ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 38 (Nº 23) Año 2017. Pág. 3

Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas TI en cumplimiento de la Ley Sarbanes–Oxley

Alignment of Cobit 5 and Coso IC-IF to define controls based on Good Practices IT in compliance with the Sarbanes-Oxley Act

MONTAÑO-ARDILA, Victor 1; COMBITA-NIÑO, Harold 2; DE-LA-HOZ-FRANCO, Emiro 3

Recibido: 23/11/16 • Aprobado: 20/12/2016

Contenido

RESUMEN:

La Ley Sarbanes-Oxley permite garantizar la integridad de la información financiera de las empresas que cotizan en bolsa, y su principal objetivo es proteger al inversionista. Actualmente y con la intensión de proteger los datos, las empresas almacenan y gestionan su información financiera en infraestructuras tecnológicas y sistemas informáticos propios. Por otra parte, COBIT 5 es el marco de trabajo que se implementa para gobernar las Tecnologías de la Información (TI) y asegurar la alineación de TI a la visión de la organización. Sin embargo, COBIT no posee las herramientas que posibiliten el tratamiento en

ABSTRACT:

The Sarbanes-Oxley Act makes it possible to guarantee the integrity of the financial information of listed companies, and its main objective is to protect the investor. Currently, in an effort to protect data, companies store and manage their financial information in their own technology infrastructures and IT systems. On the other hand, COBIT 5 is the framework that is implemented to govern Information Technology (IT) and ensure the alignment of IT to the organization's vision. However, COBIT does not have the tools that enable the detailed treatment of financial information; For this reason, it is proposed here to articulate COBIT 5 and

detalle de la información financiera; por tal razón, aquí se propone articular COBIT 5 y el Marco Integrado de Control Interno del Committee of Sponsoring Organizations of the Treadway Commission (COSO IC-IF), fundamentados en los lineamientos expuestos por las normas ISO 38500 e ISO 27001, para dar cumplimiento a la Ley Sarbanes-Oxley. Como resultado de esta articulación se obtuvo una guía para el auditor financiero, que le permita definir controles de calidad basados en buenas prácticas de controles de TI. Para lograr esto, se realizó una alineación de los procesos de COBIT con los principios de cada uno de los componentes de COSO IC-IF. Adicionalmente, se propuso cómo evaluar el cumplimiento de los requisitos de la Ley desde una perspectiva de TI, aplicando buenas prácticas en la implementación del control y la referenciación de los procesos de COBIT 5.
Palabras claves: Ley Sarbanes-Oxley, COBIT 5, Control Interno, Gobierno de Tecnología Informática, Auditor financiero, Buenas prácticas.

the Integrated Framework of Internal Control of the Committee of Sponsoring Organizations of the Treadway Commission (COSO IC-IF), based on the guidelines set forth by the ISO 38500 and ISO 27001 standards, to comply To the Sarbanes-Oxley Act. As a result of this articulation, a guide was obtained for the financial auditor, allowing him to define quality controls based on good practices of IT controls. To achieve this, an alignment of the COBIT processes was performed with the principles of each of the components of COSO IC-IF. Additionally, it was proposed how to evaluate compliance with the requirements of the Law from an IT perspective, applying good practices in the implementation of the control and referencing of COBIT 5 processes.
Key words: Sarbanes-Oxley Act, COBIT 5, Internal Control, IT Governance, Financial Auditor, Good Practices.

1. Introducción

Satisfacer criterios de confidencialidad, disponibilidad e integridad de la información financiera constituyen el objetivo fundamental de la Ley *Sarbanes-Oxley*. Mucho de lo que se ha escrito sobre la estructuración de un adecuado modelo de control interno está orientado a satisfacer de forma razonable los objetivos corporativos; sin embargo, los modelos propuestos se centran en las actividades operativas y transaccionales, olvidándose de la importancia del continente de la información. La tendencia de las organizaciones modernas es a automatizar todo proceso o actividad haciendo uso de herramientas basadas en TI, esto genera una dependencia creciente que se incrementa al vincular otros actores externos a los sistemas informáticos corporativos. Obviamente esta estrategia, que apunta a ganar eficiencia y eficacia en los procesos, genera grandes vulnerabilidades a las que las empresas deberán responder de forma efectiva.

En consecuencia, la pregunta clave que se plantean directivos y entes de control en las organizaciones es: ¿Cómo proteger adecuadamente la información financiera gestionada en los sistemas de información?. Esta pregunta es parcialmente respondida por los lineamientos del Marco de Referencia de *COBIT 5*, que define los aspectos que se deben cumplir para mantener un adecuado Modelo de Gobierno de TI, pero que en la mayoría de sus propuestas no incluye el cómo y mucho menos lo hace de forma específica para la información financiera.

En este trabajo, partiendo de un análisis de aspectos articulables entre los marcos de referencia de *COSO IC–IF* y la Ley *Sarbanes-Oxley*, se identificaron los dominios, procesos, metas de TI y actividades de control del Marco de Referencia del Modelo *COBIT 5* que, articulados con el marco de referencia de *COSO IC-IF*, apuntan a dar cumplimiento a las reflexiones anteriormente expuestas, especialmente para la información financiera y por ende para satisfacer los lineamientos de la Ley *Sarbanes–Oxley*.

Para el efecto, se adelantó una fundamentación teórica consistente, basada en los lineamientos expuestos por los marcos de referencia de mayor aceptación mundial y que son considerados como "buenas prácticas". Ello implicó todo un análisis de los marcos de referencia relacionados con el Modelo *COSO IC–IF*, *COBIT 5*, la Ley *Sarbanes-Oxley*, la Norma *ISO 38500* y la Norma *ISO 27001*. Se identificaron y fundamentaron las relaciones que finalmente permitieron proveer una guía metodológica para la revisión de cada una de las Actividades de Control de las Prácticas de Gobierno de TI (COBIT 5), definidas como de necesario cumplimiento, para satisfacer los lineamientos de la Ley *Sarbanes-Oxley*.

2. Ley *Sarbanes-Oxley*

Es la más importante regulación surgida para responder a los escándalos financieros ocurridos

en empresas estadounidenses al iniciar el tercer milenio y que se tradujeron en quiebras, fraudes y otros manejos administrativos inapropiados, que consecuentemente disminuyeron la confianza de los inversionistas respecto a la información financiera entregada por las organizaciones y ocasionando efectos negativos sobre los resultados de los mercados de capitales.

La Ley *Sarbanes-Oxley*, que puede ser consultada en (SEC, 2002), se enfoca en la creación y ejecución de procedimientos inherentes al manejo de la información financiera: documentándolos, controlándolos y comunicándolos. Según (Gutiérrez, 2004), apunta a que las empresas mejoren la confiabilidad de su información contable mediante la definición e implementación de políticas y procedimientos financieros controlados y documentados. Demandando de las organizaciones, la aplicación de un marco de control interno adecuado. Erigiéndose, producto de ello, el Marco de Control Interno Integrado *COSO IC–IF (COSO, 2016)*, como la mejor práctica de las empresas para cumplir con la Ley *Sarbanes-Oxley*.

La implantación de la Ley *Sarbanes–Oxley* obliga a la instauración de una corporación no lucrativa (*Public Company Accounting Oversaight Board* - PCAOB) encargada de supervisar las labores de auditoría realizadas en empresas públicas y cotizantes en la bolsa de valores de los Estados Unidos con el objeto de ofrecer protección a los inversionistas y a sus intereses (PCAOB, 2016). Que según (Cano & Lugo, 2016), garantiza precisión e independencia en la elaboración de informes de auditoría, los cuales deben ser de dominio público.

---

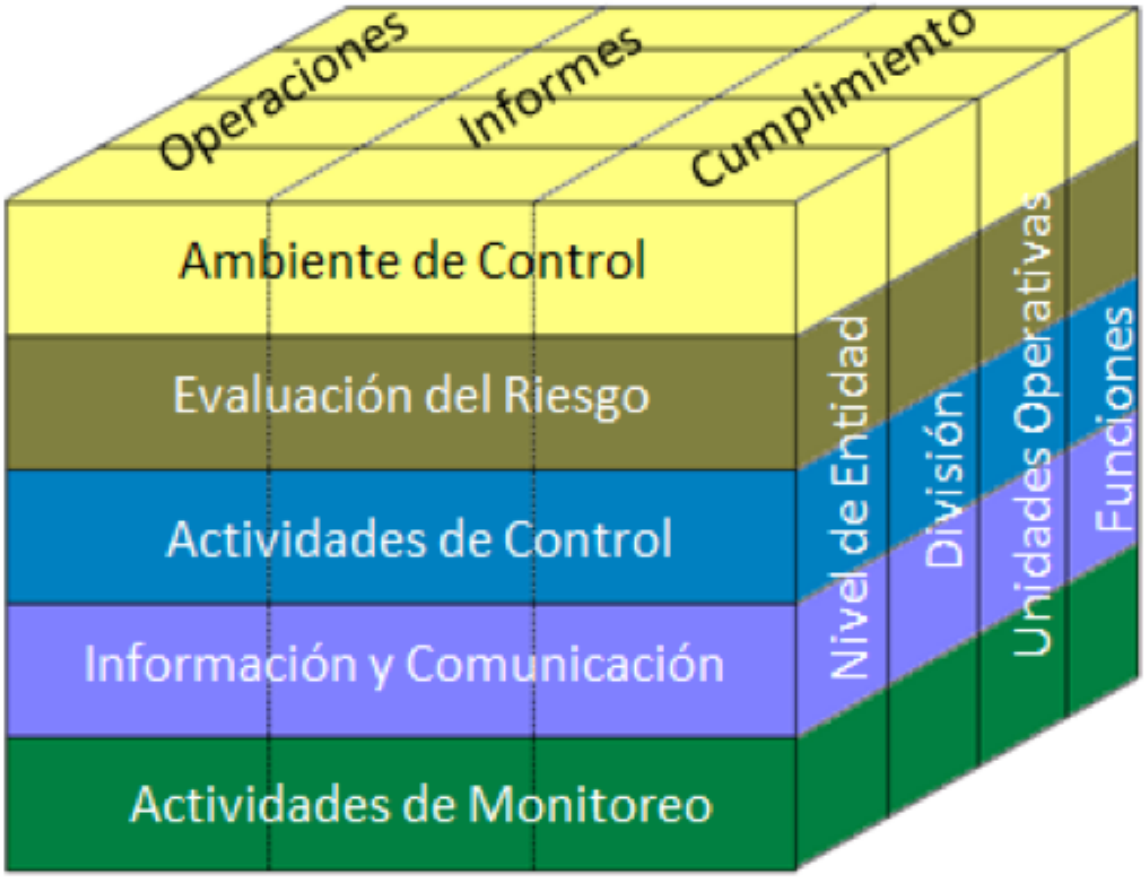
3. Relacion *Coso Ic-If* Y Ley *Sarbanes-Oxley*

El Informe COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) que puede ser consultado en (COSO IC-IF, 2013), hace referencia a la importancia de la Tecnología Informática, en relación con el entorno global de control de una organización, pero no proporciona una guía detallada para las empresas que necesitan diseñar e implementar controles específicos para su entorno según (IT Governance Institute, 2006). En la definición de Control Interno expuesta en el Informe COSO, se indica que los controles internos, independientemente de su adecuado diseño y de la efectividad y eficiencia de su operación, sólo proveen seguridad razonable de que la entidad logre sus objetivos de control. La probabilidad de lograrlos dependerá de las limitaciones que posea el sistema de control interno, el cual incluye los juicios subjetivos de las personas encargadas de la toma de decisiones, y evidentemente éstos pueden estar sujetos a errores, que podrían generar vulnerabilidades que faciliten la materialización de causas de riesgo.

El apendice “A” del documento (IT Governance Institute, 2006), para los Objetivos de Control en relación a la Ley *Sarbanes-Oxley*, contempla algunos elementos relacionados con la información financiera; no obstante, los objetivos de control y las consideraciones que expone dicho documento supera los requisitos que las organizaciones deberían tener para cumplir con dicha Ley. El marco de control interno sugerido por el documento *COSO IC–IF* (Marco Integrado de Control Interno), para el cumplimiento de la Ley *Sarbanes-Oxley*, aborda el tema de los controles de TI, pero no establece requisitos para tales objetivos de control y las actividades de control relacionadas. Del mismo modo, PCAOB Auditing Standard No. 2, que puede ser consultado en (PCAOB, 2004), señala la importancia de los controles de TI, pero no especifica qué debe ser incluido. Estas decisiones siguen siendo criterio de cada organización. En consecuencia, las organizaciones deben evaluar la naturaleza y el alcance de los controles de TI, caso por caso, para apoyar su programa de control interno.

El control interno (CI) es un proceso, efectuado por la junta de directores de la entidad, la gerencia y cualquier otro personal designado por los anteriores. El CI se diseña para proporcionar una seguridad razonable en cuanto a la consecución de los objetivos relacionados con las operaciones, la elaboración y confiabilidad de los informes y el cumplimiento de leyes y regulaciones (COSO IC-IF, 2013). *COSO IC-IF*, consta de cinco (5) componentes básicos, ver Figura 1 y Tabla 1.

Figura No 1. Estructura del Marco de Referencia COSO IC - IF



Fuente: COSO, "Internal Control—Integrated Framework," Executive Summary, USA, May 2013.

En coherencia con lo planteado por *COSO IC–IF*, la Ley *Sarbanes–Oxley* requiere de la adopción de una nueva estructura organizacional a nivel de las empresas y el estado, para permitir el control de cada uno de los aspectos definidos como críticos. Por otra parte, la mediante la creación de la *PCAOB*, la Ley *Sarbanes–Oxley*, para hacer frente a algunos evidentes conflictos de interés, prohibió a los auditores realizar cualquier otro tipo de trabajo diferente a procesos de auditoría.

4. Marco De Referencia De *Cobit 5*

Es el conjunto de mejores prácticas para el manejo de información, creado por la Asociación para la Auditoría y Control de Sistemas de Información – ISACA, consultar (ISACA, 2016), en particular, por el Instituto de Administración de las Tecnologías de la Información – ITGI, consultar (ISACA-ITGI, 2016). *COBIT 5*, provee un marco de referencia de Gobierno y Gestión de TI en las empresas y herramientas de soporte que permiten a la alta dirección reducir la brecha entre las necesidades de control, los asuntos técnicos y los riesgos del negocio. *COBIT* permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones, enfatizando en el cumplimiento normativo, ayudando a las organizaciones a aumentar el valor obtenido de TI, facilitando su alineación y simplificando la implementación del marco de referencia (ISACA-COBIT 5, 2012).

Tabla No 1. Componentes y Principios del Modelo *COSO IC-IF*

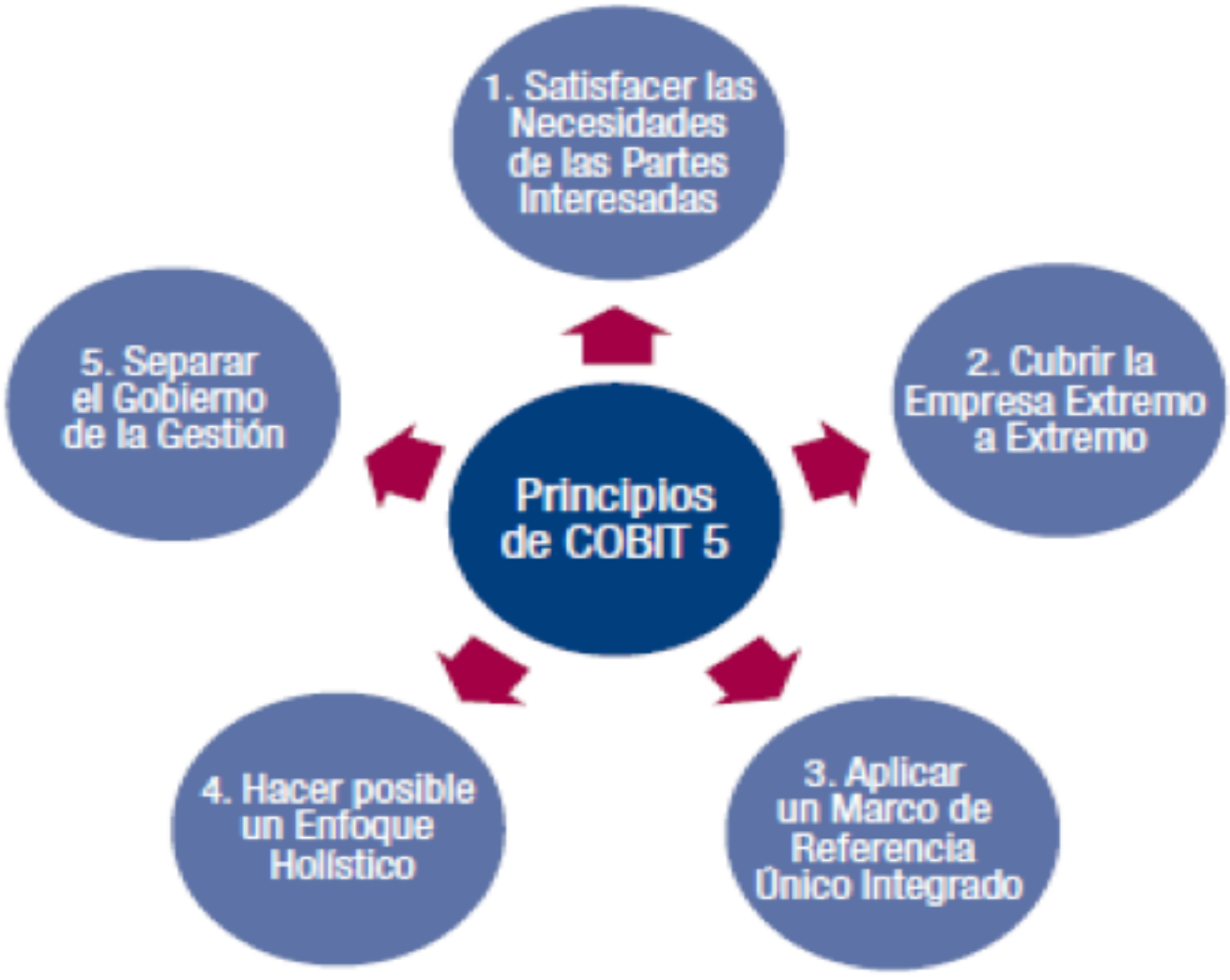
Componente	Principio
	1. La organización demuestra un compromiso con la integridad y los valores éticos.
	2. El consejo de administración demuestra la independencia de gestión y ejerce la supervisión de la evolución y los resultados de los controles internos.
	3. Administración establece, con supervisión de la Junta, estructuras, líneas de

Ambiente de Control	responsabilidad, y las autoridades y responsabilidades adecuadas en la consecución de objetivos.
	4. La organización demuestra el compromiso de atraer, desarrollar y retener a personas competentes en la alineación con los objetivos.
	5. La organización mantiene los individuos responsables de su control interno responsabilidades en la búsqueda de objetivos.
Administración del Riesgo	**6.** La organización especifica objetivos con claridad suficiente para que el identificación y evaluación de los riesgos relacionados con los objetivos.
	7. La organización identifica los riesgos para el logro de sus objetivosa través de la entidad y de los análisis de riesgos como base para la determinación de la forma en la riesgos deberían ser manejadas.
	8. La organización considera que la posibilidad de fraude en la evaluación de los riesgos para la logro de los objetivos.
	9. La organización identifica y evalúa los cambios que podrían significativamente impacto en el sistema de control interno.
Actividades de Control	**10.** La organización selecciona y desarrolla actividades de control que contribuyan para la mitigación de riesgos para asegurar el logro de los objetivos de niveles aceptables.
	11. La organización selecciona y desarrolla actividades de control generales más tecnología para apoyar el logro de los objetivos.
	12. La organización implementa las actividades de control a través de políticas que establecen lo que se espera y procedimientos que ponen las políticas en acción.
Información y comunicación	**13.** La organización obtiene o genera y utiliza relevante, la calidad información para apoyar el funcionamiento de los controles internos.
	14. La organización se comunica internamente información, incluyendo objetivos y responsabilidades para el control interno, necesarios para apoyar el funcionamiento de los controles internos.
	15. La organización se comunica con partes externas sobre asuntos que afecta al funcionamiento del control interno.
Actividades de Monitoreo	**16.** La organización selecciona, desarrolla y realiza curso y / o separada evaluaciones para determinar si los componentes del control interno son presente y funcionamiento.
	17. La organización evalúa y comunica control interno deficiencias en tiempo y forma a las partes responsables de tomar acciones correctivas, incluyendo la alta dirección y el consejo de directores, según corresponda.

Fuente: ISACA. IT Control Objetives for Sabarnes Oxley.

El marco de *COBIT 5* se basa en cinco (5) principios claves que incluyen una amplia guía para los facilitadores de gobierno y gestión de TI en la empresa, ver Figura 2.

Figura No 2. Principios de COBIT 5



Fuente: COBIT 5. "Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa"

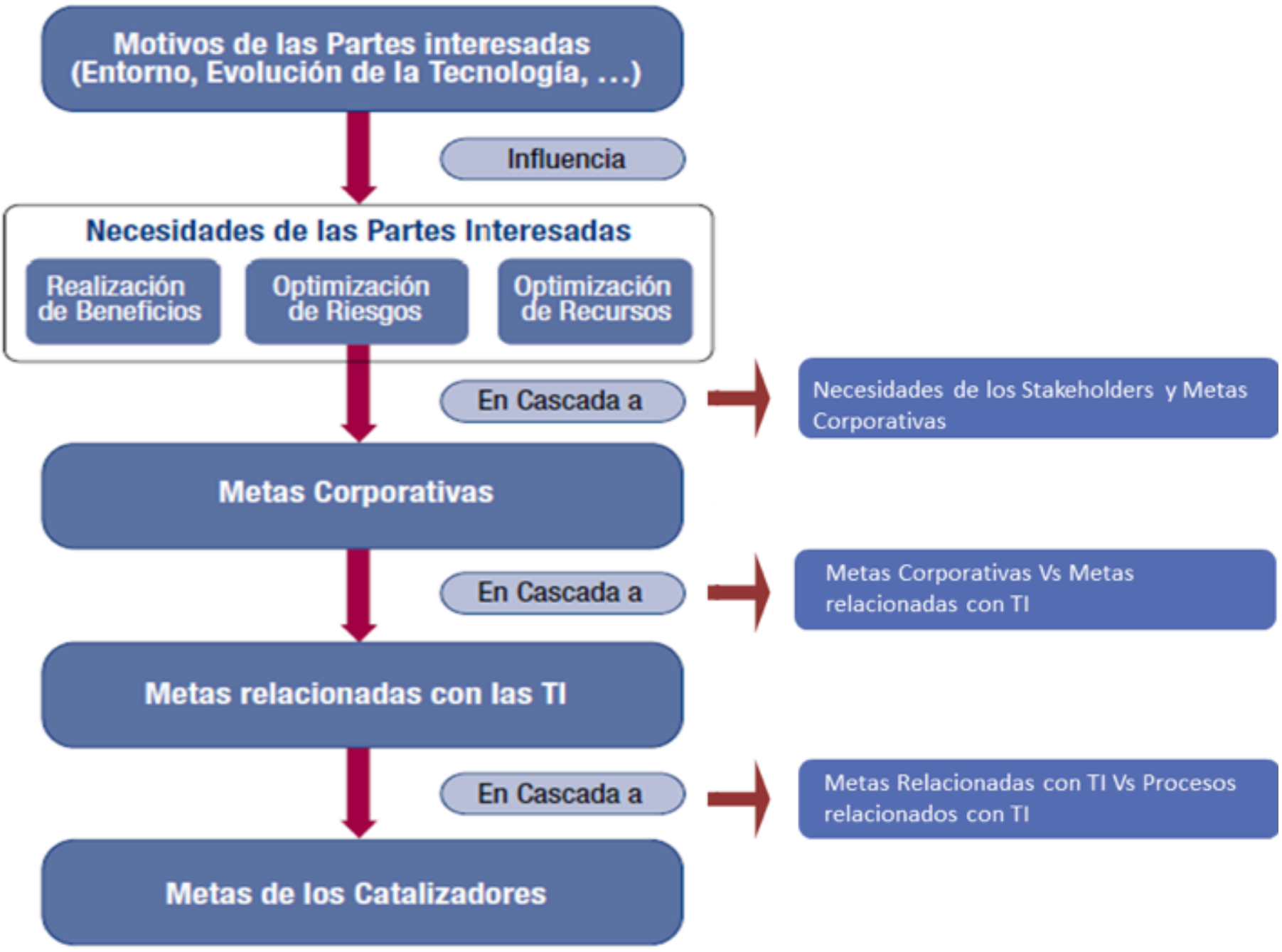
COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas abarcan diferentes tipos de actividades, requieren de estructuras organizativas propias y tienen objetivos particulares. El **Gobierno** según **(Muñoz & Martinez, 2012)**, asegura que las necesidades de los *Stakeholders*, condiciones y opciones sean evaluadas para determinar un balance en el logro de los objetivos estratégicos de la organización, con el propósito de establecer una clara dirección de la organización a través de procesos de priorización y toma de decisiones; y monitorear su desempeño y cumplimiento cotejándolo con los objetivos establecidos por la dirección. La **Gestión** según **(Muñoz & Martinez, 2012)**, posibilita la planeación, construcción, ejecución y monitoreo de actividades alineadas con la dirección; establecidas por el gobierno, para alcanzar los objetivos estratégicos de la organización. En la mayoría de las organizaciones, la gestión es responsabilidad de la dirección ejecutiva bajo el mando del CEO.

Una correcta implementación de un modelo de Gobierno de TI (GEIT) según (Muñoz & Martinez, 2012), provee a la organización receptora de las herramientas necesarias para tomar decisiones óptimas, respecto a las inversiones en tecnología, a maximizar el valor agregado del negocio por parte de las inversiones en TI y a monitorear y dar seguimiento al cumplimiento de las proyecciones estimadas producto de dichas inversiones. Un GEIT eficaz mejorará el rendimiento del negocio y el cumplimiento de los requerimientos externos. Un GEIT efectivo requiere de una serie de catalizadores con roles, responsabilidades, y la obligatoriedad de rendir cuentas en línea con el estilo y las normas operativas específicas y la responsabilidad y supervisión de que se cumplan las normas de estilo y operativas de cada empresa. Estas incluyen una cultura y comportamiento adecuados, principios y políticas rectores, estructuras organizativas, procesos de gobierno y de gestión, bien definidos y gestionados, la información requerida para apoyar la toma de decisiones, soluciones y servicio de soporte y unas capacidades adecuadas de gobierno

y de gestión, de acuerdo a lo planteado en la implementación (ISACA-COBIT 5, 2012).

El marco de referencia de *COBIT 5* establece un análisis en cascada que parte de las necesidades de los interesados y culmina con las metas de los procesos catalizadores, ver Figura 3.

Figura No 3. Visión general de la cascada de las metas de COBIT 5

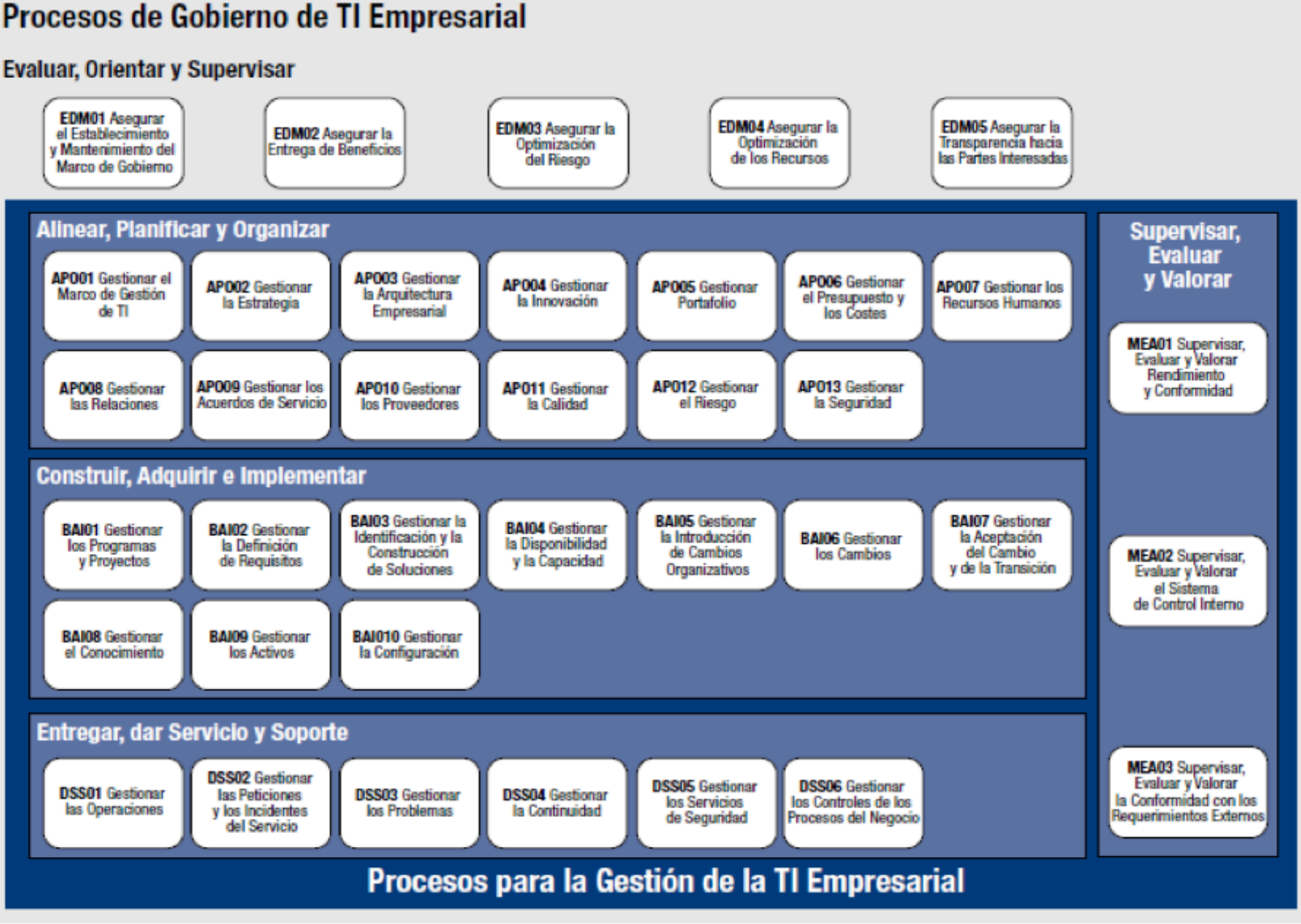


Fuente: COBIT 5. "Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa"

La secuenciación del análisis en cascada está estructurada en cuatro (4) pasos, así: **Paso 1,** Los Motivos de las Partes Interesadas Influyen en las Necesidades de las Partes Interesadas; **Paso 2,** Las Necesidades de las Partes Interesadas Desencadenan Metas Empresariales; **Paso 3,** Cascada de Metas de Empresa a Metas Relacionadas con las TI y **Paso 4,** Cascada de Metas Relacionadas con las TI Hacia Metas Catalizadoras. Una explicación más detallada puede ser consultada en (ISACA-COBIT 5, 2012).

COBIT 5 tiene definidos 37 procesos agrupados en cinco (5) dominios. Se definen cinco procesos para el Gobierno de TI Empresarial (un dominio EDM – Evaluar, Orientar Supervisar) y 32 procesos distribuidos en cuatro (4) dominios para lo referente a la Gerencia de TI Empresarial (APO – Alinear, Planificar y Organizar 13, BAI – Construir, Adquirir e Implementar 10, DSS – Entregar, Dar soporte y Servicio 6 y MEA – Supervisar, Evaluar y Valorar 3), ver Figura 4.

Figura No 4. Estructura del Marco de Referencia de COBIT 5



Fuente: (ISACA-COBIT 5, 2012). "Procesos catalizadores"

5. Articulacion *Coso*, *Cobit* Y Ley *Sarbanes–Oxley*

Las estadísticas demuestran que los dos marcos de control más ampliamente adoptados por las empresas públicas sujetas a los requisitos de la Ley *Sarbanes-Oxley* de 2002 son el *COSO IC–IF*, propuesto en 1992, y los Objetivos de Control para Información y Tecnologías Relacionadas - *COBIT* de ISACA. Aunque la Comisión de Valores de EEUU SEC, sugiere que las empresas públicas apliquen los componentes de control de COSO, cuando se busca el cumplimiento de *Sarbanes-Oxley*, ni la *SEC* ni el *Public Company Accounting Oversight Board de EEUU*, han respaldado abiertamente un marco específico de control de tecnología de la información.

COSO y *COBIT* atienden a diferentes públicos. Si bien el público objetivo del *COSO* es la gestión en general, *COBIT* está destinado a la gestión, usuarios, y los auditores (en su mayoría los auditores de TI). El marco de control de *COSO* apunta a lo relacionado con el Gobierno Corporativo, pero se tiene en cuenta de que hoy las áreas de tecnología informática son vistas como una empresa dentro de la empresa, por tanto, es necesario definir un marco de referencia y control para esa dependencia y es ahí donde *COBIT* obtiene su campo de acción. Esta distinción en efecto define y determina el alcance de cada marco de control. Debido a estas diferencias, los auditores no deben esperar una relación uno a uno entre los cinco (5) componentes de control de *COSO* y los cuatro (4) dominios de *COBIT*.

Lo importante del proceso de implantación de la Ley *Sarbanes-Oxley*, es identificar los aspectos de *COSO* que le atañen y definir el rol de la tecnología informática, en el manejo de la misma. De esta forma, los auditores podrán seleccionar los objetivos de controles pertinentes de *COBIT* y relacionarlos con la Ley *Sarbanes-Oxley* cuando asignan la estructura de control interno

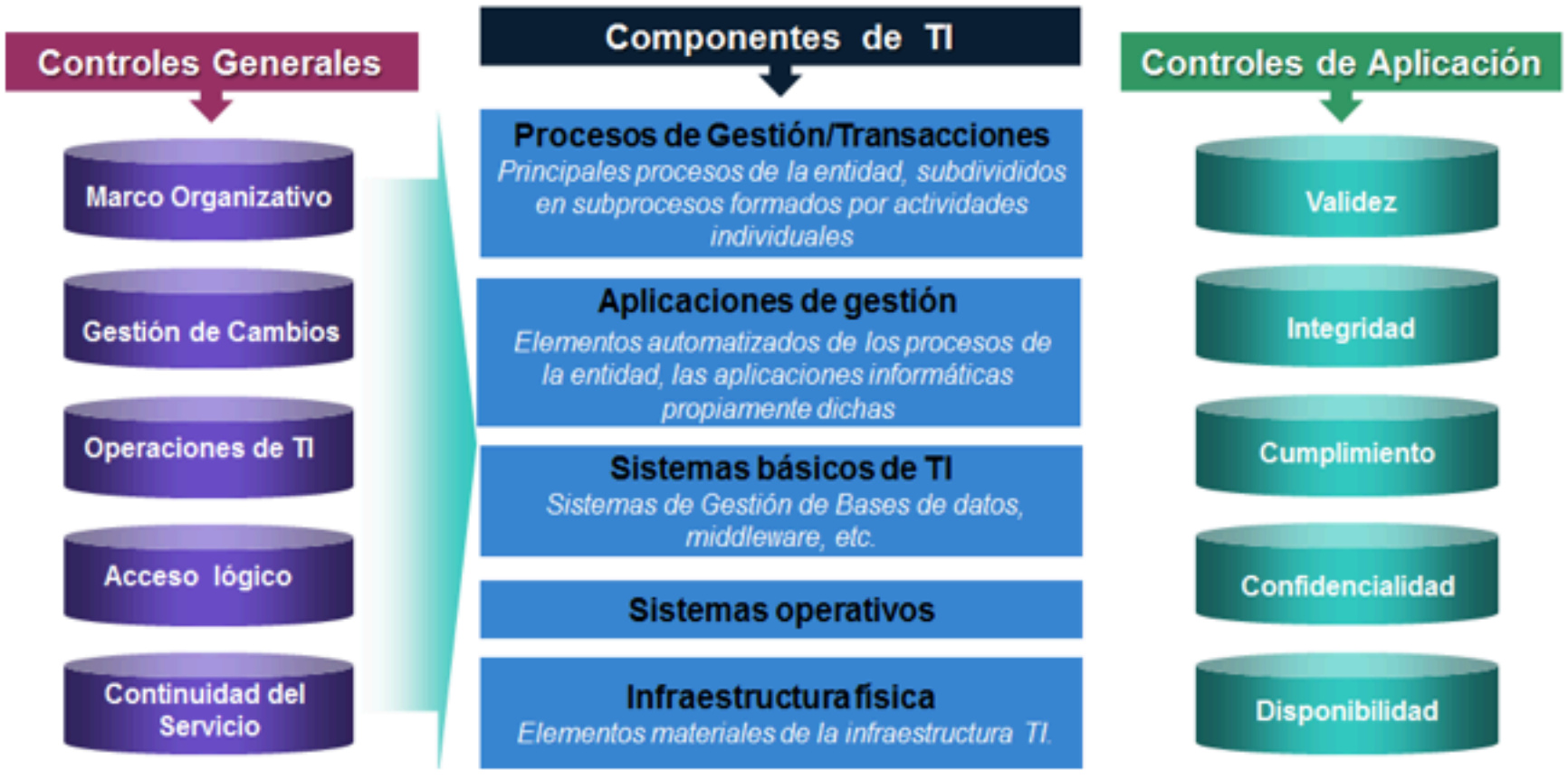
COSO (Chan, 2004). Desde el punto de vista de TI, las dos secciones de mayor visibilidad de la Ley *Sarbanes-Oxley*, para quienes están obligados a dar cumplimiento de la misma, son la 302 y 404.

La sección 302, "Responsabilidad de la Compañía por los Informes Financieros", establece los lineamientos bajo los cuales los CEOs y CFOs deberán realizar la certificación anual del control interno implementado en las compañías, (SEC, 2002).

La sección 404, "Evaluación de la Gerencia de los Controles Internos", establece obligaciones por parte de la Gerencia de la compañía, en emitir un informe anual sobre la evaluación del control interno de cada uno de los procesos del negocio. Además, esta sección requiere que los auditores externos de las compañías certifiquen la evaluación del control interno realizado por la Gerencia, sobre la emisión de los reportes financieros. Es decir, las organizaciones deben asegurar el adecuado funcionamiento del control interno, incluyendo los controles de Tecnología de Información (IT), (SEC, 2002).

El PCAOB describe controles generales o controles de entidad para los procesos de TI, para proporcionar un entorno operativo fiable y apoyar la operación efectiva de los controles de aplicación. Los controles a "nivel de entidad" se reflejan en la forma de funcionar de una organización, e incluyen políticas, procedimientos y otras prácticas de alto nivel que marcan las pautas de la organización. Son un componente fundamental del modelo *COSO* y deben tener en cuenta las operaciones TI que respaldan la información financiera. Los controles a nivel de entidad tienen influencia significativa sobre el rigor con el que el sistema de control interno es diseñado y opera en el conjunto de los procesos. La Figura 5, muestra la relación de los controles de entidad y de aplicación, con los diferentes componentes de Tecnología Informática.

Figura No 5. Modelo de Relación de Controles y Componentes de TI



Fuente: Elaboración propia

Los controles generales son las políticas y procedimientos con aplicación en el ambiente de tecnología informática de una organización, cobijan todos los componentes básicos de los sistemas de información (infraestructura, aplicaciones, datos/información y personas) y su objetivo es alinear y asegurar el correcto y seguro funcionamiento de TI. Por tanto, en un entorno informatizado el objetivo de los controles generales es establecer un marco conceptual

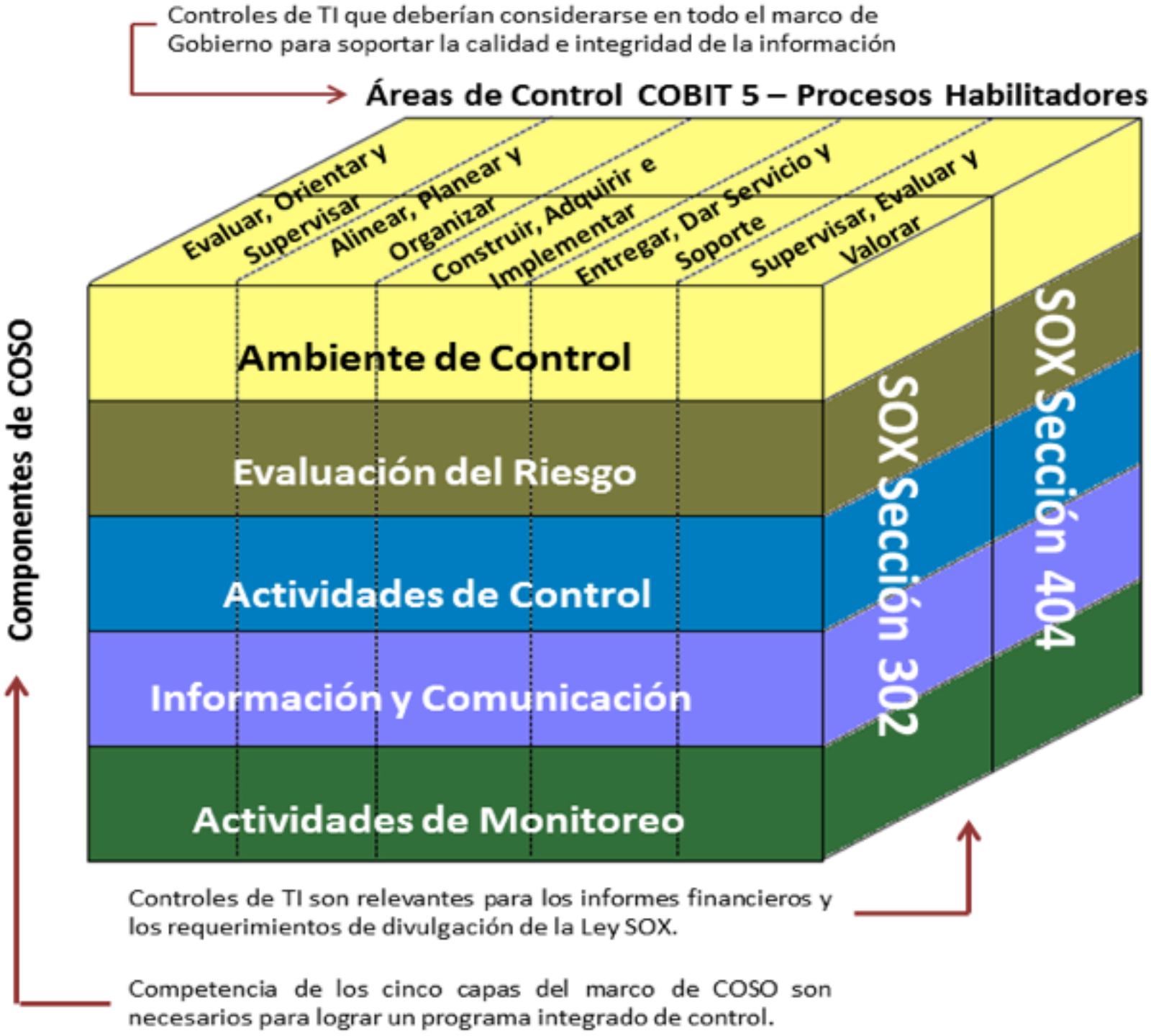
de control sobre las actividades de tecnología Informática y proveer seguridad razonable de la consecución de los objetivos generales de control interno y el correcto funcionamiento de los controles de aplicación. La Ley *Sarbanes-Oxley*, propone como controles generales claves, utilizados para auditar la efectividad de los controles internos sobre los informes financieros los siguientes: Controles Sistemas de Información y Tecnología, Ambiente de Control de TI, Operaciones Computacionales, Acceso a los programas y datos, Desarrollo de programas y Gestión del Cambio. Para mayor información consultar (Salinas, 2014).

---

6. Analizando El Marco De Referencia De *COSO* Para TI En *COBIT 5*

Para el logro de un adecuado cumplimiento de los lineamientos establecidos por la Ley *Sarbanes-Oxley*, y teniendo en cuenta lo expuesto anteriormente, en lo relativo al cumplimento de aspectos básicos del Marco de Referencia de *COSO*, para la apropiada implantación de la Ley, se puede evidenciar como los controles de TI apoyan el cumplimiento del marco de *COSO*; no obstante, éste no aborda otras áreas específicas de procesos de TI, tales como la gestión de TI o información de los servicios TI y la seguridad. *COSO* describe controles generales para el Gobierno Corporativo y estos no cambian con la introducción de tecnología informática, ya que este ambiente requiere la implantación de controles internos específicos. El Control Interno en el marco de *COSO* posee cinco (5) componentes. La Figura 6, muestra la alineación de éstos y su integración con la Ley *Sarbanes-Oxley* para lograr los objetivos de control necesarios, para una información financiera eficaz. Los componentes del marco de COSO comienzan con la identificación de los mecanismos de control y culminan con el seguimiento de los controles internos, son las capas horizontales del cubo. Las áreas de control de COBIT 5, comienzan con el dominio del gobierno (Evaluar, Dirigir y Supervisar - EDM) y terminan con el dominio de gestión de Supervisar, Evaluar y Valorar - MEA, constituyen la capa vertical del cubo y son aplicables a los cinco (5) componentes del marco *COSO*, individualmente y en conjunto.

Figura No 6. Mapeo *COBIT 5* y Ley *Sarbanes-Oxley* con el Cubo de *COSO*



Fuente: (ISACA-COBIT 5, 2012). IT Control Objetives for Sabarnes Oxley.

---

7. Propuesta De Articulación *COBIT 5* Con *COSO*, Orientado A Cumplir Los Lineamientos De La Ley *SARBANES-OXLEY*

Con base en los lineamientos establecidos por la Ley *Sarbanes-Oxley*, se han determinado los controles que apuntan al cumplimiento de los 17 principios, en el marco *COSO* de TI. En la Tabla 2, se detalla la clasificación del control, es decir, si éste opera a "nivel de entidad" o a "nivel de actividad". Nótese que un control puede no ser exclusivo de un ámbito de aplicación, es decir, un control puede tener vigencia en ambos niveles.

Tabla No 2. Áreas de *COBIT 5* / Componentes de *COSO*, válidos para Ley *Sarbanes-Oxley*

Nivel Entidad	Nivel Acitidad	Detalle Actividad/Nivel de Objetivo	Referencia COBIT 5	COMPONENTES DE COSO															
				Ambiente de Control					Administración del Riesgo				Actividades de Control			Información y comunicación			Actividades de Monitoreo	
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
		Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.	EDM01																	

EDM - EVALUAR, ORIENTAR Y SUPERVISAR - Ambiente de TI	+		Evaluar el sistema de gobierno.	EDM01.01	+	+	+		+								+	+			
	Asegurar la optimización del riesgo.			**EDM03**																		
	+		Orientar la gestión de riesgos.	EDM03.02		+			+	+	+						+	+			
	Asegurar la transparencia hacia las partes interesadas			**EDM05**																		
	+		Orientar la comunicación con las partes interesadas y la elaboración de informes.	EDM05.02		+			+								+	+			
	+		Supervisar la comunicación con las partes interesadas.	EDM05.03													+	+	+		+
APO - ALINEAR, PLANEAR Y ORGANIZAR - Ambiente de TI	**Gestionar el Marco de Gestión de TI**			**APO01**																		
	+		Establecer roles y responsabilidades.	APO01.02			+	+	+								+	+			
	+		Definir la propiedad de la información (datos) y del sistema.	APO01.06								+					+	+			
	+	+	Mantener el cumplimiento con las políticas y procedimientos.	APO01.08					+			+				+	+	+			
	Gestionar la Estrategia			**APO02**																		
	+		Comprender la dirección de la empresa.	APO02.01						+							+	+			
	+		Definir el plan estratégico y la hoja de ruta.	APO02.05					+	+							+	+			
	Gestionar los Recursos Humanos			**APO07**																		
	+		Mantener la dotación de personal suficiente y adecuada.	APO07.01				+				+										
	+		Mantener las habilidades y competencias del personal.	APO07.03	+			+														
	+		Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	APO07.05				+				+					+	+			
	Gestionar los Proveedores			**APO10**																		
		+	Supervisar el cumplimiento y el rendimiento del proveedor.	APO10.05										+	+		+	+	+			
	Gestionar la Calidad			**APO11**																		
	+		Establecer un sistema de gestión de la calidad (SGC).	APO11.01					+	+												
	+		Definir y gestionar los estándares, procesos y prácticas de calidad.	APO11.02					+	+						+	+					
	Gestionar el Riesgo			**APO12**																		
	+		Recopilar datos.	APO12.01						+	+	+	+				+	+			
	+		Analizar el riesgo.	APO12.02						+	+	+	+				+	+			
	+		Mantener un perfil de riesgo.	APO12.03						+	+	+	+				+	+			
	+		Expresar el riesgo.	APO12.04						+	+	+	+				+	+			
	+		Definir un portafolio de acciones para la gestión de riesgos.	APO12.05					+	+	+	+	+				+	+			
	+		Responder al riesgo.	APO12.06						+	+	+	+				+	+			
DSS - ENTREGAR, DAR SERVICIO Y SOPORTE - Operaciones y acceso a programas y datos	**Gestionar operaciones.**			**DSS01**																		
		+	Gestionar servicios externalizados de TI	DSS01.02						+	+	+	+	+	+		+	+			
MEA - SUPERVISAR, EVALUAR Y VALORAR - Ambiente de TI	**Supervisar, evaluar y valorar el rendimiento y la conformidad.**			**MEA01**																		
	+		Analizar e informar sobre el rendimiento.	MEA01.04						+							+	+		+	+
	+		Asegurar la implantación de medidas correctivas.	MEA01.05						+							+	+		+	+
	Supervisar, evaluar y valorar el sistema de control interno.			**MEA02**																		
	+		Supervisar el control interno.	MEA02.01													+	+		+	+
	+		Revisar la efectividad de los controles sobre los procesos de negocio.	MEA02.02					+	+							+	+		+	+
	+		Identificar y comunicar las deficiencias de control.	MEA02.04						+							+	+		+	+
	+		Garantizar que los proveedores de aseguramiento son	MEA02.05													+	+		+	+

		independientes y están cualificados.																		
	•		Planificar iniciativas de aseguramiento.	MEA02.06													•	•		•	•
	•		Estudiar las iniciativas de aseguramiento.	MEA02.07													•	•		•	•
			Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	**MEA03**																	
	•		Identificar requisitos externos de cumplimiento.	MEA03.01								•					•	•		•	•
	•		Optimizar la respuesta a requisitos externos.	MEA03.02								•					•	•		•	•

Fuente: Elaboración propia con estructura de ISACA. IT Control Objetives for Sabarnes Oxley.

8. Metodología Que Apoya La Implementación

Anteriormente se han identificado los aspectos y principios del Marco de Referencia de *COSO*, que se articulan con los lineamientos de la Ley *Sarbanes-Oxley*. Determinando los dominios y procesos del Marco de Referencia de *COBIT 5*, que se articulan con los primeros. Esto configura los fundamentos conceptuales necesarios para iniciar la evaluación del ámbito de tecnología informática de cualquier entidad, en cuanto al cumplimiento de los lineamientos establecidos por la Ley *Sarbanes-Oxley*; no obstante, un auditor de poca experiencia podría encontrarse ante un intrincado obstáculo al no saber por dónde iniciar su labor.

Para brindar un mayor apoyo al desarrollo de su labor, se tomaron como fundamento, los cinco (5) niveles del Marco de Referencia de *COSO*, estableciendo para cada uno de ellos los ámbitos concernientes al Modelo de Gobierno de Tecnología Informática, de los que se ocupa. Obviamente, es necesario identificar los dominios y los procesos del Marco de referencia de *COBIT 5*, que se deben considerar para evaluar el grado de cumplimiento por parte de la organización objeto de evaluación.

En las Tablas 3.1-3.4, se muestran los niveles del Marco de Referencia de *COSO*, sus implicaciones sobre los ámbitos de Gobierno de TI, los Procesos y las Prácticas Claves de Gobierno de TI que aplican y las preguntas que un auditor debe formular para iniciar el proceso de evaluación, del cumplimiento de los lineamientos de la Ley *Sarbanes-Oxley*.

Tabla No 3.1. Ambiente de control – COSO. Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Gobierno		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
EDM01.01	Evaluar el sistema de gobierno.	¿Están los sistemas de gobierno de TI alineados con la empresa?
APO01.03	Mantener los elementos catalizadores del sistema de gestión.	En concreto, el uso ético y procesamiento de información y su impacto en la sociedad, el medio ambiente natural e intereses de los interesados internos y externos deben alinearse con la dirección, metas y objetivos de la empresa.
Ámbito de gobierno de TI: Planeación Estratégica de TI		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO02.01	Comprender la dirección de la empresa.	¿La administración ha preparado planes estratégicos para TI que alinea los objetivos de negocio con las estrategias de TI?

APO02.05	Definir el plan estratégico y la hoja de ruta.	¿El enfoque de la planificación incluye mecanismos para relievar las solicitudes de los grupos de interés internos y externos afectados por los planes estratégicos de TI?
EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	¿La dirección de TI comunica sus planes a las partes interesadas del negocio, dueños de procesos y otras partes interesadas en la empresa?
APO02.06	Comunicar la estrategia y la dirección de TI.	¿La dirección de TI comunica sus actividades, retos y riesgos regularmente con el Director Ejecutivo (CEO) y Director Financiero (CFO)? ¿Es esta información también se comparte con el Consejo de Administración?
EDM05.03	Supervisar la comunicación con las partes interesadas.	¿Monitorea la organización de TI su estado de avance contra el plan estratégico y reacciona en consecuencia para cumplir los objetivos establecidos? ¿Analizar e informar periódicamente el avance del desempeño contra los objetivos, utilizando un método que ofrece una sucinta visión integral ajustada al sistema de vigilancia de la empresa?
MEA01.04	Analizar e informar sobre el rendimiento.	

Tabla No 3.1. Cont. Ambiente de control – COSO.
Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Procesos de TI, Organización y Relaciones		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO07.03	Mantener las habilidades y competencias del personal.	¿Los administradores de TI tienen conocimientos y experiencia adecuados para cumplir con sus responsabilidades?
APO01.06	Definir la propiedad de la información (datos) y del sistema.	¿Los sistemas, activos y datos pertinentes han sido inventariados y sus dueños identificados?
APO01.02	Establecer roles y responsabilidades.	¿Están las funciones y responsabilidades de la organización de TI definidas, documentadas y entendidas?
APO07.01	Mantener la dotación de personal suficiente y adecuada.	¿Existe un seguimiento del plan de uso de TI en la empresa y de los recursos humanos del negocio?
APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	¿La propiedad y responsabilidad de los datos ha sido comunicado a interesados adecuados y estos las han aceptado?
APO01.02	Establecer roles y responsabilidades.	La gestión de TI ha implementado una adecuada división de roles y responsabilidades para controlar que un mismo individuo tenga dominio de un proceso crítico?

Ámbito de gobierno de TI: Administrar los facilitadores y comunicar objetivos y Dirección de la Empresa		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO01.03	Mantener los elementos catalizadores del sistema de gestión.	La organización ha adoptado y promovido la cultura de gestión de la integridad, incluyendo la ética, las prácticas comerciales y las evaluaciones de los recursos humanos de la empresa?
APO01.04	Comunicar los objetivos y la dirección de gestión.	
Ámbito de gobierno de TI: Educar y entrenar usuarios		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO07.01	Mantener la dotación de personal suficiente y adecuado.	¿Ofrece la administración de TI programas educativos y de formación continua que incluyen la conducta ética, las prácticas de seguridad del sistema, las normas de confidencialidad, las normas de integridad y de las responsabilidades de seguridad de todo el personal?
APO07.03	Mantener las habilidades y competencias del personal.	

Fuente: Elaboración propia

Tabla No 3.2. Comunicación e Información - COSO. Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Comunicar objetivos de Gestión y Dirección		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO01.04	Comunicar los objetivos y la dirección de gestión.	¿La gerencia de TI revisa periódicamente sus políticas, procedimientos y normas para considerar condiciones cambiantes del negocio?
APO01.08	Mantener el cumplimiento con las políticas y procedimientos.	
APO01.08	Mantener el cumplimiento con las políticas y procedimientos.	¿Tiene la administración de TI un proceso definido para evaluar el cumplimiento de las políticas, procedimientos y normas?
MEA03.01	Identificar requisitos externos de cumplimiento.	¿La gestión de TI comprende sus funciones y responsabilidades relacionadas con el cumplimiento de la Ley Sarbanes-Oxley?
MEA03.02	Optimizar la respuesta a requisitos externos.	

Fuente: Elaboración propia

Tabla No 3.3. Administración del riesgo - COSO. Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Evaluar y Administrar el Riesgo		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
EDM03.01	Evaluar la gestión de riesgos.	¿La organización de TI tiene un marco de evaluación de riesgos de entidad y por nivel de actividad que se utiliza periódicamente para evaluar los riesgos de la información de la información financiera que afecte el logro de los objetivos? ¿Considera la probabilidad de materialización de las amenazas y el impacto?
EDM03.02	Orientar la gestión de riesgos.	
EDM03.03	Supervisar la gestión de riesgos.	
APO12.01	Recopilar datos.	¿Mide el marco de evaluación de riesgos de TI de la organización el impacto del riesgo en función de criterios cualitativos y cuantitativos, con aportaciones de las diferentes áreas del negocio, incluyendo, pero no limitado a, el intercambio de ideas de gestión, la planificación estratégica, las auditorías pasadas y otras evaluaciones?
APO12.02	Analizar el riesgo.	
APO12.03	Mantener un perfil de riesgo.	
APO12.04	Expresar el riesgo.	
APO12.05	Definir un portafolio de acciones para la gestión de riesgos.	Donde los factores de riesgo se consideran aceptables, ¿Existe documentación formal y la aceptación del riesgo residual, incluyendo una adecuada cobertura de seguro, negociación de pasivos contractuales y auto-seguro? Donde los factores de riesgo no son aceptados, la gestión de TI tiene un plan de acción para implementar la respuesta al riesgo?
APO12.06	Responder al riesgo.	

Fuente: Elaboración propia

Tabla No 3.4. Monitoreo - COSO. Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Administrar la Calidad		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
APO11.01	Establecer un sistema de gestión de la calidad (SGC).	¿Está la documentación de TI creada y mantenida conteniendo procesos, controles y actividades?
	Definir y gestionar los	

APO11.02	estándares, procesos y prácticas de calidad.	
APO11.03	Enfocar la gestión de la calidad en los clientes.	¿Existe un plan de calidad para las funciones significativas de TI (por ejemplo, el desarrollo e implementación de sistemas) y también proporciona un enfoque coherente para abordar tanto las actividades generales como específicas del proyecto de aseguramiento de la calidad?
APO11.06	Mantener una mejora continua	
Ámbito de gobierno de TI: Monitorear y evaluar el rendimiento		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
MEA01.01	Establecer un enfoque de la supervisión.	La gestión de TI ha establecido métricas apropiadas para gestionar con eficacia las actividades del día a día del departamento de TI?
MEA01.02	Establecer los objetivos de cumplimiento y rendimiento.	
MEA01.03	Recopilar y procesar los datos de cumplimiento y rendimiento.	
MEA01.04	Analizar e informar sobre el rendimiento.	¿Monitorea la gestión de TI la prestación de servicios de TI para identificar deficiencias y hace establecer planes de acción concretos de mejoramiento?
MEA01.05	Asegurar la implantación de medidas correctivas.	

Fuente: Elaboración propia

Tabla No 3.4. Monitoreo - COSO. Preguntas para evaluar cumplimiento de requisitos de Ley *Sarbanes-Oxley* por parte de TI

Ámbito de gobierno de TI: Monitorear y evaluar el Control Interno		
Referencia a COBIT 5		**Preguntas para evaluar cumplimiento**
MEA02.01	Supervisar el control interno.	¿La gerencia de TI realiza revisiones independientes de sus operaciones, incluidas las políticas, procedimientos, sistemas generales y procesos y considera en esta evaluación la adhesión a políticas y procedimientos corporativos?
MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	
MEA02.04	Identificar y comunicar las deficiencias de control.	

MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	
APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	¿La empresa tiene una función de auditoría interna de TI que se encarga de la revisión de las actividades y controles de TI, incluidos los controles generales y de aplicación?
DSS01.02	Gestionar servicios externalizados de TI	¿Hay un proceso de seguimiento de las acciones residuales?
MEA02.01	Supervisar el control interno.	¿Existe un mecanismo de control interno para permitir el monitoreo de los proveedores de servicios de terceros?
MEA02.06	Planificar iniciativas de aseguramiento.	
MEA02.07	Estudiar las iniciativas de aseguramiento.	
MEA02.08	Ejecutar las iniciativas de aseguramiento.	

Fuente: Elaboración propia

9. Resultados

Culminada la labor de identificar el cumplimiento de los requisitos establecidos por los lineamientos de la Ley *Sarbanes-Oxley*, es necesario revisar que los controles generales o "Controles de Entidad", que garantizan el cumplimiento de dichos lineamientos, se encuentren establecidos y cumpliéndose.

Anteriormente se efectuó una identificación de los aspectos que relacionan a la Ley *Sarbanes-Oxley* con el marco de referencia de *COBIT 5* y se definieron los factores que el auditor debe evaluar para verificar el adecuado cumplimiento de los mismos.

Las Tabla 4.1 y 4.2, constituye la guía final para la ejecución de pruebas relacionadas con el cumplimiento de la Ley *Sarbanes-Oxley*. En estas tablas se presenta la relación entre los Procesos para la Gestión de TI que aplican para cada uno de los factores a auditar y se identifican las Practicas Claves de Gobierno de TI, que apuntan directamente a establecer la presencia y operatividad del control. Para cada uno de los Procesos de Gestión de TI y las respectivas Prácticas Claves, involucradas en las pruebas a realizar, el auditor deberá prestar especial atención a la definición del Objetivo de Control General y la Justificación, ya que esto le permitirá mantener el foco en los resultados de cada una de las pruebas y acopiar las evidencias necesarias para argumentar su diagnóstico.

Tabla No 4.1. Gestión y definición de requerimientos (BAI02 y BAI04).
Objetivos de Control Generales y Específicos y Pruebas a las Actividades de Control

Objetivo de Control General: Los controles proporcionan una garantía razonable de que los requisitos funcionales y técnicos de negocio se mantienen con un estudio de viabilidad que tenga en cuenta las soluciones

alternativas, riesgo empresarial y aprobaciones.

Justificación: El proceso de construcción, adquisición y desarrollo de procesos de negocio, aplicaciones, infraestructura, datos y servicios debe contemplar la definición de los requerimientos del negocio en el diseño, desarrollo y adquisición de sistemas que apoyen el logro de los objetivos de negocio. Las deficiencias en esta área pueden tener un impacto significativo en la información financiera y su divulgación. Por ejemplo, sin controles suficientes sobre interfaces de aplicaciones, la información financiera puede no ser completa o precisa.

Objetivos de Control Específicos	Pruebas a las actividades de control	Referencias COBIT 5
La empresa cuenta con un sistema definido que mantiene funcional el negocio y los requisitos técnicos reciben la aprobación de todos los interesados.	Confirme, revise y analice que todos los requisitos de las partes interesadas, incluidos los criterios de aceptación pertinentes, se consideran, clasifican, priorizan y se registran de una manera que sea comprensible para los interesados, patrocinadores comerciales y personal de Ejecución Técnica.	BAI02.01
	Verificar que en los requisitos de control de los datos, información y procesos automatizados, según el caso, el riesgo de la información para el cumplimiento de leyes, reglamentos y contratos comerciales están incluidos.	BAI04.01
	Compruebe que en la evaluación de la disponibilidad actual, se ha considerado el rendimiento del sistema y la capacidad.	BAI04.03
	Compruebe que existe un plan para requisitos nuevos o modificados de servicios basado en el rendimiento del sistema, disponibilidad y capacidad.	
La empresa cuenta con un sistema para realizar estudio de factibilidad e incluyendo la formulación de soluciones alternativas.	Obtenga una copia de un reciente estudio de factibilidad.	BAI02.02
	Identificar las acciones necesarias para la adquisición o desarrollo de una solución tomando como base la arquitectura de la empresa y tenga en cuenta el alcance y las limitaciones presupuestarias.	
	Asegúrese de que el estudio se traduce en un plan de adquisición / desarrollo de alto nivel.	
La empresa cuenta con un sistema para la identificación, documentación, priorizar y mitigar el riesgo técnico y la información, y las soluciones propuestas están relacionada con el procesamiento existente y con los intereses de la empresa.	Obtenga una copia de un registro de riesgos que demuestre la implicación de las partes interesadas, incluyendo inversionistas y dueños del proceso. Asegúrese de que el patrocinador del negocio o dueño del producto influencia la decisión final de acuerdo con el modelo de negocio, con respecto a la elección de la solución, en lo relativo al enfoque de la adquisición y diseño de alto nivel.	BAI02.03 BAI02.04
	Compruebe que se ha llevado a cabo un análisis de impacto en el negocio una vez que se ha realizado la capacidad de línea de base del rendimiento del sistema.	BAI04.02

Algunos de los Objetivos de Control Específicos, poseen fondo oscuro, para indicar que es un Objetivo de Control Clave, para el cumplimiento de los lineamientos de la Ley *Sarbanes-Oxley*, y por tanto, el auditor deberá ser mucho más acucioso al practicar las pruebas sugeridas por esta guía y analizar la posibilidad de profundizar con pruebas de su autoría y decisión para la obtención de mayores evidencias que fortalezcan la contundencia de su opinión.

Tabla No 4.2. Identificar, construir y administrar soluciones (BAI03 Y BAI04).
Objetivos de Control Generales y Específicos y Pruebas a las Actividades de Control

Objetivo de Control General: Los controles proporcionan una garantía razonable de que las soluciones se identifican y se mantienen en línea con los requerimientos empresariales y abarcan el diseño, desarrollo y adquisición / compra de componentes y la asociación con proveedores / vendedores. Además, se incluyen la gestión de configuración, preparación de la prueba, el mantenimiento de los procesos de negocio, aplicaciones, infraestructura, información / datos y servicios por lo que se proporcionan las plataformas tecnológicas apropiadas para apoyar las aplicaciones de información financiera.		
Justificación: El proceso de construcción de la adquisición e implementación de aplicaciones de software y la infraestructura de tecnología incluye el diseño, la adquisición / construcción e implementación de sistemas que apoyen el logro de los objetivos de negocio. Este proceso no sólo incluye cambios importantes en los sistemas existentes, sino en los componentes de la infraestructura, incluyendo servidores, redes y bases de datos, que son fundamentales para el procesamiento de información segura y confiable. Sin aplicaciones e infraestructura adecuadas existe un mayor riesgo de que las aplicaciones de información financiera no sean capaces de transferir datos entre aplicaciones y las fallas críticas en la infraestructura no se detecten de manera oportuna.		
Objetivos de Control Específicos	**Pruebas a las actividades de control**	**Referencias COBIT 5**
La empresa tiene una técnica de desarrollo de alto nivel que permite diseños detallados que se alinean con la arquitectura de la empresa y la estrategia de TI.	Seleccione una muestra de diseños de alto nivel y verifique que está en consonancia con las normas de diseño de la empresa, arquitectura empresarial, plan de seguridad y las leyes, reglamentos y contratos. Asegúrese de que sean aprobadas de manera adecuada y se reúnen las soluciones propuestas.	BAI03.01 BAI03.02 BAI04.03
La empresa cuenta con un proceso para la adquisición o el desarrollo de componentes de la solución, que incluye todos los requisitos de control en el proceso de negocio, el apoyo a aplicaciones y servicios de infraestructura.	Seleccione y examinar todos los planes de adquisición, que deben incluir adiciones futuras de capacidad, costos de transición, el riesgo y mejoras durante el ciclo de vida del proyecto. Revise las solicitudes de cambio, el rendimiento y las revisiones de calidad, asegurar la participación activa de todos los actores afectados. Revise los requisitos de configuración de software de aplicación.	BAI03.03 BAI03.04 BAI03.05
Existen procedimientos documentados para la preparación de las pruebas de la solución, teniendo en cuenta la garantía de calidad (QA) y que los planes están alineados con el sistema de gestión de calidad de la empresa (SGC).	Revise una muestra de los planes de prueba y verifique que existe un entorno de prueba que cubre todo el alcance de la solución.	BAI03.06 BAI03.07
	Identifique registros de prueba y compruebe que los errores de las pruebas se clasifican adecuadamente como menor, significativa o crítica de acuerdo con la evaluación del riesgo realizado en la definición de requisitos y las fases de construcción de la solución.	BAI03.08

La empresa cuenta con un sistema de requisitos para la gestión del cambio en todo el ciclo de vida del proyecto.	Seleccionar una muestra de solicitudes de cambio y confirmar si mantienen la integridad y la configuración de los componentes de la solución. Evaluar el impacto de cualquier actualización importante a la solución y clasificarlo de acuerdo con criterios objetivos acordados en la base del resultado del análisis de riesgos.	BAI03.09 BAI04.03
La empresa tiene un plan para el mantenimiento continuo de las soluciones desarrolladas y probadas. Esto incluye revisiones periódicas contra las necesidades del negocio y las necesidades operacionales.	Seleccionar una muestra de proyectos y determinar que se prepararon los manuales de referencia de usuario y la documentación del sistema y de operaciones.	BAI03.10
	Compruebe que las pruebas son ejecutadas y cerradas.	
La empresa tiene un proceso para clasificar como nuevo y cambiado los servicios de TI y los niveles de servicio.	Compruebe la documentación de los niveles de servicio y la definición de nuevos servicios y cambios de TI.	BAI03.11
	Asegúrese de que los niveles de servicio para los proveedores externos se definen, acuerdan y monitorean.	BAI04.03
	Asegúrese de que están completos, incluyendo elementos tales como los tiempos de servicio, la disponibilidad, la seguridad, el cumplimiento de la continuidad y la usabilidad. Compruebe la existencia de una cartera o catálogo de servicios.	

Fuente: Elaboración propia.

En la última columna se encuentra la referencia a las Prácticas Claves de Gobierno de TI, que se relacionan con cada Objetivo Específico, esto servirá de guía para que el auditor revise lo expuesto por cada una de ellas, en el libro de Procesos Catalizadores del Marco de Referencia de *COBIT 5* y establezca posibles aspectos a revisar o profundizar.

Por ser muy extensa la Guía resultante de la labor efectuada, sólo se plantean algunos apartes de ésta, para socializar su estructura y la forma como debe ser seguida por quien ejecuta un trabajo de Auditoría basado en ella.

---

10. Discusión

En (Bargeron, Kenneth, & Chad, 2010), argumentan que la Ley *Sarbanes-Oxley* ha "tenido un efecto escalofriante en la toma de riesgos" por parte de las empresas estadounidenses que cotizan en bolsa. Utilizando una muestra de empresas británicas, como un punto de referencia, el estudio estableció que las empresas estadounidenses han reducido significativamente su inversión en I+D (Investigación y Desarrollo) y el gasto de capital global, al tiempo que ha aumentado su tenencia de efectivo. Generalizadamente concluyeron, que este comportamiento revela una reducción estadísticamente significativa en la toma de riesgos después de la adopción de la Ley *Sarbanes-Oxley*, debilitando los mercados de valores de Estados Unidos, conduciendo a las empresas nacionales a compradores de capital privado y causando que las empresas extranjeras busquen asentamiento en otros lugares.

(Litvak, 2007), utiliza una técnica diferente para medir el efecto de la Ley *Sarbanes-Oxley* en los mercados de capital de Estados Unidos. En un artículo reciente que examinó su impacto sobre las acciones de empresas que cotizan tanto en América como en el extranjero. Las acciones de empresas interrelacionadas tienden a comercializar con una prima a las acciones

para empresas similares.

El estudio publicado en (Kamar, Karaca-Mandic, & Talley, 2006), analizó si la Ley *Sarbanes-Oxley* ha impulsado a las empresas de los mercados públicos. Utilizando una muestra de 8.266 adquisiciones de firmas de capital privado en 76 países entre 2000 y 2004, encontraron que después de aprobada la mencionada Ley, se hizo más probable para las pequeñas empresas públicas de los Estados Unidos, vender a compradores de capital privado que las pequeñas firmas similares en otros lugares.

No todos los académicos se oponen a la Ley *Sarbanes-Oxley*. (COSO IC-IF, 2013), (Dyck, Morse, & Zingales, 2010), sostiene que fue un triunfo de las relaciones públicas, el haber restaurado rápidamente la confianza de los sistemas financieros y realiza una contrastación con lo ocurrido en su país donde transcurrieron dos años de peleas y discusiones, después del escándalo de Parmalat, para hacerlo.

Otorgarle al comité de auditoría independiente y no al jefe la responsabilidad de contratación del auditor, también fue un acierto, según (Dyck, Morse, & Zingales, 2010). En esta investigación se examinaron 230 presuntos fraudes corporativos en América durante 1996-2004 encontrando que, previa a la implantación de la Ley *Sarbanes-Oxley*, sólo un tercio de los grandes fraudes corporativos fueron descubiertos por quienes tienen la responsabilidad de hacerlo, es decir, como auditores, reguladores de la industria o de la SEC.

Por otro lado, los autores (Minerva, 2015) plantean lineamientos de control interno para la prevención del riesgo de fraude en la empresa, basados en los elementos claves de la sección 302, contemplada en la Ley *Sarbanes-Oxley*. Para esto desarrollan objetivos específicos para diagnosticar la situación contable actual de la empresa en cuanto a la sección 302, identificar las bases legales de la Ley con respecto a las exigencias de control interno que imponen los procesos e información contable de la empresa, describir el control interno implementado en la empresa para la información contable basado en la Ley, analizar las ventajas y desventajas de la aplicación la Ley en la prevención del riesgo del fraude de la empresa y, finalmente diseñar lineamientos de control interno para la disminución del riesgo de fraude en la empresa.

(Jaramillo & Campuzano, 2008) afirman que el impacto de ésta Ley sobre las organizaciones ha sido grande, a todas sus áreas y resaltan el impacto sobre el área de TI, su seguridad y cada uno de los aspectos detallados de los sistemas de información de la organización y de la infraestructura que la soporta. Aunque la Ley no hace una mención directa al área de TI, concluyen que el impacto de la Ley *Sarbanes-Oxley* dentro de la infraestructura de TI y en general en todos los procesos de TI, ha sido muy importante dado que el cumplimiento de la Ley *Sarbanes-Oxley* depende principalmente de unos sistemas de TI confiables y seguros.

(Raudales, 2011), resalta que los controles financieros son posibles si se cuentan con controles internos diseñados adecuadamente para gestionar los riesgos y que estén operando de forma constante y eficiente. Para lograr esto existen marcos de trabajo aceptados a nivel mundial como *COSO*.

Por tal motivo, el presente trabajo resalta la importancia de la Ley *Sarbanes-Oxley* y contribuye en su cumplimiento, mediante una propuesta basada en las buenas prácticas en TI. Como se ha mencionado anteriormente, el marco de control interno sugerido por el documento *COSO IC–IF* no aborda el tema de los controles de tecnología informática en detalle; y a esto se le suma que PCAOB *Auditing Standard No. 2*, resalta la importancia de los controles de TI, pero no especifica de forma particular, qué debe ser incluido. En conclusión las organizaciones no cuentan con una guía clara para la implementación de estos controles en TI.

---

11. Conclusiones

El impacto de la Ley *Sarbanes-Oxley* dentro de los procesos de TI es importante dado que, muy a pesar de que la Ley no hace una mención directa al área de TI, su cumplimiento depende principalmente de unos sistemas de TI confiables y seguros. Por tal motivo en el presente trabajo se enfatiza en la forma promover la confiabilidad en la información financiera, mediante

controles rigurosos en los sistemas financieros y la infraestructura tecnológica que la soporta.

Con la integración de *COBIT* y *COSO* se desarrolló un modelo de auditoría, que permitió determinar, cuáles son los controles y aspectos de TI que se están aplicando dentro de la organización, determinando el nivel de madurez de la empresa en el área de TI con el objetivo de dar cumplimiento a la Ley *Sarbanes-Oxley*. Se realizó una alineación de los procesos de *COBIT* con los 17 principios de cada uno de los componentes de *COSO*. Además, se propuso como evaluar el cumplimiento de los requisitos de Ley *Sarbanes-Oxley* desde una perspectiva de TI, por cada ámbito de gobierno, y teniendo en cuenta los procesos de *COBIT 5*; esto a través de unas preguntas formuladas para el auditor. Finalmente se presenta un guía para el desarrollo de pruebas que tienen como fin validar el cumplimiento de la Ley *Sarbanes-Oxley*, relacionando los procesos de TI que aplican, y proponiendo buenas prácticas para implementar el control.

Como futuro trabajo se propone la implementación de las guías propuestas dentro de una organización y la evaluación de los resultados; esto con el fin de identificar una metodología de implementación basada en las guías y retroalimentar la presente propuesta.

Referencias

Gutiérrez, H. (Diciembre de 2004). *Sarbanes-Oxley, estableciendo nuevas reglas.* (A. y. CV., Productor) Recuperado el 18 de Noviembre de 2016, de Boletín ASI Noticias.: http://www.auditoria.com.mx/not/boletin/2004/0412.htm

COSO. (Noviembre de 2016). *Committee Of Sponsoring Organizations of the treadway commission.* Recuperado el 18 de Noviembre de 2016, de Welcome to COSO: http://www.coso.org/

SEC. (30 de July de 2002). *Public Law 107-204.* Recuperado el 18 de November de 2016, de Sarbanes-Oxley Act of 2002.: https://www.sec.gov/about/laws/soa2002.pdf

PCAOB. (18 de Noviembre de 2016). *pcaobus.org*. (P. C. Board, Productor) Recuperado el 18 de Noviembre de 2016, de https://pcaobus.org/Pages/default.aspx

Cano, M., & Lugo, D. (2016). *Nueva Ley frente a los fraudes contables (Ley Sarbanes-Oxley, Julio-30, 2002)*. (U. S. Affairs, Productor) Recuperado el 18 de Noviembre de 2016, de interamerican-usa.com: http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm

COSO IC-IF. (Mayo de 2013). *coso.org.* Recuperado el 18 de Noviembre de 2016, de Internal Control - Integrated Framework (Executive Summary): http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

IT Governance Institute. (30 de Abril de 2006). *thelia.org.* Recuperado el 18 de Noviembre de 2016, de IT Control Objectives for Sarbanes-Oxley, 2nd edition: http://www.theiia.org/chapters/pubdocs/135/ITGI_Spreadsheet.pdf

PCAOB. (17 de Junio de 2004). *pcaobus.org.* Recuperado el 18 de Noviembre de 2016, de Auditing Standard 2: https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2.aspx

ISACA. (Noviembre de 2016). *isaca.org*. (ISACA, Productor) Recuperado el 18 de Noviembre de 2016, de ISACA trust in, and value from, information systems: https://www.isaca.org/Pages/default.aspx

ISACA-ITGI. (2016). *isaca.org/ITGI*. (I. G. Institute, Productor) Recuperado el 18 de Noviembre de 2016, de IT Governance Institute: http://www.isaca.org/ITGI/Pages/default.aspx

ISACA-COBIT 5. (2012). *isaca.org/cobit.* Recuperado el 18 de Noviembre de 2016, de A Business Framework for the Governance and Management of Enterprise IT: http://www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf

Muñoz, R., & Martinez, M. (17 de Diciembre de 2012). Caracterización de Procesos de Gestión de TI basados en COBIT 5 y mapeo con ISO27002, ITIL, CMMI DEV, PMBOK, para la implementación en la industria Editorial Colombiana, apoyando el proceso de transformación

digital. *Monografía de Maestría en Gestión de Informática y Telecomunicaciones*, 55. (U. ICESI, Ed.) Santiago de Cali, Valle del cauca, Colombia: Biblioteca digital Universidad ICESI.

Chan, S. (1 de Octubre de 2004). Mapping COSO and CobiT for Sarbanes-Oxley Compliance. *IT Audit Magazine, 7*.

Salinas, J. (19 de Noviembre de 2014). *elempresario.mx*. (elempresario.mx, Productor) Recuperado el 18 de Noviembre de 2016, de Control Interno y uso de TI en las organizaciones: http://elempresario.mx/auditoria/control-interno-uso-ti-organizaciones

Bargeron, L., Kenneth, L., & Chad, Z. (Febrero de 2010). Sarbanes-Oxley and corporate risk-taking . *Journal of Accounting and Economics, 49*(1-2), 34-52.

Litvak, K. (2007). Sarbanes-Oxley and the Cross-Listing Premium. En T. M. Association (Ed.), *The Louis & Myrtle Moskowitz Conference on the Impact of Sarbanes-Oxley on Doing Business. 105*, págs. 1857-1898. Michigan Law Review.

Kamar, E., Karaca-Mandic, P., & Talley, E. (12 de Mayo de 2006). Going-Private Decisions and the Sarbanes-Oxley Act of 2002: A Cross-Country Analysis. *Social Science Research Network (SSRN)*.

Dyck, A., Morse, A., & Zingales, L. (9 de Noviembre de 2010). Who Blows the Whistle on Corporate Fraud? *The journal of finance, 65*(6), 2213-2253.

Minerva, I. (Junio de 2015). Lineamientos de control interno para la prevención del riesgo de fraude en la empresa Pastas Sindoni, C.A. basados en la sección 302 contemplada en la ley Sarbanes_Oxley. *Trabajo de Grado para optar al título de Magister en Ciencias Contables*, 125. La Morita, Carabobo, Venezuela: Universidad de Carabobo.

Jaramillo, J., & Campuzano, S. (2008). *repository.eafit.edu.co.* (U. EAFIT, Ed.) Recuperado el 18 de Noviembre de 2016, de Impacto de la Ley Sarbanes-Oxley a la seguridad de los sistemas de TI: https://repository.eafit.edu.co/handle/10784/2740#.WC-xoKLhBPU

Raudales, C. (2011). *academia.edu.* Recuperado el 18 de Noviembre de 2016, de Control de la gestión de las Tecnologías de la Información para el control financiero basado en estándares internacionales: https://www.academia.edu/6382367/Ensayo_Carlos_Raudales

---

1. Docente Tiempo Completo, Programa de Contaduría Pública, Universidad de la Costa – CUC, Colombia. E-mail: vmontano@cuc.edu.co

2. Docente Tiempo Completo, Programa de Ingeniería de Sistemas, Universidad de la Costa – CUC, Colombia. Email: hcombita@cuc.edu.co

3. Investigador Asociado, Programa de Ingeniería de Sistemas, Universidad de la Costa – CUC, Colombia. Email: edelahoz@cuc.edu.co

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 38 (Nº 23) Año 2017

[Índice]