



UNIVERSIDAD NACIONAL DE COLOMBIA

# Diseño de un *framework* para el gobierno de información con base en COBIT

**Carolina Rincón López**

Universidad Nacional de Colombia - sede Medellín Facultad  
de minas - Escuela de Ingeniería de la Organización  
Medellín, Colombia  
Abril  
2016



# Diseño de un *framework* para el gobierno de información con base en COBIT

**Carolina Rincón López**

Trabajo final de maestría presentado como requisito parcial para optar al Título de

**“Magíster en Ingeniería  
Administrativa”**

Director:  
PhD. Miguel David Rojas López

Grupo de investigación:  
CINCO

Universidad Nacional de Colombia - sede Medellín Facultad  
de minas - Escuela de Ingeniería de la Organización  
Medellín, Colombia  
Abril  
2016

## DEDICATORIA

A Nancy, Hernan, Laura y Sebastian quienes representan fortaleza e incondicionalidad.

A Alejandro, por su apoyo y motivación para ser cada día mejor.

## **AGRADECIMIENTOS**

Gracias a mi tutor por creer en la importancia del tema y guiarme en el desarrollo de este trabajo.

A la organización de seguros colombiana que permitió el desarrollo de la propuesta de *framework* de gobierno de información con base en sus buenas prácticas de gobierno de tecnología de información - TI.

## TABLA DE CONTENIDO

RESUMEN.....	7
ABSTRACT .....	8
INTRODUCCIÓN.....	9
1. MARCO TEÓRICO .....	11
1.1 <i>Framework</i> .....	11
1.2 <i>Control Objective for Information and Related Technologies - COBIT -</i> .....	12
1.3 Activo de información .....	13
1.4 Gobierno de información .....	14
1.5 Calidad de información.....	15
1.6 Gestión del ciclo de vida de la información.....	16
2. SECTOR SEGUROS EN COLOMBIA .....	17
3. TRABAJOS RELACIONADOS.....	21
4. PROPUESTA .....	28
4.1 <i>Framework</i> Gobierno de Información .....	28
4.2 Procedimiento Identificación de activos de información.....	33
4.2.1 Encuesta identificación de activos .....	33
4.2.2 Roles y responsabilidades .....	35
4.2.3 Clasificación de información .....	35
4.2.4 Actividades de calidad de información .....	36
4.2.5 Actividades de conservación de información.....	37
4.2.6 Cumplimiento normativo .....	37
5. CONCLUSIONES .....	39
6. REFERENCIAS .....	40

## RESUMEN

Desde 1874 el sector asegurador colombiano presenta crecimientos en los productos de generales y vida. Especialmente, en la segunda década del siglo XXI, el crecimiento se ha mantenido entre el 5% y el 10%, a pesar de que no se trata de un producto tangible y el negocio se basa en probabilidades de ocurrencia de riesgos.

Al ser una industria con pólizas expedidas por más de veintiún mil millones de pesos al año, es un negocio que debe velar por el cumplimiento de leyes y normas de diferentes entes regulatorios. Algunas de estas tienen como objetivo el tratamiento adecuado de información, obligando a las organizaciones a tener controles en los procesos que garanticen lo exigido por la ley.

Por otro lado, la toma de decisiones en las compañías se basa en la confianza que tengan los altos directivos en la información. Además, con la evolución tecnológica se incrementan los riesgos asociados con la disponibilidad, oportunidad, calidad y conservación de la información, por lo que es necesario establecer directrices que eviten la materialización de estos.

Se propone un *framework* de gobierno de información, que tiene como objetivo conocer los activos de información, asignación de roles y responsabilidades y la definición de lineamientos para el tratamiento adecuado de la información. De esta forma, la organización podrá responder solicitudes de entes regulatorios, tomar decisiones acertadas y ver disminuciones de costos ya sea por eliminar los procesos o por inversiones acertadas en tecnología.

El capítulo uno de este trabajo es el marco teórico, en el cual se incluyen los conceptos claves para la propuesta. El capítulo dos, relata brevemente la evolución del sector asegurador en Colombia, contexto en el cual se desarrolla la base del trabajo actual. Seguido, está el tercer capítulo, que resume de acuerdo al tiempo la evolución del concepto de gobierno de información desde la definición de activo de información hasta arquitectura de información. Luego, en el capítulo cuatro, se desarrolla la propuesta, la cual se trata de un *framework* de gobierno de información y una descripción del procedimiento de identificación de activos de información. Posteriormente, se presentan las conclusiones relacionadas con el diseño del *framework*.

## **ABSTRACT**

Since 1874, the Colombian insurance market has had a growth in the General and Life lines of insurance. In the last years, it has steadily grown by 5% and 10%, despite not being a tangible product and that the business is based on the risk materialization probability.

Being an industry with more than 21 billion pesos in issued policies per year, it has to comply with several laws and regulations. Some of them aim the appropriate information processing, forcing the insurance companies to apply controls in their process in order to meet these regulations.

On the other hand, decision taking in these kind of companies is highly based in the trust that senior management has on the information. Furthermore, the technological capabilities nowadays increase the risks associated with availability, opportunity, quality and conservation, which requires establishing directives in order to mitigate the materialization of those risks.

The proposal is related to an information governance framework, which objective is to know the information assets in order to assign rights and responsibilities for defining guidelines for proper manage of information. So, the organization will be able for facing the legal requirements, decision making based on trust and decreasing cost.

Chapter one of this work is the theoretical framework, which talks about the key concepts of the proposal. Chapter two briefly talks the evolution of the insurance industry in Colombia, which is the domain this work is developed on. After that, chapter three summarizes the evolution of the Information Governance concept, from the definition of information asset to the notion of information architecture. Then, chapter four details the proposal, which is an information governance framework and a description of the information asset identification process, which starts out an information governance program. Finally, conclusions are presented.



## INTRODUCCIÓN

El Gobierno de información es un concepto en desarrollo, el cual debe implementarse en organizaciones independientemente de su tamaño y sector económico. Stoner *et al.* (1996) definen organización como las relaciones múltiples entre personas dirigidas por un líder con el propósito de cumplir metas comunes definidas en la planeación. También, exponen estructura organizacional como la forma de dividir las actividades de una compañía para el cumplimiento de objetivos. Wohlhaupter (2012) afirma que en cada organización el trabajo se divide en procesos, con los que se pretende generar valor a través de la eficacia y la eficiencia. Dicho lo anterior, la organización es la unión de varios procesos que tienen como propósito el cumplimiento de una misma meta, la cual se logra por medio de decisiones basadas en información. Razón por la cual, la organización debe conocer su información y definir normas para el tratamiento adecuado de la misma. Sin embargo, las compañías se inclinan a valorar los activos tangibles como la infraestructura tecnológica, porque representan una forma de agilizar los procesos, disminuir la operatividad y facilitar el manejo de la información. No obstante, en el momento en que ésta falta o no es de buena calidad, invierten esfuerzos en el mejoramiento y disponibilidad de los datos.

Constantemente se crea información en los procesos o se necesita de ella para ejecutarlos y la toma de decisiones depende de la calidad y oportunidad de la misma. Además, actualmente existen normas que exigen a las organizaciones ser conscientes sobre el valor de los datos y la información. Como en las compañías de seguros, las cuales están vigiladas por la Superintendencia financiera, Superintendencia de salud, Superintendencia de industria y comercio, entre otros. Asimismo, existen leyes como *Habeas Data* que exigen calidad y seguridad en el acceso y al momento de compartir información de las personas.

Lo anterior se evidencia en trabajos como el de Glazer (1991), el cual afirma que los avances en tecnologías de información – TI - llevan a un aumento considerable en el volumen de la información y la velocidad con la cual se transmite, siendo necesario que la información *per se* y la gestión de la misma sean considerados variables como la tecnología, al momento de tomar decisiones en aquellas organizaciones donde la información es el principal insumo de los procesos. Černá (2014) afirma que se está pasando de una sociedad industrializada a una sociedad informada donde la información es usada para la toma de decisiones en las organizaciones y es durante este proceso cuando es evidente el valor que tiene el activo para las mismas y debe tratarse adecuadamente. Igualmente, Shi *et al.* (2007) mencionan a Nicolls (2002), quien reconoce la información como un activo y sugiere que el tratamiento de ella obedece a la importancia que ésta tenga dentro de la organización. Mientras que Losee (1997) menciona que el valor de la salida de cualquier tipo de proceso es la información; consecuente con Rafaeli (2003), quien dice que la información es un producto de entrada y de salida en la creación de bienes y servicios (mencionado por Kooper *et al.* 2011).

Grimstad & Myrseth (2011) mencionan el triángulo de dependencia entre el contexto legal en el cual se desenvuelve la organización, el tipo de negocio y los activos de información que usan para la ejecución de sus actividades. Partiendo de esto y conociendo la importancia de la información en el desempeño de la organización, es necesario, definir una guía de buenas prácticas que permita la gestión adecuada de la información empresarial. Ésta debe contener procesos para disponer de información correcta y oportuna en el momento indicado; además, asegurar el cumplimiento de normas provistas por entes regulatorios. Esto se debe a que la implementación de un *framework* en una organización habilita el logro de metas, por medio de la estandarización de procesos, definición de roles y responsabilidades y el establecimiento de una dirección que permita a cada uno de ellos tener el objetivo común.

Kerr & Murthy (2013) presentan COBIT como el *framework* más usado por las firmas auditoras para la evaluación de procesos en las organizaciones, con el propósito de medir la confianza de la información financiera en cada una de ellas, en especial en aquellas que deseen cumplir con la ley **Sarbanes-Oxley<sup>1</sup> - SOX** -. Además, mencionan el proceso de Definir Arquitectura de información y gestión de datos como dos de los procesos relevantes para evaluar dicha confianza.

Partiendo de lo anterior, la propuesta del *framework* para el gobierno de información empresarial se hará con base en COBIT; también se identificarán otras propuestas resaltando elementos de éxito, falla o faltantes para luego proponer una guía del “cómo” de COBIT de los procesos relacionados con la gestión de información de este marco internacional.

---

<sup>1</sup> **Sarbanes-Oxley - SOX**, es una ley Estadounidense creada en el 2002 con el objetivo de dar respuesta a los escándalos financieros de la época. Busca controlar procesos financieros en cualquier tipo de organización. (Consultorio contable EAFIT)

# 1. MARCO TEÓRICO

## 1.1 *Framework*

Un *framework*, según Othman *et al.* (2014) es una guía para establecer dominios, objetivos, procesos con entradas y salidas, roles y responsabilidades con el fin de establecer gobierno en la organización.

Ogan *et al.* (2016) menciona a Stilgoe *et al.* (2013), quien define *framework* como una guía con pasos y trayectorias que permite discusiones de gobierno enfocadas al establecimiento de una dirección y al soporte.

Van Heesch (2012) menciona la norma ISO 2011 para definir un *framework* como un conjunto de prácticas desarrolladas y ejecutadas dentro de un dominio específico. Azapagic (2004) mencionado por Ogan *et al.* (2016) afirma que el desarrollo de un *framework* se concibe como el medio para controlar, administrar o influenciar estándares o normas.

Chen & Xu (2014) agregan que un *framework* efectivo debe ser claro para todas las partes involucradas, incluyendo documentación comprensible y precisa (mencionado en Ogan *et al.*, 2016)

Ogan *et al.* (2016) describen los componentes de la implementación efectiva de un *framework*, ver tabla 1. Estos se describen a continuación.

- Descripción detallada del alcance del *framework*, de las necesidades y el valor de la implantación. Es necesario detallar los problemas, necesidades y oportunidades de mejora para los que se desea implantar el *framework*, ya que aquellos son los que impulsan a una organización al desarrollo de una guía.  
El alcance del *framework* debe incluir las variables dependientes, independientes y de control; se refiere a aquellos factores influyentes dentro del *framework*, es decir, que dado un cambio sobre ellas se produce un cambio en el sistema. Este componente describe también una evaluación para validar la efectividad del mismo.
- Hacer investigación rigurosa sobre los procesos, evaluación de resultados de las actividades actuales y futuras ayuda a definir objetivos y metas alcanzables, para evitar múltiples interpretaciones del *framework*.
- Realizar una guía de implementación incluye una planificación, matriz de decisiones y estrategia de ejecución.
- La re-usabilidad se refiere a la capacidad que debe tener el *framework* para evolucionar de acuerdo con el tiempo y espacio. Eliminando información redundante y con documentación sencilla y efectiva.

COMPONENTE	DESCRIPCIÓN
Descripción y aplicación	Presentación del propósito del <i>framework</i> , incluyendo variables relacionadas con oportunidades de mejora. Es decir, debe mencionar el efecto positivo de la ejecución.
Descripción de objetivos y metas	Presentación de resultados esperados.
Guía de implementación	Contiene planificación, matriz de decisiones y descripción de la implementación.
Asegurar la reusabilidad del <i>framework</i>	Capacidad de adaptación al cambio del <i>framework</i>

Tabla 1. Implementación efectiva de un *framework*.  
Elaborado a partir de Deinsam D. Ogan, 2016

De acuerdo con lo anterior, un *framework* describe procesos de un dominio paso a paso con sus controles e indicadores. Se puede interpretar como el desarrollo del ciclo PHVA, ya que se debe hacer una planeación, ejecución y evaluación del *framework* para antes y durante su implementación. Además, es una forma de estandarizar procesos y orientarlos al cumplimiento de objetivos.

## 1.2 Control Objective for Information and Related Technologies - COBIT -

Othman *et al.* (2014) presentan COBIT, como la guía de gobierno y gestión de TI, más usada por las organizaciones a nivel mundial. *Information Systems Audit and Control Association - ISACA-* por 15 años ha diseñado diferentes versiones del marco de trabajo con base en el uso, implantación y necesidades de las compañías. Se basa en la gestión del riesgo, por lo que se presenta como una guía de 4 dominios: Planear y Organizar, Adquirir e implementar, entregar y dar soporte y monitorear y evaluar. Cada dominio ofrece controles diferentes para los riesgos que se presentan en ellos, y una organización puede o no adoptar la totalidad de los procesos COBIT.

La versión más reciente de este *framework* es COBIT 5 presentado por ISACA en el 2012, la cual consolida la versión anterior con otros *frameworks* como VAL IT, Risk IT y se fortalece con otros estándares internacionales como ISO 27000, ITIL, TOGAF, PMBOK, DMBOK, COSO, PRINCE2, entre otros. Además, los procesos y controles se exponen con base en cinco principios: Entender las necesidades del negocio, cubrir totalmente la organización, uso de una sola guía de gobierno y gestión, habilitar un enfoque holístico diferenciando los conceptos de gobierno y gestión (Wolden *et al.*, 2015). La figura 1 expone estos dos conceptos, muestra que gobierno implica conocer las necesidades del negocio, priorizarlas, establecer una dirección por medio de objetivos, roles y responsabilidades para que la gestión pueda operar y con base en esa operación poder monitorear (G) el desempeño de los procesos. Mientras que la gestión toma la dirección establecida por el gobierno para planear, hacer y monitorear (g); la gestión debe retroalimentar al gobierno para que evalúe el logro de metas y objetivos.

Con base en lo anterior, se observa que COBIT es una guía de gobierno y gestión que presenta las mejores prácticas de TI para que por medio de los procesos tecnológicos se habilite la estrategia de la organización.

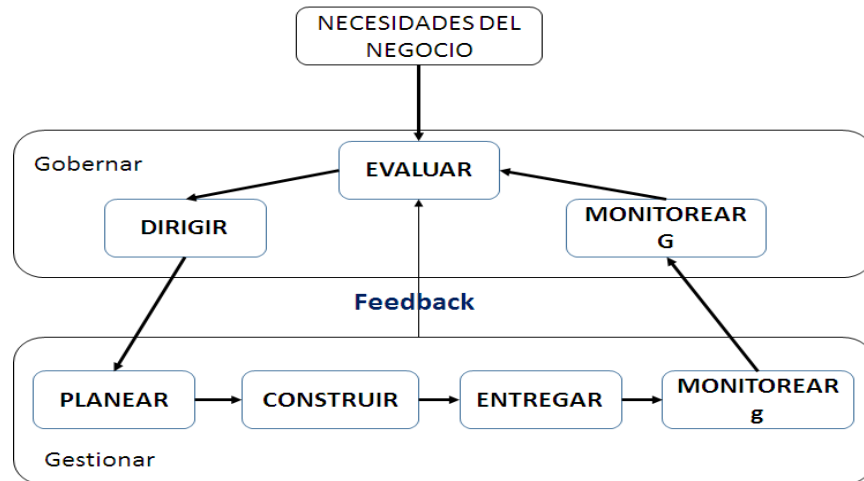


Figura 1. COBIT 5. Diferenciación de Gobierno y gestión.  
Fuente: Adaptado de COBIT® 5, Figura 15. © 2012 ISACA®

En la quinta versión expone 37 procesos diferenciando gobierno de los de gestión, mostrando la relación entre ellos por medio de las entradas y salidas de cada uno. Por esta razón, este *framework* es el medio por el cual una organización puede estandarizar los procedimientos y enfocarlos en la misma dirección, mejorando los controles y procesos de seguridad y disminuyendo riesgos asociados con la tecnología (Kerr & Murthy, 2013).

Es posible concluir que la estandarización de proceso implementando COBIT en una organización tiene como objetivo la alineación de la estrategia corporativa con la estrategia de TI, porque permite evaluar si los procesos de TI tienen objetivos que habiliten el logro de metas de la organización.

### 1.3 Activo de información

Información se define como datos provistos de significado (Checkland & Scholes, 1990). Mingers (1996) la define como datos procesados y útiles, lo que indica que la información es producto de la subjetividad, es decir, depende del observador. Además, describe un dato como un símbolo con un formato almacenado que por sí solo no tiene interpretación. Eaton & Bawden (1991) y Cleveland (1985) consideran los datos y la información como activos con características especiales. Godfrey *et al* (1997) y Henderson & Peirson (1998) (mencionados por Moody & Walsh, 1999) definen un activo como aquel que representa beneficios económicos futuros y tiene el potencial de servicio, es controlado por la organización y es resultado de una transacción del pasado. Partiendo de esto, Moody & Walsh (1999) afirman que la

información es entrada o salida de procesos que pueden representar ingresos para la organización; además, de acuerdo con su ciclo de vida debe tener controles para una adecuada gestión. También, la mayoría de las veces la información es el resultado de la ejecución de una tarea; así, la información se ajusta a la definición de activo, el cual mejora el desempeño en la toma de decisiones, el éxito en el mercado y en los procesos de trabajo. Agregan que los activos de información son un recurso económico clave y uno de los más importantes activos de la organización. Además, comentan a Godfrey, Hodgson, Holmes & Kam (1997) y Henderson y Peirson (1998) quienes añaden que la organización puede obtener un beneficio con la información al venderla o conservarla.

Partiendo de lo anterior, se infiere que un activo de información es la recopilación de datos provistos de significado para la organización, debe ser identificable, valorable y con propietario, el cual define el tratamiento del activo durante todo el ciclo de vida, para que éste tenga un valor apreciable dentro del dominio en donde se crea y usa.

#### **1.4 Gobierno de información**

El gobierno de información es un conjunto de actividades que define responsabilidad en toma de decisiones sobre la valoración, creación, captura, análisis, distribución, almacenamiento, uso, control y disposición de la información”. Responde a las preguntas “¿qué información se necesita?, ¿cómo se puede usar? y ¿quién es responsable por ella? (Kooper *et al.* 2011). Estos autores en su definición permiten observar que lo esperado del gobierno de información es la definición de lineamientos, roles y responsabilidades durante el ciclo de vida de la información.

Guetat & Dakhli (2015) mencionan a McLennan (2014), quien define gobierno de información como “actividades y prácticas desarrolladas para controlar el uso de la información”, agrega que actualmente se evalúa la información como un activo importante para la organización, por lo que proteger y gestionar adecuadamente la información es asunto de todas las personas. También, exponen cómo el gobierno de información y el gobierno de datos se relacionan y usan como sinónimos, sin embargo, exponen gobierno de información como una disciplina relativamente nueva que abarca gobierno de datos, gestión estratégica, gestión de procesos de negocio y gestión del riesgo. también presentan el concepto de McManus (2004) y White *et al* (2007) los cuales dicen que el gobierno de información provee una guía de responsabilidad enfocándose en los principios básicos, reglas, estructuras administrativas, métodos de gestión y acceso a información que hace que su implantación sea efectiva en la organización. Asimismo, caracterizan el gobierno de datos como el establecimiento de derechos de decisión que permita promover el comportamiento deseado en el uso de los datos. Por su parte, Caldo (2011) (mencionado por Alves de Freitas *et al* (2013)) expresa el gobierno de datos como una práctica empresarial que orquesta personas, procesos y tecnología con el fin

de identificar roles y responsabilidades acorde con el inventario de información de una organización con el fin de asignar la mejor calidad a los mismos.

Por su parte, Grimstad & Myrseth (2011) mencionan a Khatri and Brown (2010) para enumerar los dominios del gobierno de información: 1). Aclarar el rol de la información como un activo. 2). Establecer los requisitos de uso de los datos. 3). Establecer el significado de la información para los usuarios de la misma. 4). Especificar los requisitos de acceso a la información. 5). Determinar el ciclo de vida de la información, el cual incluye creación, distribución, almacenamiento y descarte.

El gobierno de información se presenta como el marco de referencia de una organización, que establece lineamientos para identificar activos de información, dueños y usuarios, nivel de confidencialidad, requisitos de calidad, flujos de información que especifican medios de captura, procesos de distribución y transformación, tiempos de retención y procedimientos de descarte basados en el contexto en el cual se desenvuelve la organización.

### **1.5 Calidad de información**

Haug *et al.* (2011), mencionan otros autores como Lederman *et al.* (2003); Tayi & Ballou (1998); Watts & Shankaranarayanan (2009) para definir la calidad como el grado en que la información cumple con el propósito para el cual fue creada.

De acuerdo con COBIT 5, la información tiene 13 dimensiones:

- Exactitud: el grado en el cual la información es correcta y confiable.
- Objetividad: la información está libre de prejuicios.
- Confiabilidad: la información es verdadera y confiable.
- Reputación: la información es vista con base en su origen y contenido.
- Relevancia: la información es útil para la tarea que se necesita.
- Completitud: el grado en el cual la información no falta.
- Actualidad: la información está actualizada para la tarea que se necesita.
- Cantidad apropiada: el volumen de información es el apropiado para la ejecución de la tarea que lo necesita.
- Representación concisa: la información es compacta.
- Consistencia: el grado en el cual la información se presenta en el mismo formato.
- Interpretación: la información está con el idioma, símbolos y unidades definidas.
- Entendimiento: el grado en el que la información es comprensible.
- Fácil de manipular: información fácil de manipular y aplicable a las tareas.

Juddoo (2015) afirma que las dimensiones de calidad son el medio para conocer las medidas de la misma relacionadas con la información, permite conocer cómo mejorar los datos. Además, presenta los componentes de la calidad de información: dimensiones, perfilamiento, limpieza y reglas de calidad.

Perfilamiento se refiere a conocer bases de datos y extraer de ellas información sobre los datos, estadísticas que permitan medir las dimensiones de calidad.

Limpieza consiste en aplicar reglas de negocio con el objetivo de mejorar los datos.

Las reglas de calidad son definiciones que permiten conocer si hay errores en la información, también se usan para la limpieza. Ellas son necesarias para la ejecución del perfilamiento.

## **1.6 Gestión del ciclo de vida de la información**

Existen procedimientos de gestión del ciclo de vida de la información (*Information lifecycle management - ILM*) buscan automatizar el almacenamiento y eliminación de información; Hu (2008) expone que ILM se compone de políticas, prácticas y herramientas con el objetivo de crear valor a la organización mediante una infraestructura adecuada basada en el costo-beneficio. Propone categorizar los datos por estadísticas de consulta: activos, no tan activos, históricos o archivados. Además, presenta el ciclo de vida de la información en cinco etapas: captura y recepción de información, distribución, uso, mantenimiento y disposición.

Al-Fedaghi (2008) afirma que ILM es el proceso que mide el valor de la información, basado en la definición apropiada del tiempo de almacenamiento y eliminación.

Liu *et al.* (2009), mencionan las características de la información, presentando el ciclo de vida de ésta en seis etapas: creación, protección, uso, migración, almacenamiento y descarte. Agregan que ILM es un modelo de gestión que permite controlar el ciclo de vida de la información de toda una organización, desde la creación hasta el descarte. También, afirman que las organizaciones almacenan constantemente información de diversos tipos y en diferentes medios; conocer el tiempo y forma de vida de la información se convierte en un proceso que permite maximizar el valor de la información. En el capítulo 4 se complementa el ciclo de vida de la información.

ILM es un proceso de reconocimiento del valor de la información, busca estar al tanto del flujo de la información con el propósito de desarrollar soluciones tecnológicas con base en él, con el objetivo de mejorar el desempeño de aplicaciones y disminuir costos por almacenamiento.



## 2. SECTOR SEGUROS EN COLOMBIA

El *framework* propuesto en este trabajo, se desarrolla con base en actividades de gobierno de información ejecutadas al interior de una empresa colombiana de seguros. Por esta razón, es necesario conocer parte de la historia de esta industria en el país.

A continuación, con base en Junguito & Rodríguez (2010), en el ensayo “La empresa y la industria aseguradora colombiana en el contexto económico de finales del XIX y XX”, presentan brevemente la historia de la industria aseguradora en Colombia; exponen la primera empresa de seguros del país, constituida en 1874 con un capital de dos millones de pesos, la cual tenía como propósito ocuparse de operaciones económicas permitidas por la ley y relacionadas con los seguros de todo tipo. Esta empresa se conoció como Compañía Colombiana de Seguros, Colseguros, la cual empezó con la expedición de pólizas de transporte e incendio en 1875. La compañía colombiana se creó con capital del estado y accionistas, los cuales eran empresarios y personas de la alta sociedad del país, lo que dio una ventaja frente a empresas extranjeras, ya que conocían los riesgos a los que estaba expuesto el mercado colombiano.

En 1901, se constituyó la Sociedad Seguros de Vida que en 1903 se fusionó con la Compañía Colombiana de Seguros. La estrategia de la segunda, para evitar la competencia fue la fusión, por lo que en 1922, implemento esto nuevamente con la Compañía General de Seguros, la cual se había creado en 1909.

Para el año de 1923 se crea la Superintendencia bancaria, a la cual se le atribuyó la vigilancia de las empresas aseguradoras. En 1926, la Compañía Colombiana decide en conjunto con la Superintendencia bancaria separar los negocios de vida de los negocios de generales, creando la Compañía Colombiana de Seguros de Vida. El mercado de seguros de vida era el más competido para la época, ya que el único conocimiento requerido para el negocio era el de los patrones de mortalidad, lo que dio lugar a un crecimiento en empresas colombianas y extranjeras ofreciendo el mismo producto.

La suma de la participación de las dos compañías en el mercado fue del 30.4% en 1927, es decir, casi la tercera parte del sector. Sin embargo, los productos de generales tenían una participación del 45% aproximadamente, mientras que vida era el 15%, por debajo de otra empresa Colombiana, Mutualidad de Bucaramanga.

La ley 105 de 1927 ordeno a las empresas extranjeras, con deseos de participar en la industria colombiana, cumplir con las leyes internas y ser vigiladas por la Superintendencia Bancaria. Esto implicó renovar el permiso de operación cada año, presentar información a la Superintendencia cuando esta lo solicitaba y hacer reservas para responder a los asegurados.

En la década de los treinta las empresas extranjeras de vida observaron que las leyes dispuestas para su desarrollo iban en contra de sus objetivos, por lo que se

detuvo el crecimiento de participación de éstas, lo que aumento a 51% la participación de las compañías locales.

Hacia el año de 1938 las aseguradoras nacionales tomaron fuerza por un informe publicado por la Superintendencia, en el que restringía el pago de primas a organizaciones por fuera de Colombia con el argumento de ser negocios en crecimiento que no aportaban a la economía del país.

En tiempos de la segunda guerra mundial, el Superintendente Bancario quiso regular el negocio de seguros, decretando un capital mínimo para las diferentes compañías. Con esto se creó un medio propicio para la constitución de estas organizaciones, dando lugar a La Andina de Seguros y Seguros Bolívar en 1938 y 1939 respectivamente. Ambas cumplieron con los requisitos exigidos por la ley, Andina se dedicó a los ramos de daños y Bolívar a vida y accidentes personales. Por los años cuarenta, se formalizó la compañía Suramericana de Seguros, la cual tuvo participación de 32 empresas, de las cuales 31 eran antioqueñas. Para esos días, La Colombiana de Seguros, Seguros Bolívar y Suramericana de Seguros, era las organizaciones líderes en Colombia.

Durante la segunda guerra mundial, por las políticas expedidas por la Superintendencia, se incrementó la participación de las compañías nacionales, pasando del 44% de participación en 1937, al 60% en 1946, lo que demuestra el desplazamiento de la participación de las organizaciones internacionales.

Entre 1949 y 1966 las compañías de seguros nacionales presentaron crecimientos del 5% anual. Se resalta el incremento del sector, no solo en participación de mercado, también las empresas nacionales aumentaron en número, pasando de 31 en 1950 a 73 en 1961. La Colombiana de Seguros empezó a disminuir su participación, mientras que Seguros Bolívar y Suramericana de Seguros aumentaron sus primas vendidas en ese período de tiempo.

La Superintendencia Bancaria, durante 1954 y 1955, amplió las regulaciones del sector. Empezó por revisar los modelos de pólizas y sugirió cambios en los patrones de mortalidad para los seguros de vida. Adicionalmente, hizo validaciones sobre las prácticas contables con el objetivo de expedir un manual para las organizaciones con los requisitos de información que debían cumplir. Más tarde, la Superintendencia quiso vigilar las tarifas de los seguros, los mecanismos como se calculaban. Sin embargo, expuso la deficiencia de métodos para validar si la información era confiable y suficiente para realizar la evaluación. Por esta razón, la Superintendencia buscó asesoría y con ella se dio lugar a la creación de una oficina de estadística, la cual buscaba tener métodos y herramientas suficientes para la evaluación de la información usada en la tarificación de productos.

Las aseguradoras nacionales buscaban tener un mercado con más competencia, además de tener menos regulaciones. Por esto en 1976 se creó la Federación de Aseguradores Colombianos – FASECOLDA – que tenía como objetivo “promover la

industria al hacer presencia ante las autoridades de Gobierno, Congreso y otras fuerzas vivas del País”.

En 1990 se dio una apertura comercial, permitiendo el ingreso de compañías extranjeras al mercado. El sector pasó a ser dinámico, con variedad en productos y libertad para tarifar. Este comportamiento, dio lugar a la creación de seguros obligatorios en el país, estableciendo la seguridad social en Colombia. Este nuevo sector contemplaba salud, riesgos profesionales, accidentes de tránsito, seguros previsionales y rentas vitalicias, estos últimos para personas pensionadas y ahorradores de fondos privados de pensiones.

Antes de 1990 el sector asegurador colombiano, no tenía libertad en creación y tarificación de productos, además, el valor reasegurado tenía un tope máximo por año y cualquier movimiento debía hacerse con previa autorización de la Superintendencia Bancaria. Para principios de los años noventa, la dinámica del sector cambió al tener libertad en las negociaciones con empresas reaseguradoras, definición de tarifas, incremento de competencia e inversión extranjera. Sin embargo, la Superintendencia empezó a proteger los derechos del consumidor, exigiendo a las aseguradoras tener información veraz y clara en las pólizas de los clientes, exponiendo información de coberturas y exclusiones. Además exigió consistencia entre las notas técnicas y las pólizas.

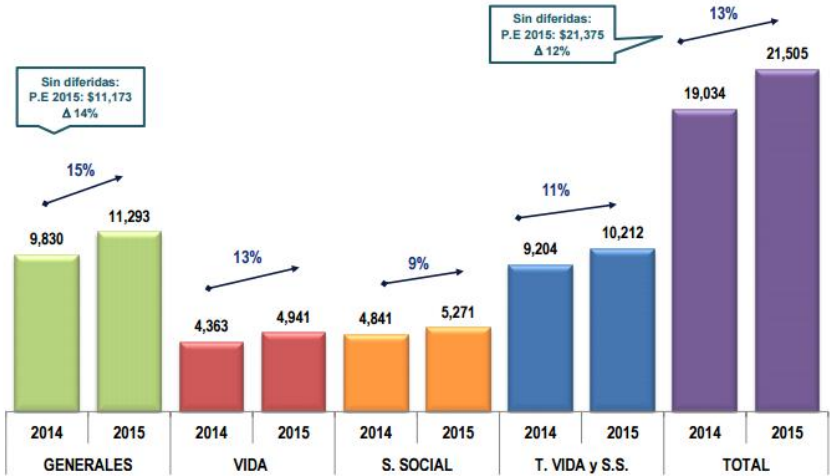


Grafico 1. Primas emitidas enero - diciembre 2015  
Fuente: tomada de Fasecolda.

El sector asegurador colombiano presenta crecimientos anuales del 10%. Incluso en tiempos de crisis financiera se dio este crecimiento, por lo que la perspectiva futura se muestra positiva para este sector por el potencial de crecimiento que tiene la región latinoamericana (Fundación Maphre, 2014).

En el 2015 el crecimiento de cada ramo fue del 15% para generales y del 13% para vida. En el gráfico 1, se puede observar el comportamiento de cada uno en ese período de tiempo.

Al tratarse de productos intangibles y venta de prevención de riesgos, el sector asegurador tiene una fortaleza mantenida a pesar de ser vigilado y controlado. Como ya se mencionó, pasó de necesitar aprobación desde el diseño de productos hasta la tarifa a ser una industria con autonomía. Sin embargo, el sector continúa con vigilancia a su información, especialmente financiera y aquella en la que se involucre al cliente.

A partir de esto, es notable la necesidad de información confiable que permita a estas organizaciones cumplir con los requerimientos exigidos por la ley y tomar decisiones acertadas en los negocios.

### 3. TRABAJOS RELACIONADOS

Inicialmente, se estructura el momento histórico de la ocurrencia de cada uno de los aportes hechos en el tema de gobierno de información desde la definición de activo de información hasta la relación de gobierno de información con arquitectura de información.

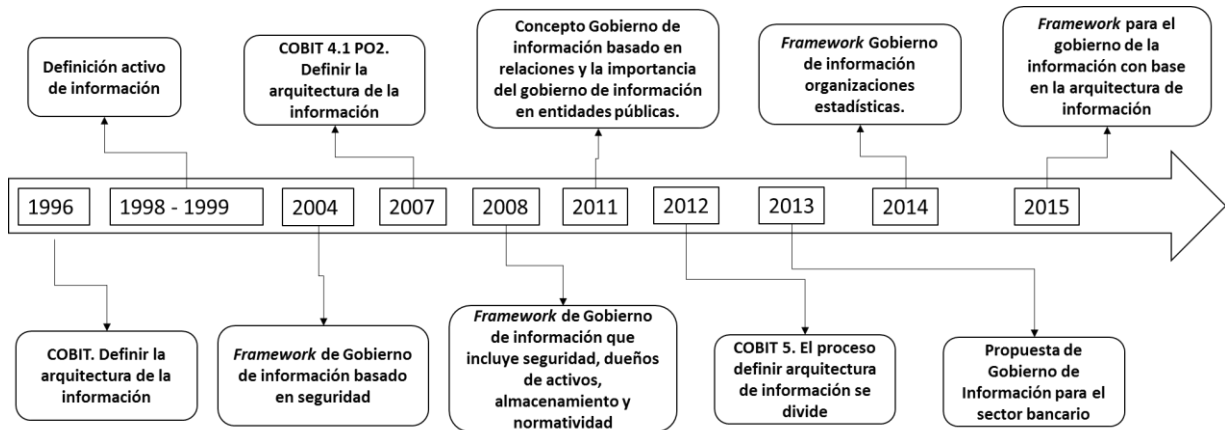


Figura 2. Evolución del concepto de información como activo hacia el concepto de gobierno de información.

Fuente: Elaboración propia.

En la figura 2, se presenta la evolución en el tiempo de los conceptos de activo de información y gobierno de información, registrados en trabajos académicos y el momento en el que se presenta en COBIT, el proceso de Definir la Arquitectura de Información.

Donaldson & Walker (2004) introducen el concepto de Gobierno de información por medio de un *framework* desarrollado por la Sociedad Nacional de Salud (NHS por sus siglas en inglés), basado en la expectativa de los pacientes relacionada con la seguridad, confidencialidad, completitud y oportunidad de la información almacenada de los diagnósticos y tratamientos.

La figura 3 muestra los objetivos del *framework* propuesto por la NHS, para que todas las organizaciones asociadas a ésta establezcan el tratamiento adecuado a la información de los pacientes desde el momento de captura hasta almacenamiento. Estandarización, pretende conocer todos los requerimientos asociados a la información. Propiedad, se refiere a conocer el dueño de la información quien es el responsable en la toma de decisiones sobre ella. Indemnización y soporte que se le da a las organizaciones que trabajan dentro de las políticas presentadas en este *framework*. Cumplimiento regulatorio de la normatividad vigente y actualizaciones de la misma.

Asimismo, un reporte publicado por *Economist Intelligence Unit* (2008) incluye en su definición de gobierno de información *records management*, normatividad, seguridad, flujos de datos, dueños de información y almacenamiento de información.

Kooper *et al.* (2011), afirman que no existe una definición común y académica para gobierno de información y el trabajo se resume en determinar el concepto partiendo de los principios de TI. Además, parten de lo dicho por Maes (1999), quien expone que la información es el vínculo que falta entre TI y el negocio, y agregan que la información es un activo intangible y un recurso del negocio independiente de TI. También declaran que una organización consciente de la información con un gobierno establecido hace que la organización sea más efectiva en los procesos y aclara que el gobierno no es solo al momento de crear la información. Estos autores, incluso mencionan que el gobierno de información se ve como un *framework* que tiene como objetivo optimizar el valor de la información. La definición de gobierno de información se fundamenta en actores y la relación que tengan estos con la información, sosteniendo que un *framework* jerárquico puede ser contraproducente para gobernar la información, debido a que tiene varios estados y en cada uno interviene un actor diferente.

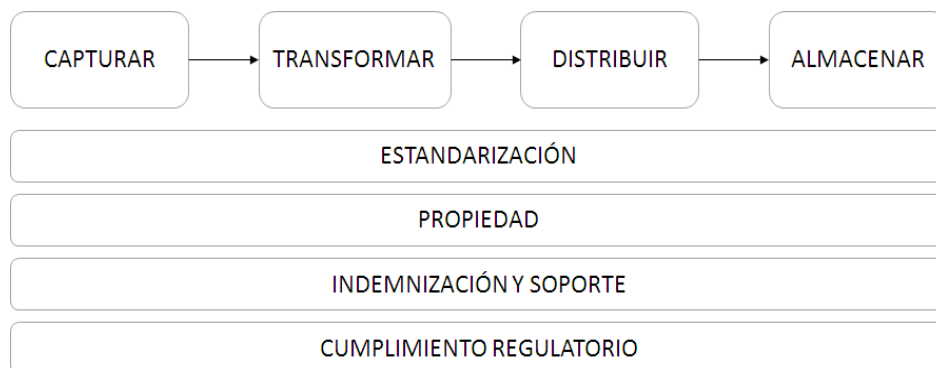


Figura 3. *Framework* gobierno de información de la NHS. Elaborado a partir de Donaldson & Walker (2004)

Grimstad & Myrseth (2011) mencionan la importancia del gobierno de información en entidades públicas, además exhiben la relación entre éste y la estrategia de metadata para inteligencia de negocios. Presentan el triángulo de la dependencia mencionado anteriormente, agregando un sexto dominio a los cinco presentados por Khatri and Brown (2010) (mencionados por Grimstad & Myrseth (2011)), el dominio de cumplimiento normativo. Además, exponen la diferencia entre gobierno y gestión, el primero lo resumen como la definición de quién toma decisiones sobre la información, mientras que la gestión está relacionada con la ejecución de esas decisiones.

De Abreu Faria *et al.* (2013) mencionan a Soares (2011) quien declara que “el gobierno de información es la definición de políticas para optimizar, asegurar y

apalancar la información como un activo de la organización mediante la alineación de objetivos”. Además, aportan que el gobierno de información involucra aquella que es estructurada y no estructurada, es decir, bases de datos en medios digitales, archivos en papel, correos electrónicos, entre otros. La propuesta de estos autores, se centra en la definición de un *framework* para el sector bancario y se fundamenta en la propuesta de Hohman (2011) quien expone el gobierno de información como un programa en el que participan personas, procesos y herramientas. Las personas, son las responsables por la definición de la estrategia del gobierno de información en toda la organización; los procesos, se refieren a la ejecución del programa; Las herramientas, son los procedimientos, metodologías, aplicaciones, entre otras usadas para crear, capturar, gestionar, almacenar, preservar y descartar información. También exponen a Samuelson (2010), el cual identifica cuatro pilares en el *framework* de gobierno: personas, políticas, tecnología y gestión del riesgo. Tomando lo anterior los autores De Abreu Faria *et al.* (2013) formulan un marco de gobierno de información con base en tres pilares: personas, políticas y tecnología. En la figura 4 se muestra el *framework* propuesto por estos autores, en él se observan los factores relevantes para el sector bancario y la relación con cada pilar.

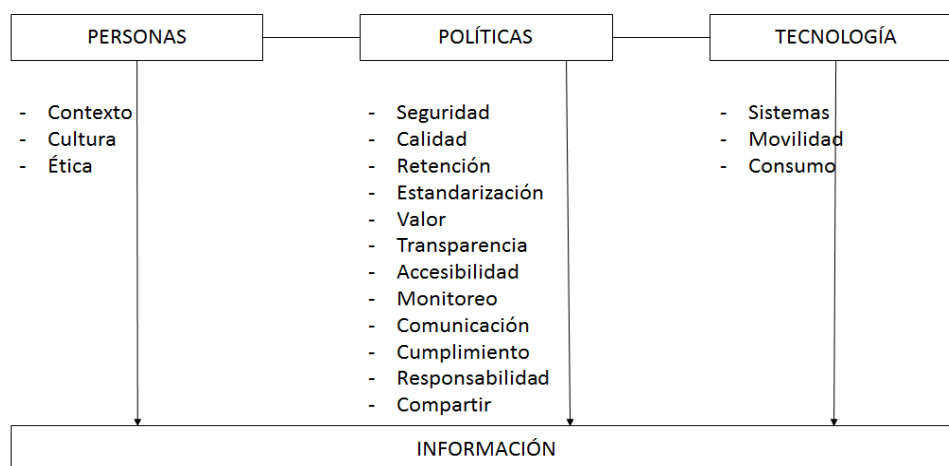


Figura 4. *Framework* Gobierno de Información para entidades bancarias.

Fuente: tomado de De Abreu Faria *et al.* (2013)

Kusumah (2014) usa el *framework* de la compañía IBM en la investigación para proponer un modelo de gobierno de información para una organización estadística. Éste consiste en tres dimensiones: personas, procesos y tecnología. En el modelo propuesto se asigna actividades a cada dimensión. Así, las personas son las que deben crear conciencia sobre el buen uso de la información; además, deben conocer su rol y la responsabilidad que éste conlleva. Por otro lado, las actividades relacionadas con procesos son aquellas en las que deban implementar políticas o controles con base en el problema o necesidad de la organización; finalmente, la tecnología debe garantizar la seguridad y privacidad de la información, también debe apalancar la rápida toma de decisiones por medio de una vista única de información.

Analizando la propuesta de Kusumah (2014) y De Abreu Faria *et al.* (2013), se observa que son similares, la diferencia radica en que para uno es proceso y el segundo es políticas. Ambos direccionan a la definición y ejecución de políticas.

Guetat & Dakhli (2015) proponen un *framework* de gobierno de información con el que demuestran la diferencia entre éste y gobierno de TI y la dependencia existente entre ellos para un gobierno de información efectivo. La figura 6 expone la propuesta de Guetat & Dakhli (2015), en la cual sugieren 4 pilares: estrategia corporativa, normatividad, calidad de información y seguridad de información. Afirman que para ser efectivo el gobierno de información, los objetivos de éste deben estar alineados con la estrategia corporativa, además, en este pilar se deben conocer los repositorios de información sobre procesos, reglas y restricciones de la organización. El bloque de normatividad se refiere a conocer normas internas y externas que restringen los procesos corporativos y por consiguiente afectan el gobierno de información.



Figura 6. *Framework* Gobierno de información  
Fuente: Guetat & Dakhli (2015)

Calidad de información se refiere a la expectativa de calidad que tenga la organización frente a los datos. Seguridad de información se relaciona con la documentación de requerimientos de seguridad que tenga la información en cada proceso. Adicionalmente, los autores plantean 4 capas de acción para que el gobierno de información funcione al interior de la organización: organización y negocio, arquitectura, gestión del cambio y por último los métodos y las herramientas. Organización y negocio se refiere a toda la información sobre procesos, roles y responsabilidades. Arquitectura hace referencia a la arquitectura empresarial y arquitectura de aplicaciones con el fin de conocer estándares y lineamientos para la construcción de las aplicaciones y repositorios de información de la organización. Métodos y herramientas, describen todo aquello que soporta las actividades de gobierno de información. Gestión del cambio, se asocia al modelo de gestión cultural con el objetivo de superar la resistencia al cambio en la organización.



En la tabla 2, se estructura un comparativo entre la versión reciente de COBIT y la anterior, con el fin de presentar los procesos que absorbieron prácticas en la última versión. COBIT en su versión 4.1, presenta en el proceso PO2 llamado: Definir la arquitectura de información, prácticas como la definición de un esquema de información en la que se relacionen dueños, clasificación y conservación de la misma con base en la estrategia de la organización. Además, propone la creación de un diccionario de datos como medio para establecer un lenguaje estándar comprensible por personas del negocio y de TI. Igualmente, sugiere procedimientos de calidad, que evalúen la integridad, consistencia y disponibilidad de la información. Sin embargo, en la versión reciente de COBIT, la número 5, el proceso anterior está embebido en los procesos APO01 y APO03. El primero se refiere a Gestionar el marco de gobierno de TI, en la práctica APO01.06 pretende definir los propietarios de la información y un esquema de clasificación de acuerdo con la confidencialidad, lo cual mapea con otra norma internacional, ISO 27001.

COBIT 4.1 PO2	COBIT 5. APO01.06	COBIT 5. APO03.02
1. Definición de un esquema de información. 2. Creación de un diccionario de datos. 3. Administrar la integridad	1. Definir información y propietarios de sistemas.	1. Esquema de clasificación de datos: incluye información del propietario, definición de niveles de seguridad y tiempos de conservación. 2. Diccionario de datos.

Tabla 2. Mapeo COBIT 4.1 con COBIT 5.

Fuente: Elaboración propia, a partir de COBIT® 5 © 2012 ISACA® y COBIT® 4.1 2007 ISACA®

El proceso APO03, Gestionar la arquitectura empresarial, menciona que la organización debería establecer una arquitectura común en la que intervengan procesos de negocio, información, arquitectura de aplicaciones y arquitectura de infraestructura con el propósito de lograr una alineación entre la estrategia organizacional y la estrategia de TI. La práctica APO03.02 Definir arquitectura de referencias, establece un modelo de arquitectura de información con base en la clasificación de la misma y la estrategia organizacional.

En la tabla 3 se relacionan las investigaciones expuestas en este apartado, con el objetivo de dar una visión global de los avances realizados y los trabajos propuestos para continuar explorando en el campo de conocimiento.

Se observa que los trabajos son investigaciones realizadas entre el 2004 y el 2015, lo que permite concluir que el concepto de gobierno de información está en etapa de desarrollo y aunque se ejecuten propuestas en diversos campos, el objetivo es el mismo para todos, incrementar el valor de la información para optimizar el uso de recursos en la organización y disminuir el impacto de los riesgos o evitar que ocurran. Un *framework* de gobierno de información es particular para cada tipo de organización y debe ser soportado por calidad, seguridad y conservación.

AUTORES	PROPUESTA	TRABAJO FUTURO
Donaldson & Walker (2004)	<i>Framework</i> basado en la seguridad de la información.	No se expone
Economist Intelligence Unit (2008)	Encuesta en la que se presentan las dimensiones que debe contemplar el gobierno de información	No se expone
Kooper <i>et al.</i> (2011)	Definición de gobierno de información basado en las relaciones. No es una definición jerárquica.	Medición del valor de la información Rol de creador de la información Gobierno de información para intercambios en diferentes redes o grupos.
Grimstad & Myrseth (2011)	Relación entre el gobierno de información y la definición de la metadata de una organización, particularmente en el sector público.	No se expone
De Abreu Faria <i>et al.</i> (2013)	<i>Framework</i> de tres dimensiones y veinte factores. Además proponen una definición del concepto de gobierno de información.	No se expone
Kusumah (2014)	<i>Framework</i> de gobierno de información basado en el <i>framework</i> de IBM. Definen tres dimensiones: personas, procesos y tecnología.	No se expone
Guetat & Dakhli (2015)	<i>Framework</i> de gobierno de información basado en la definición de arquitectura de información. Incluye la estrategia organizacional, la normatividad, seguridad, calidad, procesos de negocio, gestión del cambio, arquitectura y herramientas.	Análisis de la arquitectura de información con el fin de definir indicadores que permitan medir la efectividad del gobierno de información.
COBIT	No especifica el gobierno de la información, se centra en la arquitectura de información específicamente en calidad, conservación y seguridad de los datos.	No se expone

Tabla 3. Resumen sobre trabajos relacionados

Fuente: Elaboración propia.

Los factores de éxito o falla de cada *framework* se podrían relacionar con el trabajo a futuro de cada propuesta. Para cada una de ellas en los que no se expone, se podría inferir que faltó un análisis más riguroso. Además, se observa que en varias investigaciones se menciona que un Gobierno de Información bien definido puede disminuir costos, mejorar el desempeño y disminuir el impacto de los riesgos. Esto

da lugar a nuevas investigaciones, relacionadas con el desarrollo de modelos dinámicos que permitan simular el comportamiento de una organización para validar estas premisas. También, se deduce que COBIT no es la base de ninguna de las investigaciones. Por otro lado los trabajos revisados están por fuera de Colombia, así se da la posibilidad de validar en compañías locales la forma en que ellas abordan el gobierno de información.

## 4. PROPUESTA

La ley SOX se implementa en las organizaciones con el propósito de mostrar que su información financiera es confiable, es el medio que tiene Estados Unidos para vigilar las compañías que cotizan acciones en la bolsa de Nueva York. Para confirmar esto, las firmas auditoras generalmente usan COBIT como marco de referencia para evaluar la confianza en la información y nivel de madurez de cada uno de los procesos de TI. Uno de los procesos presentados por COBIT en la versión 4.1 es “Definir la arquitectura de la información” y en COBIT 5 se incluye el proceso dentro de definir el gobierno de TI y arquitectura empresarial y presenta la información como un habilitador de los 38 procesos propuestos para el gobierno y gestión de TI. Lo anterior demuestra la relevancia que tiene COBIT para el desarrollo de buenas prácticas de TI, por lo que a partir de éste se desea estandarizar un proceso que guíe la implementación del gobierno de información en una compañía.

Inicialmente se presentará la propuesta general de gobierno de información, que busca potenciar el valor de la información y luego se presentará el proceso que da lugar a la implementación del *framework*.

### 4.1 *Framework* Gobierno de Información

El Gobierno de información es un concepto en desarrollo, el cual debe implementarse en organizaciones independientemente de su tamaño y sector económico. Stoner *et al.* (1996) definen organización como las relaciones múltiples entre personas dirigidas por un líder con el propósito de cumplir con metas comunes definidas en la planeación. También, exponen estructura organizacional como la forma de dividir las actividades de una compañía para el cumplimiento de objetivos. Wohlhaupter (2012) afirma que en cada organización el trabajo se divide en procesos, con los que se pretende generar valor a través de la eficacia y la eficiencia. Dicho lo anterior, la organización es la unión de varios procesos que tienen como propósito el cumplimiento de una misma meta, la cual se logra por medio de decisiones basadas en información. Razón por la cual, la organización debe conocer su información y definir normas para el tratamiento adecuado de la misma

La base del *framework* de gobierno de información propuesto, se toma del diseño realizado al interior de un área de tecnología de una organización colombiana del sector seguros, con el objetivo de dar cumplimiento a la circular 042 y 052 de la superintendencia financiera del 2011. Además, se complementa con otras propuestas y se mapea con las prácticas presentadas en los procesos APO02 de COBIT 4.1, COBIT 5. APO01.06 y COBIT 5. APO03.02 explicados en la tabla 2.

Para el diseño de esta guía se tiene claro la diferencia entre dato e información, se entiende por dato cualquier símbolo que por sí solo no tiene significado. Información es la recopilación de datos con interpretación de acuerdo al contexto en el que se

analizan. Tomando la definición de activo de información adoptada por una compañía de seguros colombiana, la recopilación identificable de datos provistos de significado que representan un valor para la organización por su venta o conservación se conoce como activo de información, además, por tener un ciclo de vida definido y su pérdida o mal uso representen un riesgo para la organización.

La figura 7 presenta el ciclo de vida de la información interpretado en flujo de información, el cual comprende etapas de creación, transformación, distribución, almacenamiento y descarte. Durante cada una de estas etapas se tiene un gobierno para garantizar disponibilidad e integridad de la información. Con base en esto se eligen los pilares de la información, los cuales pueden ser tres: seguridad, calidad y conservación. La conservación tiene una característica particular, porque ocurre al final del ciclo, es decir, siendo un pilar hace parte del flujo de información. Además, como se observa en la tabla 2, estas son las categorías en las que se pueden agrupar las prácticas propuestas por las versiones de COBIT. Adicionalmente, son los factores que dan lugar a la materialización de riesgos dentro de la organización. Seguridad se refiere a la clasificación que debe tener la información de acuerdo con el contenido. Calidad debe entenderse como completitud, integridad, consistencia, unicidad, conformidad y veracidad de los datos. Conservación es el tiempo y medio de almacenamiento, el cual varía por regulación externa o interna y de hacerse rigurosamente puede representar ahorros significativos para la organización o por el contrario, representar un alto costo.

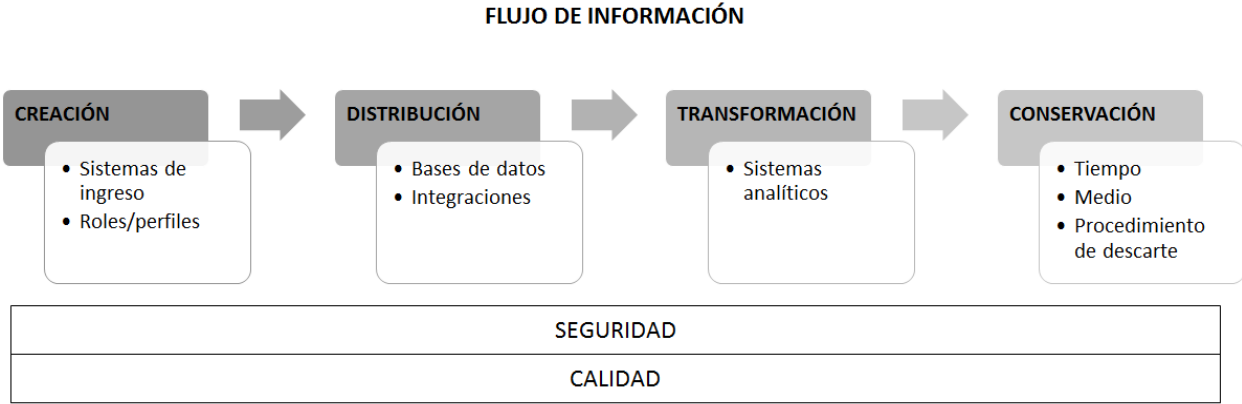


Figura 7. Ciclo de vida de la información  
Fuente: elaborado a partir de COBIT® 5 © 2012 ISACA®

En las organizaciones, los procesos responden a necesidades del negocio y generan valor apalancando el cumplimiento de los objetivos. Por esta razón, es necesario contar con personal y tecnologías idóneas. Además, la información es la base de los procesos, ella puede ser el insumo para la ejecución o el resultado o ambos. Además, dependiendo del contexto en el que una organización se desempeñe, ésta se ve expuesta a riesgos, por lo que es necesario identificarlos y definir la forma en la que se controlará la materialización de ellos. La figura 8

describe esta caracterización de la organización, en la que se muestra la información como un bloque sobre el que se soporta la estrategia corporativa, los procesos ejecutados por personas con tecnología y la información soportada en calidad, seguridad y conservación. Los controles se establecen dentro de la organización para evitar los riesgos externos e internos.

El objetivo de proponer un marco de gobierno de información es potenciar el valor de la información, permitiendo a la organización el logro de metas y objetivos, toma de decisiones efectiva que tengan como base información confiable. Para lograrlo, el primer paso es concientizar a las personas sobre el valor que tiene la información, lo que requiere que cada proceso conozca los activos de información que crea o usa. El siguiente paso, es establecer la confidencialidad de estos; muchas veces las personas no conocen si la información que manejan es privada o no, esto da lugar a almacenamientos inapropiados, compartir archivos, bases de datos, entre otros con terceros ajenos a procesos u organización y es en momentos así donde riesgos como el reputacional se materializan. En Colombia, leyes como la 1581 y 1273 de *habeas data* obligan a las organizaciones que administran información personal a tener niveles de seguridad que garanticen el uso apropiado y aprobado de la información, además, no permite compartirla sin aprobación de cada una de las personas que suministran los datos. También, la Superintendencia de Salud, vigila dentro de esta misma ley, la información de historia clínica, la cual solo debe ser conocida por el paciente y su médico.

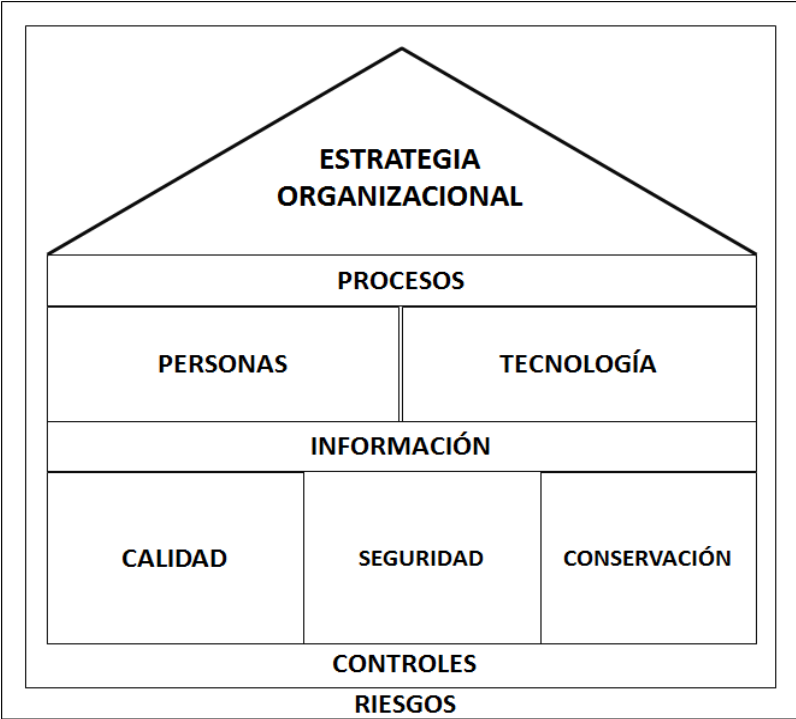


Figura 8. Caracterización de la organización  
Fuente: elaboración propia

Luego de conocer los activos de información y su clasificación, es necesario conocer de principio a fin las etapas por las que pasan, para definir controles no solo de seguridad, sino también de calidad que garanticen la integridad por cada una de ellas. Información de mala calidad no solo tiene como consecuencia tomar malas decisiones, también implica fraudes, sanciones y re-procesos. Un ejemplo de normatividad vigente para empresas vigiladas por la Superintendencia Financiera, es la circular 029 de 2014 básica jurídica, la cual expone un requerimiento mínimo de calidad de información de personas naturales o jurídicas con el propósito de llevar un control que permita evitar el lavado de activos o financiación del terrorismo.

La conservación de la información se define para cada activo, la cual dependerá del medio físico o electrónico. Dada la naturaleza de la organización, se deberá conocer la normatividad vigente para cada uno de ellos y con base en ella establecer procedimientos para almacenar y destruir. También, se debe concientizar a los dueños de la información en el costo indirecto en el que se incurre al almacenar por tiempo indeterminado la información.

Se observan varios puntos claves del marco de gobierno de información:

1. Activos de información.
2. Roles y responsabilidades: dueños, usuarios y custodios de información.
3. Flujos de información basados en los tres pilares, calidad, seguridad y conservación.
4. Normatividad vigente.
5. Gestión del cambio o creación de cultura sobre el buen uso de la información.
6. Riesgos y controles de información

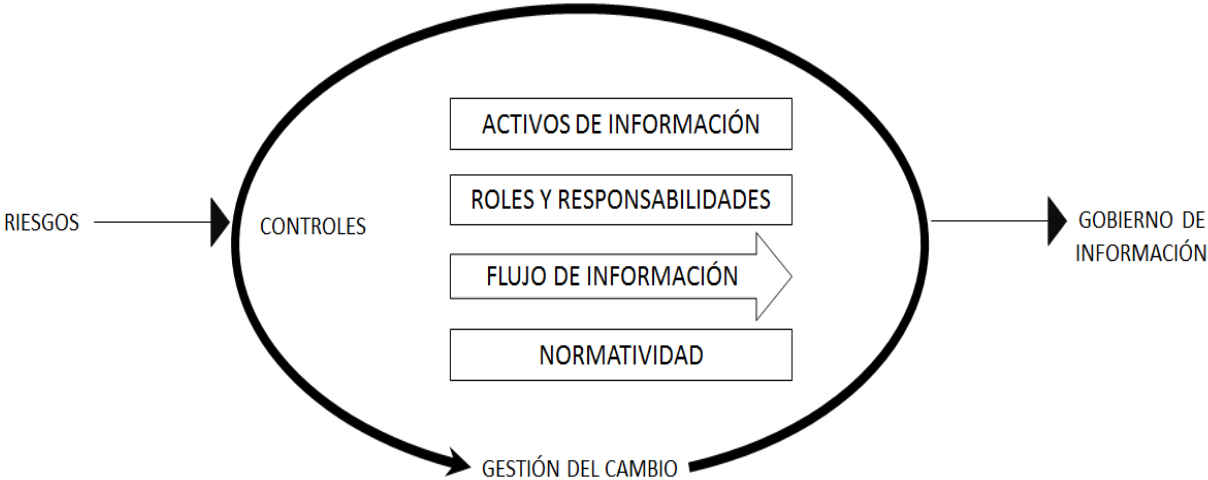


Figura 9. *Framework* Gobierno de información  
Fuente: elaboración propia.

Dicho lo anterior, se propone el *framework* de gobierno de información expuesto en la figura 9, en ella es claro que para establecer un gobierno de información es necesario que cada organización conozca los activos de información, además, asignarles roles y responsabilidades; conocer flujos de información permiten visualizar el mapa de la información y los diferentes actores en él y la normatividad debe ser conocida para disminuir, el riesgo legal y la exposición a otros por diferentes factores; adicionalmente, conociendo el riesgo asociado a la información se proponen controles generales. Asimismo, la gestión del cambio es necesaria para la implementación efectiva del *framework*, porque ayuda a disminuir la aversión al cambio de las personas en la organización.

Si se hace una fusión entre la caracterización de la organización y la propuesta de marco de gobierno de información, se podría reemplazar las bases de información, calidad, seguridad y conservación con esta, así, el gobierno de información no quedará ajeno a la estrategia corporativa y los riesgos y controles de información se incluirán dentro de la caracterización de los procesos corporativos. Ver figura 10.

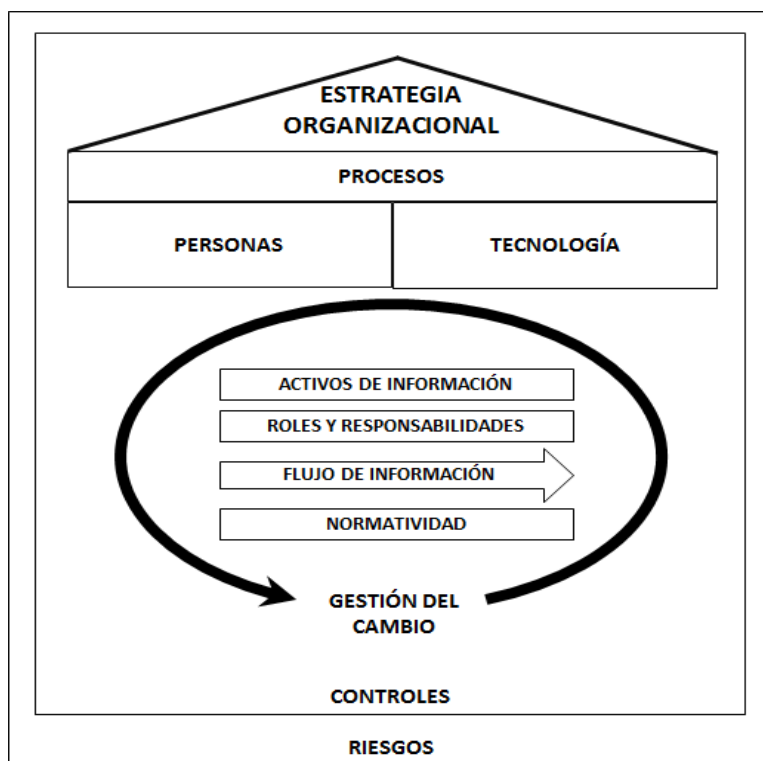


Figura 10. *Framework* propuesto Gobierno de información dentro de la organización.

Fuente: elaboración propia.



## **4.2 Procedimiento Identificación de activos de información**

El primer paso del gobierno de información, consiste en la identificación de activos de información. Este paso entrega como resultado el inventario actualizado, identificación de roles, clasificación, controles de calidad, conservación y flujos de información, todo esto es la caracterización del activo de información. Con esto se pretende definir quién toma decisiones y quién es el responsable de implementarlas.

En la figura 11 se presenta el procedimiento de identificación de activos de información propuesto para la organización, el cual se esquematiza con base en las actividades desarrolladas al interior de la misma.

Dentro del procedimiento de identificación de activos de información, está la actividad publicar, este paso es necesario y hace parte de la gestión de cambio propuesta en el *framework* porque los dueños de los activos de información y las definiciones que se hacen sobre ellos deben ser conocidos por cada persona en la organización, especialmente por quienes desarrollan soluciones tecnológicas.

Dicho lo anterior, es necesario definir:

1. Cómo identificar un activo de información
2. Roles y responsabilidades
3. Clasificación de la información
4. Actividades de calidad y conservación de información

### **4.2.1 Encuesta identificación de activos**

Anteriormente se mencionó la definición de activo de información, el cual es la recopilación identificable de datos provistos de significado que tienen valor para los procesos y su manipulación por personas no autorizadas podría representar un riesgo para la organización.

Para identificar activos de información se propone la siguiente encuesta:

1. Cuál es la información usada en el proceso: entrada y salida
2. ¿La información del punto anterior tiene un flujo de información identificable? Es decir, cuenta con proceso de captura, distribución (otro proceso la usa), transformación y almacenamiento.
3. ¿La pérdida de esta información ocasiona re-procesos?
4. ¿La manipulación sin autorización de esta información por personas externas pone en riesgo el objetivo de la organización o da ventaja competitiva a otros?
5. ¿El almacenamiento de esta información es regulado por entes externos?
6. ¿Cómo dueño, puede tomar decisiones sobre controles de calidad, seguridad y conservación o sigue los lineamientos definidos por alguien más?
7. ¿Conoce el flujo de la información?

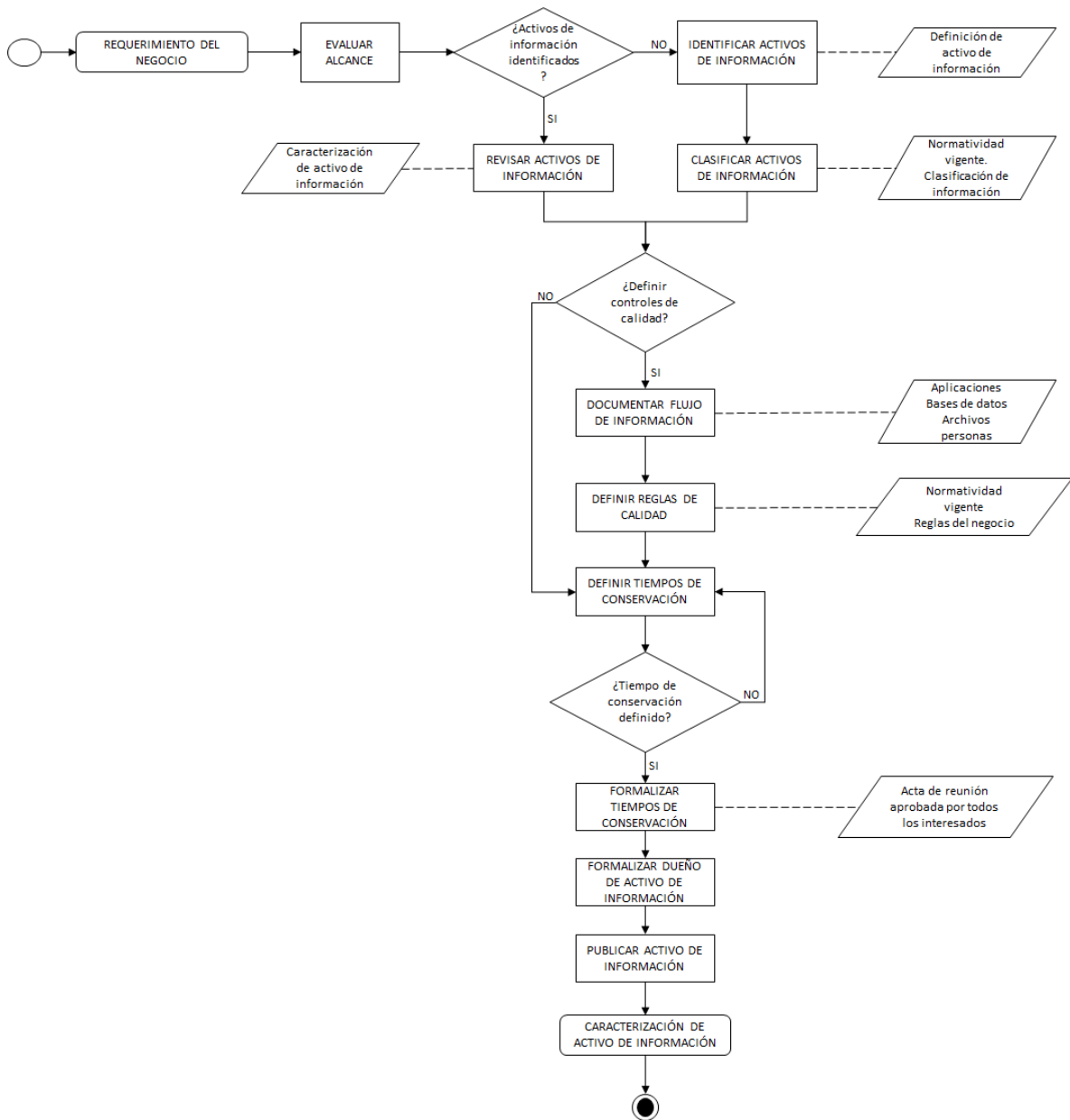


Figura 11. Proceso identificación de activos de información.  
Fuente: elaboración propia para la organización.

Con base en estas preguntas es posible saber si un proceso es usuario o dueño de información. En ocasiones un activo de información incluirá información de otros activos, por lo que los dueños de ambos activos deberán comunicar las necesidades entre ellos y lograr un consenso.

Un indicador propuesto para este procedimiento es:

### *Cantidad procesos corporativos con activos identificados / Total de procesos corporativos*

Con él se pretende conocer cuántos procesos conocen los activos de información, con el propósito de monitorear la responsabilidad que tiene cada uno con la administración estos, es decir, deben actualizarlos por cambios en el dueño, en el mismo proceso o incluir nuevos si es el caso.

#### **4.2.2 Roles y responsabilidades**

**Dueño:** es aquel quien responde por el activo de información ante la organización. Debe conocer los usuarios de sus activos y tomar decisiones relacionadas con calidad, seguridad y conservación. Además, debe monitorear constantemente el cumplimiento de los controles que defina (Córdova, 2003).

**Custodio:** es quien debe implementar los controles definidos por el dueño del activo de información y responder por ellos al dueño (Córdova, 2003).

**Usuario:** personas que usan la información como parte de su trabajo diario; deben cumplir con los controles de calidad, seguridad y conservación. Sin embargo, no toman decisiones relacionadas con estos (Córdova, 2003).

#### **4.2.3 Clasificación de información**

De acuerdo con Córdova (2003), existen 4 niveles de seguridad: general, uso interno, confidencial y restringido.

**Información general o de uso público:** información que está a disposición de cualquier persona interna o externa a la organización.

**Información de uso interno:** información para la ejecución de tareas diarias. Es de acceso libre para las personas de la organización. Su divulgación tiene impacto moderado.

**Información confidencial:** Información conocida por un grupo reducido de personas para el cumplimiento de las funciones. El dueño del activo de información confidencial es quien debe autorizar o no su divulgación.

**Información Restringida:** información que solo puede ser conocida por un grupo reducido de personas. Si la información cae en manos de terceros es sinónimo de riesgo alto para la organización.

En una organización del sector asegurador en Colombia, se implementa la misma clasificación. Sin embargo, la información restringida se diferencia de la confidencial en que almacena un *log* de auditoría, el cual permite conocer quién accede a la información, qué hace con ella, fecha y desde donde la accede.

Adicionalmente, la clasificación de la información es entrada de procesos de seguridad, como el DSS05 Gestionar los servicios de seguridad, de COBIT 5, en el cual se debe encriptar información para evitar que personas no autorizadas puedan ver la información al acceder directamente a bases de datos o para evitar fugas por ataques de seguridad. Además, conociendo la clasificación es posible determinar cómo blindar los sistemas de información. De esta forma se propone un indicador para medir cuanta de la información clasificada está correctamente gestionada:

*Cantidad de log de auditoría para activos de información confidenciales / Total de activos de información confidenciales.*

Este indicador permite vigilar que toda la información clasificada como confidencial almacene una traza que reporte sobre modificaciones de la misma.

También, es necesario tener un indicador de pruebas de seguridad, es decir, una guía que ponga en conocimiento las buenas prácticas de desarrollo de aplicaciones y den lugar a decisiones sobre la información. Es decir, permitir al negocio asumir el riesgo o no por dar un tratamiento inadecuado a la información. De la misma forma, es importante llevar un registro de los ataques de seguridad recibidos y cuáles de ellos son reincidentes.

#### **4.2.4 Actividades de calidad de información**

La calidad es un atributo medible, el dueño de la información debe ser consciente del cumplimiento de la expectativa de calidad que tienen los usuarios de la información, ya que los procesos corporativos se pueden ver afectados por falta o baja confiabilidad de la información.

Con base en el procedimiento de identificación de activos de información, se propone documentar reglas de negocio y de calidad de datos relacionadas con las siguientes dimensiones de calidad: completitud, conformidad, consistencia, unicidad e integridad; entendidas de la siguiente forma:

Completitud: validación de información de carácter obligatorio.

Conformidad: validación de formatos. Por ejemplo: un correo electrónico debe ser del tipo usuario@dominio.com

Consistencia: relación entre diferentes datos. Ejemplo: tipo de identificación con edad. Dirección con municipio. Una extensión debe tener un teléfono.

Unicidad: Clave primaria única. Ejemplo: un número de documento para una sola persona.

Integridad: validación de datos maestros. Ejemplo: el código de un país debe existir en el listado maestro.

Se eligen estas dimensiones porque a través de un perfilamiento de datos es posible conocer su comportamiento y con base en él aplicar remediación, la cual puede ser

limpieza de datos o buscar en que parte del sistema está el error y solucionarlo de raíz.

Para las dimensiones en las que se deba conocer si la información es real, se propone elaborar indicadores sobre procesos de negocio, especialmente de procesos usuarios de la información. Hacer esto permite conocer donde enfocar los esfuerzos y saber que tan efectiva es o no una iniciativa de calidad de información. Un ejemplo de esto es el envío de correspondencia física, para ejecutar el proceso es necesario conocer la dirección de las personas, no obstante, este proceso puede ser solo usuario de la información de las personas y no estar involucrado en la captura de la misma. Un buen proceso de recolección de información puede evitar devoluciones por dirección errada. De esta forma, el indicador de calidad de información puede ser de dos tipos, aquel que da información sobre cómo están los datos, es decir, el que mide las dimensiones de calidad o puede ser un indicador de desempeño de la calidad de información, el cual requiere vinculación con los procesos usuarios.

#### **4.2.5 Actividades de conservación de información**

La información debe estar almacenada de acuerdo con las reglas del negocio y la normatividad vigente. El dueño de información tiene la obligación de conocer la legislación que rige el activo de información, también los usuarios de éste y con base en ellos se define por cuánto tiempo estará almacenada.

Se propone conformar un comité con el dueño del activo de información, entes reguladores al interior de la organización, personas con conocimiento legal y personas de TI, para validar desde diferentes puntos vista el tiempo de conservación y formalizarlo. A partir de esto, el dueño debe velar por la implementación de la decisión y hacer seguimiento periódico del cumplimiento.

También, es necesario conocer las estadísticas de consulta de cada activo de información, con el fin de clasificarlo y tomar decisiones sobre el medio de almacenamiento o eliminación. Este procedimiento tiene como objetivo ahorrar en costos de almacenamiento, por esto es necesario hacer un análisis apropiado y tomar decisiones que permitan lograr esta meta. Una iniciativa de ILM es conveniente y permite al negocio y al área de TI trabajar conjuntamente para conseguir procesos conscientes de la información y del almacenamiento de esta.

Este procedimiento deberá tener un indicador que informe sobre la cantidad de activos de información con políticas de conservación aprobadas y otro de desempeño; costear el almacenamiento de información podrá dar una visión sobre la eficacia de este procedimiento.

#### **4.2.6 Cumplimiento normativo**

Como se ha dicho antes, los lineamientos relacionados con activos de información responden a normas internas o externas a la organización; tener conocimiento de estas, da lugar a una gestión adecuada de la información. De acuerdo con la

Cancillería colombiana, “un normograma regula la base legal que contiene las normas tanto internas como externas aplicables a una entidad. En este caso encontrará Decretos, decretos ley, leyes, directivas presidenciales, decretos reglamentarios, normas internacionales, resoluciones y circulares que reglamentan el desarrollo de las funciones” de la organización. La tabla 4 presenta un ejemplo de normograma que rige el tratamiento de la información en Colombia.

NORMA	DESCRIPCIÓN
Circular Externa 042 de 2012 de la Superfinanciera de Colombia (anteriormente 022 de 2010 y 052 de 2007)	Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios
Circular Externa 014 y 038 de 2009 de la Superfinanciera: Control interno de la información (la 038 modifica a la 014)	Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI)
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto número 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Resolución 816 de 2004	Por la cual se regula la difusión, acceso y utilización de la información en los Sistemas de Seguridad Social Integral y de Protección Social administrados por el Ministerio de la Protección Social
Artículo 15 Constitución Política de Colombia	Derecho a la intimidad Protección de datos
Ley Estatutaria 1266 de 2008 Hábeas Data	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley 1273 de 2009	De la protección de la información y de los datos.
Delitos informáticos	Y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Resolución 1995 de 1999	Por la cual se establecen normas para el manejo de la Historia Clínica
Resolución 3374 de 2000 y 1832 de 1999	Por la cual se reglamentan los datos básicos que deben reportar los prestadores de servicios de salud y las entidades administradoras de planes de beneficios sobre los servicios de salud prestados
Resolución Número 2346 de Julio de 2007	Por la cual se regula la práctica de evaluaciones médicas ocupacionales y el manejo y contenido de las historias clínicas ocupacionales

Tabla 9. Normograma para el tratamiento de información

Fuente: Elaboración propia.

## 5. CONCLUSIONES

El desarrollo de un *framework* de gobierno de información tiene como objetivo presentar el valor que tiene la información en la organización como habilitadora de estrategias o como riesgo en caso de no ser tratada adecuadamente. La implementación de un marco de gobierno de información, implica conocer los activos de información y la organización necesita saber qué información tiene, cómo la tiene, dónde la tiene, quién la usa, quien la custodia y quien toma decisiones sobre ella para apalancar iniciativas que optimicen el valor de la información lo cual se podría traducir en ahorros o nuevo ingresos.

El procedimiento propuesto de identificación de activos de información, reúne prácticas propuestas por COBIT y busca habilitar el *framework* propuesto en este trabajo, presentando la importancia que tiene para la organización el conocimiento de los activos de información, tomándolos como base en el desempeño de los procesos y diseño de soluciones tecnológicas.

En Colombia existen diversas normas que regulan los tres pilares de la información, realizar un normograma, entendido como un repositorio de normas, resoluciones, entre otros, y mantenerlo actualizado es un instrumento base para la definición de controles adecuados de información, ya que con este se delimitan los objetivos de las estrategias organizacionales.

Este *framework* se diseñó tomando como base un proceso de gestión de información de una compañía colombiana de seguros, el cual busca generar sinergias entre el área de TI de la organización y los diferentes negocios mediante información confiable y oportuna.

Aunque la propuesta tiene una base de ejecución real, el trabajo futuro debe involucrar validaciones en organizaciones de otros sectores económicos como el financiero, alimentos, entre otros. Además, como se dijo en la revisión de literatura, es conveniente realizar investigaciones que no solo desarrollen el concepto de gobierno de información, sino también diseñe modelos que permitan valorar económicamente el tratamiento adecuado de la información.

## 6. REFERENCIAS

1. Al-Fedaghi, S. (2008). On Information Lifecycle Management. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE* (pp. 335-342). IEEE.
2. Alves de Freitas, P., Andrade dos Reis, E., Senra Michel, W., Gronovicz, M. E., & De Macedo Rodrigues, M. A. (2013). Information Governance, Big Data and Data Quality. In *Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on* (pp. 1142-1143). IEEE.
3. Cancillería colombiana. Normograma. Recuperado el 22 de marzo de 2016, <http://www.cancilleria.gov.co/ministry/juridicainterna/normograma>
4. Checkland, P., & Scholes, J. (1990). *Soft Systems Methodology in Action*. New York: John Wiley and Sons.
5. Cleveland, H. (1985). The Twilight of Hierarchy: Speculations on the Global Information Society. *Public Administration Review*, 45(1), 185–195.
6. Černá, M. (2014). Aspects of Information Management in Context with IS Selection by SME. *Procedia Engineering*, 745 – 750.
7. Consultorio contable EAFI. Sarbanes Oxley. Recuperado el 29 de febrero de 2016, <http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b5.pdf>
8. Córdova, N. (2003). *Plan de seguridad informática para una entidad financiera. Lima Perú, Ing* (Doctoral dissertation, Thesis, Universidad Mayor de San Marcos).
9. de Abreu Faria, F., Macada, A. C. G., & Kumar, K. (2013). Information governance in the banking industry. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 4436-4445). IEEE.
10. Donaldson, A., & Walker, P. (2004). Information governance—a view from the NHS. *International journal of Medical informatics*, 73(3), 281-284.
11. Eaton, J. J., & Bauden, D. (1991). What Kind of Resource Is Information. *International Journal of Information Management*, 11(2), 156–165.
12. Fasecolda (2015). Cifras de la industria año 2015. Recuperado en marzo 13 de 2016, [http://www.fasecolda.com/files/7414/5713/3119/Cifras\\_ao\\_2015.pdf](http://www.fasecolda.com/files/7414/5713/3119/Cifras_ao_2015.pdf)
13. Fundación Maphre (2014). Evolución del mercado Asegurador latinoamericano 2003 – 2013. Recuperado en marzo 13 de 2016, [https://www.fundacionmapfre.org/documentacion/publico/i18n/catalogo\\_imagenes/grupo.cmd?path=1080543](https://www.fundacionmapfre.org/documentacion/publico/i18n/catalogo_imagenes/grupo.cmd?path=1080543)
14. Glazer, R. (1991). Marketing in an information-intensive environment: strategic implications of knowledge as an asset. *The Journal of Marketing*, 1-19.
15. Guetat, S. B. A., & Dakhli, S. B. D. (2015). The Architecture Facet of Information Governance: The Case of Urbanized Information Systems. *Procedia Computer Science*, 64, 1088-1098.



16. Grimstad, T., & Myrseth, P. (2011). Information governance as a basis for cross-sector e-services in public administration. In *E-Business and E-Government (ICEE), 2011 International Conference on* (pp. 1-4). IEEE.
17. Hohman, C. (2011). Information Governance: Who is watching over your information?, Recuperado en marzo 01 de 2016, <http://www.incontextmag.com/article/Information-Governance-Who-is-watching-over-your-information>
18. Haug, A., Zachariassen, F., & Van Liempd, D. (2011). The costs of poor data quality. *Journal of Industrial Engineering and Management*, 4(2), 168-193.
19. Hu, W. (2008). Information lifecycle modeling framework for construction project lifecycle management. In *Future Information Technology and Management Engineering, 2008. FITME'08. International Seminar on* (pp. 372-375). IEEE.
20. Isaca. (2015). COBIT 5 Spanish. Obtenido de <http://www.isaca.org/COBIT/Pages/COBIT5-spanish.aspx>
21. Juddoo, S. (2015). Overview of data quality challenges in the context of Big Data. In *Computing, Communication and Security (ICCCS), 2015 International Conference on* (pp. 1-9). IEEE.
22. Junguito, R. & Rodriguez, A. (2010). *La empresa y la industria aseguradora colombiana en el contexto económico de finales del XIX y XX*. Fasecolda.
23. Kerr, D. S., & Murthy, U. S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: an international survey. *Information & Management*, 50(7), 590-597.
24. Kooper, M. N., Maes, R., & Lindgren, E.O.R. (2011). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, 31(3), 195-200.
25. Kusumah, R. (2014). Designing information governance in statistical organization. In *Information Technology Systems and Innovation (ICITSI), 2014 International Conference on* (pp. 201-205). IEEE.
26. Liu, H., Wang, X., & Quan, Q. (2009). Research on the enterprise' model of information lifecycle management based on enterprise architecture. In *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on* (Vol. 3, pp. 165-169). IEEE.
27. Losee, R. (1997). A discipline independent definition of information. *Journal of American Society for information Science*, 48(3), 254-269.
28. Mingers, J. (1996). An Evaluation of Theories of Information with Regard to the Semantic and Pragmatic Aspects of Information Systems. *Systemic Practice and Action Research*, 9(3), 187–209.
29. Moody, D., & Walsh, P. (1999). Measuring the Value Of Information-An Asset Valuation Approach. In *ECIS* (pp. 496-512).

30. Othman, M., Ahmad, M. N., Suliman, A., Arshad, N. H., & Maidin, S. S. (2014). COBIT principles to govern flood management. *International journal of disaster risk reduction*, 9, 212-223.
31. Shi, X., Li, D., Zhu, H., & Zhang, W. (2007). Research on Supply Chain Information Classification Based on Information Value and Information Sensitivity. In *Service Systems and Service Management, 2007 International Conference on* (pp. 1-7).
32. Stoner, J., Freeman, E., & Gilbert, D. (1996). *Administración. 6ta. Edición. Prentice Hall. México.*
33. Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. *IFAC-PapersOnLine*, 48(3), 1846-1852.
34. Ogan, D. D., Ndekugri, I. E., Oduoza, C. F., & Khatib, J. M. (2016). Principles for developing an effective framework to control minerals and rocks extraction impacts, mitigate waste and optimise sustainable quarries management. *Resources Policy*, 47, 164-170.
35. Van Heesch, U., Avgeriou, P., & Hilliard, R. (2012). A documentation framework for architecture decisions. *Journal of Systems and Software*, 85(4), 795-820.
36. Wohlhaupter, P. (2012). *Research in Business Process Management: A bibliometric analysis* (Doctoral dissertation, University of Ulm).