios.
- [ ] Administración de los datos.
- [ ] Administración de instalaciones.
- [ ] Administración de operaciones de tecnología.
- [ ] Documentación.

Esta usted de acuerdo o en desacuerdo, en que los 19 requerimientos de TI identificados son validos, apropiados y sirven de base para el modelo de Gobierno de TI para entidades

bancarias de Colombia

- ◯ De acuerdo
- ◯ En desacuerdo

Teniendo en cuenta el modelo de Gobierno de TI para entidades bancarias de Colombia del resumen ejecutivo (numeral 2.3, pag. 7), considera usted que el modelo propuesto es adecuado o inadecuado

- ◯ Es Adecuado
- ◯ Es Inadecuado

Teniendo en cuenta la estructura del modelo de Gobierno de TI para entidades bancarias de Colombia del resumen ejecutivo (numeral 2.4, pag. 8), considera usted que la estructura del modelo propuesto es adecuada o inadecuado

- ◯ Es Adecuado
- ◯ Es Inadecuado

Respecto a la autoevaluación de nivel de madurez de Gobierno de TI propuesta (numeral 2.5, pag 9), usted la considera apropiada o inapropiada

- ◯ Es Apropiada
- ◯ Es Inapropiada

En cuanto a las 7 fases para la implementación del modelo de Gobierno de TI, descritas en el resumen ejecutivo (numeral 2.6 pag. 12), usted las considera adecuadas y suficientes para la llevar a cabo la implementación

- ◯ Si son adecuadas y suficientes
- ◯ No son adecuadas o suficientes

Considerando de forma global el resumen ejecutivo enviado, usted considera viable o inviable la implementación del modelo propuesto de Gobierno de TI para entidades bancarias de Colombia

- ◯ Es Viable
- ◯ Es Inviable

Para terminar, y agradeciéndole de nuevo por su tiempo en el diligenciamiento de esta encuesta, le solicitamos que por favor diligencie los siguientes datos personales (los cuales son opcionales) nombres y apellidos

En que empresa trabaja actualmente

Que cargo desempeña

Submit

ANEXO 7

Comparación de procesos de TI

Con el fin de identificar y validar el cumplimiento de la normatividad establecida por la Superintendencia Financiera a las entidades bancarias de Colombia, se revisó el estado de cumplimiento de los 19 requerimientos clave del Sistema de Control Interno para la Gestión de Tecnología (SIC) y se determino lo siguiente en cuanto a los estándares, políticas, directrices y procedimientos implementados **en el Banco de Occidente**. (sin decir con esto que todos los demás bancos cuenten con los mismo procedimientos)

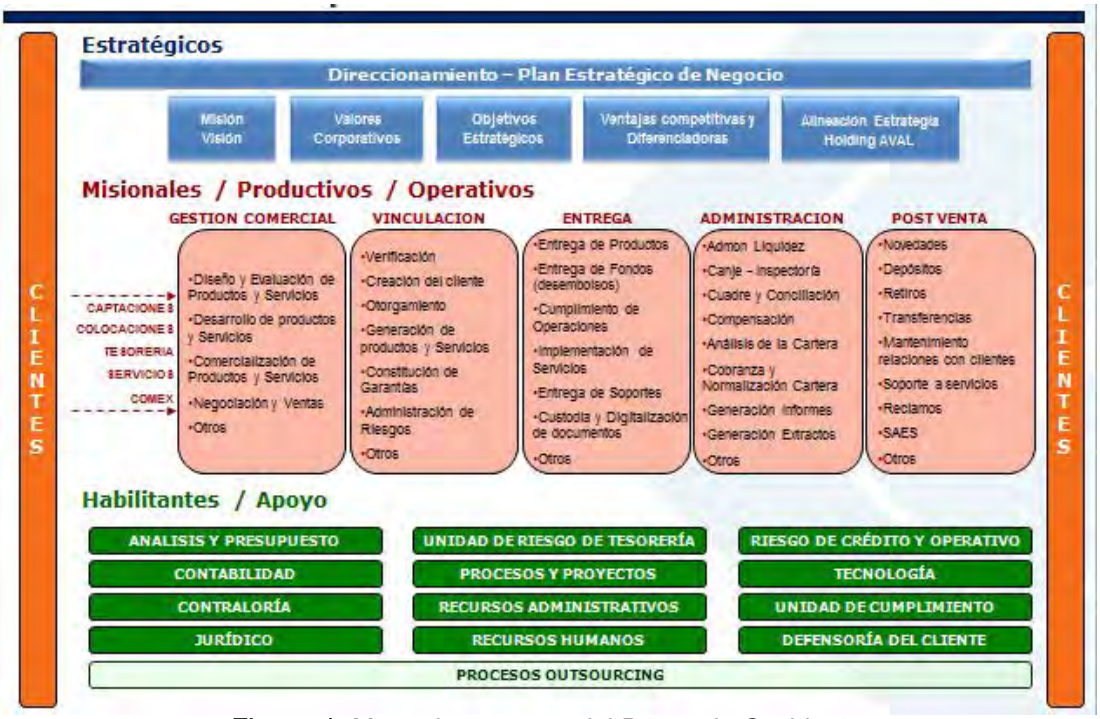


Figura 1: Mapa de procesos del Banco de Occidente

El Banco de Occidente dentro de su cadena de valor cuenta con 3 grupos de procesos: **los procesos estratégicos** son los que se encargan de dar un direccionamiento estratégico y de enfocar los objetivos a las estrategias**, los procesos misionales**, productivos y operativos son aquellos que se hacen indispensables para posicionar los productos y servicios que afectan directamente la satisfacción del cliente y por último los **procesos de apoyo** que son los que ayudan a soportar todas las operaciones del negocio.

Como parte de los procesos de apoyo, la división de Tecnología cuenta con una serie de procesos y estrategias alineadas con el negocio cuya función principal es

agregar valor a través de soluciones tecnológicas y procesos innovadores, efectivos y seguros. Para cumplir con esto, se definió un mapa de procesos de TI donde se involucra todo lo relacionado a la Gestión del área.

A continuación, en la figura 15 se muestra el mapa de procesos interno de TI del Banco de Occidente, este tiene un enfoque hacia la gestión y gobierno e involucra todas las áreas que componen la división.

Cada proceso tiene un líder responsable que es el encargado de velar por el cumplimiento de los procedimientos y lineamientos establecidos. Adicional a esto, cada uno cuenta con un listado de subprocesos que ayudan en la gestión del mismo.

Figura 2: Mapa de procesos de TI del Banco de Occidente

1.1 Desarrollar e Implementar Productos y Servicios

El objetivo del proceso es asegurar la implementación en tiempo y forma de los requerimientos presentados por las Unidades de Negocio del Banco a través de tareas del ciclo de vida del software definido en este proceso.

Responsable: Subgerente de Soluciones Funcionales y Subgerente de Desarrollo y Mantenimiento de Aplicaciones.

Subprocesos	Procedimientos
DS01 – Realizar ingeniería de requerimientos	DS01-01 Realizar análisis de la situación actual DS01-02 Elaborar documento de especificaciones DS01-03 Verificar y validar documentos de especificaciones
DS02 – Diseñar requerimientos	DS02-01 Definir Arquitectura e infraestructura de la aplicación DS02-02 Diseñar Solución del Requerimiento DS02-03 Diseñar Modelo Lógico de Datos DS02-04 Diseñar Modelo Físico de Datos
DS03 – Desarrollar requerimientos	DS03-01 Preparar y desarrollar la Solución DS03-02 Realizar Pruebas Unitarias DS03-03 Gestionar Conversión de Datos
DS04 – Probar requerimientos	DS04-01 Elaborar plan de pruebas DS04-02 Diseñar casos de pruebas DS04-03 Preparar datos de pruebas DS04-04 Ejecutar pruebas DS04-05 Evaluar pruebas DS04-06 Ejecutar pruebas de aceptación de usuario DS04-07 Instalar En Ambiente de Pruebas DS04-08 Administrar Servicios en Ambiente de Pruebas
DS05 – Implementar requerimientos	DS05-01 Preparar Implementación DS05-02 Instalar en Producción DS05-03 Brindar soporte en período de estabilización DS05-04 Elaborar y Aprobar Manuales
DS06– Administrar versiones	DS06-01 Solicitar Fuentes de versión DS06-02 Administrar Fuentes de Versión DS06-03 Preparar Release para instalar DS06-04 Armar Release DS06-05 Atender Entrega de Versión de Proveedor

1.2 Evaluar y Priorizar Requerimientos

El propósito de este macroproceso es definir la forma en que la División de Procesos y Proyectos junto con la División de Tecnología participan en la estructuración, ordenamiento y planeación de la ejecución de los requerimientos del Banco.

Responsable: Subgerente de Soluciones Funcionales.

1.3 Gestionar Entrega de Servicios

El objetivo de este proceso es diseñar y ejecutar estrategias para mejorar la satisfacción del usuario y detectar oportunidades para la mejora de los servicios prestados por TI.

Responsable: Subgerente de Soluciones Funcionales.

Subprocesos	Procedimientos
GS01 – Administrar Relación con usuarios	GS01-01 Gestionar satisfacción del usuario GS01-02 Gestionar comunicación con el usuario GS01-03 Preparar y dictar capacitación GS01-04 Administrar Control Documental GS01-05 Validar asignación del requerimiento
GS02 – Administrar Indicadores y Acuerdos	GS02-01 Crear Indicadores / Acuerdos GS02-02 Reportar Indicadores / Acuerdos

1.4 Soportar Servicios

El propósito de este proceso es asegurar que el usuario tenga acceso a los servicios apropiados que soportan las funciones del negocio.

Responsable: Subgerente de Desarrollo y Mantenimiento de Aplicaciones, Subgerente de Infraestructura de Tecnología.

Subprocesos	Procedimientos
SS01 – Atender Servicios de Mesa de Ayuda	SS01-01 Brindar Soporte Telefónico SS01-02 Administrar Base de Conocimiento
SS02 – Atender Incidentes	SS02-01 Resolver Incidentes Normales SS02-02 Resolver Incidentes de Emergencia
SS03 – Atender Problemas	SS03-01 Identificar y resolver problemas SS03-02 Gestionar proactivamente problemas
SS04 – Administrar Instalaciones	SS04-01 Recibir y guardar versión SS04-02 Atender Instalaciones SS04-03 Actualizar información de usuarios y equipos SS04-04 Realizar Instalaciones de Hardware

1.5 Planear y Desarrollar Requerimiento

Este proceso va encaminado hacia los siguientes objetivos:

- Definir las actividades del requerimiento de una manera concreta con el fin de consolidarlas en un plan de trabajo facilitando su seguimiento y correcta ejecución para alcanzar el éxito del mismo.
- Preparar y coordinar con las áreas facilitadoras la asignación del recurso o la contratación del mismo durante el tiempo requerido por el proyecto.
- Coordinar con las áreas facilitadoras de recursos logísticos la obtención de los mismos para garantizar su asignación en el momento preciso.
- Coordinar todos los requerimientos necesarios para establecer relación directa con terceros para los casos en que no intervienen las áreas de soporte del Banco.

Responsable: Subgerente de Soluciones Funcionales.

1.6 Gestionar Infraestructura

El propósito de este proceso es asegurar que el usuario tenga acceso a los servicios de infraestructura que soportan las funciones del negocio.

Responsable: Subgerente de Infraestructura de Tecnología.

Subprocesos	Procedimientos
GIF01 – Gestionar Servicios de Infraestructura	GIF01-01 Administrar y Gestionar Capacidad GIF01-02 Administrar y Gestionar Disponibilidad GIF01-03 Gestionar continuidad del servicio GIF01-04 Monitorear Servicios y Operación de Infraestructural GIF01-05 Gestionar Operación y Producción de Infraestructura GIF01-06 Administrar Respaldos y Recuperación GIF01-07 Administrar Centro de Cómputo
GIF02 - Gestionar Servicios de Soporte	GIF02-01 Gestionar problemas: Analizar e investigar problemas GIF02-02 Gestionar problemas: Resolver problemas GIF02-03 Operar y administrar plataformas GIF02-04 Optimizar plataformas GIF02-05 Gestionar seguridad de infraestructura GIF02-06 Administrar inventario de infraestructura GIF02-07 Administrar almacenamiento
GIF03 - Gestionar y Coordinar Despliegue	GIF03-01 Administrar y gestionar configuraciones GIF03-02 Administrar y gestionar cambios GIF03-03 Gestionar liberaciones: Definir lineamientos y estrategias de Liberación GIF03-04 Gestionar liberaciones: Realizar puesta en operación GIF03-05 Definir estrategia de servicios TI

1.7 Gestionar Arquitectura

El propósito de este proceso es asegurar que la arquitectura existente soporte todas las implementaciones tecnológicas y aplicaciones existentes y a futuro.

Responsable: Director de Arquitectura.

Adicional a los procedimientos establecidos para cada proceso, existen otros procedimientos que se enfocan básicamente en cumplir los requerimientos de la Ley Sarbanes Oxley (SOX),dentro de estos podemos encontrar los siguientes:

- Procedimiento para la Atención, Control y Solución de Requerimientos de Entes de Control (Interno y Externo) a la División de Tecnología
- Procedimiento para monitorear actividades usuarios privilegiados y DBA
- Procedimiento para la administración de usuarios en los ambientes de desarrollo, pruebas y producción del Banco de Occidente
- Procedimiento para Manejo de datos de ambientes de pruebas y desarrollo (enmascaramiento)
- Procedimiento para manejo de Incidentes en Base de Datos de Producción

En la tabla 7 se realiza una relación entre los procesos de TI del Banco de Occidente y su cumplimiento a los 19 requerimientos establecidos en la Circular 014 de 2009.

PROCESOS DE TI	RQ01	RQ02	RQ03	RQ04	RQ05	RQ06	RQ07	RQ08	RQ09	RQ10	RQ11	RQ12	RQ13	RQ14	RQ15	RQ16	RQ17	RQ18	RQ19
GESTIÓN DE ARQUITECTURA																			
Establecer estándares y metodología de Arquitectura de TI								X											
Diseñar e implementar Arquitectura de TI								X											

GESTIONAR INNOVACIÓN																		
Administrar modelo operativo de TI																	X	
GESTIONAR SERVICIOS DE INFRAESTRUCTURA																		
Administrar y gestionar capacidad		X									X							
Administrar y gestionar disponibilidad		X									X							
Gestionar continuidad del servicio		X									X	X						
Monitorear servicios y operaciones de Infraestructura		X									X							
Gestionar operación y producción de Infraestructura		X									X							
Administrar respaldos y recuperación		X									X	X						
Administrar centro de computo		X									X	X						
GESTIONAR SERVICIOS DE SOPORTE																		
Gestionar problemas: Analizar y gestionar problemas																		
Gestionar problemas: resolver problemas																		
Operar y administrar plataformas																		
Gestionar seguridad de Infraestructura													X					
Administrar inventario de Infraestructura																		

Administrar almacenamiento																X			
GESTIONAR Y COORDINAR DESPLIEGUE																			
Administrar y gestionar configuraciones																			
Administrar y gestionar cambios										X									
Gestionar liberaciones: Definir lineamientos y estrategias de liberación																	X		
Gestionar liberaciones: Realizar puesta en operación																	X		
Definir estrategia y servicios de TI	X																		
SOPORTAR SERVICIOS																			
Atender servicios de mesa de ayuda																			
Atender Incidentes						X													
Administrar Instalaciones																			
GESTIONAR ENTREGA DE SERVICIOS																			
Administrar relación con usuarios														X					X
Administrar indicadores y acuerdos																			X
ADMINISTRACIÓN DE RECURSOS																			

Gestión del negocio de TI				X															
Gestión del talento																			
Gestión de compras y contratación			X				X				X								
EVALUAR Y PRIORIZAR REQUERIMIENTOS																			
Identificar y plantear requerimiento																			
Precotizar, priorizar y planear requerimiento																			
DESARROLLAR E IMPLEMENTAR PRODUCTOS Y SERVICIOS																			
Realizar ingeniería de requerimientos					X														X
Diseñar requerimientos					X														
Desarrollar requerimientos					X														
Probar requerimientos					X	X													
Implementar requerimientos					X				X										
Administrar versiones					X				X										

Tabla 1: Relación entre los procesos de TI del Banco de Occidente y su cumplimiento a los 19 requerimientos establecidos en la Circular 014 de 2009

Modelo y guía de implementación de Gobierno de TI para Entidades Bancarias en Colombia

Model and Implementation Guide IT Governance for Banks in Colombia

Hernando Peña Villamil
PMP, ITIL, CobIT, ISO27001 IA
Vicepresidente de Finanzas - PMI Bogotá -Colombia
Director de Membresía - ISACA Capítulo Bogotá- Colombia (126)
Consultor de Gobierno de IT
hdo.pena@gmail.com

María Helena Correa Correa
Estudiante de la Maestría en Gestión de Informática y Telecomunicaciones.
Ingeniera de Sistemas y Computación, Universidad Javeriana, Cali (Colombia).
maryh15@gmail.com

Breyner Alexander Parra Rojas
Estudiante de la Maestría en Gestión de Informática y Telecomunicaciones.
Ingeniero de Sistemas, Universidad Icesi, Colombia.
breyneralexander@gmail.com

Resumen

En este artículo se presenta un modelo de Gobierno de TI, con su respectiva guía de implementación en entidades bancarias de Colombia. El objetivo del modelo es apoyar la satisfacción de necesidades de desempeño corporativas y legales de este sector. Este modelo se sustenta en los 19 requerimientos de TI que fueron extraídos de la circular 014 de 2009, los 6 principios de la norma ISO38500:2008 y los marcos de apoyo tales como CobiT 4.1, CMMI-DEV, ISO 27001, ISO 27002 e ISO 9001. A partir de aquí se determinó cuales actividades de los marcos de apoyo ayudarían a cumplir con los objetivos de los 6 principios de ISO 38500:2008 y finalmente se determinó una serie de indicadores de gestión que permitan evaluar el cumplimiento de las metas propuestas. Adicional al modelo, se cuenta con una guía de implementación basada en el planteamiento del IT

Governance Institute, “IT governance implementation”[1] que consta de siete fases: Obtener el compromiso de la dirección, determinar el estado actual, establecer el estado futuro deseado, identificar las brechas, definir el plan de implementación, desarrollar el plan de implementación y monitorear el desempeño de la implementación. Con esto se pretende que los Bancos puedan tener una base y una referencia para la implementación de Gobierno de TI que les permita alinearse con las estrategias del negocio y satisfacer las necesidades de la organización.

Palabras clave

Gobierno de TI, ISO38500, requerimientos de TI, Modelo de madurez.

Abstract

This article presents a model of IT governance, with their respective implementation guide for banks in Colombia. The goal of this model is to help to meet corporate and legal sector regulations. This model has 19 IT requirements that were extracted from the Circular 014 of 2009, a frame where are the six basic principles of the standard ISO38500:2008 and support frameworks like CobiT 4.1, CMMI-DEV, ISO 27001, ISO 27002 and ISO 9001, from here was determined activities of support frameworks that help to achieve the objectives of the 6 principles of ISO 38500:2008 and finally was identified a number of performance indicators to assess the performance of the proposed goals. In addition to the model, it has a guide based implementation raised by the IT Governance Institute, IT Governance Implementation consists of seven phases: Get management commitment, determine the current state, set the desired future state, identify gaps, define the implementation plan, develop the implementation plan and monitor implementation performance. This is to allow banks to have a basis and reference for the implementation of IT governance that allows alignment with business strategies and meet the needs of the organization.

---

[1] **IT governance implementation guide using COBIT and Val IT**. IT Governance Institute

Keywords

IT Governance, ISO38500, IT requirements, Maturity model.

1. Introducción

Son establecimientos bancarios las instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito. Es importante saber que todas las entidades que hacen parte del sistema financiero están sujetas a la regulación y supervisión por parte de las autoridades de intervención: el Congreso de la República, el Ministerio de Hacienda y Crédito Público y la Superintendencia Financiera. Así mismo, estas son las encargadas de crear los marcos normativos y de velar porque los recursos de las personas, empresas y el gobierno se encuentren seguros en manos de las diferentes instituciones. Además, la Superintendencia Financiera también tiene funciones de inspección, vigilancia y control sobre las entidades.

Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros; sin embargo, el problema es que hasta ahora, no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

2. Autoevaluación de Gobierno de TI

Si bien es cierto el sector bancario cuenta con diferentes decretos, normas y circulares las cuales no solo regulan la actividad bancaria como tal, sino que además algunas de ellas son exclusivas para controlar y garantizar la gestión de la tecnología (circular externa 014 de 2009), ello no implica que necesariamente tengan establecido un Gobierno de TI. Por tal motivo, una autoevaluación es un buen punto de partida para que los responsables de TI de las entidades bancarias determinen un estado actual y uno deseado contra un estado ideal, dentro de la escala propuesta.

Como punto de partida para la definición y posterior implementación de Gobierno de TI en el sector bancario colombiano, se hace pertinente realizar dos actividades:

1. Autoevaluación de nivel de madurez de Gobierno de TI: Esta autoevaluación tiene por objetivo que los responsables de TI de los bancos se realicen un autodiagnóstico para determinar en que grado de nivel de madurez de Gobierno de TI se encuentran con respecto a la escala propuesta. Así mismo, se establece en que nivel desean estar. Al ser una autoevaluación, se presume que los encargados de TI la responden de forma correcta y verídica.
2. Comparación de procesos de TI: Para el modelo de gobierno de TI en las entidades bancarias de Colombia, se parte de los 19 requerimientos de TI que la circular externa 014 de 2009 obliga a los bancos a cumplir. Aun así, se realizó una comparación entre dichos requerimientos y los procesos de TI del Banco de Occidente, a partir de su respectivo mapa de procesos y sus planes estratégicos de tecnología.

La autoevaluación es una herramienta para la revisión del nivel de madurez de una organización y puede abarcar criterios como el liderazgo, estrategia, sistema de gestión, recursos y/o procesos, con fin de identificar fortalezas, debilidades y oportunidades tanto para la mejora, como para la innovación. Para crear la estructura de la autoevaluación del nivel de madurez de Gobierno de TI en entidades bancarias, se usó la Norma ISO 38500 como base y se apoyó en los conceptos de nivel de madurez de CobiT, CMMI-DEV e ISO 9004.

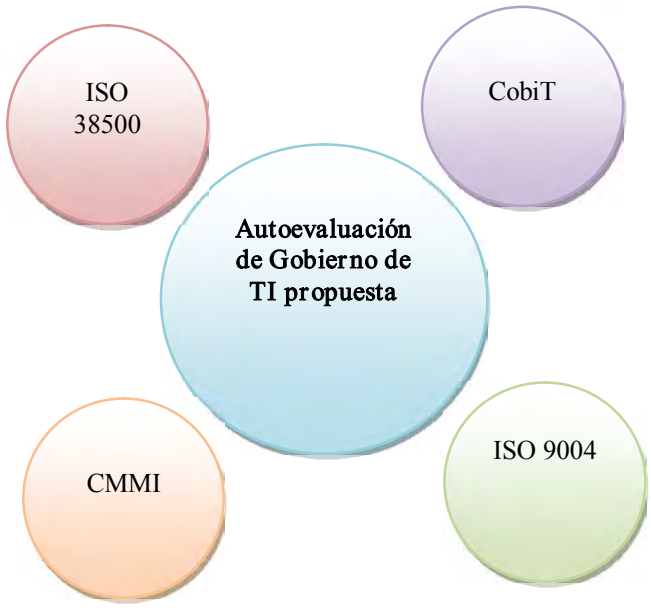


Figura 1: Autoevaluación de Gobierno de TI Propuesto

Para la realización de la autoevaluación de Gobierno de TI se siguieron 3 pasos: En el primero se definió como base la norma ISO 38500 y se dividieron el cumplimiento de sus 6 principios y las 3 tareas principales en niveles de madurez, utilizando como pauta los modelos de madurez de CobiT, CMMI-DEV e ISO 9004. Posteriormente, se utilizó el formato de autoevaluación de la norma ISO 9004 para presentar la propuesta y permitir que los encargados de TI que las diligencien definan su nivel actual y el nivel deseado. Por último, se adicionó a la autoevaluación una guía para su diligenciamiento, la cual incluye términos y pautas relevantes para la realización de la autoevaluación.

Por cada uno de los 6 principios que establece la norma ISO 38500, se plantearon actividades divididas en 3 bloques que corresponden a las tareas principales (Evaluar, Dirigir y Supervisar). Cada actividad cuenta con 5 niveles de madurez (determinado con base en la respuesta a varias preguntas). El primer nivel es el cumplimiento básico de una actividad de la norma. Para lograr el nivel 2 se debe cumplir con el 100% de la(s) actividades del nivel 1 más la(s) actividad(es) del nivel 2. Para alcanzar el nivel 3 de madurez se debe cumplir con las actividades de los niveles 1, 2 y 3; y así sucesivamente.

3. Modelo de Gobierno de TI para Entidades Bancarias en Colombia

El presente modelo de Gobierno de TI propuesto recoge el espíritu de la Circular 014 de 2009, la cual como tiene como objetivo primario que las entidades bancarias de Colombia creen y/o fortalezcan un sistema de control interno que permita la evaluación continua de su eficiencia, contribuya al logro de sus objetivos de negocio y fortalezca la apropiada administración de los riesgos a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia.

3.1. Contexto del modelo

Las entidades bancarias de Colombia se encuentran regidas por la Circular 014 del 2009; la cual define las Normas de Control Interno para la Gestión de la Tecnología. En dicha circular se establece que las entidades bancarias deberán diseñar un Sistema de Control Interno (SCI) para la gestión de la tecnología, que responda a las políticas, necesidades y expectativas de la entidad y a las exigencias normativas, con el propósito de contribuir al logro de los objetivos institucionales. El SCI obliga a los responsables de TI de las Entidades Bancarias a contar con estándares, políticas, directrices y procedimientos debidamente aprobados, orientados a cubrir 19 requerimientos: *i)* Plan estratégico de tecnología, *ii)* Infraestructura de tecnología, *iii)* Relaciones con proveedores, *iv)* Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico, *v)* Administración de proyectos de sistemas, *vi)* Administración de la calidad, *vii)* Adquisición de tecnología, *viii)* Adquisición y mantenimiento de software de aplicación, *ix)* Instalación y acreditación de sistemas, *x)* Administración de cambios, *xi)* Administración de servicios con terceros, *xii)* Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica, *xiii)* Continuidad del negocio, *xiv)* Seguridad de los sistemas, *xv)* Educación y entrenamiento de usuarios, *xvi)* Administración de los datos, *xvii)* Administración de instalaciones, *xviii)* Administración de operaciones de tecnología y *xix)* Documentación.

Por tal motivo y para dar cumplimiento a la ley, las entidades bancarias cuentan con un Sistema de Control Interno para la gestión de tecnología, el cual esta encaminado a cubrir los 19 requerimientos mencionados y a contribuir al logro de los objetivos institucionales.

El marco de Gobierno de TI seleccionado fue el ISO 38500:2008, debido a que es una Norma Internacional que provee un estándar para que la dirección de las organizaciones evalúen, dirijan y monitoreen el uso de las tecnologías de la información. Los marcos de apoyo que complementan el marco base y apoyan las estrategias de Gobierno de TI son: CobiT 4.1, CMMI-DEV, ISO 27001, ISO 27002 e ISO 9001. Después de determinar los requerimientos de TI, el marco base y los marcos de apoyo, se procedió a definir el modelo, el cual consistió (apoyados con CobiT) en agrupar los 19 requerimientos de TI seleccionados en los 6 principios de la Norma ISO 38500:2008; dicho "mapeo" fue obtenido de IT Governance Network Netherlands y se muestra en la figura 2. Posterior a esto, se determinó cuales actividades de los marcos de apoyo ayudarían a cumplir con los objetivos de los 6 principios de ISO 38500:2008 y finalmente se determinó una serie de indicadores de gestión que permitan evaluar el cumplimiento de las metas propuestas.

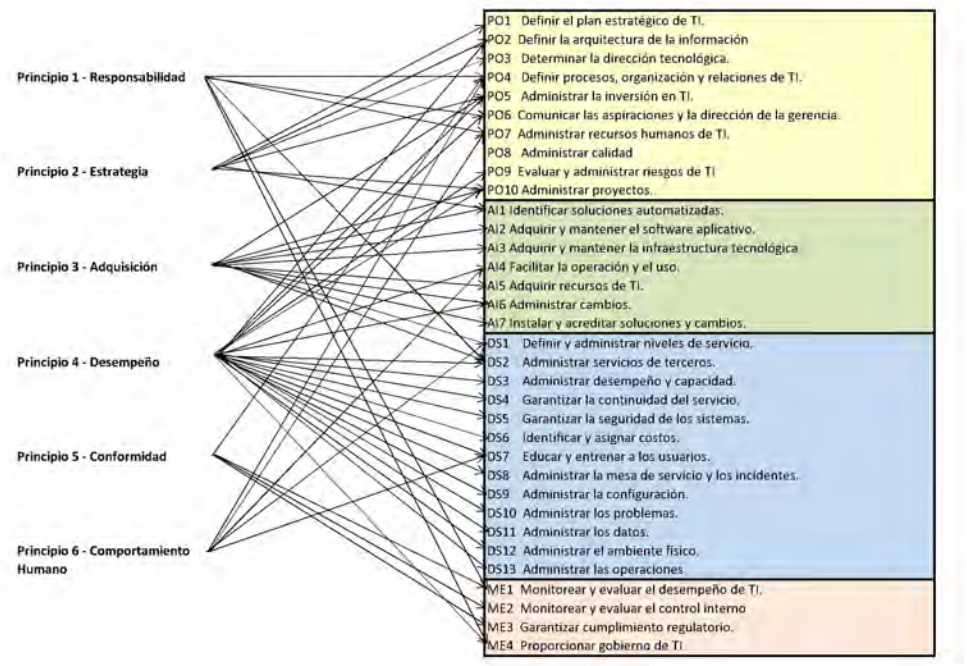


Figura 2: Relación entre principios de gobierno ISO 38500 y procesos CobiT[2]

[2] "**A Foundation for Security**", IT Governance Network Netherlands, http://itgovernance.com/nl/index.php?option=com_content&view=article&id=72&Itemid=89.

3.2. Estructura del modelo

El modelo de Gobierno de TI para las Entidades Bancarias planteado en este proyecto, responde a las actividades principales definidas por la norma ISO 38500 de Evaluar la utilización actual y futura de las TI. Dirigir la preparación e implementación de los planes y políticas que aseguren que la utilización de las TI de modo que alcancen los objetivos institucionales y Controlar el desempeño de la tecnología de la información, a través de sistemas de medición adecuados.

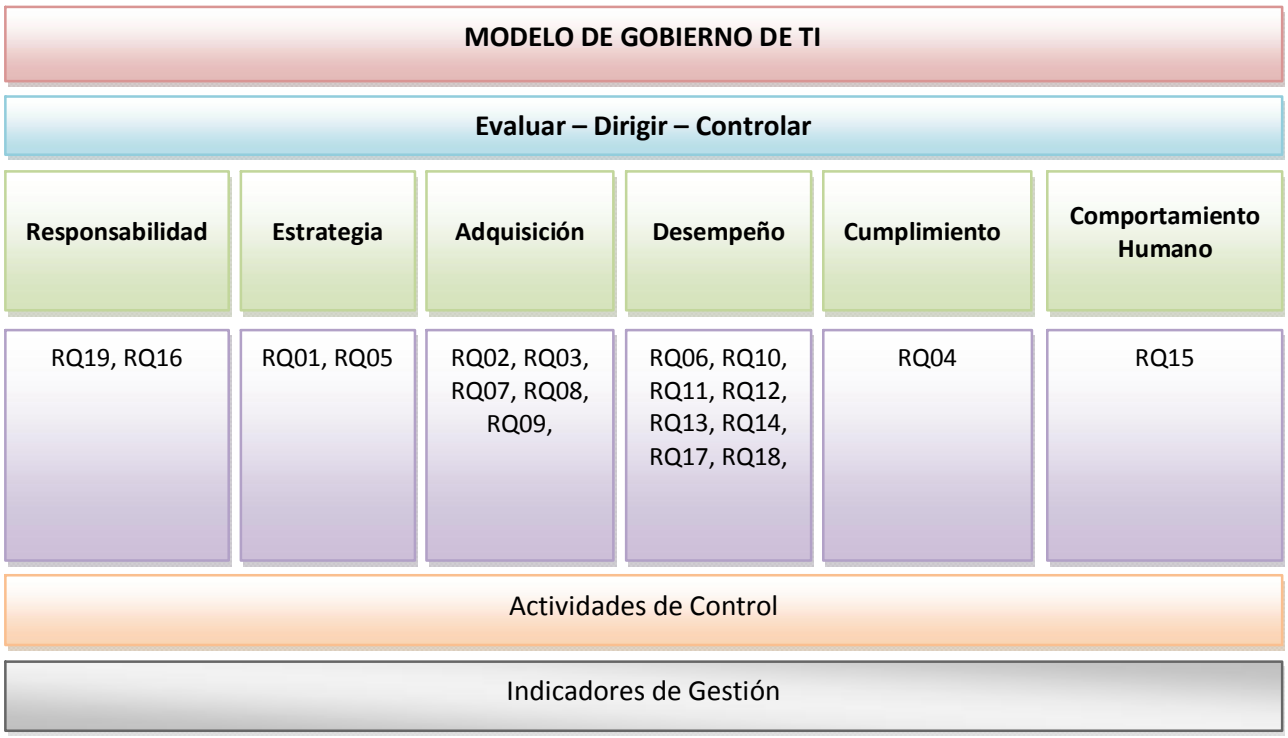


Figura 3: Modelo de Gobierno de TI propuesto

El modelo de Gobierno de TI para entidades bancarias se encuentra estructurado de la siguiente manera: 6 principios, 19 Requerimientos de TI, 137 Actividades de control y 56 Indicadores de gestión

Principios	Requerimientos de TI		Actividades de Control	Indicadores
Responsabilidad	**RQ16**	Administración de los datos.	13	5
	RQ19	Gestión de la Documentación.	7	1

Estrategia	**RQ01**	Plan estratégico de tecnología.	6	3
	RQ05	Administración de proyectos de sistemas.	14	3
Adquisición	**RQ02**	Infraestructura de tecnología.	4	3
	RQ03	Relaciones con proveedores.	4	1
	RQ07	Adquisición de tecnología.	4	3
	RQ08	Adquisición y mantenimiento de software de aplicación.	10	2
	RQ09	Instalación y acreditación de sistemas.	9	3
Desempeño	**RQ06**	Administración de la calidad.	8	3
	RQ10	Administración de cambios.	5	3
	RQ11	Administración de servicios con terceros.	4	3
	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	6	3
	RQ13	Continuidad del negocio.	10	2
	RQ14	Seguridad de los sistemas.	12	3
	RQ17	Administración de instalaciones.	5	3
	RQ18	Administración de operaciones de tecnología.	5	3
Cumplimiento	**RQ04**	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	5	3
Comportamiento Humano	**RQ15**	Educación y entrenamiento de usuarios.	6	6

Tabla 1: Estructura del modelo de Gobierno de TI propuesto

Los 6 principios del modelo fueron obtenidos la norma ISO 38500:2008, de igual manera las 137 Actividades de Control y los 56 Indicadores de Gestión, fueron transcritas de CobiT 4.1, ISO 27002:2008, CMMI-DEV y/o ISO 9001:2008

4. Guía de implementación del modelo de Gobierno de TI para Entidades Bancarias de Colombia

Con el fin de proporcionar una guía que facilite la implementación del Modelo de Gobierno de TI en las entidades bancarias de Colombia, se definieron dos actividades específicas: *i)* Se documentó una guía de implementación del modelo y *ii)* Se documentó un ejemplo de implementación de un requerimiento de TI del modelo propuesto. Finalmente, la base para la guía de implementación del modelo, fue la planteada por el IT Governance Institute, IT

governance implementation[3] que consta de siete fases: *i)* Obtener el compromiso de la alta dirección, *ii)* Determinar el estado actual, *iii)* Establecer el estado futuro deseado, *iv)* Identificar las brechas, *v)* Definir el plan de implementación, *vi)* Desarrollar el plan de implementación y *vii)* Monitorear y controlar el desempeño de la implementación.

5. Conclusiones

En este artículo se presenta un modelo de Gobierno de TI para Entidades Bancarias en Colombia. El gobierno de TI está orientado a la realidad actual de la industria, sin importar el tipo o tamaño de la organización y no se avizora algún tipo impedimento que haga que el gobierno de TI no sea aplicado a las industrias. Lo que definitivamente si existe, son diferencias de tipo organizativas, culturales, económicas y legislativas dependiendo del sector de la industria, lo que implica que TI debe estar adaptada a estas necesidades propias.

Lo anterior implica que si bien es cierto gobierno de TI es un "producto genérico" que puede adaptarse a cualquier tipo de organización, si se hace imperativo realizar un amoldamiento a la realidad de la industria particular que desea implementarlo. En el modelo se adapta este "producto genérico" para que cubra los requerimientos de TI que deben cumplir las entidades Bancarias debido a las leyes que los rigen para poder, de esta manera, cubrir lo que implica tener un Gobierno de TI a nivel organizacional y a nivel de reglamentación normativa.

Respecto a los marcos de referencia que se usaron para el desarrollo del modelo, todos son muy valiosos y están precedidos de muchas horas de trabajo, de muchas personas con un conocimiento y experiencia indiscutible; así mismo, se observa que los marcos base de Gobierno de TI tienen muchas cosas en común y no es difícil hacer asociaciones entre ellos, por tal motivo cualquier marco base (sabiendo aplicar) resultará útil para la implementación de Gobierno de TI.

---

[3] **IT governance implementation guide using COBIT and Val IT**. IT Governance Institute

En cuanto a la guía de implementación desarrollada permite poder tener un punto de partida para las entidades Bancarias que deseen aplicar el modelo en sus compañías de acuerdo a las prácticas ya utilizadas para otros modelos.

Referencias Bibliográficas

1. **Superintendencia Financiera de Colombia** *Circular Externa 014 del 2009*, Colombia. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc

2. **Superintendencia Financiera de Colombia**, *Circular externa 038 de 2009*, Colombia, www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce038_09.doc

3. **Superintendencia Financiera de Colombia**, *Circular externa 052 de 2007,* Colombia, www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce052_07.rtf

4. **Superintendencia Financiera de Colombia**, *Decreto 633 de 1993*, Colombia, http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/estatuto/parte01.pdf

5. **Asobancaria**, *Información al consumidor financiero*. Colombia, 2012 http://www.asobancaria.com/portal/page/portal/Asobancaria/info_consumidor/sistema_financiero_y_banca/

6. **Ministerio de Hacienda de Colombia,** *Fusiones y Adquisiciones en el Sector Financiero Colombiano: Análisis y Propuestas sobre la Consolidación Bancaria.* Colombia, 2012 http://www.minhacienda.gov.co/portal/page/portal/HomeMinhacienda/regulacionfinanciera/Presentaciones/Presentaciones/7_ANIF-MULTIBAN-FINAL0606.pdf

7. **Ingrid Lucía Muñoz Periñán MsC, Gonzalo Ulloa Villegas**, *Artículo: Gobierno de TI - Estado del arte*, Revista S&T, Universidad Icesi, Cali, 2011 http://www.icesi.edu.co/biblioteca_digital/bitstream/10906/5568/1/Gobierno_de_TI.pdf

8. **ISACA Manuel Ballester Ph D,** *Gobierno de las TIC ISO/IEC 38500*. The ISACA Journal Online published, 2010, http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/jpdf1001-online-gobierno.pdf

9. **IT Governance Institute**, *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.2008,* http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

10. **IT Governance Institute,** *Informe: Global Status Report on the Governance of Enterprise IT,* 2011, http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf

11. **ISACA - Centro de Conocimiento**, *Caso de Estudio: Banco Supervielle S.A., Argentina*, http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/COBIT-Caso-de-Estudio-Banco-Supervielle-SA-Argentina.aspx

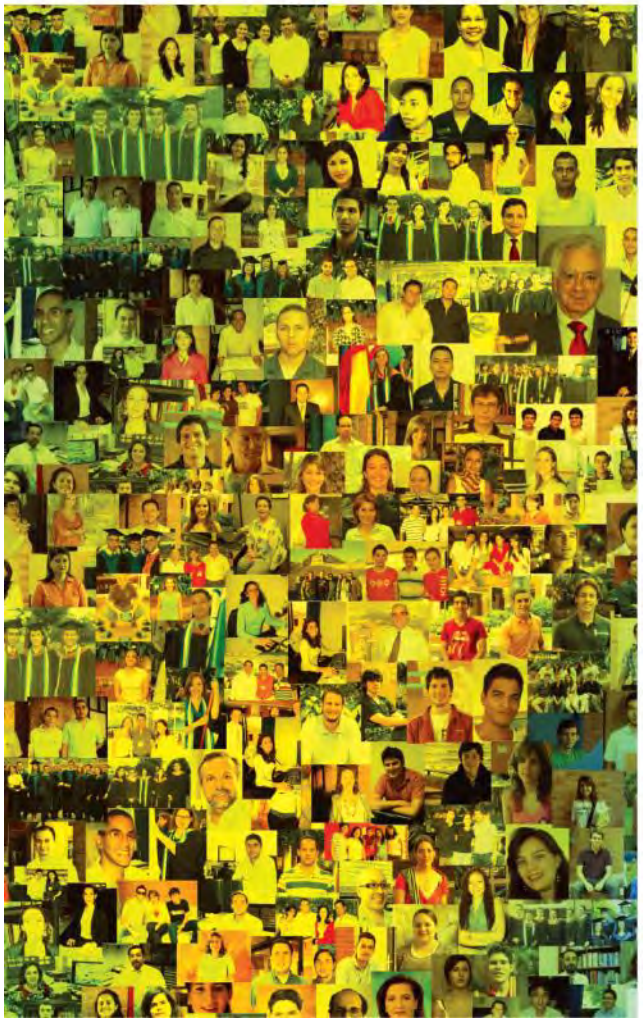
12. **ISACA - Centro de Conocimiento**, Caso *de Estudio: Grupo Bancolombia Implements COBIT to Help Ensure Compliance and Improve Processes.* http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Grupo-Bancolombia.aspx

13. **ISACA Manuel Ballester, Ph.D,** *Artículo: Gobierno de las TIC ISO/IEC 38500, Isaca Journal*, 2010,

14. **Antonio Fernández Martínez**, *Gobierno de las TI para universidades,* Universidad de Almería; Faraón Llorens Largo, Universidad de Alicante, 2011

15. **ISACA. Steven De Haes, Ph.D., Wim Van Grembergen, Ph.D.**, *Artículo: Moving From IT Governance to Enterprise Governance of IT*, Isaca Journal, 2009.

LA CALIDAD
HACE
LA DIFERENCIA



Modelo y guía para la implementación de Gobierno de TI en Entidades Bancarias de Colombia

María Helena Correa Correa

Breyner Alexander Parra Rojas

UNIVERSIDAD ICESI

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD
PRIMERA UNIVERSIDAD PRIVADA DEL SUROCCIDENTE COLOMBIANO

Planteamiento del Problema

- Los Bancos dependen hoy en día de TI para su funcionamiento y desarrollo; y hacen grandes esfuerzos e inversiones en tecnología con el objetivo de ser más eficientes y más seguros; el problema es que no existía un modelo de Gobierno de TI adaptado a las necesidades del sector bancario colombiano.

Objetivo General

- Proponer un modelo de Gobierno de TI y una guía para su implementación en entidades bancarias de Colombia, que satisfaga las necesidades legales y corporativas de este sector, teniendo en cuenta que no sería útil aplicar al pie de la letra modelos de Gobierno de otros sectores colombianos, ya que la infraestructura, tecnología, modelo de negocio y sobre todo, legislación, es diferente. Tampoco es pertinente aplicar exactamente modelos de gobierno de TI bancario de otros países dadas las diferencias culturales, operativas, económicas y de legislación existentes con respecto a Colombia.

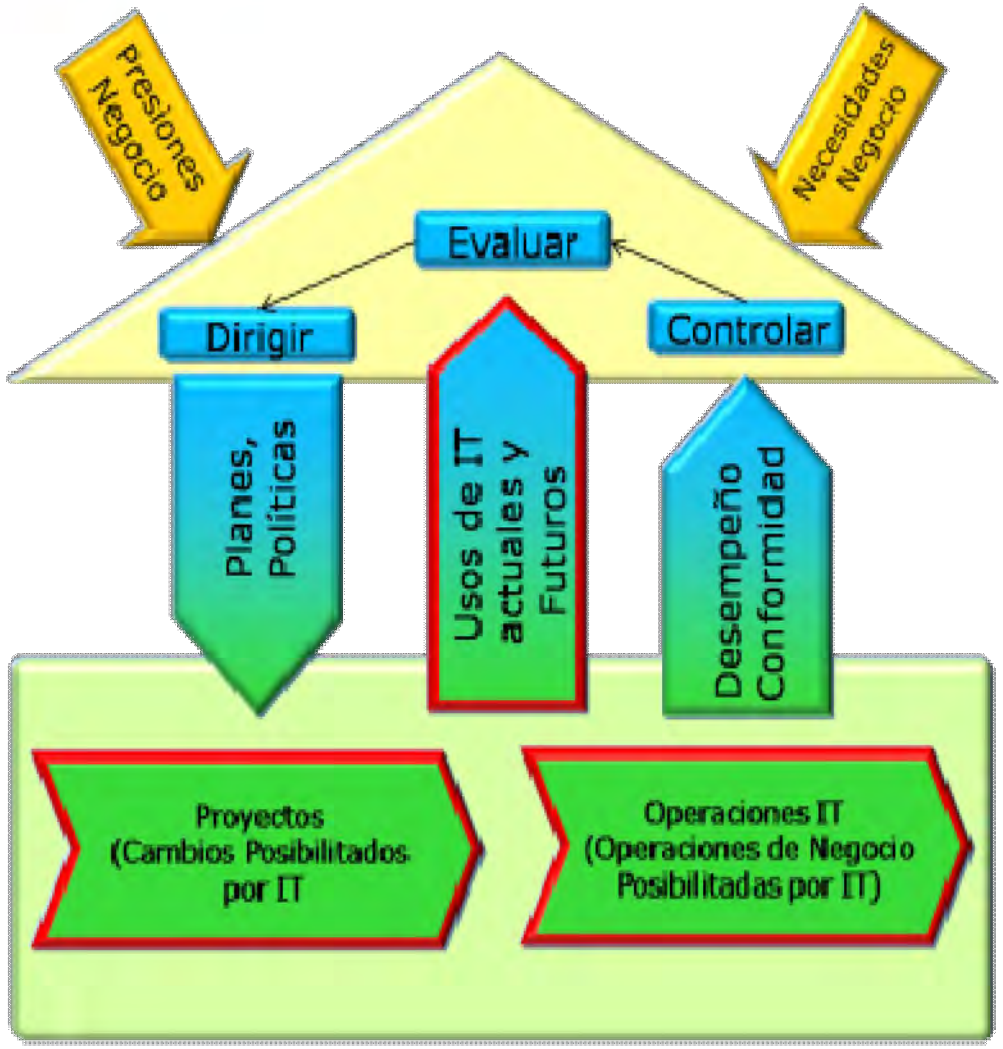
Objetivos Específicos

- Realizar un análisis del contexto del sector bancario en Colombia, incluyendo las principales disposiciones legales que los rigen.
- Realizar un análisis de los marcos para Gobierno de TI existentes y determinar cuáles son los más apropiados para la creación del modelo a implementar.
- Crear una autoevaluación de nivel de madurez de Gobierno de TI
- Desarrollar un modelo de Gobierno de TI, basado en los marcos seleccionados.
- Crear una guía de implementación para el modelo de Gobierno de TI desarrollado.
- Validar el modelo y la metodología por un grupo de expertos, a partir de una Rubrica que permita su evaluación.

Resumen del Modelo

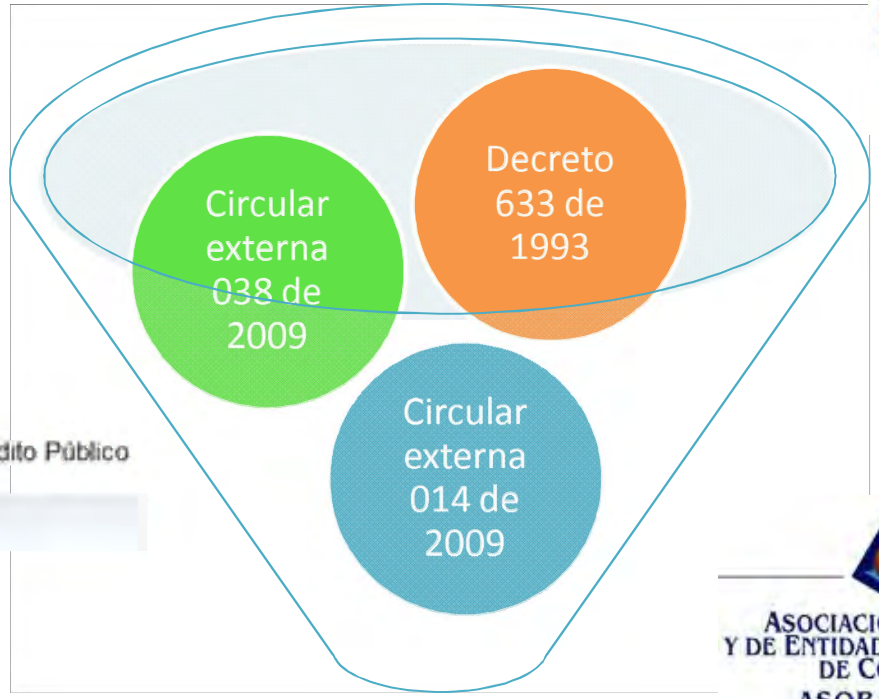
- El presente modelo de Gobierno de TI propuesto recoge el espíritu de la Circular 014 de 2009, la cual tiene como objetivo primario que las entidades bancarias de Colombia creen y/o fortalezcan un sistema de control interno que permita la **evaluación continua de su eficiencia**, contribuya al **logro de sus objetivos de negocio** y fortalezca la apropiada **administración de los riesgos** a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia.

Gobierno de TI



- Estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, agregando valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre inversiones en TI.
- El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio.
- Facilita que la empresa:
  - Aproveche al máximo su información
  - Maximice los beneficios.
  - Capitalice oportunidades
  - Gane ventajas competitivas

Contexto



Sector Bancario Colombiano

Contexto

Sistema de Control Interno (SCI)

define

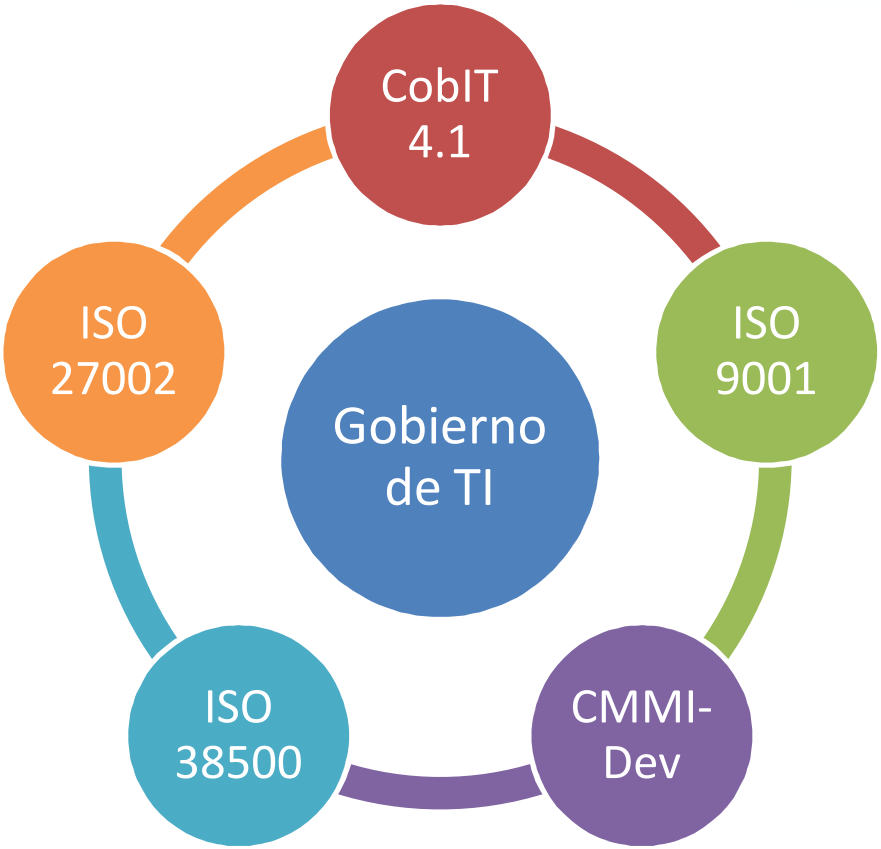
Normas de Control Interno para la Gestión de TI

Estándares, políticas, directrices y procedimientos orientados a cumplir

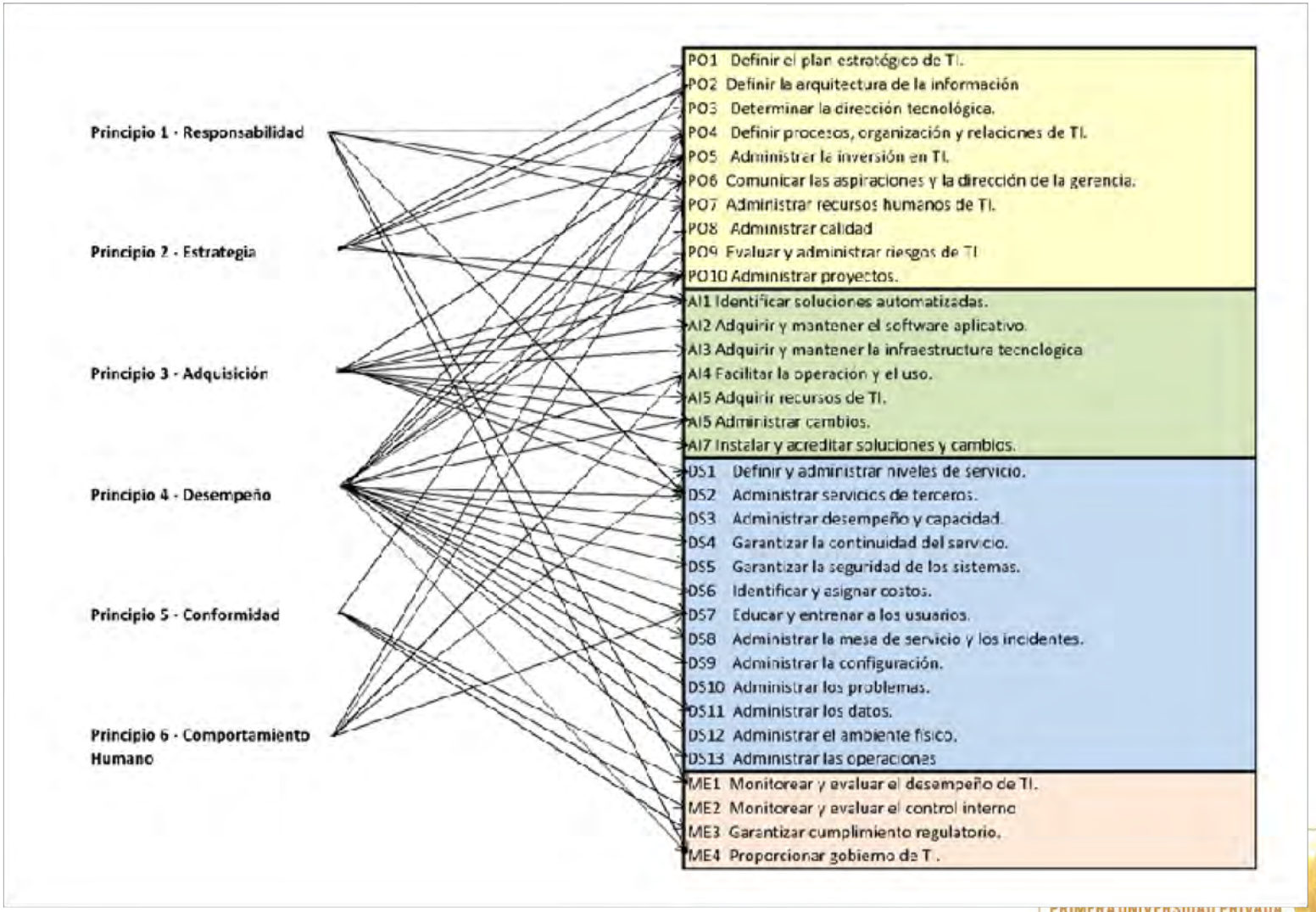
19 Requerimientos de TI

1. Plan estratégico de tecnología.
2. Infraestructura de tecnología.
3. Relaciones con proveedores.
4. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
5. Administración de proyectos de sistemas.
6. Administración de la calidad.
7. Adquisición de tecnología.
8. Adquisición y mantenimiento de software de aplicación.
9. Instalación y acreditación de sistemas.
10. Administración de cambios.
11. Administración de servicios con terceros.
12. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
13. Continuidad del negocio.
14. Seguridad de los sistemas.
15. Educación y entrenamiento de usuarios.
16. Administración de los datos.
17. Administración de instalaciones.
18. Administración de operaciones de tecnología.
19. Gestión de la Documentación.

Marcos para Gobierno de TI



Modelo de Gobierno de TI



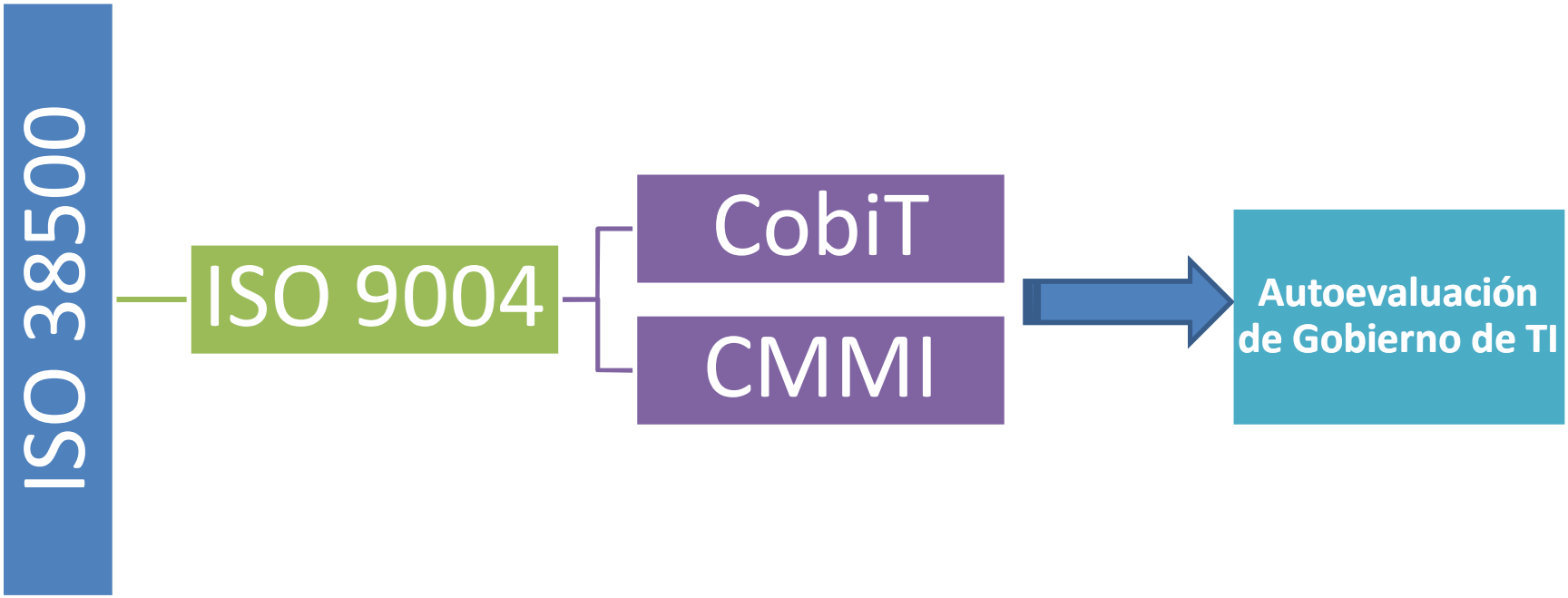
Modelo de Gobierno de TI

MODELO DE GOBIERNO DE TI					
Evaluar – Dirigir – Controlar					
Responsabilidad	**Estrategia**	**Adquisición**	**Desempeño**	**Cumplimiento**	**Comportamiento Humano**
RQ19, RQ16	RQ01, RQ05	RQ02, RQ03, RQ07, RQ08, RQ09,	RQ06, RQ10, RQ11, RQ12, RQ13, RQ14, RQ17, RQ18,	RQ04	RQ15
Actividades de Control					
Indicadores de Gestión					

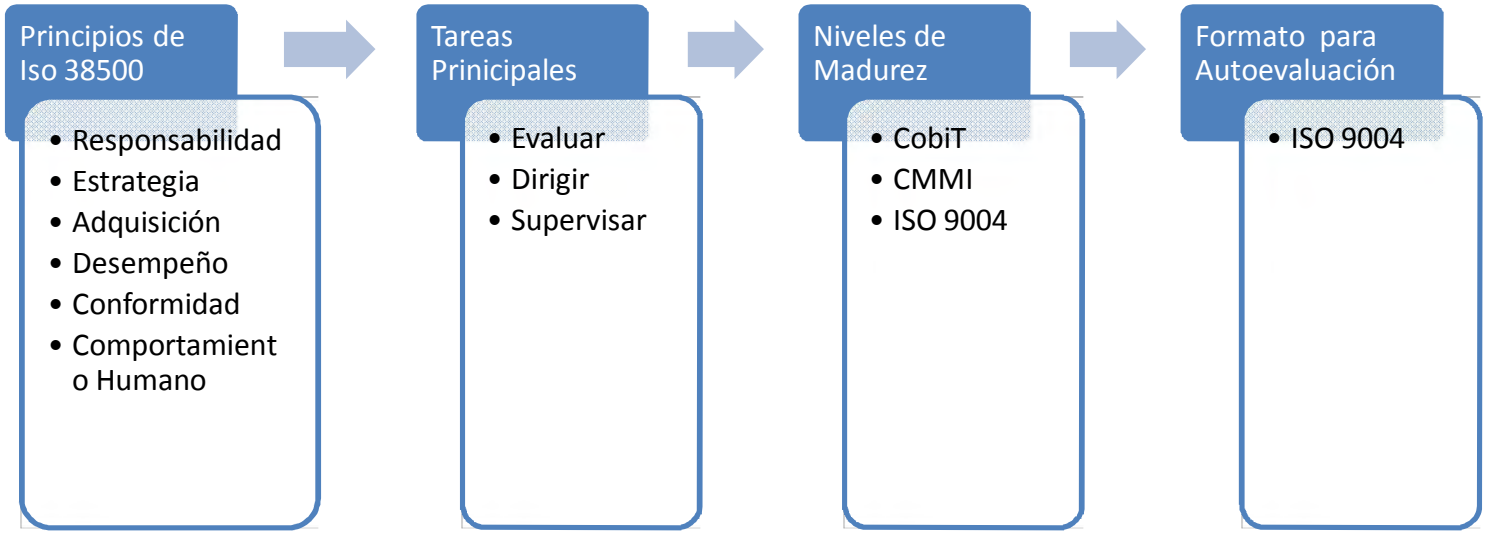
Modelo de Gobierno de TI

Principios	Requerimientos de TI		Actividades de Control	Indicadores
Responsabilidad	RQ16	Administración de los datos.	13	5
	RQ19	Gestión de la Documentación.	7	1
Estrategia	RQ01	Plan estratégico de tecnología.	6	3
	RQ05	Administración de proyectos de sistemas.	14	3
Adquisición	RQ02	Infraestructura de tecnología.	4	3
	RQ03	Relaciones con proveedores.	4	1
	RQ07	Adquisición de tecnología.	4	3
	RQ08	Adquisición y mantenimiento de software de aplicación.	10	2
	RQ09	Instalación y acreditación de sistemas.	9	3
Desempeño	RQ06	Administración de la calidad.	8	3
	RQ10	Administración de cambios.	5	3
	RQ11	Administración de servicios con terceros.	4	3
	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	6	3
	RQ13	Continuidad del negocio.	10	2
	RQ14	Seguridad de los sistemas.	12	3
	RQ17	Administración de instalaciones.	5	3
	RQ18	Administración de operaciones de tecnología.	5	3
Cumplimiento	RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	5	3
Comportamiento Humano	RQ15	Educación y entrenamiento de usuarios.	6	6

Autoevaluación nivel de madurez



Autoevaluación nivel de madurez



Guía de implementación del Modelo

Guía de implementación del IT Governance Institute, IT governance implementation

Consta de

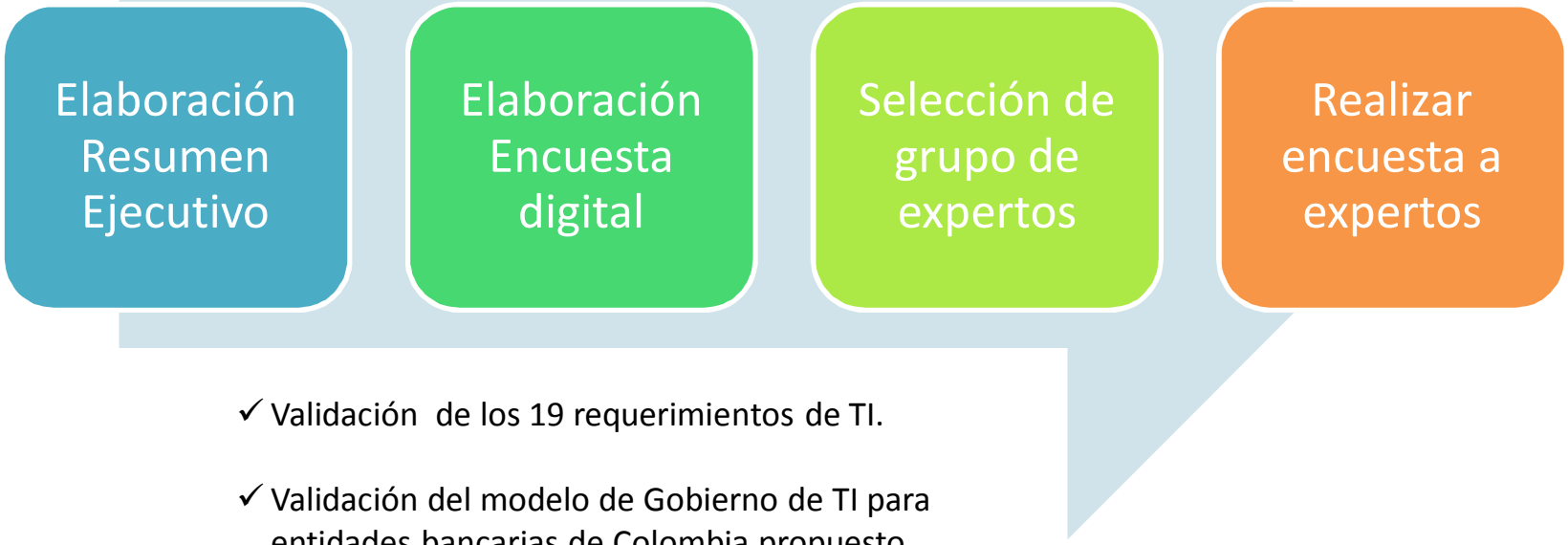
- ✓ Fase 1: Obtener el compromiso de la alta dirección.
- ✓ Fase 2: Determinar el estado actual.
- ✓ Fase 3: Establecer el estado futuro deseado.
- ✓ Fase 4: Identificar las brechas
- ✓ Fase 5: Definir el plan de implementación
- ✓ Fase 6: Desarrollar el plan de implementación
- ✓ Fase 7: Monitorear y controlar el desempeño de la implementación

Contiene → Objetivo

Contiene → Actividades

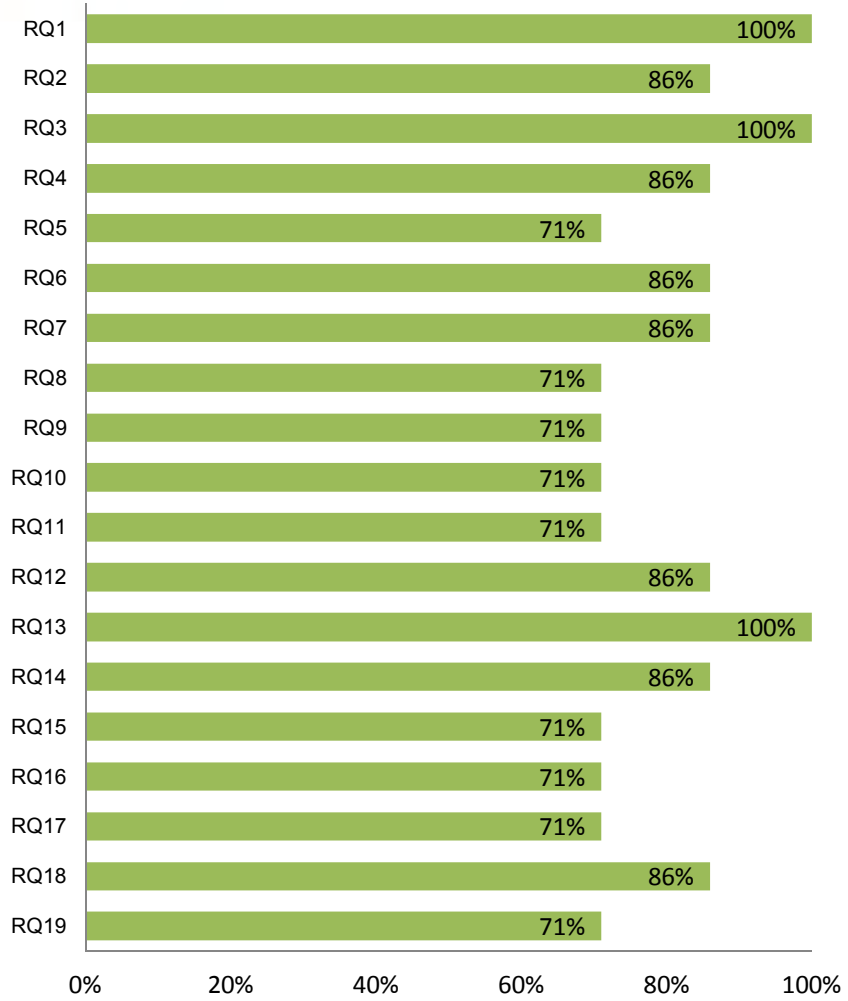
Contiene → Entregables

Validación de la propuesta



- ✓ Validación de los 19 requerimientos de TI.
- ✓ Validación del modelo de Gobierno de TI para entidades bancarias de Colombia propuesto.
- ✓ Validación de la autoevaluación de nivel de madurez de gobierno de TI propuesta
- ✓ Validación de la aplicabilidad de la guía de implementación propuesta.

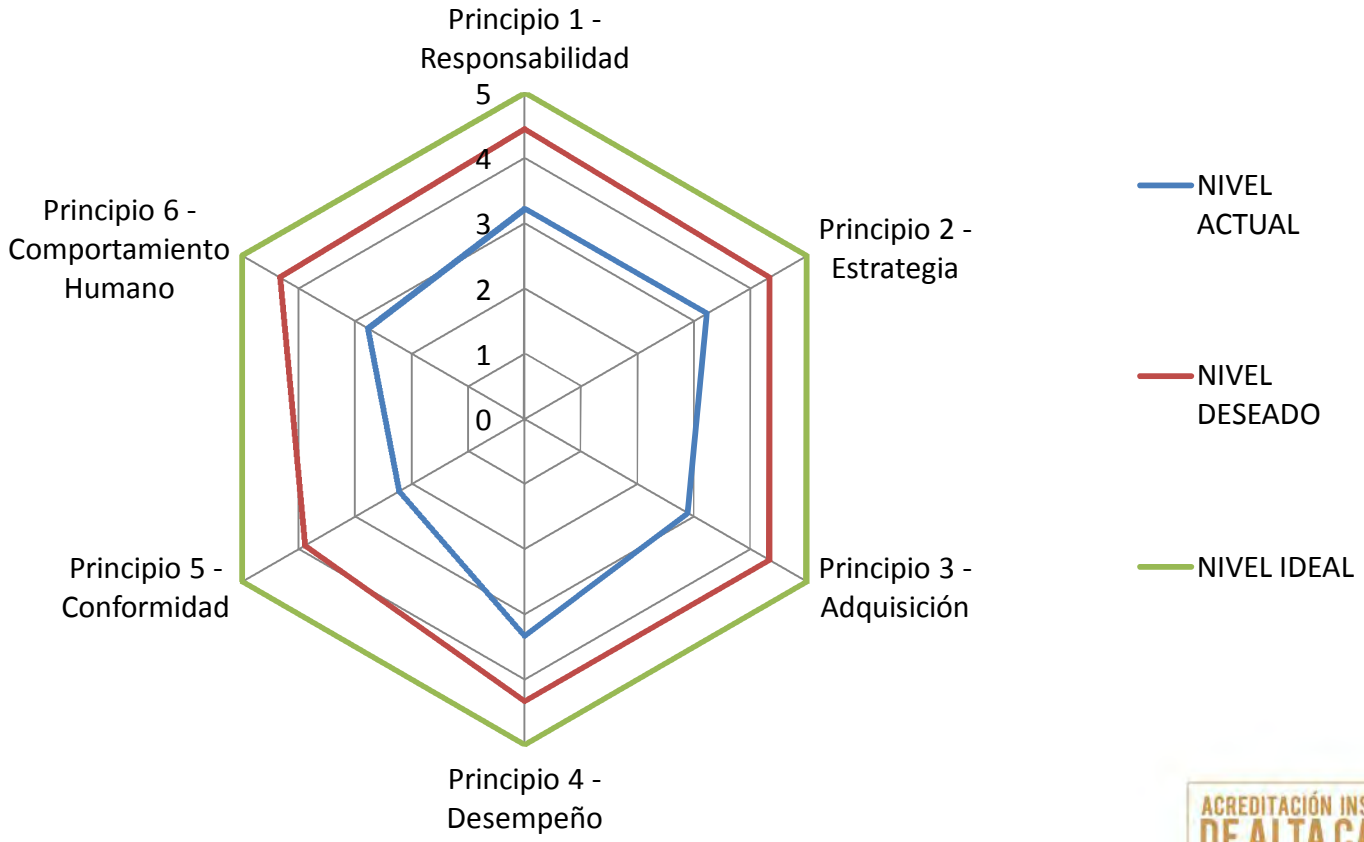
Resultados obtenidos



RQ01	**Plan estratégico de tecnología.**	**RQ11**	**Administración de servicios con terceros.**
RQ02	Infraestructura de tecnología.	RQ12	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
RQ03	Relaciones con proveedores.	RQ13	Continuidad del negocio.
RQ04	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	RQ14	Seguridad de los sistemas.
RQ05	Administración de proyectos de sistemas.	RQ15	Educación y entrenamiento de usuarios.
RQ06	Administración de la calidad.	RQ16	Administración de los datos.
RQ07	Adquisición de tecnología.	RQ17	Administración de instalaciones.
RQ08	Adquisición y mantenimiento de software de aplicación.	RQ18	Administración de operaciones de tecnología.
RQ09	Instalación y acreditación de sistemas.	RQ19	Gestión de la Documentación.
RQ10	Administración de cambios.		

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD
PRIMERA UNIVERSIDAD PRIVADA DEL SUROCCIDENTE COLOMBIANO

Resultados obtenidos



Bibliografia

- **Superintendencia Financiera de Colombia** *Circular Externa 014 del 2009*, Colombia. http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce014_09.doc
- **Ingrid Lucía Muñoz Periñán MsC, Gonzalo Ulloa Villegas**, *Artículo: Gobierno de TI - Estado del arte*, Revista S&T, Universidad Icesi, Cali, 2011 http://www.icesi.edu.co/biblioteca_digital/bitstream/10906/5568/1/Gobierno_de_TI.pdf
- **ISACA Manuel Ballester Ph D,** *Gobierno de las TIC ISO/IEC 38500*. The ISACA Journal Online published, 2010, http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/jpdf1001-online-gobierno.pdf
- **IT Governance Institute**, *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.2008,* http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.
- **IT Governance Institute,** *Informe: Global Status Report on the Governance of Enterprise IT,* 2011, http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf
- **ISACA - Centro de Conocimiento**, *Caso de Estudio: Banco Supervielle S.A., Argentina*,
- http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/COBIT-Caso-de-Estudio-Banco-Supervielle-SA-Argentina.aspx
- **ISACA - Centro de Conocimiento**, Caso *de Estudio: Grupo Bancolombia Implements COBIT to Help Ensure Compliance and Improve Processes.* http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Grupo-Bancolombia.aspx
- **ISACA Manuel Ballester, Ph.D,** *Artículo: Gobierno de las TIC ISO/IEC 38500, Isaca Journal*, 2010,
- **Antonio Fernández Martínez**, *Gobierno de las TI para universidades,* Universidad de Almería; Faraón Llorens Largo, Universidad de Alicante, 2011
- **ISACA. Steven De Haes, Ph.D., Wim Van Grembergen, Ph.D.**, *Artículo: Moving From IT Governance to Enterprise Governance of IT*, Isaca Journal, 2009.

Muchas Gracias

Maria Helena Correa – maryh15@gmail.com

Breyner Alexander Parra - breyneralexander@gmail.com