ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 38 (Nº 46) Año 2017. Pág. 3

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

## Approach of framework for information governance based on COBIT

Carolina RINCÓN López 1; Miguel David ROJAS López 2; Maria Elena VALENCIA Corrales 3

Recibido: 12/05/2017 • Aprobado: 12/06/2017

**Contenido**



**RESUMEN:**
En el siglo XXI el sector asegurador Colombiano creció entre el 5% y 10%, para el 2016 las compañías toman decisiones fundamentadas en la confiabilidad en la información, por otra parte la tecnología incrementa riesgos asociados con disponibilidad, oportunidad, calidad y conservación de la información. Se propone un framework de gobierno de información, con el objetivo de conocer los activos de información, asignación de roles y responsabilidades y la definición de lineamientos para el tratamiento adecuado de la información.
**Palabras clave**: Framework, COBIT, Gobierno de información, Activo de información.

**ABSTRACT:**
Since 1874, the Colombian insurance market grown by 5% and 10%, for the year 2016 the companies take decisions based in the trust that senior management has on the information, furthermore, Technology increase the risks associated with availability, opportunity, quality and conservation of information. 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.
**Keywords:** Framework, COBIT, information governance, Information asset

# 1. 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  - 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 identificaran 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.

# 2. Estructura teórico-practica

## 2.1 *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.

1. 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.
2. 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*.
3. Realizar una guía de implementación incluye una planificación, matriz de decisiones y estrategia de ejecución.
4. 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 *framework*, 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 *framework* | Capacidad de adaptación al cambio del *framework* |

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.

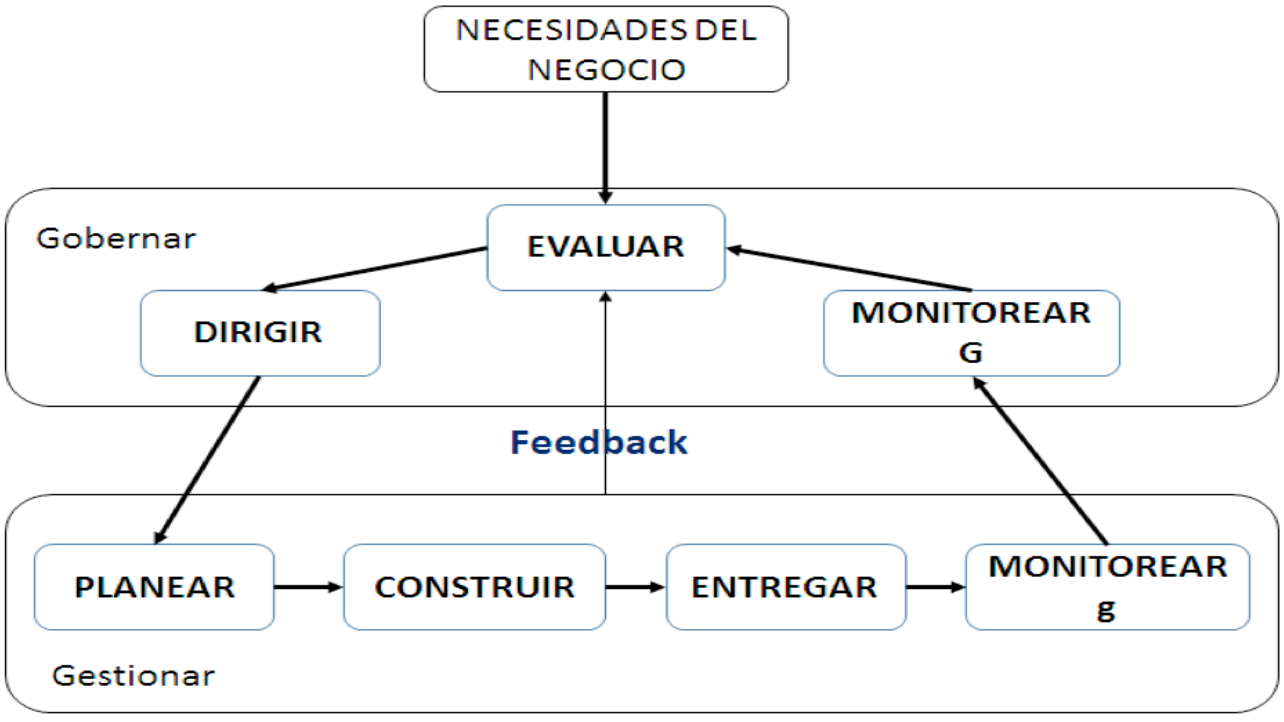
## 2.2 Control Objective for Information and Related Technologies -COBIT-

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 *framework's* 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.

## 2.3 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.

---

# 3. Aproximación Metodológica

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*.

## 3.1. *Framework* Gobierno de Información

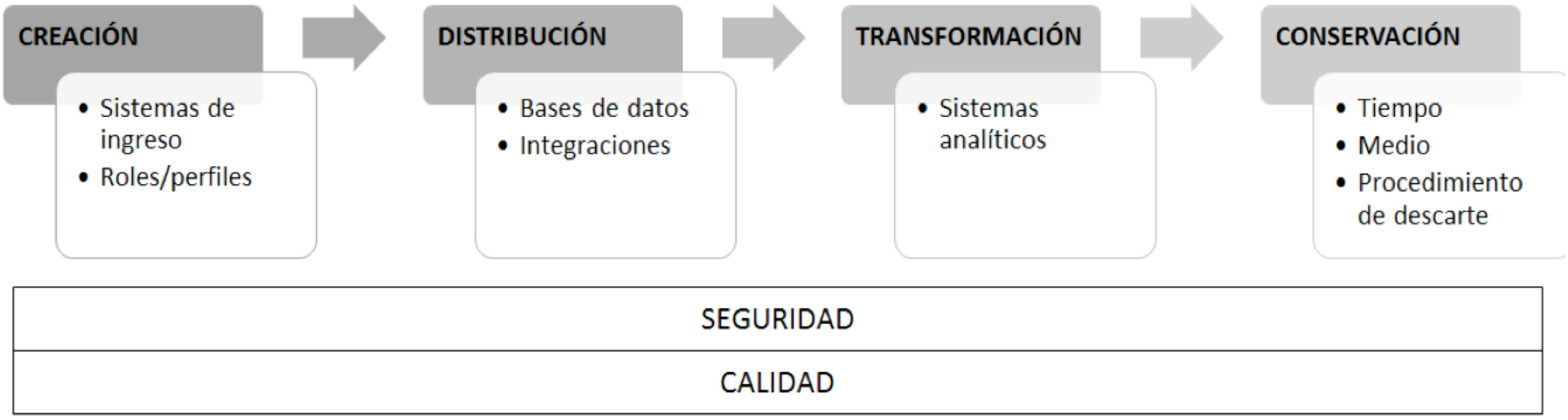
El Gobierno de información es un concepto en desarrollo, el cual debe implementarse en organizaciones independientemente de su tamaño y sector económico. Stoner et al. (1996) definen organización como las relaciones múltiples entre personas dirigidas por un líder con el propósito de cumplir con metas 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 2 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 2.** Ciclo de vida de la información

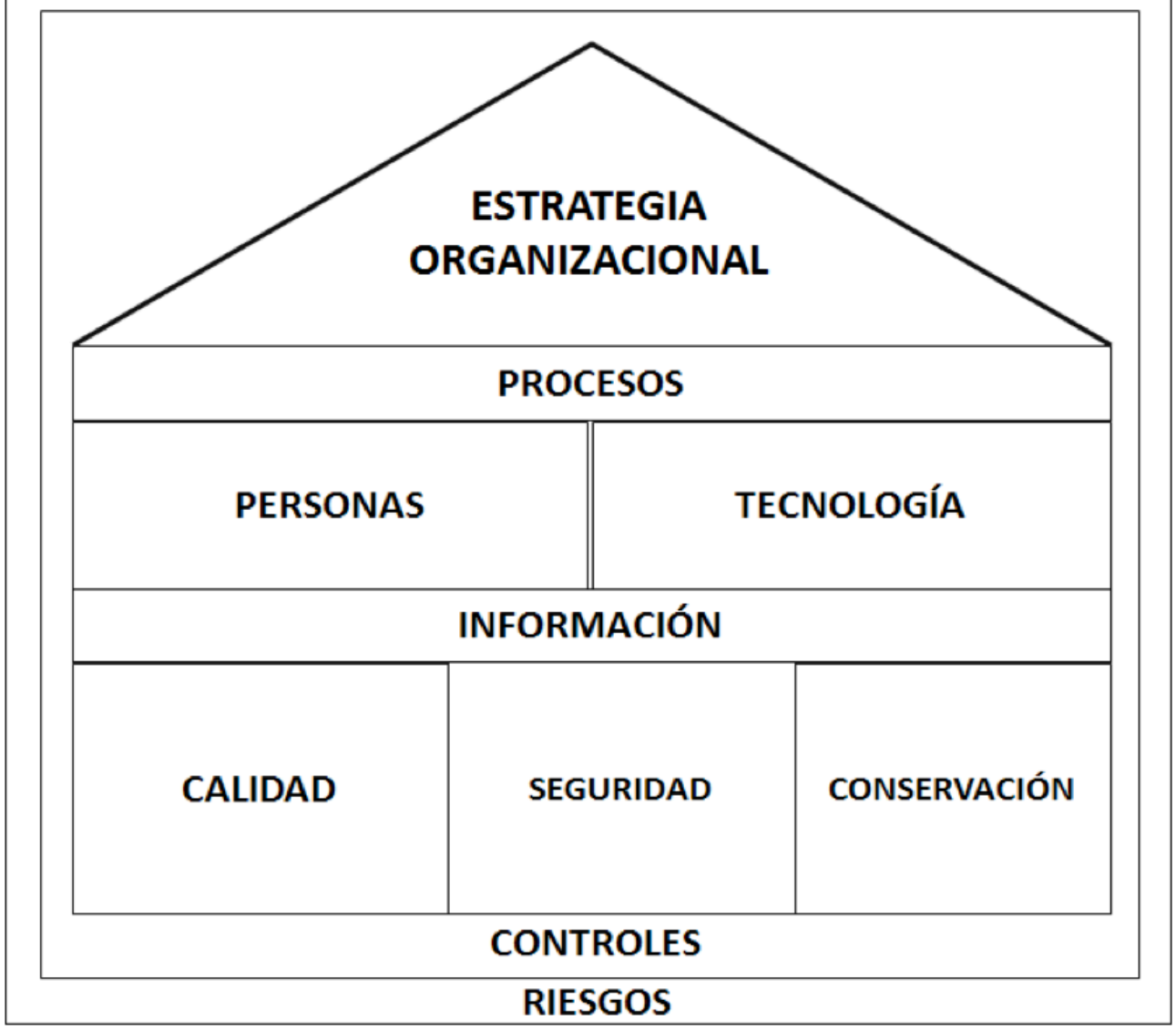



Fuente: elaborado a partir de COBIT® 5 © 2012 ISACA®

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 3 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 3.** Caracterización de la organización




Fuente: elaboración propia

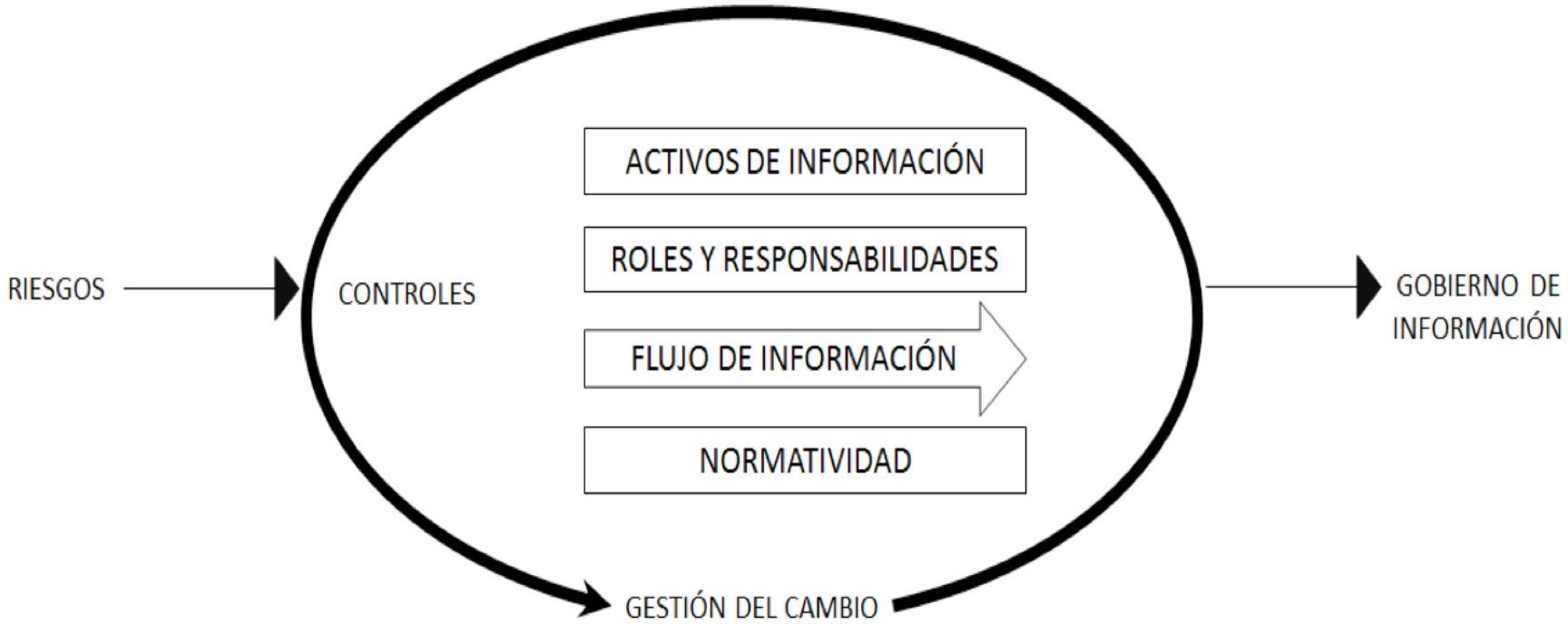
Luego de conocer los activos de información y su clasificación, es necesario conocer de principio a fin las etapas por las que pasan, para definir controles no solo de seguridad, sino también de calidad que garanticen la integridad por cada una de ellas. Información de mala calidad no solo tiene como 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 4.** *Framework* Gobierno de información

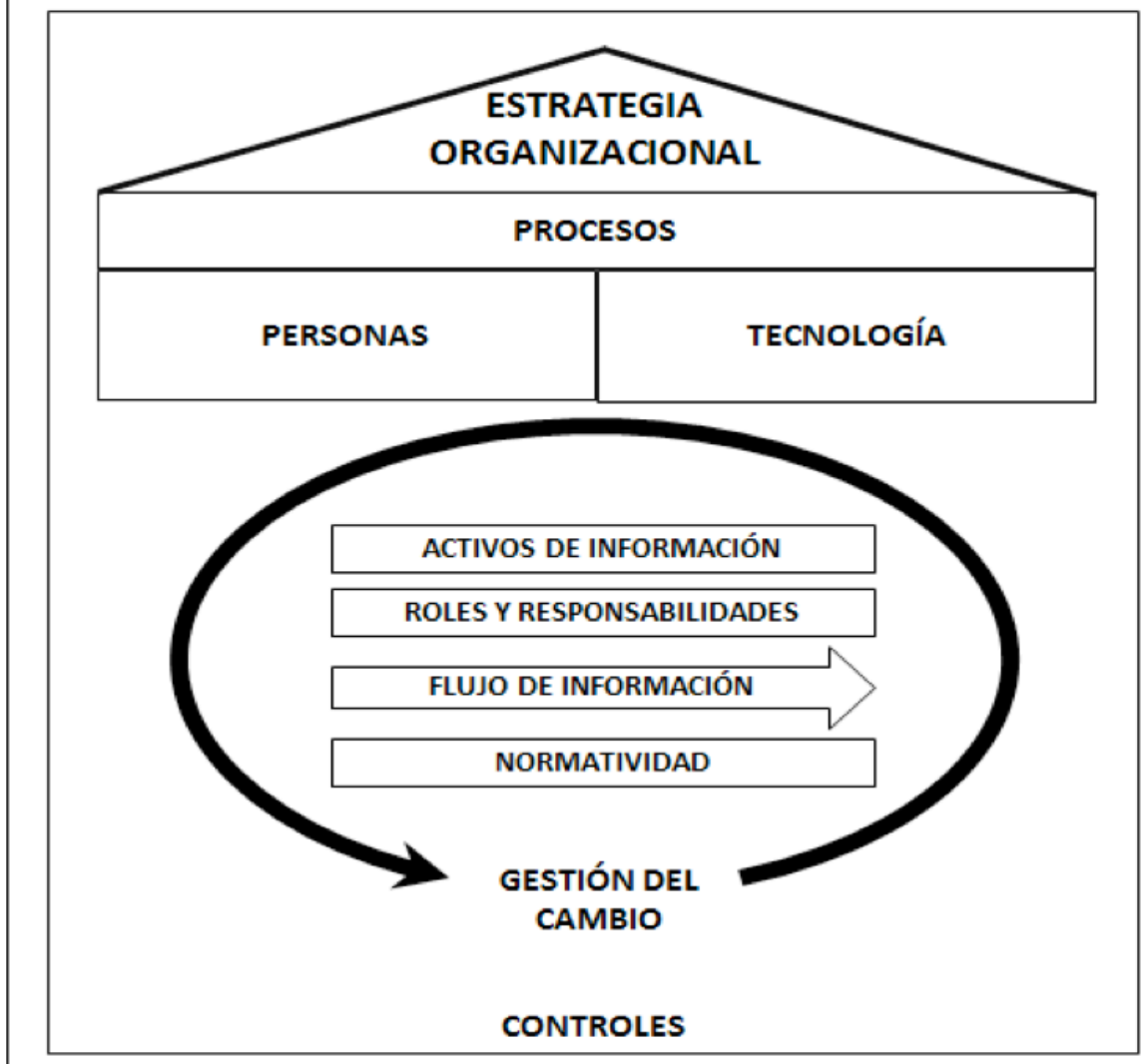



Fuente: elaboración propia.

Dicho lo anterior, se propone el *framework* de gobierno de información expuesto en la figura 4, 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 5.

**Figura 5.** *Framework* propuesto Gobierno de información dentro de la organización.




Fuente: elaboración propia.

## 3.2. 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

### 3.2.1. 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?

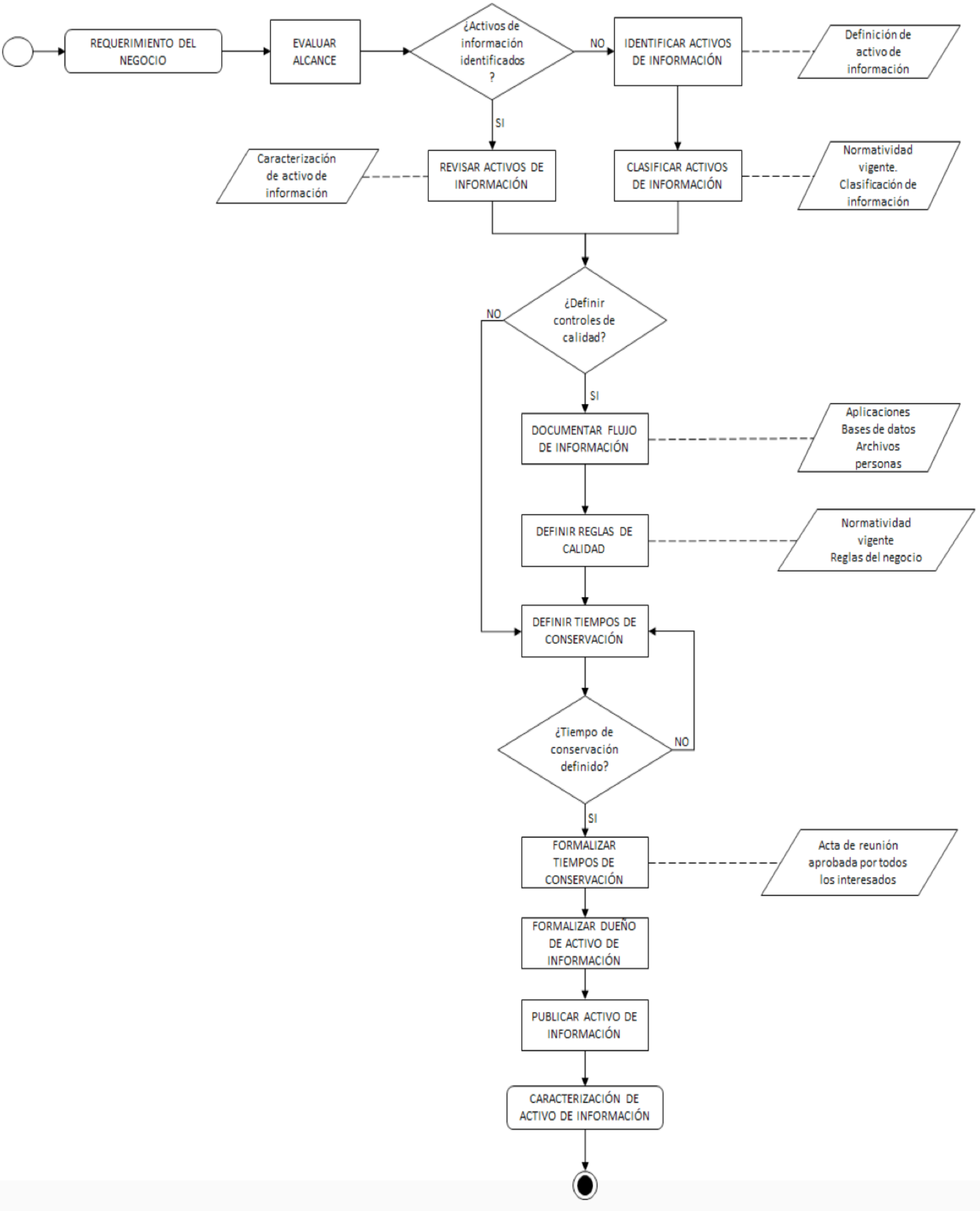
4. ¿La manipulación sin autorización de esta información por personas externas pone en riesgo el objetivo de la organización o da ventaja competitiva a otros?

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 6.** 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.

### 3.2.2. 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).

### 3.2.3. 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.

### 3.2.4. 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.

### 3.2.5. 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.

### 3.2.6. 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<br>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.

# 4. 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 nuevos 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.

# Referencias bibliográficas

Al-Fedaghi, S. (2008). On Information Lifecycle Management. InAsia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 335-342). IEEE.

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.

Cancillería colombiana. Normograma. Recuperado el 22 de marzo de 2016, http://www.cancilleria.gov.co/ministry/juridicainterna/normograma

Checkland, P., & Scholes, J. (1990). Soft Systems Methodology in Action. New York: John Wiley and Sons.

Cleveland, H. (1985). The Twilight of Hierarchy: Speculations on the Global Information Society. Public Administration Review, 45(1), 185–195.

Černá, M. (2014). Aspects of Information Management in Context with IS Selection by SME. Procedia Engineering, 745 – 750.

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

Córdova, N. (2003). Plan de seguridad informática para una entidad financiera. Lima Perú, Ing (Doctoral dissertation, Thesis, Universidad Mayor de San Marcos).

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.

Donaldson, A., & Walker, P. (2004). Information governance—a view from the NHS. International journal of Medical informatics, 73(3), 281-284.

Eaton, J. J., & Bauden, D. (1991). What Kind of Resource Is Information. International Journal of Information Management, 11(2), 156–165.

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

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

Glazer, R. (1991). Marketing in an information-intensive environment: strategic implications of knowledge as an asset. The Journal of Marketing, 1-19.

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.

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.

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

Haug, A., Zachariassen, F., & Van Liempd, D. (2011). The costs of poor data quality. Journal of Industrial Engineering and Management, 4(2), 168-193.

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.

Isaca. (2015). COBIT 5 Spanish. Obtenido de http://www.isaca.org/COBIT/Pages/COBIT5-spanish.aspx

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.

Junguito, R. & Rodriguez, A. (2010). La empresa y la industria aseguradora colombiana en el

contexto económico de finales del XIX y XX. Fasecolda.

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.

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.

Kusumah, R. (2014). Designing information governance in statistical organization. In Information Technology Systems and Innovation (ICITSI), 2014 International Conference on (pp. 201-205). IEEE.

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.

Losee, R. (1997). A discipline independent definition of information. Journal of American Society for information Science, 48(3), 254-269.

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.

Moody, D., & Walsh, P. (1999). Measuring the Value Of Information-An Asset Valuation Approach. In ECIS (pp. 496-512).

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.

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).

Stoner, J., Freeman, E., & Gilbert, D. (1996). Administración. 6ta. Edición. Prentice Hall. México.

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.

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.

Van Heesch, U., Avgeriou, P., & Hilliard, R. (2012). A documentation framework for architecture decisions. Journal of Systems and Software, 85(4), 795-820.

Wohlhaupter, P. (2012). Research in Business Process Management: A bibliometric analysis (Doctoral dissertation, University of Ulm).

---

1. Ingeniería de sistemas Maestría en ingeniería de la organización Universidad Nacional de Colombia

2. Doctor en Ingeniería- Universidad Nacional de Colombia . Profesor asociado Universidad Nacional de Colombia. Facultad de Minas. Medellín, Antioquia, Colombia. Email: mdrojas@unal.edu.co

3. M.B.A., Docente Universidad Católica Luis Amigó, email: maria.valenciaco@amigo.edu.co

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 38 (Nº 46) Año 2017
Indexada en Scopus, Google Schollar

[Índice]

[En caso de encontrar algún error en este website favor enviar email a webmaster]