ANÁLISIS DE LA LEY SOX Y DEFINICIÓN DE ESTRATEGIAS PARA LA IMPLEMENTACIÓN Y EL CUMPLIMIENTO DE LOS REQUERIMIENTOS TECNOLÓGICOS PARA LAS COMPAÑÍAS EMISORAS DE VALORES.

Yiseth Eliana Ariza Mateus

Universidad Ean

Facultad de Ingeniería

Maestría en Gerencias de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

10/septiembre/2022

ANÁLISIS Y ESTRATEGIAS DE LA LEY SOX APLICADAS A LAS EMISORAS DE VALORES Y SUS EFECTOS EN LOS AMBIENTES DE CONTROL INTERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Yiseth Eliana Ariza Mateus

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de Sistemas de Información y Proyectos tecnológicos

Director (a):

Dra. Marisol Martínez de la Peña

Modalidad:

Monografía

Universidad Ean

Facultad de Ingeniería

Maestría en Gerencias de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

10/septiembre/2022

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

Dedicatoria

A mi esposo y a mi hijo por acompañarme durante este recorrido y por ser la fuerza que me mantuvo en pie hasta lograr el objetivo. Los amo.

Agradecimientos

Culminar este programa de maestría es comprobar que la constancia, el esfuerzo, el trabajo duro y la convicción de tener un propósito claro son la fórmula ideal para llegar hasta el final y lograr el objetivo.

Gracias a Dios por mantenerme con la fe intacta y darme las fuerzas necesarias para no renunciar en el camino.

Gracias a la universidad EAN por poner este programa a disposición de los estudiantes que buscamos traspasar fronteras de conocimiento y poner a prueba nuestra fuerza interior y nuestros límites.

Gracias a mi mentora Gloria Bravo por ser una valiosa guía antes de iniciar este proceso, su sabio consejo y sus acertados análisis sobre el futuro me permitieron decidir adecuadamente sobre el camino educativo a elegir.

Gracias a cada uno de los docentes por compartir sus conocimientos, por permitirme aprender, por el acompañamiento y la exigencia; al director de la maestría, ingeniero Alexander García por creer desde el principio en mi idea y orientarme con el fin de hacerla posible, gracias al profesor Jhon Aguirre por sus aportes clave en el momento oportuno.

Gracias a *PayU* por ser la fuente inagotable de recursos para aterrizar este proyecto y a mi líder Margarita Chedraui por su apoyo incondicional.

Gracias infinitas e inconmensurables a mi esposo y a mi hijo; su paciencia, su amor infinito, sus palabras de aliento cuando todo parecía imposible fueron clave para cumplir este objetivo. Gracias por permitirme robarles nuestro tiempo en familia, jamás lo habría logrado sin ustedes.

Resumen

La presente monografía busca identificar los requerimientos tecnológicos para dar cumplimiento a la ley SOX en las empresas emisoras de valores en EE. UU. y definir estrategias que permitan su correcta implementación tomando como base el marco de referencia COBIT 2019.

El trabajo inicia con el análisis general de la Ley SOX y la identificación de los requerimientos tecnológicos de esta; una vez conocidos los requerimientos y teniendo en cuenta que el marco COBIT 2019 es utilizado para la administración de la tecnología, se valida cuáles de sus dominios pueden ser tomados como referencia para cumplir con las exigencias tecnológicas al implementar la ley SOX.

Adicionalmente se elabora un instrumento de evaluación basado en los dominios del marco COBIT para obtener el nivel de madurez tecnológica (ELC, ITGC, controles automáticos) de las empresas con respecto al cumplimiento a los exigido por la ley.

Finalmente, se establecen las estrategias que permitirán la adecuada. implementación y el cumplimiento de los requerimientos tecnológicos de la ley SOX basado en el marco de referencia COBIT 2019.

Palabras clave: SOX, COBIT 2019, Control Interno, *ITGC, ELC*, ISACA, PCAOB

Abstract

The purpose of this paper is to identify the technological requirements of the SOX law that companies issuing shares on the U.S. stock exchange must comply with to establish strategies to comply with the requirements based on the COBIT 2019 framework.

The work begins with a general analysis of the SOX Act and the identification of its technological requirements; once the requirements are known and considering that the COBIT 2019 framework is used for technology management, it is validated which of its domains can be taken as a reference to comply with the technological requirements when implementing the SOX Act.

In addition, an evaluation instrument based on the domains of the COBIT framework is developed to obtain the level of technological maturity (ELC, ITGC, automatic controls) of the companies with respect to compliance with the requirements of the law.

Finally, strategies are established that will enable the proper implementation and compliance with the technological requirements of the SOX law based on the COBIT 2019 framework.

Key words: SOX, COBIT 2019, Internal Control, ITGC, ELC, ISACA, SEC, PCAOB

Contenido

Pág.

Lista de Ilustraciones

Pág.

Lista de Tablas

Pág.

1. Introducción

En el año 2002, a tan solo una década de haber empezado el recorrido por el aun inexplorado mundo de los sistemas de información, cuando apenas unos años atrás se había dado el estreno del *Windows* 95, así como del primer estándar formal de *HTML* y se lanzaba al mercado el primer *IPOD*, estalla uno de los escándalos financieros más sonados en toda la historia de los Estados Unidos y talvez del mundo, al descubrirse los millonarios fraudes financieros por prácticas irregulares de contabilidad realizados entre empresas emisoras de valores supuestamente sólidas como *ENRON, TYCO y Worldcom* en complicidad con sus firmas de auditoría.

Este escándalo lleva a la quiebra a pequeños, medianos y grandes inversionistas quienes basados en los excelentes resultados financieros que mostraban las empresas decidieron comprar sus acciones sin imaginar que sus números era el resultado de cifras arregladas; esta situación erosionó por completo como el público percibía el mercado y socavo la confianza en el gobierno, y de las agencias encargadas de supervisar el mercado (Kecskés, 2017).

Con base en lo anterior se hizo imperativo establecer acciones que permitieran revisar con lupa cada una de las cifras que las empresas emisoras de valores reportaban en sus estados financieros; por lo que el Congreso de los Estados Unidos decide crear la Ley SOX y empezar a realizar una vigilancia más contundente no solo a las empresas si no a las firmas de auditoría.

A partir de ese momento los requisitos para poder ingresar, así como para permanecer en la Bolsa de Valores de Estados Unidos se convirtieron en verdaderos retos para las empresas, las cuales debían cumplir con un sinfín de exigencias para la gestión del control interno, que en la mayoría de los casos solo se lograban con grandes

inversiones de tiempo y dinero y sin la certeza que lo implementado pudiera dar repuesta a lo requerido por la Ley.

La implementación de la ley cambia de manera radical la manera en la que las empresas deben gestionar sus marcos de control interno desde la perspectiva financiera y tecnológica, la mayoría de las empresas se enfocan en atender la parte financiera para dar cumplimiento a la normativa, dejando a un lado o dando menor importancia a uno de los retos más grandes que deben afrontar y es la forma en la que SOX afecta la administración de los sistemas informáticos relacionados con la información financiera.

Lo anterior se sustenta basado en que, en la mayoría de las empresas los procesos de información financiera son impulsados por los sistemas de tecnología de la información (Damianides, 2004) por lo que todos los sistemas de TI involucrados en la información financiera y otros procesos que la afectan deben ser evaluados, documentados y probados (Damianides, 2004, pág. 1), por lo que deben desarrollar infraestructuras de TI más rentables para cumplir con los requisitos de la SOX. (Sarctoni, 2005).

Es en este punto donde el objetivo de esta investigación surge como protagonista e invita a cuestionar sobre cuales deben ser las estrategias desde la perspectiva tecnológica que las empresas cuyo objetivo es ingresar a la bolsa de valores de Estado Unidos deben implementar para cumplir con los requerimientos de la ley para realizar procesos de implementación efectivos y eficientes.

En primer lugar y ante el gran desafío de la ley SOX desde la perspectiva tecnológica se plantea como primera estrategia conocer a profundidad los requerimientos que plantea la normativa para la administración de TI, es la única manera de entender el alcance y el impacto que su implementación puede tener en el negocio.

En segundo lugar, se expone la forma en la que empresas pueden atender los mencionados requerimientos basadas en marcos de referencia para la gobernabilidad de las TI como COBIT cuya definición y dominios les permite administrar los sistemas de información y desarrollar el proyecto tecnológico de manera efectiva.

Una vez conocidos los requerimientos y la forma en las que es posible darle cumplimiento, se plantea como tercer paso evaluar el estado actual de la gobernabilidad de TI y su ambiente de control basado en lo planteado por el Marco de Referencia COBIT 2019 (ISACA, 2019).

Finalmente, se plantean las estrategias y la hoja de ruta que se recomienda a las empresas seguir para que se cumpla con lo exigido por la ley una vez esta se ha implementado, pero sobre todo para mantener un estado de mejora continua que sostenga el proceso con el paso del tiempo de manera eficiente y efectiva.

2. Formulación del problema de investigación

Las empresas que tienen como objetivo ingresar al mercado bursátil en la Bolsa de Valores de EE. UU. deben implementar Sistemas de Control Interno robustos que permitan dar cumplimiento a las drásticas y rigurosas exigencias de la Ley SOX que comprometen los resultados en los mercados bursátiles,

La Ley SOX *(Sarbanes Oxley)* tiene un alcance global en las empresas, que abarca desde la alta gerencia, pasando por los procesos *core,* con alto impacto en las administración y control de la tecnología, así como las transacciones financieras.

Cuando las empresas deciden implementar la Ley SOX no son conscientes de los requerimientos y los cambios a nivel empresarial que esta implica ya que consideran que esta solo afecta a las áreas financieras, desconociendo por completo el gigantesco alcance que se tiene en la administración de las tecnologías de la información, por lo que inician procesos de implementación que terminan convirtiéndose en costosos reprocesos y evaluaciones negativas para las compañías emisoras.

El anterior análisis para la formulación del problema lleva a plantear la siguiente pregunta de investigación:

Pregunta de investigación:

¿Cuáles deben ser las estrategias que las empresas cuyo objetivo es ingresar a la bolsa de valores de Estado Unidos deben implementar para cumplir con los requerimientos tecnológicos de la ley para tener procesos de implementación efectivos y eficientes?

3. Objetivos

3.1 Objetivo general

Formular estrategias que le permitan a las compañías emisoras de valores que buscan cotizar en bolsa de Estados Unidos asegurar el cumplimiento de los requerimientos tecnológicos de la Ley SOX basado en el marco de referencia COBIT 2019 *(Control Objectives for Information and related Technology).*

3.2 Objetivos específicos

- Analizar la Ley SOX y los requerimientos a cumplir en materia de control para la gestión de TI.
- Identificar los dominios del marco COBIT que pueden ser tomados como referencia para cumplir con los requerimientos tecnológicos al implementar la ley SOX
- Evaluar el nivel de madurez en la que se encuentra el entorno tecnológico de las empresas para cumplir con los requerimientos de la ley SOX.
- Establecer estrategias para fortalecer el sistema de gestión de TI teniendo como marco de referencia COBIT con el fin de garantizar el adecuado cumplimiento de los requerimientos tecnológicos de la ley SOX en compañías emisoras de valores.

4. Justificación

Los procesos de información financiera dependen cada vez más de los sistemas informáticos, dichos sistemas, ya sean de planificación de recursos empresariales (ERP), por ejemplo, SAP®, Oracle® *Financials y Workday*®, o de otro tipo, están profundamente integrados en el inicio, la autorización, el registro, el procesamiento y la presentación de informes de las transacciones financieras, por lo tanto, los sistemas informáticos están inextricablemente ligados al proceso global de información financiera y deben ser evaluados, junto con otros procesos importantes, para el cumplimiento de las disposiciones del control interno de la información financiera *(ICFR -Internal Control Over Financial Reporting*) de la Ley Sarbanes-Oxley. (ISACA, 2014)

Después de más de dos décadas de auditorías de la SOX, el enfoque de las empresas se ha desplazado más hacia la gestión del riesgo y la garantía de un mejor valor de sus inversiones, incluyendo la aplicación de los controles de la ley SOX. Por ejemplo, muchas empresas se han beneficiado de la implantación racionalizando sus plataformas y arquitecturas de aplicaciones e infraestructuras informáticas. (ISACA, 2019)

El hecho de que el cumplimiento de la ley SOX se vea como un proyecto más, o como una oportunidad estratégica para que el departamento de TI reduzca el número de proyectos pendientes, vendrá determinado por la forma en que el director financiero, el director de información o el director de TI posicionen el cumplimiento de la ley SOX ante la dirección (Lahti, 2005).

Tomando como base que un gran porcentaje de las empresas asocian el cumplimiento de la SOX como una iniciativa de finanzas y pueden no involucrar a TI, o limitar la

participación de TI o limitar la participación de TI a la periferia del proyecto, esto puede ser más fácil de decir que de hacer (Lahti, 2005).

Debido a esta percepción "limitada" del cumplimiento de SOX, el proceso de posicionamiento con la dirección ejecutiva para incluir a TI en esta iniciativa puede requerir un esfuerzo significativo (Lahti, 2005).

El cumplimiento de la ley Sarbanes-Oxley tendrá un impacto significativo en la organización de TI de la mayoría de las empresas públicas, sin embargo, hay un enorme problema: no hay una mención específica a la TI en la Sección 404 y, lo que es más importante, no hay detalles sobre la organización de TI deben establecerse dentro de una organización de TI para cumplir con la legislación de Sarbanes-Oxley.

Si no hay una mención específica en la Sección 404 sobre lo que la TI debe hacer para cumplir con la ley Sarbanes-Oxley, la pregunta lógica sería: ¿Cómo puedo cumplir con algo sin saber lo que tengo que hacer para cumplir?

Aunque las directrices de COBIT existen desde 1996, sus direccionamientos y mejores prácticas se han convertido casi en la norma de facto para los auditores y el cumplimiento de la SOX.

5. Marco Teórico

Los requerimientos de IT para el cumplimiento de la ley SOX han sido objeto de estudio debido a la relevancia que estos tienen para el logro de su implementación. El marco teórico contempla desde el marco legal las principales leyes que regulan la implementación de la ley tales como la Circular básica jurídica 029 de 2014 que indica las principales normas de control interno para la gestión de la tecnología.

De igual forma se relaciona el marco conceptual donde se listan los principales temas que deben ser conocidos para entender el contexto de la ley, en este apartado el principal insumo para el desarrollo de la monografía son La ley SOX, el marco de referencia COBIT 2019 así como la guía de los Objetivos de control de TI para Sarbanes-Oxley estos dos últimos generados por ISACA.

Por último, dentro se relacionan algunos estudios que se han hecho para analizar como la implementación de SOX ha cambiado la manera de administrar el ambiente de TI, dentro de los cuales uno de los que más se asocia al desarrollo de la monografía el estudio de cómo SOX ha cambiado la administración de las tecnologías de la información en las empresas y el estudio de BASDA (Asociación de Desarrolladores de Software de Aplicaciones Empresariales) sobre las Implicaciones tecnológicas de la ley Sarbanes-Oxley.

5.1 Marco Legal

5.1.1 Estándar de auditoria No. 5 de la PCAOB (AS No. 5)

“Esta norma establece los requisitos y proporciona la dirección que se aplica cuando un auditor es contratado para realizar una auditoría de la evaluación de la dirección de la eficacia del control interno sobre la información financiera ("la auditoría del control interno sobre la información financiera") que se integra con una auditoría de los estados financieros” (PCAOB, 2016).

El estándar No. 5 contempla los siguientes puntos: (PCAOB, 2016)

- Integración de las auditorías
- Planeación de las auditorías
- Papel de evaluación de riesgos
- Escalamiento de la auditoría
- Como abordar el riesgo de fraude
- Utilización del trabajo de otros
- Identificación de los controles a nivel de la entidad
- Materialidad
- Utilización de un enfoque descendente
- Identificación de las cuentas y revelaciones significativas y sus afirmaciones relevantes
- Comprensión de las fuentes probables de declaraciones erróneas
- Selección de los controles a probar
- Evaluación de controles
- Relación del riesgo con las pruebas a obtener
- Consideraciones especiales para las auditorías de años posteriores
- Evaluación de las deficiencias identificadas
- Indicadores de debilidades materiales

En conclusión, la norma indica que “el auditor debe formarse una opinión sobre la eficacia del control interno sobre la información financiera mediante la evaluación de las pruebas obtenidas de todas las fuentes, incluidas las pruebas de control realizadas por el auditor, los errores detectados durante la auditoría de los estados financieros y cualquier deficiencia de control identificada” (PCAOB, 2016).

5.1.2 Circular básica jurídica 029 de 2014

La circular básica jurídica 029 de 2014 “contempla los pronunciamientos jurisprudenciales vigentes en materia financiera, aseguradora y del mercado de valores” (Colombia, Superintendencia financiera de, 2009).

La Circular Básica Jurídica está dividida en tres Partes:

“PARTE I. Instrucciones generales aplicables a las entidades vigiladas; que contiene las disposiciones aplicables de forma transversal a todas las entidades vigiladas por esta Superintendencia“ (Superintendencia Financiera de Colombia, 2014).

“PARTE II. Mercado intermediado; que contiene las instrucciones que regulan de forma particular los establecimientos de crédito; las sociedades de servicios financieros; las sociedades capitalizadoras; las entidades aseguradoras, reaseguradoras y sus corredores; así como las otras instituciones o actividades sometidas a la supervisión de esta Superintendencia” (Superintendencia Financiera de Colombia, 2014).

“PARTE III. Mercado des intermediado; que contiene las instrucciones aplicables a los emisores de valores; a las entidades y actividades del mercado de valores; así como lo relacionado con el Sistema Integral de Información del Mercado de Valores (SIMEV) y con los Fondos de Inversión Colectiva (FIC´s)” (Superintendencia Financiera de Colombia, 2014).

Si bien es cierto el caso particular para el tema de estudio, se abarca en la parte III se revisa también la parte I que contempla un capítulo específico sobre control interno y más aún sobre las normas de control interno para la gestión de la tecnología, el cual se detalla a continuación.

Título 1 – Aspectos Generales

Capítulo IV. Sistema de control interno.

Normas de control interno para la gestión de la tecnología.

Hoy por hoy, la tecnología se ha convertido en una parte fundamental para la consecución de los objetivos así como para la entrega de la promesa de valor de las empresas a todos los usuarios finales, de manera segura, con calidad y cumplimiento, de esta forma, se hace imperativo trabajar para que el diseño del sistema de control interno para administrar la tecnología de respuesta a las políticas, requerimientos y expectativas de las compañías, así como a los requerimientos normativos referentes al tema (Superintendencia Financiera de Colombia, 2014).

Todas las compañías están llamadas a crear, desarrollar, documentar y socializar políticas para la administración de la tecnología; así como para los recursos, procesos, procedimientos, metodologías y controles requeridos para asegurar su cumplimiento (Superintendencia Financiera de Colombia, 2014).

Este capítulo enlista de manera específica aquellos aspectos por verificar para realizar una correcta gestión de la tecnología, los cuales se alinean por completo con los requerimientos de la ley SOX:

- ✓ Plan estratégico de tecnología
- ✓ Infraestructura de tecnología
- ✓ Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico
- ✓ Administración de proyectos de sistemas
- ✓ Administración de la calidad
- ✓ Adquisición de tecnología
- ✓ Adquisición y mantenimiento de software de aplicación
- ✓ Instalación y acreditación de sistemas
- ✓ Administración de cambios
- ✓ Administración de servicios con terceros

- ✓ Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica
- ✓ Continuidad del negocio
- ✓ Seguridad de los sistemas
- ✓ Educación y entrenamiento de usuarios
- ✓ Administración de los datos
- ✓ Administración de instalaciones
- ✓ Administración de operaciones de tecnología
- ✓ Documentación (Superintendencia Financiera de Colombia, 2014).

La circular sustenta el caso de estudio basado en su estructura que define como la superintendencia financiera regula las empresas que cotizan en la bolsa de valores y todos aquellos requisitos que se deben cumplir para entrar y para permanecer en el mercado bursátil.

5.1.3 Circular 014 de 2009 - Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI).

La Ley SOX basa su razón de ser en la necesidad imperante de tener un sistema de control interno determinado y supervisado, por lo que es importantes que las entidades supervisadas le den relevancia al robustecimiento de los ambientes de control interno, así como a la evaluación constante de su eficacia y efectividad (Colombia, Superintendencia financiera de, 2009)

Con base en lo anterior la circular 014 de 2009, considera importante que estas definan, establezcan y conserven un Sistema de Control Interno el cual debe contribuir en la consecución de sus objetivos y en el fortalecimiento de la correcta administración de los riesgos a los que se encuentran expuestas al ejecutar su actividad principal, llevándolas a cabo de manera segura, transparente y eficiente (Colombia, Superintendencia financiera de, 2009).

Basado en lo anterior, la circular permite establecer un marco conceptual y normativo para el sistema de control interno como parte indispensable del gobierno corporativo de empresas sujetas de supervisión basado en modelos suficientemente avalados a nivel internacional (Sección 404 de la ley SOX) que contemplan en detalle la generalidad, el contenido y el alcance del sistema de control interno, con los siguientes objetivos: (Colombia, Superintendencia financiera de, 2009).

1. Incrementar la cantidad de operaciones eficientes y eficaces de las entidades supervisadas (Colombia, Superintendencia financiera de, 2009)
2. Evitar y mitigar fraudes, ya sea dentro o fuera de la empresa (Colombia, Superintendencia financiera de, 2009).
3. Guiar a los líderes de las empresas supervisadas sobre los deberes que están llamados a cumplir basado en la normatividad vigente, especificando la responsabilidad sobre control interno por parte de los diferentes órganos sociales (Colombia, Superintendencia financiera de, 2009).
4. Incentivar tanto la autorregulación como el autocontrol, considerando, sin obviar la responsabilidad innata de los directivos, todos los colaboradores de la empresa están llamados a evaluar y controlar el trabajo que cada uno ejecuta (Colombia, Superintendencia financiera de, 2009).

Para la implementación de la Ley SOX, esta circular es fundamental teniendo en cuenta que define e indica los lineamientos, así como los plazos para el establecimiento de un sistema de control interno, considerando que un sistema eficiente de control interno resulta fundamental.

1. Definición o adaptación de los componentes mínimos para establecer una estructura de control interno adecuada (Colombia, Superintendencia financiera de, 2009).

2. Definición o adaptación de los sistemas de información y comunicación para lograr un nivel de seguridad considerable relacionada con la exactitud, validez y oportunidad de la información generada por la empresa (Colombia, Superintendencia financiera de, 2009).
3. Definición o adaptación del sistema para la gestión de riesgos (Colombia, Superintendencia financiera de, 2009).
4. Adecuación de la composición y funcionamiento de los órganos de administración y control. (Colombia, Superintendencia financiera de, 2009)
5. Definición o adaptación de las actividades de control (Colombia, Superintendencia financiera de, 2009).
6. Definición o adaptación de los controles que lleven a la gerencia, así como a los líderes de cada proceso a realizar constantemente el monitoreo al funcionamiento del sistema de control interno y a implementar las mejoras que sean requeridas (Colombia, Superintendencia financiera de, 2009).
7. Llevar a cabo una evaluación independiente referente a la efectividad del sistema de control interno (Colombia, Superintendencia financiera de, 2009).

5.1.4 Ley Sarbanes-Oxley del 2002

Desde la perspectiva legal, la Ley SOX se reglamenta por 11 secciones las cuales a su vez están subdivididas en artículos que definen, los cuales se relacionan a continuación.

La sección 1, hace referencia al establecimiento del Consejo de supervisión de la contabilidad de las empresas públicas, cuyo objetivo es monitorear la auditoría de las empresas que deben ajustarse a las reglamentaciones del mercado de valores, y temas asociados, para así velar por los intereses de los inversionistas y fomentar el interés

público en la elaboración de reportes de auditoría informativos, precisos e independientes.

Tabla 1. Relación de los artículos que componen las secciones de la Ley SOX

SECCION 1	**9 artículos**	**Consejo de supervisión de la contabilidad de las empresas públicas.**
		Establecimiento del consejo para para supervisar la auditoría de las empresas que están sujetas a las leyes de valores, y asuntos relacionados, con el fin de proteger los intereses de los inversores y promover el interés público interés público en la preparación de informes de auditoría informativos, precisos e independientes.
SECCION 2	**9 artículos**	**Independencia del auditor**
		La Junta podrá, caso por caso, eximir a cualquier persona, emisor, empresa de contabilidad pública o transacción de la prohibición de prestar servicios bajo la Ley de Intercambio de Valores de 1934, en la medida en que dicha exención sea necesaria o adecuada para el interés público y sea coherente con la protección de los inversores.
SECCION 3	**8 artículos**	**Responsabilidad corporativa**
		Se exige que se presenten informes periódicos firmados por el director ejecutivo y el director financiero
SECCION 4	**9 artículos**	**Información financiera mejorada**
		Garantizar que toda la información financiera sea presentada de acuerdo con las normas establecidas
SECCION 5	**1 artículo**	**Análisis de conflicto de intereses**
		Tratamiento de los analistas de valores por parte de las asociaciones de valores registradas.
SECCION 6	**4 artículos**	**Recursos y autoridad de la comisión**
		Administración de los recursos, así como de las competencias de la comisión
SECCION 7	**5 artículos**	**Estudios e informes**
		Presentación de la información financiera incluyendo la contabilidad interna, información crediticia, infracciones, bancos de inversiones
SECCION 8	**6 artículos**	**Responsabilidad de fraude empresarial y penal**
		Responsabilidad y administración sobre eventos de fraude
SECCION 9	**6 artículos**	**Aumento de las penas por delitos de cuello blanco**
		Responsabilidad y administración por delitos de cuello blanco
SECCION 10	**1 artículo**	**Declaraciones de impuestos de las empresas**
		Responsabilidad de los directores sobre los impuestos
SECCION 11	**7 artículos**	**Responsabilidad de fraude empresarial**
		Administración de las acciones y la responsabilidad que la empresa asume frente a eventos de fraude

Fuente: Elaboración propia basada en (Commission, 2002). Secciones que componen la ley SOX.

La sección 2, hace referencia a la importancia de la independencia del auditor, indicando que la Junta podrá, por cada caso, eximir a cualquier persona, emisor,

empresa de contabilidad pública o transacción de la prohibición de prestar servicios bajo la Ley de Intercambio de Valores de 1934, en la medida en que dicha exención sea necesaria o adecuada para el interés público y sea coherente con la protección de los inversores.

La sección 3, define la responsabilidad corporativa exigiendo que se presenten informes periódicos firmados por el director ejecutivo y el director financiero. La sección 4, exige que la información financiera presentada sea íntegra y mejorada, y que sea presentada de acuerdo con las normas establecidas. La sección 5, da alcance al manejo del conflicto de intereses, por su parte la sección 6 da los lineamientos sobre los recursos y autoridad de la comisión y como estos son administrados basados en sus competencias.

La sección 7, entrega los lineamientos para la presentación de estudios e informes, asegurando la presentación de la información financiera incluyendo la contabilidad interna, información crediticia, infracciones, bancos de inversiones. La sección 8, tiene como objetivo administrar todo los relacionado con la responsabilidad corporativa y la responsabilidad del fraude penal, para garantizar que exista responsabilidad y administración sobre eventos de fraude

La sección 9, contiene todo lo relacionado con el aumento de las penas por delitos de cuello blanco y la responsabilidad de la vigilancia y acciones de la administración al respecto. La sección 10, contempla la responsabilidad por parte de la administración en la presentación y declaración de impuestos. Finalmente, la sección 11, se enfoca en la responsabilidad específicamente del fraude penal.

5.2 Marco conceptual

5.2.1 LEY SOX (Sarbanes-Oxley)

En 2002, la exuberancia general que definía los mercados de capitales de finales de los 90 había desaparecido. El suceso de la burbuja de las puntocom y los escándalos

corporativos emergentes -*WorldCom, Adelphia, Tyco y Enron*- erosionaron por completo la confianza del público en el mercado y socavaron la confianza en el gobierno, y en las de las agencias encargadas de supervisar el mercado. (Kecskés, 2017)

Las razones de los escándalos empresariales fueron numerosas. En primer lugar, el enorme optimismo hizo que los inversores tuvieran un exceso de confianza, por lo que no actuaron con precaución en sus transacciones. Esto dio lugar a la burbuja de las puntocom, por ejemplo, un fenómeno desencadenado por el súbito interés en el sector de las tecnologías de la información y las perspectivas que prometía. Sin embargo, la exuberancia también se mezcló con la codicia empresarial. Los sistemas de remuneración recompensaban generosamente a los directores generales y otros miembros de la dirección. (Kecskés, 2017)

El cambio a una remuneración basada en los resultados y la entrega de acciones hizo que los directivos menos escrupulosos se interesaran más por los beneficios a corto plazo que por la sostenibilidad. (Kecskés, 2017)

Para empeorar las cosas, el 11 de septiembre de 2001, el ataque terrorista contra el *World Trade Center* creó un ambiente de incertidumbre y paranoia. Todo ello se reflejó en el comportamiento de los mercados bursátiles; el gobierno y el poder legislativo se dieron cuenta de que había que hacer algo para restablecer la confianza del público. (Kecskés, 2017)

Es así como, el presidente George W. Bush el 30 de julio de 2002, firmó la Ley Sarbanes-Oxley y anunció su programa de 10 puntos en el que se identificaban tres factores clave de la debacle empresarial: La falta de información fiable para los inversores, La falta de responsabilidad de los directivos de las empresas y El fracaso del sistema de auditoría. (Cohen, 2005).

La Ley Sarbanes - Oxley fue promulgada con el objetivo de establecer nuevos y mejorados estándares para la contabilidad corporativa, el gobierno corporativo y la generación de reportes financieros. (Cifuentes, 2006)

La ley SOX define los deberes del director general (CEO), del director financiero (CFO) y del auditor, incluyendo la responsabilidad personal de cada uno de ellos de garantizar la credibilidad de los informes financieros proporcionados a las partes interesadas.

Según (Morales, 2005) en esta ley se agrupan seis grandes áreas que intervienen en el desarrollo de los mercados financieros:

- Mejora de la calidad de la información pública y de sus detalles
- Reforzamiento de responsabilidades del gobierno corporativo de las sociedades.
- Mejora de las conductas y los comportamientos éticos exigibles: mayores exigencias de responsabilidad en los temas de gestión indebida de información confidencial.
- Aumento de la supervisión de las actuaciones en los mercados cotizados.
- Incremento del régimen sancionador asociado a incumplimientos.
- Aumento de exigencia y presión sobre la independencia efectiva de los auditores

La ley SOX cuenta con 11 sesiones que abarcan desde la supervisión a la contabilidad de las empresas, así como la independencia de las firmas auditoras, la responsabilidad empresarial, conflicto de intereses hasta llegar a los informes que surgen como resultado de la aplicación de la ley.

En la tabla 2, se presenta la estructura de la ley SOX con las 11 sesiones que la componen.

Tabla 2. Estructura de la Ley SOX

Sesión	Nombre
I	Junta de Supervisión de Firmas de Contabilidad Pública
II	Independencia de los Auditores.
III	Responsabilidad
IV	Revelaciones Financieras Mejoradas.
V	Conflicto de intereses de los Analistas
VI	Recursos y Autoridad de la Comisión.
VII	Estudios e Informes.
VIII	Responsabilidad Corporativa y Fraude Criminal: Fraude y Responsabilidad Corporativa.
IX	Mejoramiento de Sanciones por Crímenes de Cuello y Corbata.
X	Declaraciones de Impuestos Corporativos.
XI	*"Accountability"* de Fraudes Corporativos.

Fuente: Elaboración propia adaptado de (SEC, 2020)

5.2.2 COBIT

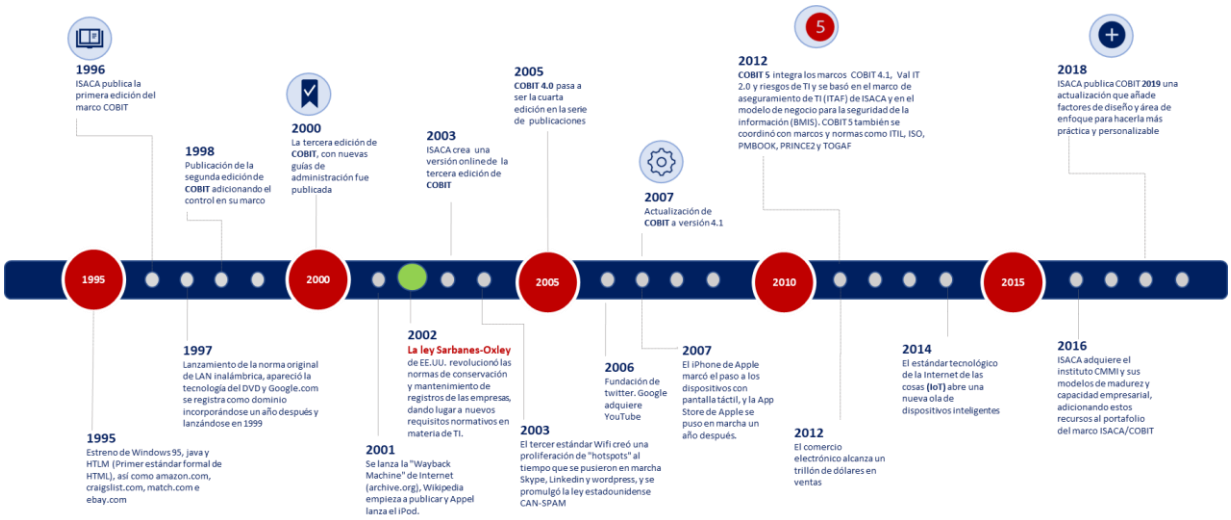
Concepto

COBIT *(Control Objectives for Information and Related Technologies)* es un marco utilizado en la gestión de TI (tecnologías de la información). Proporciona listas y descripciones de las mejores prácticas con las que los directivos y otros expertos pueden evaluar sus programas de TI y crear objetivos de mejora. COBIT también pretende ayudar a las organizaciones a crear, organizar y utilizar estrategias relacionadas con sus funciones y gestión de TI y a reducir los riesgos asociados al uso no moderado de las TI. (Dziak, 2019).

Hasta la fecha, el marco COBIT ha tenido 6 versiones desde su creación en 1996, las cuales han sido precedidas por diferentes sucesos, así como el nacimiento de nuevos riesgos como resultado de nuevas tecnologías, que evidencia la necesidad de incluir, modificar, eliminar o complementar la ruta establecida.

En la ilustración 1, se observa una línea de tiempo histórica del marco, así como los diferentes sucesos que se han presentado en materia tecnológica a largo de 26 años.

Ilustración 1. Línea de tiempo histórica del marco COBIT



Fuente: Elaboración propia basado en (ISACA, 2019)

Objetivo

El marco de referencia COBIT, contiene las buenas prácticas a través de un grupo de dominios y procesos, y mostrando las actividades en una estructura manejable y lógica. Todas las prácticas que contiene COBIT reflejan el consenso de los conocedores del tema; tienen un enfoque dirigido de manera rigurosa al control y un poco menos a la ejecución. (IT Governance Institute, 2007).

El éxito de las áreas de TI para cumplir los requerimientos de la empresa está en que la alta gerencia establezca un sistema de control interno o un marco de trabajo, por lo que COBIT ayuda al cumplimiento de estas necesidades como se relaciona a continuación:

- Generando una conexión con las exigencias del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado

- Listando y reconociendo los recursos de tecnología más relevantes a ser utilizados
- Estableciendo los controles de la alta gerencia que deben considerarse (IT Governance Institute, 2007).

La orientación hacia procesos que tiene COBIT se organiza en una estructura de procesos, que subdivide al área de tecnología en 40 procesos considerando las áreas de planear, construir, ejecutar y monitorear, mostrando una vista de las áreas de tecnología de punta a punta (IT Governance Institute, 2007)

COBIT soporta la gobernabilidad de las áreas de tecnología al ofrecer un modelo de trabajo que asegura lo siguiente:

- La alineación entre el área de tecnología y los objetivos de negocio
- TI habilita al negocio y maximiza los beneficios
- El uso adecuado y responsable de los recursos tecnológicos
- Gestión apropiada de los riesgos de tecnología (IT Governance Institute, 2007).

La ilustración 2, muestra como está estructurado el gobierno de TI en el marco COBIT.

Ilustración 2. Áreas de enfoque del gobierno de TI.

Fuente: (IT Governance Institute, 2007).

- Alineación estratégica. Su objetivo es asegurar la alienación entre los planes de negocio de TI, establecer, conservar y revisar el valor agregado de las áreas de tecnología; y alinear las operaciones de TI con las operaciones de la empresa (IT Governance Institute, 2007)
- Entrega de valor: Su objetivo es garantizar que las áreas de tecnología entreguen los beneficios definidos en la estrategia, encaminados en la optimización de costos y en la entrega del valor concreto de las áreas de tecnología (IT Governance Institute, 2007).
- Administración de Recursos: Se enfoca en óptima administración de los recursos críticos de tecnología incluidas aplicaciones, información, infraestructura y personas (IT Governance Institute, 2007).
- Administración de riesgos: La gobernabilidad de los riesgos está sujeta a la conciencia que sobre estos exista por parte de las directivas de la empresa, al adecuado conocimiento del apetito de riesgos que define la empresa, a la comprensión de las exigencias de cumplimiento, a la claridad de los riesgos más relevantes, así como a la identificación de las responsabilidades de la gestión de riesgos al interior de la compañía (IT Governance Institute, 2007)
- Medición del desempeño realiza un monitoreo al ciclo desarrollado desde su implementación hasta la finalización, validando el correcto uso de los recursos el comportamiento de los procesos y el servicio entregado (IT Governance Institute, 2007).

Con base en lo anterior el objetivo de COBIT es “investigar, elaborar, disponer y promover un marco de control de gobierno de TI autorizado, actualizado y aceptado internacionalmente, para la adopción, por parte de las empresas y el uso diario, por parte

de gerentes de negocio, profesionales de TI y profesionales de aseguramiento" (Muñoz, 2011; IT Governance Institute, 2007).

Estructura

Una de las bases de COBIT es la diferenciación realizada entre gobierno y gestión, siguiendo este principio, se busca que las empresas establezcan diferentes procesos de gobierno y diferentes procesos de gestión para proveer un gobierno y una gestión del entorno IT completos.

Cuando se contemplan los procesos para gobierno y gestión en el funcionamiento de la empresa, lo que logra diferenciar los dos tipos de procesos son los objetivos.

Los procesos de gobierno contemplan los objetivos de gobierno de las partes interesadas – dar el valor agregado, administrar óptimamente el riesgo y los recursos – e involucra tareas enfocadas a validar opciones estratégicas, dando la dirección de TI y monitoreando la entrega, como se observa en la ilustración 3.

Por su parte los procesos de gestión abarcan las áreas encargadas del PBRM *(Plan, Build, Run and Monitor)* de TI de la empresa y deben ofrecer cobertura de TI de punta a punta, a pesar de que los entregables de cada tipo de proceso son diferentes y están dirigidos a distinta audiencia, de forma general al referirse a administrar proceso, todos los procesos deben contar con actividades de 'planificación', 'construcción o implementación',' ejecución' y 'supervisión' del proceso.

Ilustración 3. Áreas claves del sistema de Gobierno COBIT 2019

Fuente: (ISACA, 2019)

La parte de procesos indica como este ha sido organizado a través de diferentes actividades para la consecución de los objetivos y lograr así que los resultados obtenidos aporten con lo que el área de TI en conjunto quiere obtener.

Con respecto a las Estructuras organizativas son aquellas partes clave que la empresa tiene para decidir sobre diferentes aspectos y finalmente, los Principios, Políticas y Marcos de referencia son lo que hacen que la forma ideal de ejecutar los procesos se convierta en el quehacer diario de este.

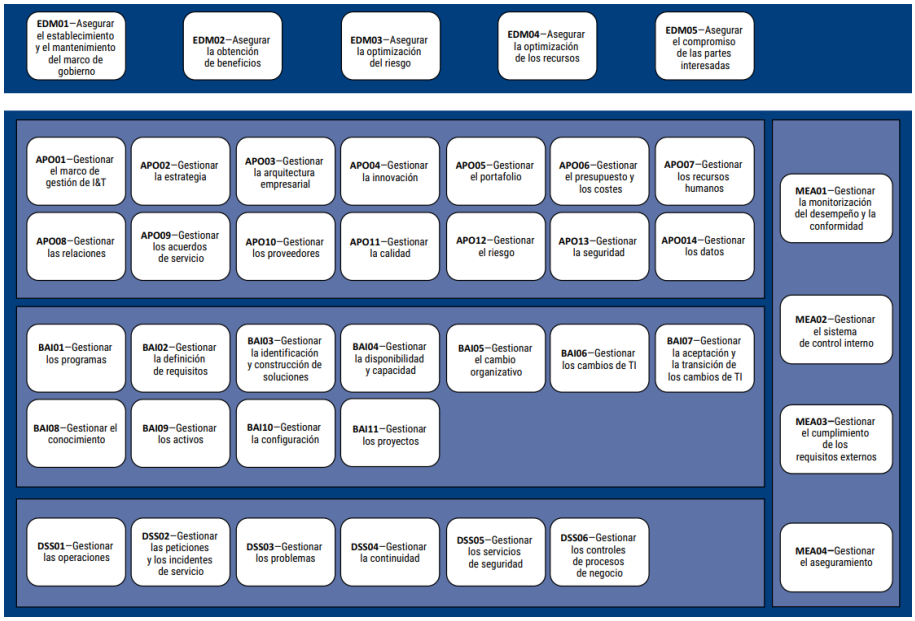
COBIT 2019 cuenta con un modelo de procesos que define de manera detallada el funcionamiento de los procesos de gobierno y de gestión, esto permite identificar los

procesos que generalmente hacer para de las actividades de las áreas de tecnología, este modelo de referencia genera un lenguaje universal y estándar tanto para TI como para el negocio. (ISACA, 2019)

El modelo de procesos que propone COBIT 2019 es robusto, no obstante, en el mercado existen más opciones que pueden ser tomados como referencias por parte de las empresas, por supuesto, cada negocio es diferente por lo que su conjunto de procesos debe definir de manera particular. (ISACA, 2019)

El marco de referencia de procesos de COBIT 2019 muestra los procesos de gobierno y de gestión de TI de la empresa como se observa en la Ilustración 4 donde se muestra el conjunto completo de los 40 procesos de gobierno y gestión dentro de COBIT 2019.

Ilustración 4. Procesos de Gobierno y Gestión dentro de COBIT 2019



Fuente: (ISACA, 2019).

1. Dominio de Gobierno

Este dominio se compone de cinco procesos; dentro de cada proceso, se contemplan las prácticas EDM (Evaluar, Dirigir y Monitorizar por sus siglas en inglés).

- Evaluar, Dirigir y Monitorizar (EDM).

Asegura que los objetivos de la empresa sean logrados, evaluando las necesidades de los interesados y tiene como objetivo las siguientes actividades como se muestra en la Tabla 4, Objetivos del principio EDM – Evaluar, Dirigir y Monitorizar. (ISACA, 2019)

Tabla 3. Objetivos del principio EDM – Evaluar, Dirigir y Monitorizar.

Dominio	Principio	#	Objetivos del principio
Gobierno	**EDM** (Evaluar, Dirigir y Monitorizar)	1	Asegurar el establecimiento y mantenimiento del marco de gobierno.
		2	Asegurar la obtención de beneficios.
		3	Asegurar la optimización del riesgo.
		4	Asegurar la optimización de recursos.
		5	Asegurar el compromiso de las partes interesadas.

Fuente: (ISACA, 2019)

2. Dominio de Gestión.

Se compone de cuatro principios los cuales están alineados con las áreas de responsabilidad de PBRM (Planificar, Construir, Ejecutar y Monitorear, por su sigla en inglés) garantizado el cubrimiento de TI punta a punta Cada dominio contiene varios procesos los cuales se mencionan a continuación: (ISACA, 2019).

- Alinear, Planificar y Organizar (APO)

Contempla las estrategias y las tácticas donde se identifica la manera en que TI puede aportar de mejor forma con los objetivos del negocio, es necesario contempla que la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Alinear, Planificar y Organizar da los lineamientos para ofrecer soluciones y ofrecer servicios de la manera más adecuada (ISACA, 2019).

El proceso APO tiene como objetivo las siguientes actividades como se muestra en la Tabla 5. Objetivos del principio APO – Alinear, Planificar y Organizar.

Tabla 4. Objetivos del principio APO

Dominio	Principio	#	Objetivos del principio
Gestión		6	Gestionar el marco de gestión de I&T

	APO (Alinear, Planificar y Organizar)	7	Gestionar la estrategia.
		8	Gestionar la arquitectura empresarial.
		9	Gestionar la innovación.
		10	Gestionar el portafolio.
		11	Gestionar el presupuesto y los costes.
		12	Gestionar los recursos humanos.
		13	Gestionar las relaciones.
		14	Gestionar los acuerdos de servicio.
		15	Gestionar los proveedores.
		16	Gestionar la calidad.
		17	Gestionar el riesgo.
		18	Gestionar la seguridad.
		19	Gestionar los datos

Fuente: (ISACA, 2019)

- Construir, adquirir e implementar (BAI).

El objetivo de este dominio es gestionar que nuevos proyectos generen soluciones para cubrir las necesidades de la empresa que sean entregadas oportunamente y según el presupuesto, adicionalmente que la implementación de sistemas funcione de manera correcta y que las actualizaciones no generen problemas en las operaciones actuales del negocio (ISACA, 2019)

Para cumplir con la estrategia de TI, los desarrollos que se hagan requieren ser identificadas, desarrolladas o adquiridas, así como implementadas y amarradas a los procesos del negocio (ISACA, 2019)

El proceso BAI tiene como objetivo las siguientes actividades como se muestra en la Tabla 6. Principio de gestión BAI – Construir, adquirir e implementar:

Tabla 5. Principio de gestión BAI – Construir, adquirir e implementar.

Dominio	Principio	#	Objetivos del principio
Gestión	**BAI (Construir, adquirir e implementar)**	20	Gestionar programas
		21	Gestionar la definición de requisitos.
		22	Gestionar la identificación y construcción de soluciones.
		23	Gestionar la disponibilidad y la capacidad.
		24	Gestionar el cambio organizacional.

		25	Gestionar los cambios de TI
		26	Gestionar la aceptación y transición de cambios de TI.
		27	Gestionar el conocimiento.
		28	Gestionar los activos.
		29	Gestionar la configuración
		30	Gestionar los proyectos.

Fuente: (ISACA, 2019).

- Entregar, dar Servicio y Soporte (DSS)

Este dominio contempla la entrega de los servicios requeridos y busca que los servicios de las áreas de tecnología se den basados según lo priorice la empresa, este dominio está enfocado en la optimización de los costos, asegurando que las áreas hagan uso de los sistemas de forma más productiva y segura, las actividades contempladas en la Tabla 7. Indican el Principio de gestión DSS – Entregar, dar Servicio y Soporte: (ISACA, 2019).

Tabla 6. Principio de gestión DSS – Entregar, dar Servicio y Soporte

Dominio	Principio	#	Objetivos del principio
Gestión	**DSS (Entregar, dar Servicio y Soporte)**	31	Gestionar las operaciones.
		32	Gestionar las peticiones y los incidentes del servicio.
		33	Gestionar os problemas.
		34	Gestionar la continuidad.
		35	Gestionar los servicios de seguridad.
		36	Gestionar controles de los procesos de negocio.

Fuente: (ISACA, 2019).

- Monitorizar, Evaluar y Valorar (MEA).

El monitoreo y evaluación de los procesos debe contemplarse en su totalidad con cierta periodicidad, no hay otra forma de conocer y validar si se cumple con los procesos, pero además cual es el nivel de calidad de la ejecución de los controles definidos, para lograrlo dentro de este abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. (ISACA, 2019)

La evaluación y la valoración permiten identificar a tiempo problemáticas por medio de la medición del desempeño y adicionalmente garantiza que el ambiente de control definido sea efectivo y eficiente (ISACA, 2019).

El principio MEA tiene como objetivo las siguientes actividades como se muestra en la Tabla 8. Principio de gestión MEA – Monitorizar, evaluar y valorar.

Tabla 7. Principio de gestión MEA – Monitorizar, Evaluar y Valorar.

Dominio	Principio	#	Objetivos del principio
Gestión	**MEA (Monitorizar, Evaluar y Valorar)**	37	Gestionar la monitorización del rendimiento y la conformidad
		38	Gestionar el sistema de control interno
		39	Gestionar el cumplimiento de los requisitos externos
		40	Gestionar el aseguramiento

Fuente: (ISACA, 2019).

COBIT y SOX IT

SOX IT y COBIT están estrechamente relacionados toda vez que COBIT abarca dentro de sus 40 componentes los tres principales requerimientos tecnológicos necesarios para implementar la ley SOX, la cual, de manera general busca garantizar la correcta administración de la tecnología para asegurar la razonabilidad de la información financiera, tarea para la que COBIT resulta ser una de las mejores opciones disponibles.

La aplicación del instrumento es una de las estrategias más relevantes ya que será el insumo principal para la definición de los planes de acción para ejecutar el proyecto.

5.2.3 PCAOB - *Public Company Accounting Oversight Board* (Consejo de Supervisión Contable de Empresas Públicas)

La PCAOB es una entidad sin ánimo de lucro creada por el Congreso de los Estados Unidos para vigilar los procesos de auditoría de las empresas que cotizan en bolsa, esto con el fin de asegurar a los inversores y generar el interés público en la preparación de

reportes de auditoría reveladores, puntuales y adicionalmente que demuestren independencia.

Adicionalmente, la PCAOB monitorea las auditorías de los corredores y agentes de bolsa, contemplando los informes de cumplimiento entregados en virtud de las leyes federales de valores (PCAOB, 2020).

La PCAOB tiene cuatro funciones principales:

Registrar a las empresas de contabilidad pública que preparan informes de auditoría para emisores, corredores y agentes (PCAOB, 2020)

Establecer o adoptar normas de auditoría y de certificación, control de calidad, ética e independencia (PCAOB, 2020).

Vigilar las auditorías y los sistemas de control de calidad de las empresas registradas (PCAOB, 2020)

Investigar y disciplinar a las empresas de contabilidad pública registradas y a sus personas asociadas por violaciones de determinadas leyes, reglas o normas profesionales (PCAOB, 2020).

En apoyo de su misión, también lleva a cabo investigaciones económicas y análisis de riesgos, relacionados con sus interlocutores y con otros reguladores nacionales e internacionales.

La PCAOB *(Public Company Accounting Oversight Board)* tiene la facultad para crear estándares y normas de auditoría, control de calidad e independencia a ser implementados por las firmas de contaduría pública registradas, en la preparación y emisión de reportes de auditoría, tal y como es requerido por dicha Ley o por las reglas de la SEC, o que puedan ser necesarios o apropiados en el interés público o para protección de los inversionistas (PCAOB, 2016)

5.2.4 SEC - *Securities and Exchange Commission*

La SEC Contribuye a mantener la integridad estructural de los mercados de capitales estadounidenses regulando el flujo de información sobre las empresas públicas y haciendo cumplir la normativa sobre valores.

Las empresas públicas son una piedra angular de la economía estadounidense, ya que producen bienes y servicios que elevan el nivel de vida, proporcionan empleo y aumentan el bienestar económico de la nación.

Para iniciar o hacer crecer una empresa, las corporaciones pueden obtener capital del público vendiendo acciones de sí mismas. Es más probable que los inversores inviertan en esos valores corporativos si tienen la información adecuada para tomar decisiones acertadas, si las operaciones de los mercados de capitales son transparentes y si las fuertes sanciones minimizan el impacto de los participantes en el mercado sin escrúpulos o negligentes. La Comisión del Mercado de Valores (SEC) se creó para garantizar y mantener esas condiciones.

La misión de la SEC siguió evolucionando en el siglo XXI. La Ley Sarbanes-Oxley de 2002 introdujo cambios de gran alcance en la estructura y el funcionamiento de los mercados de valores. Algunos de ellos fueron la exigencia de que los directivos se responsabilizaran personalmente de las afirmaciones realizadas en los estados financieros, la creación del Consejo de Supervisión Contable de Empresas Públicas para supervisar a los contables que auditan dichos estados, y la protección de los denunciantes que informan sobre malas prácticas y fraudes empresariales.

Durante la crisis financiera mundial de 2008 se intensificó el interés del público por la regulación financiera, y la SEC participó intensamente en los esfuerzos por castigar a los considerados responsables de las inversiones de riesgo relacionadas con la convulsión económica. Investigó acusaciones de fraude de gran repercusión, como el esquema

Ponzi de Bernie Madoff; la gestión de Madoff y otros casos por parte de la agencia fue muy criticada por no haber advertido las señales de alarma.

La Ley Dodd-Frank de Reforma de Wall Street y Protección del Consumidor de 2010 esbozó nuevas normas para el sistema de regulación financiera de Estados Unidos, incluida la Regla Volcker, destinada a controlar la especulación de los bancos. (Samuel, 2021)

5.2.5 ISACA

Alrededor del mundo ISACA cuenta con más de cien mil personas usuarias directas de los conocimientos que se encuentran disponibles en su plataforma sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento (ISACA, 2022).

Fundada en 1969, ISACA, es una institución independiente y sin ánimo de lucro, da charlar internaciones, publica el ISACA® *Journal* y genera estándares internaciones de control y auditoría de SSII, con el fin de guiar a sus asociados a robustecer y generar valor para y desde los sistemas de información (ISACA, 2022).

Dentro de las labores más conocidas de ISACA se encuentra la entrega de los certificados mundialmente utilizados tales como (CISA®) *Certified Information Systems Auditor®, (CISM®) Certified Information Security Manager®, (CGEIT®) Certified in the Governance of Enterprise IT® y (CRISCTM) Certified in Risk and Information Systems Control TM* (ISACA, 2022).

ISACA es la entidad dueña del marco COBIT y se encarga de realizar continuamente nuevas versiones de este con el fin de asegurar que se mantenga alineado con las nuevas tecnologías. (ISACA, 2022)

5.3 Marco teórico

5.3.1 Teoría y Gestión de las organizaciones – Proceso de control

La administración del control es fundamental en este trabajo, es de aquí donde parte todo el ejercicio y la raíz de la ley SOX, si bien es cierto la monografía está enfocada al impacto tecnológico que tienen las empresas al implementar SOX, no se podría definir este sin la concepción básica del control y su objetivo esencial que es regular.

El control en su definición más general es aquella función administrativa que permite medir y evaluar el desempeño y toma la acción correctiva cuando sea identificada. De este modo, el control es un proceso esencialmente regulador (Escuela Pública digital Universidad de la Punta).

Implementar control desde cualquier instancia que se requiera, busca y debe obtener beneficios desde diferentes perspectivas, no obstante, más allá de lo que se busque controlar, el valor agregado se da en la definición de medidas correctivas que permitan la consecución de los planes de manera exitosa y talvez más relevante aún busca evitar que situaciones que se han presentado se repitan en el futuro, lo que por defecto lleva a obtener información de las situaciones presentadas y los planes de acción implementados, reduce costos y ahorra tiempo al evitar repetir malas prácticas del pasado (Escuela Pública digital Universidad de la Punta).

En este sentido el control va más allá de meramente establecer actividades para monitorear procesos, los controles buscan dar valor agregado a las compañías, evitar pérdidas de cualquier índole, adicionalmente siempre se debe tener en el alcance que nunca la implementación de un control debe ser más alto que el valor de un proceso en sí.

La ley SOX desde su concepción básica de control tiene como objetivo establecer un marco de control interno que primero permita identificar situaciones generadoras de riesgos para definir actividades que las monitoreen.

Desde la perspectiva de ITGC o controles generales de tecnología (por sus siglas en inglés), se busca controlar aspectos básicos de las aplicaciones, pero a su vez críticos y fundamentales para la correcta ejecución de cada una de las actividades que se realizan a través de éstas.

5.3.2 ¿Cómo SOX ha cambiado la administración de las tecnologías de la información en las empresas?

Este estudio sobre la premisa de que la ley SOX afectará a todos los sistemas informáticos relacionados con la información financiera plantea los siguientes interrogantes, ¿Qué significa esto exactamente? ¿Qué deben cambiar las empresas para cumplirla?, adicionalmente relaciona una lista de chequeo que permite evidenciar el estado actual de la empresa frente a los requerimientos de la ley SOX.

Dado que en la mayoría de las empresas los procesos de información financiera son impulsados por las aplicaciones tecnológicas, todos los sistemas de TI involucrados en la generación de datos financieros deben ser evaluados, documentados y probados para lograr el cumplimiento de Sarbanes-Oxley (Damianides, 2004, pág. 1).

Debido al importante impacto que TI puede tener en el buen funcionamiento de una empresa, los diferentes equipos de líderes deben aumentar la gobernanza y el cumplimiento de la ley Sarbanes Oxley a TI.

Adicionalmente el estudio referencia un cuestionario basado en el marco COBIT, el cual incluye los objetivos de control que se encuentran en los dominios Planificar y Organizar y Supervisar y Evaluar y algunos del dominio Entregar y Apoyar, el cual, puede ser utilizado por las empresas para hacer un diagnóstico sobre su estado actual en el entorno tecnológico y determinar que debería hacerse para cumplir con los requerimientos de la ley SOX.

Por otro lado, el informe indica que nunca se conseguirá un modelo de empresa completamente libre de riesgos, y el cumplimiento de la ley Sarbanes-Oxley no ofrece ninguna garantía de que las empresas sean totalmente seguras. Pero si no examinan los procesos que las empresas están aplicando para garantizar que sus prácticas de control interno están en un nivel aceptable, está claro que a largo plazo la organización se beneficiará de la mejora del entorno de control, lo que se traduce como que el cumplimiento de la ley Sarbanes-Oxley puede convertirse en una ventaja competitiva (Damianides, 2004).

El estudio refuerza que abordar el cumplimiento como una oportunidad única para establecer modelos de gobernanza sólidos puedes ayudar a mejorar la gobernanza de las TI en toda la empresa y mejorar la comprensión de las TI por parte de los ejecutivos (Damianides, 2004).

De acuerdo con el informe la implementación de SOX también puede dar a las empresas la oportunidad de mejores decisiones de negocio basadas en una información de mayor calidad y más oportuna. Otras ventajas son la mejora de la alineación entre las iniciativas de los proyectos y los requisitos de negocio, la reducción de la pérdida de activos intelectuales y las posibles violaciones del sistema, operaciones más eficientes y eficaces, una mejor gestión de los riesgos y una contribución al cumplimiento de otros requisitos normativos como la privacidad (Damianides, 2004).

5.3.3 TI y la Ley Sarbanes-Oxley.

Este articulo indica que muy pocas publicaciones se centran en la ley como parte integrante de un marco práctico de gobierno corporativo o reconocen la contribución de la tecnología más allá de los controles de TI generalizados que operan en los niveles de infraestructura y aplicación empresarial y reconoce que, sin embargo, las TI tienen un

papel importante en los paradigmas clave del Gobierno Corporativo (Sally & Lepeak, 2004).

El informe hace referencia a dos secciones de la Ley SOX la sección 409 (Información en tiempo real del emisor) y la sección 802 (Sanciones penales por alteración de documentos) que de acuerdo con lo relacionado en el informe deberían dársele la misma importancia que a las secciones 302 (Responsabilidad Corporativa de los controles de divulgación) y la 404 (Evaluación de los controles internos por parte de la dirección).

El articulo basado en una investigación realizada por la consultora META indica como cuatro marcos corporativos tienen una relación directa con las tecnologías de la información (Sally & Lepeak, 2004).

El primero de los marcos es la Gestión ética, la integridad y los valores éticos son componentes clave de control de una organización, pero ¿Cómo las tecnologías de la información se pueden relacionar con la gestión ética? Pues bien, los grupos de TI desempeñan un papel destacado, aunque no reconocido, que permite a las organizaciones hacer frente a algunos de los principales retos éticos en la era electrónica. Por ejemplo, la confidencialidad de los clientes y empleados, el intercambio de información y el uso de Internet y el correo electrónico son áreas críticas de preocupación (Sally & Lepeak, 2004).

El segundo de los marcos es el Cumplimiento Normativo, el cual hace referencia a que todas estructuras, incluidas las de TI, deben organizarse adecuadamente para gestionar el cumplimiento de la normativa. Sarbanes - Oxley cae de lleno en esta disciplina.

El cumplimiento normativo debe abarcar todos los mandatos que afectan a una organización, pero más allá de la importancia obvia de abordar todos los requisitos de cumplimiento, las organizaciones deben coordinar sus esfuerzos para aprovechar y

optimizar los recursos, esto es especialmente importante cuando se definen los planes de TI para las aplicaciones, herramientas y sistemas de apoyo (Sally & Lepeak, 2004).

El tercer marco hace referencia a la Gestión de riesgos el cual indica que un enfoque empresarial para gestionar objetivos financieros, operativos, de cumplimiento y de información debe incluir un componente de gestión de riesgos, aunque la Ley SOX ordena una evaluación anual de los controles internos sobre la información financiera, ninguna evaluación de los controles es completa y eficaz sin una evaluación previa de los riesgos asociados.

Los controles se basan en el riesgo, al igual que las auditorías externas realizadas para atestiguar la evaluación de la dirección sobre el diseño y la eficacia operativa de los controles internos sobre la información financiera.

El último de los marcos hace referencia a la Gestión de Rendimiento el cual se realiza o a través de los famosos KPI *(Key Performance indicators)* o a través de cualquier otro método que permita gestionar el rendimiento de las plataformas de la compañía, no obstante, y aun siendo esenciales para evaluar las capacidades de la organización no constituyen un medio adecuado para respaldar la presentación de informes financieros base de la ley SOX.

De acuerdo con el estudio, los bancos, por ejemplo, han abordado la gestión del riesgo para reservas, las carteras de inversión, las tenencias de derivados, etc., pero en algunos casos, amplían su actual evaluación del riesgo crediticio para considerar la exposición a violaciones de la seguridad en Internet y las vulnerabilidades asociadas que pueden dar lugar a deficiencias de control de la SOX (Sally & Lepeak, 2004).

De esta forma y de acuerdo con el artículo lo imperativo, por lo tanto, es abordar las cuestiones individuales de gobierno corporativo como parte de todo el paquete de gobierno. Las organizaciones deben abordar estos esfuerzos desde el nivel ejecutivo

hacia abajo, impulsándolos y coordinándolos a través de un director de cumplimiento de la empresa o una designación similar, aprovechando el papel de apoyo fundamental que puede desempeñar el área de las tecnologías de la información.

La segunda parte del estudio hace referencia a las dos secciones de la Ley SOX inicialmente la sección 409 – información en tiempo real del emisor y que obliga a informar rápidamente de los acontecimientos que puedan afectar a los resultados financieros de una empresa, este requisito afecta de lleno al departamento de TI, quienes deberán saber si los sistemas financieros clave son capaces de proporcionar la información requerida en tiempo real o debe valerse de software adicional para responder.

Para preparase para estos requerimientos, los profesionales del control de TI deben evaluar las capacidades tecnológicas de su organización en las siguientes categorías:

- Calidad de las capacidades de modelización financiera
- Disponibilidad de portales internos y externos
- Amplitud y adecuación de los activadores y alertas financieras
- Adecuación de los depósitos de documentos
- Adecuación de las pistas de auditoría de los documentos capturados
- Capacidad para adoptar rápidamente herramientas de reporte

El gran reto para poder cumplir con esta sección es que los sistemas de reporte actual de manera autónoma, el escenario ideal es que éstos estén integrados a los sistemas financieros y de planificación de recurso empresarial y así obtener información en tiempo real.

Por otro lado, para la Sección 802 - Sanciones penales por alteración de documentos el estudio indica que las cuestiones relacionadas con la TI incluyen la política y las

normas sobre la retención, protección y destrucción de registros, el almacenamiento en línea, los registros de auditoría, la integración con un repositorio empresarial, la tecnología de mercado, el *software* SOX y mucho más.

En este sentido la importancia de las tecnologías de la información radica en tener sistemas de almacenamiento lo suficientemente robusto que permita la conservación de documentos por lo menos los cinco años que por auditoria deben almacenarse.

Dada la rápida obsolescencia de la tecnología, algunos de los soportes actuales podrían quedar obsoletos en los próximos tres o cinco años (Sally & Lepeak, 2004).

Los datos de auditoría conservados hoy pueden ser irrecuperables no por la degradación de los datos, sino por la obsolescencia de los equipos y los medios de almacenamiento. equipos y medios de almacenamiento obsoletos. En de almacenamiento. Deberíamos ver esto como un imperativo de los registros (Sally & Lepeak, 2004).

En resumen, las organizaciones necesitan integrar la gestión interfuncional de las TI y secciones 409 y 802 en sus esfuerzos generales de cumplimiento de SOX. Para reiterar, debe haber un único punto de contacto similar a un director de cumplimiento que dirija e impulse estos esfuerzos. La clave para los esfuerzos de las secciones 409 y 802 es definir una línea de tiempo con hitos y un conjunto de resultados y capacidades clave para implementar (Sally & Lepeak, 2004)

5.3.4 La Ley Sarbanes-Oxley impacta los sistemas.

Este artículo hace referencia a cómo además de su impacto en la gestión financiera, el procesamiento y la presentación de informes, SOX afecta a las organizaciones de TI, ya que intentan desarrollar infraestructuras de TI más rentables para cumplir con los requisitos de la SOX (Sarctoni, 2005).

Los directores generales y los directores financieros esperan que la organización de TI implemente soluciones tecnológicas y de software adecuadas que controlen y automaticen los procesos y sistemas empresariales dentro de las directrices de cumplimiento de la SOX.

Dentro de los problemas de cumplimiento de SOX que se indica debe el área de IT solucionar se encuentran los siguientes:

Acceso autorizado a los sistemas y a la información. El control de acceso a la información y a los sistemas debe ser garantizado por los equipos de tecnología a partir de la implementación de controles que aseguren de quién en su organización tiene acceso a qué sistemas y datos, basado en las funciones de cada cargo; esto teniendo en cuenta que los empleados de su organización tienen más conocimientos sobre los procesos, sistemas y controles internos implementados, con este conocimiento, pueden hacer más daño a los sistemas y datos que alguien de fuera de su organización.

Adicionalmente se debe contemplar que a medida que el papel de un empleado cambia dentro de la organización, la capacidad del empleado para entrar y acceder a sistemas y datos específicos debería cambiar.

Como control compensatorio, periódicamente, las organizaciones deben realizar auditorías de los niveles de acceso de los empleados a los sistemas y datos de la organización. Durante estas auditorías, se debe hacer una revisión de los derechos de acceso de los empleados y se deben hacer modificaciones para reflejar adecuadamente los cambios en las responsabilidades de los empleados o las diferencias organizativas que requerirían cambiar los derechos de acceso de los empleados en su organización

Garantizar la integridad y exactitud de los datos. La integridad y exactitud de la información es uno de los principales pilares de la Ley SOX, que requiere que se incluya cualquier dato que afecte a los informes y procesos financieros de una organización.

En este sentido mediante el buen uso de las tecnologías de la información y la automatización de actividades y procesos una organización puede desarrollar una infraestructura tecnológica que ayude a garantizar la exactitud e integridad de su data financiera (Sarctoni, 2005)

Asegurar y auditar la actividad de los usuarios. Esta es una de las actividades que más incomodidad ha causado en los empleados de las compañías que cotizan en bolsa de valores debido a la necesidad de estar constantemente expuestos a revisiones y monitoreos sobre sus actividades, así como al cambio frecuente de contraseñas de acceso.

De igual forma para las empresas ha sido un reto que las ha llevado a replantear sus servicios de mesas de ayuda para la atención de requerimientos para dar cumplimiento a las exigencias de la Ley y aquí las tecnologías de la información han ganado importancia, convirtiéndose en el principal aliado para lograr la ejecución de estos procesos de forma automática.

Para la mayoría de las organizaciones que cotizan en bolsa, el cumplimiento de la SOX se ha convertido en una actividad muy costosa para la organización. Para ayudar a mitigar el coste y el impacto organizativo del cumplimiento de la SOX, una organización debe utilizar sus capacidades de TI para ayudar a automatizar tantos procesos de cumplimiento como sea posible dentro de la corporación (Sarctoni, 2005)

5.3.5 Los controles generales de tecnología (ITGC) y el líder contable.

Este artículo habla sobre la estrecha relación entre los controles generales de tecnología con los procesos contables haciendo énfasis en que un fuerte líder en la contabilidad de gestión supervisa los datos, así como las implementaciones, actualizaciones y mejoras, a través de los Controles Generales de tecnología (ITGC) (Murphy, 2016)

La tecnología de la formación existe para servir al negocio, los líderes de contabilidad deben tender un puente entre las TI y la empresa definiendo las necesidades de información, asumiendo un papel de liderazgo y participando plenamente con el área de tecnología en la satisfacción de estas necesidades, es evidente la importancia de los Controles Generales de la Tecnología de la Información (ITGC), no obstante no es claro si se dedica tiempo a comprender realmente los ITGC de la organización (Murphy, 2016).

Los directores financieros de las empresas que cotizan en bolsa firman habitualmente la certificación de la Sección 302 cada trimestre, dando fe de la idoneidad de los controles internos de su organización sobre la información financiera. Los controles internos sobre la información financiera, a veces denominados controles informáticos generales (CGI) son un aspecto crítico de estos controles.

En este punto el artículo invita a cuestionarse sobre los siguientes puntos, ¿Se conoce el alcance de los controles y se comprenden las lagunas de control interno? ¿Se conoce el plan de pruebas de estos controles informáticos?, esto considerando que la Sección 302 requiere que el CEO y el que el CEO y el CFO, pero no el CIO, den fe de la exactitud de los informes. Cuando se trata de la SOX y la ITGC, ¿podemos realmente dejar la TI a los informáticos?

En este sentido, el artículo realiza un *overview* del alcance de los ITGC pero muestra como estos nos pueden estar separados de la gestión contable, si bien es cierto los ITGC son las actividades de control físico, de desarrollo, de procedimiento y operativo que supervisan y protegen la infraestructura de los sistemas de información, las personas del equipo contable, debe desempeñar un papel muy activo a la hora de definir quién puede ver, quién puede cambiar y quién puede añadir algo a los datos de los sistemas.

Los equipos de TI entienden la tecnología, las personas de contabilidad los datos, así como su propósito y valor. Son dueños de los datos, ya sea directamente o en nombre de la empresa.

Basado en lo anterior se definen entonces las mejores prácticas como se menciona a continuación:

1. Participación y liderazgo en las implementaciones, actualizaciones y mejoras de los sistemas por parte del área contable, quienes deben definir sus necesidades de información y mantenerse al tanto de los avances del proyecto.
2. Una vez que haya alcanzado los objetivos anteriores y se haya establecidos las necesidades de información de los sistemas, el siguiente paso es aprovechar estos sistemas para todos los informes críticos. Informe de la fuente que se ha asegurado de que es fiable, en lugar de descargar la información en hojas de cálculo poco fiables y no controladas, hojas de cálculo.
3. El cumplimiento de los ITGCs puede llevar a la organización al cumplimiento, pero no a la seguridad y ciertamente no a la excelencia. Una buena gobernanza, unas necesidades bien definidas y unos controles internos eficaces deberían ser fines en sí mismos. El cumplimiento es un producto secundario. Los líderes de contabilidad deben adquirir el compromiso y tener el conocimiento para ayudar a la organización a aprovechar los ITGCs para un éxito empresarial continuo.

5.3.6 Encontrando las sinergias entre SOX y la evaluación de riesgos de TI

Este artículo se basa en un debate entre profesionales del sector financiero de diferentes empresas, las cuales se encontraban en diferentes etapas de desarrollo de los esfuerzos de cumplimiento ya que tras haber aplicado los requisitos iniciales de cumplimiento de la Ley Sarbanes-Oxley en 2002, están buscando formas de ahorrar racionalizando sus procesos de cumplimiento.

Dado que las tecnologías de la información son un componente importante del cumplimiento de la Ley SOX, se considera que algunas de las estrategias/sinergias pueden encontrarse en las evaluaciones/cumplimiento de TI. Por ejemplo, en una institución con 4.000 aplicaciones, hasta 300 podrían tratar aspectos de la gestión de transacciones, valoración e informes financieros y de gestión, y ser relevantes para la ley SOX; en consecuencia, es lógico que si hay oportunidades para las sinergias SOX-TI, pueden comenzar en el área de evaluación de riesgos tecnológicos. (Nathoo, 2007)

En particular el estudio se centra en las evaluaciones SOX-IT y describe una serie de pasos que pueden ayudar a las instituciones a racionalizar sus numerosas evaluaciones. (Nathoo, 2007)

Estos pasos son:

1. Comparar los ámbitos de las normativas.
2. Comprender los objetivos.
3. Resolver la cuestión de la propiedad.
4. Diseñar las evaluaciones.

Cuando se hace referencia a comparar las normativas se pretende buscar esas similitudes entre los diferentes cumplimientos en el caso de las entidades financieras deben atender, en este sentido, SOX obliga a evaluar riesgos y la calidad de los controles relativos a la información financiera exigencia similar que tiene la Ley GrammLeach-Bliley (GLBA) – Ley de Modernización de estados financieros de 1999 en lo que respecta a las cuestiones de conocimiento del cliente y de la privacidad; de igual forma sucede para la ya antigua Ley FDICIA y para Basilea II para todo lo relacionado con la gestión de riesgo y la evaluación de riesgos y controles. (Nathoo, 2007)

Las anteriores leyes consideran al igual que SOX la atención de riesgos informáticos clásicos que pueden desencadenar en deficiencias materiales en los estados financieros

a través del a implementación de controles que en términos generales serían cinco, controles de acceso, la seguridad del perímetro de todos los sistemas y aplicaciones para protegerlos contra los hackers, el sabotaje y otros acceso externo no autorizado, seguridad a nivel de aplicación para proteger, por ejemplo, la privacidad de las personas, medidas de gestión de la continuidad del negocio para prevenir o mitigar las interrupciones de los sistemas de TI que podrían afectar a la empresa y segregación de funciones para contrarrestar las oportunidades de fraude y error en el procesamiento de las transacciones. (Nathoo, 2007)

Pasando al segundo paso al que hace referencia el informe, comprender los objetivos se refiere a como atacar el problema central de planificar un programa único de evaluaciones de TI que satisfaga las necesidades de todos los diferentes regímenes normativos, así como las de la gestión del riesgo operativo. (Nathoo, 2007)

El tercer paso que se analiza indica que es necesario resolver la cuestión de la propiedad. Es muy común encontrar empresas donde los programas de evaluación de riesgos están muy repartidos, pueden estar evaluando los procesos al mismo tiempo y bajo diferentes metodologías, esta situación hace que las áreas se desgasten atendiendo una y otra vez los mismos requerimientos o unos similares. (Nathoo, 2007)

En este sentido, es importante que al interior de la empresa exista un área centralizada de riesgo operativo que defina las políticas y metodologías para realizar las diferentes evaluaciones que permita optimizar los ejercicios y obtener resultados con menos intervenciones y menos desgaste para las áreas operativas.

Finalmente, el último paso es el diseño de las evaluaciones, en este punto lo más importante es asegurarse que esta evaluación cumple con todos los objetivos, cubre un alcance adecuado y se ajusta a las políticas y el plan desarrollados por el área

centralizadora, de esta forma se pueden abarcar en una misma evaluación requerimientos para más de una normatividad.

En conclusión, el informe indica que no existe una receta que todas las instituciones puedan utilizar para transformar mágicamente un y complejo laberinto de requisitos de cumplimiento en un proceso único y armonizado. De hecho, ese resultado puede no ser necesariamente el mejor. Sin embargo, al racionalizar con éxito sus evaluaciones y sus procesos para llevar a cabo evaluaciones unificadas en toda la empresa, las instituciones que se analizaron han identificado los solapamientos de los requisitos normativos y los imperativos de gestión, un paso clave para unificar los múltiples objetivos de las distintas evaluaciones. (Nathoo, 2007).

5.3.7 Ramificaciones de la Ley Sarbanes Oxley (SOX) en el gobierno de las TI

En la mayoría de las empresas, los sistemas de información contable y financiera y de elaboración de informes están incorporados o integrados en sistemas de información, a pesar de las importantes funciones que estos sistemas desempeñan para facilitar las iniciativas de cumplimiento de la Ley SOX, la ley no menciona las funciones de los CIO, aunque sí estipula funciones específicas para los CEOs, los CFOs y los auditores. (Karanja & Zaveri, 2013)

El artículo basado en un detallado análisis de la literatura existente sostiene que las unidades de TI, bajo el liderazgo de los CIO, contribuyen significativamente en la adquisición, el diseño, la implementación y la gobernanza de estos sistemas de información, de esta forma el artículo tiene como objetivo debatir al respecto.

Como ya es bien sabido la tecnología día a día gana más terreno en todos los sectores empresariales, es por eso por lo que las inversiones en tecnología se han incrementado de manera exponencial y según un estudio de la revista *Information Week*

entre el año 2011 y 2012 las empresas que invirtieron de manera significativa en tecnología lo hicieron hasta en un 40% del total de los gastos.

No obstante, muchas empresas aun lo logran percibir los beneficios económicos de sus inversiones en tecnología y esto, según el estudio, se debe a la total desalineación que existe entre las áreas de tecnología y las estrategias empresariales. (Karanja & Zaveri, 2013).

La ley SOX promulga la imperiosa necesidad de lograr la tan anhelada alienación entre las TI y las estrategias empresariales, razón por la cual este estudio se centra en investigar específicamente como afecta la ley SOX al gobierno de las TI.

Según las directrices de cumplimiento de la Ley SOX, el papel de la TI está implícito y más si se tiene en cuenta que en la mayoría de las empresas los sistemas de información contable y financiera y de elaboración de informes incorporan o están integrados en sofisticados sistemas de información convirtiendo a las TI sean un socio necesario e importante en la iniciativa de cumplimiento de la Ley SOX de la empresa. (Karanja & Zaveri, 2013).

Según el estudio el rol del CIO es determinante al momento de cumplir con las exigencias de la ley SOX, esto basado en que este tiene entre otras, responsabilidades tales como establecer la estrategia de TI, dirigir las inversiones en TI, gestionar las iniciativas de externalización de TI y garantizar la seguridad e integridad de los datos y la información, las cuales alinean por completo a TI con SOX, por lo que se asumiría que sería el CIO el responsable de dar respuesta a los requerimientos tecnológicos desde la perspectiva SOX. (Karanja & Zaveri, 2013)

El estudio defiende vehementemente la importancia del rol del CIO considerando que es fundamental para que las empresas puedan cumplir con las normas. En su mayor parte, las herramientas que se requieren para reunir, agregar, analizar, evaluar, informar

y aplicar los informes contables y los estados financieros son facilitados por la unidad de TI y están bajo su gestión. Las empresas que tienen líderes de TI más experimentados se asocian con menos debilidades materiales.

Esta investigación desarrolla hipótesis que demuestran la importancia de la gobernanza de la tecnología de la información en la gestión de los recursos, capacidades y habilidades de TI en la gestión de riesgos, la alineación estratégica y la creación de valor empresarial. La unidad de análisis en este estudio es la capacidad organizativa de TI, que está representada por los CIO. Los CIO están a cargo de la ITG y, por lo tanto, de la gestión del complejo conjunto de recursos y capacidades relacionados con la TI.

El estudio analiza dos periodos de tiempo con eventos de tecnología que impactaban el mundo en los cuales se evidencia como la contratación del CIO mejora notablemente el desempeño y disminuye las debilidades al momento de ser evaluados por SOX.

Adicionalmente se indica que, con la creación de nuevos puestos de CIO, las empresas señalaron un cambio en su estrategia de TI y de negocio, ya que los nuevos CIOs se incorporaron para abordar cuestiones que antes no se atendían o no estaban consolidadas bajo una unidad de negocio.

En consecuencia, las capacidades de TI generan ventajas competitivas porque las empresas que cumplen los requisitos de la Ley SOX notifican menos debilidades materiales en el control interno y están aisladas de las repercusiones de las reacciones negativas del mercado bursátil, de igual forma los beneficios superiores a los normales, resultado del cumplimiento de los requisitos de la Ley SOX, generan recursos de inversión que se reinvierten, lo que conduce a un aumento de las capacidades de TI. (Karanja & Zaveri, 2013)

En consecuencia, las empresas utilizan capacidades informáticas superiores para reducir costes, aumentar la calidad, ofrecer productos/servicios innovadores y

diferenciados y mejorar los procesos empresariales. Los resultados de este estudio de investigación apoyan firmemente la recomendación de que la Ley SOX reconozca y defina explícitamente las funciones y responsabilidades del CIO. (Karanja & Zaveri, 2013).

5.3.8 Sarbanes-Oxley: La dimensión tecnológica

El documento afirma que la naturaleza y las características del uso de la tecnología de la información por parte de una empresa en su sistema de información afectan al control interno de esta sobre la información financiera. (Chan, 2004).

Debido a la falta de orientaciones definitivas, los auditores deben considerar cuidadosamente la dimensión tecnológica de SOX y determinar la forma y el grado en que sus sistemas tecnológicos contribuyen a cumplir los requisitos de la ley. Un examen de las principales implicaciones de la sección 302 y 404 en materia de riesgos y controles informáticos, así como la consideración de los marcos de control informático existentes, pueden ayudar a que las empresas se encaminen hacia el cumplimiento.

Con base en lo anterior el informe indica que se deben tener en cuenta ciertos aspectos para poder alinear las tecnologías de la información con requisitos que desde la perspectiva financiera tiene la ley SOX, aspectos entre los que se encuentran, el marco de control informático, la adaptación de la evaluación, la determinación de la relevancia, el aprovechamiento y la integración del control y pasar de ser más reactivos a proactivos.

Con respecto al marco de control tecnológico el informe indica que, dado que los procesos de los sistemas y los asientos generados por los mismos son parte integrante de los informes financieros, el control general de las TI y de las aplicaciones debe documentarse y evaluarse sobre la base de un marco de evaluación de la gestión y de las conclusiones que sea compatible con el mapeo de los procesos empresariales para mejorar la coherencia y la calidad. (Chan, 2004)

Así también, indica que de acuerdo con la opinión de muchos auditores el marco de control informático COBIT se alía bien con los esfuerzos de cumplimiento de SOX, lo cual refuerza aún más la relevancia su utilización para los proyectos SOX y revela una alta concentración de procesos de TI en torno a los componentes de "actividades de control" e "información y comunicación" de COSO, (Chan, 2004) base del cuestionario de diagnóstico utilizado para el desarrollo de este proyecto.

No obstante, también menciona que cuando se utiliza un marco de control establecido, es probable que los auditores tengan que adaptar los objetivos de control a la ley Sarbanes-Oxley. Por ejemplo, algunos objetivos de control de COBIT no son aplicables a los requisitos de SOX. La eficiencia operativa de las TI y las métricas de rendimiento, aunque son fundamentales para evaluar la madurez de la capacidad de las TI de una organización, no constituyen un medio adecuado para respaldar la presentación de informes financieros precisos, completos y justos. (Chan, 2004).

Un componente clave del trabajo de SOX relacionado con las TI implica la asignación de los objetivos de control, por ejemplo, la autorización y la salvaguarda de los activos, un objetivo de control clave de la organización se relaciona en gran medida con los objetivos de TI de garantizar la seguridad, la confidencialidad y la privacidad de la información.

Adicionalmente para garantizar la coherencia de la ejecución de los esfuerzos de mapeo de control, el informe afirma que deben entenderse claramente varias distinciones y suposiciones clave, en particular las que se basan en los términos utilizados en las afirmaciones de los estados financieros desde la perspectiva contable. Las siguientes afirmaciones comunes de los estados financieros, por ejemplo, pueden adquirir un significado nuevo o adicional en el contexto de las TI.

Existencia y ocurrencia: El control debe abordar la posibilidad de que se produzcan transacciones duplicadas, retransmitidas o ficticias en todas las etapas del procesamiento, las interfaces y la alimentación de los sistemas.

Medición: Se utilizan diferentes mediciones para las TI, como los criterios de medición definidos por la dirección para operaciones y procesamientos informáticos específicos. Los umbrales y criterios de medición predeterminados deben adaptarse y documentarse en función de los requisitos de las respectivas empresas, sobre la base de su relevancia para la información financiera.

Integridad y precisión: Los principios de "fiabilidad e integridad de la información" del marco COBIT 2019 pueden ser útiles para respaldar la afirmación de integridad de Sarbanes-Oxley en el entorno informático. El informe trimestral requerido por la ley sobre los cambios materiales en las TI que afectan a la información financiera y su mantenimiento, por ejemplo, puede incluirse en la agenda de TI de Sarbanes-Oxley de la organización.

Presentación y divulgación: los principios de "Cumplimiento y disponibilidad" de COBIT 2019, que se refieren a la disponibilidad de la información requerida por los procesos comerciales, las leyes, los reglamentos y los acuerdos contractuales, pueden ser una referencia útil para respaldar las afirmaciones de presentación y divulgación.

Debido a que muchos de los controles internos de los informes financieros dependen de las TI, es importante resaltar los facilitadores tecnológicos clave de los procesos comerciales y fomentar un entendimiento mutuo de la definición de los controles internos entre la empresa y los miembros de TI.

El siguiente de los aspectos que contempla el informe habla sobre la determinación de la relevancia indicando que, aunque el entorno de procesamiento de TI abarca muchos controles clave que son significativos y críticos para el éxito de la función de TI, puede

tener poca relación con el programa de cumplimiento de la ley Sarbanes-Oxley. Para que se les preste una atención prioritaria en las iniciativas de la ley Sarbanes-Oxley las actividades de control de TI deben cumplir criterios específicos que ayuden a garantizar la relevancia de los requisitos de la ley.

El informe plantea que realizar algunas preguntas pueden utilizarse como punto de partida para evaluar si los esfuerzos de TI son relevantes para Sarbanes-Oxley entre las que se encuentra por ejemplo validar si el negocio es dependiente de la tecnología o si esta es crítica para el negocio; también se debe confirmar si existen deficiencias significativas conocidas o debilidades materiales en las que esté pendiente una solución tecnológica y comprobar si el tratamiento informático está directa o indirectamente relacionado con la elaboración puntual de informes financieros entre otras.

El siguiente punto analizado es el aprovechamiento e integración del control, SOX requiere que los informes se eleven desde el nivel de transacción hasta su destino final en los estados financieros. En el transcurso de este viaje, los procesos de control interno en las unidades comerciales importantes deben examinarse de principio a fin, lo que a su vez requiere una evaluación integrada de los controles automatizados, dependientes de TI y manuales en relación entre sí. (Chan, 2004)

Debido a que los controles de TI están impulsados por el negocio, la documentación de TI generalmente comienza con una comprensión razonable de los procesos comerciales manuales significativos y el flujo de información. Cuando la documentación se presenta como paquetes comerciales y de TI separados, la información común tanto para el negocio como para TI tiende a duplicarse.

Un programa de cumplimiento de SOX puede servir como una oportunidad perfecta para demostrar verdaderamente el vínculo entre los procesos *core* del negocio y de TI y para promover una asociación de cuatro vías entre TI, auditoría interna, finanzas y las

unidades comerciales *core* del negocio. Cuando la información de control disponible se identifica, localiza, comunica y comparte entre estas partes, todos se benefician. (Chan, 2004).

El último de los aspectos que abarca el informe habla de pasar de la reactividad a la proactividad. Teniendo en cuenta que el camino de implementación de la Ley SOX desde la perspectiva IT puede resultar complejo, es posible que durante este viaje se logren identificar importantes oportunidades de mejora, tales como la eliminación de la redundancia en los controles, mejora en los servicios o valor agregado en los proyectos más allá de los requerimientos de cumplimiento, situación que permite refutar todos aquellos detractores de la ley que pueden llegar a indicar hasta que su implementación puede llegar a tener impacto en el resultado final. (Chan, 2004)

5.3.9 La ley Sarbanes-Oxley aumenta los costes de TI, pero obliga a las empresas a prepararse.

Este artículo periodístico basado en afirmaciones de CIO y gerentes de departamentos de tecnología se enfoca en como la implementación de la Ley SOX ha representado un aumento en el costo económico en los departamentos de TI, esto considerando que la ley ha estimulado un mayor gasto en áreas como la gestión y seguridad de registros, así como la compra de nuevas herramientas necesarias para garantizar la precisión de los datos financieros. (Thibodeau, 2005)

No obstante, el artículo también deja ver como estos mismos ejecutivos de TI indican que a pesar del gasto se puede evidenciar los beneficios que esta implementación trae no solo para IT sino para toda la compañía.

Otras de las ventajas identificadas por los ejecutivos indican que el cumplimiento de la Ley SOX los llevo a establecer en los departamentos una oficina que gestiona los

problemas de TI asociados con la ley, además de la protección de la propiedad intelectual y la privacidad de los datos. (Thibodeau, 2005)

Otros gerentes de TI indicaron que la respuesta corporativa necesaria para cumplir con Sarbanes-Oxley les proporciona marcos organizativos, de gobierno y educativos que deberían ayudarlos a lidiar con el cumplimiento en el futuro. (Thibodeau, 2005)

Adicionalmente, el reporte indica que los líderes son conscientes de la importancia de asegurarse de que los altos ejecutivos y los miembros de la junta se tomen el cumplimiento lo suficientemente en serio, considerando que las consecuencias de no cumplir son significativas

Finalmente, el artículo indica que los CIO afirman que ayudar a una empresa a cumplir con sus requisitos reglamentarios es una tarea que los gerentes de TI deben asumir de buen grado que se convierte en una gran oportunidad para demostrar su liderazgo.

5.3.10 Implicaciones tecnológicas de la ley Sarbanes-Oxley.

El artículo hace un resumen de los principales puntos de un informe realizado por la Asociación de Desarrolladores de Software de Aplicaciones Empresariales (BASDA) el cual advierte sobre las repercusiones de la ley Sarbanes-Oxley para las TI y los retos que esto trae para los directivos financieros haciéndose énfasis en que estos tendrán que confiar en los departamentos de TI para que sean el centro de la aplicación de la reingeniería de procesos importantes que les permita llegar al cumplimiento de la ley. (Jaques, 2005)

De acuerdo con el estudio realizado por la BASDA muchas empresas subestiman el reto de la implementación de la ley, ya que se requiere de la adopción de un marco de contabilidad financiera que pueda generar informes financieros fácilmente verificables con datos de origen rastreables garantizando que los datos permanezcan intactos y no pueden sufrir revisiones no documentadas, tarea entonces que resulta retadora si no se

cuenta con la disposición, recursos, liderazgo y conocimiento para hacerlo. (Jaques, 2005)

Otro de los puntos que menciona el estudio hace referencia a las tendencias que se han venido generando a raíz de la adopción de SOX, que se mencionan a continuación:

1. Las empresas se están dando cuenta de que pueden mejorar los procesos empresariales, los controles, la toma de decisiones efectiva y la rentabilidad mediante la inversión que realizan en el cumplimiento de la normativa.
2. El elemento informático del cumplimiento es un reto. Los sistemas existentes se muestran excesivamente complejos, duplicados y fragmentados, con solapamientos en los sistemas manuales y automáticos.
3. El papel del director de informática es muy importante para entender y cumplir con la normativa. Se exige una mayor responsabilidad y un mayor rendimiento de la inversión en TI.
4. Los directores financieros buscan que los costes de cumplimiento disminuyan, al tiempo que minimizan el riesgo de incumplimiento. Tiene que haber un cumplimiento sostenible y rentable
5. La empresa debe cumplir con SOX, no sólo el software. El estudio subraya que SOX conlleva una serie de responsabilidades para los responsables de las empresas, lo que les confiere una influencia sin precedentes a la hora de configurar las agendas corporativas.

En este sentido, el estudio indica que todas las acciones de TI deben integrarse y coordinarse con la gama más amplia de iniciativas de SOX, así pues, las TI ya no son una utilidad dentro del negocio, sino una parte integral de la función de gestión.

Por otro lado, el estudio también hace referencia a factores de éxito que se han identificado para la implementación de la norma y que pueden aplicar aquellas empresas que inician su viaje de adopción SOX. (Jaques, 2005)

1. Seleccionar un equipo de proyecto eficaz.
2. Evaluar minuciosa el alcance y el riesgo del proyecto.
3. Identificar temprano los controles empresariales inexistentes o débiles con planes sólidos para su sustitución;
4. Revisar minuciosa todas las acciones del proyecto;
5. Comunicar eficazmente las funciones y responsabilidades de la Ley a todos los empleados.

Alineado con los factores de éxito BASDA destaca las lecciones aprendidas que han venido identificado las empresas que se encuentran trabajando o ya implementaron la norma. (Jaques, 2005)

1. Elegir un marco de gobierno a partir del cual trabajar.
2. Integrar la TI con SOX y la agenda más amplia de control interno.
3. Realizar un inventario exhaustivo de todos los activos de TI, tanto de los sistemas como de las aplicaciones.
4. Considerar el impacto de la arquitectura de aplicaciones y el efecto que tiene en las funciones y responsabilidades individuales.
5. Abordar la interfaz de usuario final, donde el personal crea sus propios informes a partir de una serie de sistemas que están fuera del marco de control central.
6. Comprender cómo se controla la subcontratación y exigir que los proveedores subcontratados y los proveedores clave aporten pruebas de su propio cumplimiento mediante los diferentes informes disponibles.

En conclusión, BASDA considera que el cumplimiento de la normativa también aporta importantes beneficios en términos de mejora de los procesos. Sin embargo, el estudio advierte que no se debe subestimar el duro trabajo necesario para cambiar tanto los sistemas como los procesos actuales, y la integración de las TI es fundamental para ambos elementos. (Jaques, 2005).

5.3.11 Gestión de los controles informáticos para el cumplimiento de la SOX.

La gestión de los controles de TI para el cumplimiento de la ley SOX ha sido uno de los aspectos de los cuales menos se ha documentado lo cual resulta poco entendible si se considera que los sistemas de TI son parte integral de todos aspectos de las organizaciones modernas esto gracias al uso omnipresente de los sistemas para lograr un procesamiento eficiente de las transacciones.

La razón principal por la cual sucede esto es debido a la complejidad que conlleva cumplir SOX para TI, en primer lugar, la ley cuenta con 11 sesiones las cuales deben ser adaptadas por las empresas, pero siempre revisando como éstas le aplican basado en sus configuraciones informáticas, que pueden llegar a ser tan diferentes y variadas como se quiera. (Bone, 2009)

Por otro lado, la ley exige a las empresas que empleen un marco de control interno común para juzgar su cumplimiento. Esto parece sensato, pero el marco más utilizado -el marco COSO para los controles internos- ofrece poca orientación para los controles relacionados con la TI, razón por la cual fue desarrollado el marco COBIT sin que este resulte ser suficiente para dar cumplimiento al marco SOX, por lo que debe haber una especie de alineación entre los dos marcos de referencia (COSO – COBIT).

El informe indica que, para lograr el establecimiento de los controles de IT, es necesario como primer paso establecer una hoja de ruta para el cumplimiento de los requerimientos de IT, lo cual se logra identificando los controles relevantes tomando

como base como mínimo los 12 objetivos de control de IT que tiene la ley y revisar como pueden asignarse a los definidos por COBIT. (Bone, 2009)

Una vez identificados los controles clave, debe definirse en esa hoja de ruta como y con qué frecuencia serán revisados, tanto si utiliza hojas de cálculo, una base de datos o un sistema ERP completo, se necesita alguna forma de supervisar los controles con la suficiente frecuencia como para garantizar que los cambios en el entorno de control siguen estando dentro de las normas. (Bone, 2009)

Definidos los controles y la forma y frecuencia de revisarlos, es importante hacer un mantenimiento y seguimiento de estos, a través de definición de tableros de control que permitan monitorear los resultados que se están obteniendo, así como cambios que sean requeridos según el comportamiento del ambiente de control, lo cual se puede lograr a través de la implementación de una herramienta de supervisión.

Nada de lo anterior será posible si no se invierta en la “herramienta” más crucial para la implementación de SOX, el talento humano, la complejidad del cumplimiento de la ley SOX y de la adaptación de los controles de TI a sus requisitos exige una inversión en el cuidado y la alimentación de los profesionales de TI y de los que no lo son.

Los cambios en el negocio provocan cambios en sus sistemas de TI; por lo tanto, a medida que el negocio evoluciona con el tiempo, la dirección debe invertir constantemente en formación y concienciación para garantizar que todas las partes interesadas comprendan la compleja naturaleza de los controles de TI. Es fundamental que las empresas elaboren una comprensión y un léxico comunes para el entorno de control de TI, a fin de garantizar la conformidad con las normas. (Bone, 2009)

A pesar de parecer una tarea de titanes, una inversión en controles internos fuertes, un tablero de control eficaz y personas expertas en control interno garantizarán que el

buen gobierno de los controles internos sobre la información financiera se convierta en una ventaja competitiva para las organizaciones modernas. (Bone, 2009).

5.3.12 Descubrir el valor empresarial de las inversiones en TI para el cumplimiento de la ley Sarbanes-Oxley.

Este artículo se refiere de manera directa sobre como las inversiones en IT que se requieren para dar cumplimiento a la ley SOX pueden dar valor agregado a las empresas que están en el proceso.

Lo anterior se sustenta si se toma en consideración que la ley SOX afecta muchos aspectos de la tecnología de los servicios financieros ya que varios sistemas tecnológicos funcionan como custodios de la información a nivel de transacción principal aspecto para el cual la Ley exige transparencia, estos sistemas incluyen los libros mayores, los sistemas de información financiera, el software de planificación de recursos empresariales (ERP) y de gestión de procesos empresariales (BPM), los sistemas centrales y los repositorios de datos. (García, 2005)

Tanto los proveedores como las empresas a las que prestan sus servicios deberían darse cuenta de que la combinación adecuada de estas soluciones puede acabar aportando un valor más amplio que el mero cumplimiento de la normativa si se aplican a objetivos empresariales concretos de seguridad del cliente, gestión del riesgo empresarial (ERM) y eficiencia operativa. (García, 2005)

El informe menciona que se pueden encontrar dos tipos de respuestas por parte de las empresas a los requerimientos tecnológicos de SOX, por un lado, están las empresas que aplazan las inversiones por miopía, subestimando las inversiones en TI que serán necesarias, y por otro las empresas que combinan las inversiones tácticas con un propósito empresarial estratégico.

Esto último requiere que las empresas desarrollen un marco empresarial para el cumplimiento de la normativa y las iniciativas de riesgo empresarial más amplias. También requiere que los proveedores respondan a la creciente mentalidad de ERM ampliando sus soluciones más allá de las funciones de la ley Sarbanes-Oxley e incorporando una profunda experiencia en el ámbito de los servicios financieros a sus modelos de negocio. (García, 2005)

Al igual que muchos otros informes, en este se hace reiterativo que las inversiones en tecnología serán erróneas si se deja al departamento de TI al margen de la planificación estratégica y se le hace intervenir sólo a posteriori para averiguar cómo aplicar el plan establecido por los directores de negocio y los auditores. (García, 2005)

La normativa de la SOX exige un buen gobierno corporativo y evitar costosas sorpresas en toda la organización. Las inversiones para satisfacer esos requisitos no deben producirse en el vacío, sino dentro de un marco de ERM. Esto requiere un cambio cultural y organizativo para las muchas empresas que todavía gestionan la gobernanza, el riesgo, el cumplimiento y la información financiera en silos separados de negocio, producto y geografía. (García, 2005)

5.3.13 Superar la gran brecha.

El artículo de la reducción de la gran brecha es una muy interesante entrevista al presidente internacional de ISACA Everett C. Johnson Jr., quien habla directamente sobre cómo lograr que los directores ejecutivos (CEO) y las juntas directivas presten mayor atención a cómo TI sirve a los objetivos comerciales y cierre la gran brecha entre los altos ejecutivos y los profesionales de TI y de cómo la ley Sarbanes Oxley es un primer paso para lograr que los ejecutivos corporativos y las juntas directivas hagan del gobierno de TI una prioridad. (Aaccoullum, 2006)

La entrevista se centra en como la cuarta edición del principal producto de ISACA *(Control Objectives for Information and Related Technology* - COBIT), y como esta insta a líderes corporativos y profesionales de TI para alinear los sistemas y procesos de TI de su organización con los objetivos comerciales y el cual requiere un nuevo pensamiento por parte de la gerencia y TI.

En total la entrevista consta de once (11) preguntas que buscan dar una claridad sobre la versión del marco COBIT del año 2007 así como del rol que desempeñan tanto los auditores de TI como los líderes de las áreas tecnológicas para lograr que la alta gerencia este alineada con el rol de TI y así lograr el valor de la función de TI en la estrategia empresarial.

Las once preguntas con un breve resumen de su respuesta se relacionan a continuación en la Tabla 9.

Tabla 8. Resumen de la entrevista al presidente de ISACA.

Pregunta	Resumen de la respuesta
1. Sarbanes-Oxley ha puesto el foco en los controles financieros y comerciales basados en tecnología. ¿Cómo están respondiendo los auditores de TI a este desafío?	Uno de los grandes retos para los auditores de TI, especialmente para aquellos que no tienen antecedentes financieros es delinear los controles de TI que afectan o no los informes financieros, adicionalmente han tenido que ampliar su pensamiento sobre problemas de gobierno, llevándolos a centrarse más en el negocio y a combinar habilidades técnica y blandas para ser capaces de pensar estratégicamente y analizar problemas de forma crítica.
2. ¿Qué les dice a los profesionales de TI que	Los esfuerzos se han visto reflejados ya que las organizaciones que implementaron un gobierno de TI

objetan el esfuerzo continuo y los costos de cumplimiento involucrados con SOX?	efectivo hace años tuvieron la menor dificultad para cumplir con SOX ya que se tenían los procesos de pensamiento y el marco en su lugar. Adicionalmente, indica que una parte importante del gobierno de TI es el proceso de gestión de riesgos que realmente debe implementarse para que TI cumpla con los requisitos reglamentarios de una manera rentable, sin este proceso, una entidad puede estar en perfecto cumplimiento de la normativa, pero no estar aportando mucho valor a la organización. Ese es un argumento muy sólido para adoptar un enfoque de gobierno de TI mucho más amplio.
3. Un estudio reciente de ITGI encontró que más de la mitad de las empresas carecen de una estructura formal que alinee la TI con las estrategias y objetivos comerciales. ¿Por qué TI y el negocio no están más alineados y cuáles son los riesgos?	Los riesgos son evidentes, si la función de TI va en una dirección y el negocio va en otra, hay una gran desconexión y no se obtendrá el valor de la función de TI. Aquellas organizaciones que han alineado la TI con el negocio están viendo los beneficios. No es un tema que los directores ejecutivos se sientan cómodos discutiendo, particularmente con terceros, algunos directores de información (CIO) lo imponen en la agenda del director ejecutivo y, cuando los directores ejecutivos se involucran, es muy efectivo.
4. ¿Qué hay de nuevo en la versión revisada recientemente de COBIT?	La versión 4 de COBIT hace hincapié en la gobernabilidad de TI, logrando reunir todos los componentes: los objetivos de control de alto nivel, los de control detallados, las

	pautas de gestión y algunos modelos de madurez. Se ha reorganizado la información de manera que el documento sea mucho más fácil de usar. Una de las cosas que se hicieron fue analizar COBIT de "abajo hacia arriba" y "de arriba hacia abajo" para asegurar de que las cosas estuvieran integradas y el documento funcionara en todos los niveles de pensamiento. *** Versión 4 2007**
5. ¿Cuál es el pensamiento detrás del mayor énfasis en las medidas en esta versión?	Se trata de la cuestión de obtener valor de sus inversiones en TI. Hay una filosofía de gestión que dice "obtienes lo que mides". Parte de obtener valor y poder medir lo que está obteniendo es identificar los tipos correctos de medidas que puede usar para monitorear el desempeño de TI desde la perspectiva de la alta gerencia. Se abordan temas con los que el CEO puede identificarse, si va a gastar US $ 30 millones en un nuevo sistema, echemos un vistazo y preguntemos: "¿Por qué está haciendo esto?" "¿Cuáles son los beneficios?" Ahora asegúrate de conseguirlos.
6. ¿Qué está haciendo para llegar a los altos ejecutivos y gerentes de TI que no están	Se ha visto un crecimiento en la visibilidad de COBIT en un 50 por ciento en los últimos tres* años, sin embargo, se encuentran organizaciones que usan COBIT, pero su director ejecutivo no sabe que lo están haciendo. Existe un alto grado de satisfacción entre las organizaciones que

familiarizados con COBIT?	han implementado COBIT. A algunos les resulta muy fácil de implementar, a otros les resulta más difícil, pero están contentos con los resultados en términos de tener un marco de control, tener un proceso de gobierno, ayudar a proporcionar beneficios comerciales e involucrar a la junta. **Versión 4 2007**
7. ¿Cómo responde a los críticos que argumentan que no hay marco común para evaluar los controles y riesgos de TI relacionados con la información financiera?	Los objetivos de control de TI para Sarbanes-Oxley, publicado por ITGI, ha logrado ser un estándar para las empresas en términos de controles Sarbanes-Oxley. COBIT ha sido ampliamente utilizado por entes de auditoria tanto internos como externos, así como por la gerencia como marco para implementar y evaluar los controles de TI relacionados con la información financiera.
8. ¿La profesión necesita un conjunto común de mejores prácticas para auditar TI y tratar con el riesgo de TI?	El ITGI ha hecho una serie de cosas para alinear COBIT 4.0 con otros estándares, como ITIL, ISO 17799, el Foro de Seguridad de la Información, entre otros, estos son diferentes estándares para diferentes propósitos. Se hicieron algunos cambios en COBIT para que funcione bien con estos por lo que no se requiere un marco más ya que se tiene uno alineado que armoniza y muestra cómo funcionan muy bien juntos.
9. Ha mencionado que los auditores de TI deben ampliar su enfoque a los	La población de auditores de TI se divide en diferentes áreas de interés. En el nivel de gestión de auditoría de TI, muchas personas están interesadas y persiguen estas

objetivos comerciales. ¿Cómo se están adaptando los auditores de TI a su rol cambiante?	áreas comerciales y de gestión. Un ejemplo es la certificación de Auditor Certificado de Sistemas de Información (CISA) de ISACA, una de las áreas de contenido de este examen, se enfoca en el gobierno de TI, en el reconocimiento de que una parte importante del trabajo de auditoría de TI es garantizar que la empresa cuente con estructura, políticas, rendición de cuentas, mecanismos y prácticas de monitoreo para cumplir con los requisitos definidos por el negocio, todo lo cual requiere conocimiento un amplio conocimiento de este.
10. ¿Qué tipo de habilidades necesitan los auditores de TI de hoy?	En algunos aspectos, en un alto nivel, las habilidades que necesitan los auditores de TI no han cambiado demasiado. Necesitan una comprensión de cómo los sistemas procesan la información comercial, los riesgos de TI asociados con eso, las tecnologías subyacentes y cómo se administra la TI. Toda el área se ha vuelto mucho más desafiante en términos de comprensión de todos los problemas técnicos. Otro impulsor es Sarbanes-Oxley y el consiguiente aumento del enfoque en el buen gobierno corporativo. La parte de gobierno de TI involucra problemas comerciales mucho más amplios que requieren evaluar un conjunto integral de riesgos y asegurarse de que todos estén identificados y abordados adecuadamente, y medir el rendimiento de TI. Estos son

	más problemas de gestión que estrictamente de TI. Los auditores de TI no solo necesitan habilidades técnicas más profundas, sino que también necesitan más habilidades comerciales y de gestión.
La otra cara de la moneda es que muchos auditores sin experiencia en TI están siendo asignados para auditar TI para satisfacer la creciente demanda de este trabajo. ¿Cuál es su opinión sobre esta práctica?	Es importante que un especialista que no sea de TI aprenda cómo funcionan los sistemas, cuáles son los riesgos y cómo funcionan los controles contra esos riesgos en un entorno de TI. Los auditores de TI necesitan una mejor comprensión de cómo fluye la información comercial a través de un sistema y qué cosas malas le pueden pasar en el camino. Necesitan entender: ¿Cuáles son algunos de los riesgos? ¿Cuál es el papel de los controles, como los controles de acceso y la seguridad, en ese proceso? ¿Cómo afectan el desarrollo de sistemas, el mantenimiento de sistemas y las actualizaciones de sistemas a la confiabilidad del proceso? También hay una diferencia entre comprender los riesgos y tener una comprensión suficiente de la tecnología para auditarla.

Fuente: Elaboración propia basada en (Aaccoullum, 2006)

6. Metodología

6.1 Tipo de investigación

Actualmente se cuenta con una amplia variedad de tipos de fuentes que pueden generar ideas de investigación, cada una de estas fuentes que se pueden encontrar desde el mismo lugar donde estamos y el ambiente que nos rodea, hasta la infinita bibliografía disponible en repositorios controlados, así como en sitios de internet un poco menos restrictivos se convierten en ideas de investigación (Hernández-Sampieri & Mendoza, 2018, pág. 23).

A partir de los objetivos formulados, se trabaja este proyecto de investigación a través del método cualitativo. No obstante, a pesar de ser definido como cualitativo, se requiere establecer ciertas medidas tales como el nivel de madurez de las empresas para implementar la Ley SOX.

Adicionalmente, se requiere como punto principal una mirada más detallada de aspectos como los requerimientos tecnológicos que más retos representan para las empresas al momento de implementar la Ley SOX, así como las barreras de tiempo, conocimiento y disponibilidad de recursos de muchas empresas que se presentan antes y durante el proceso de implementación de la Ley, lo que sustenta y justifica aún más la elección del método cualitativo.

De acuerdo con Hernández Sampieri en su obra “Metodología de la investigación”, “En la búsqueda cualitativa, en lugar de iniciar con una teoría y luego “voltear” al mundo empírico para confirmar si ésta es apoyada por los datos y resultados, el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa (Esterberg, 2002). Dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general.”

(Hernández-Sampieri & Mendoza, 2018, pág. 8).

Para cumplir con los objetivos de este proyecto de investigación, se realiza de una amplia consulta de teorías sobre el tema desarrollado y se le da un carácter descriptivo soportado en la exploración variada de fuentes disponibles en los repositorios autorizados.

Para lograr desarrollar la investigación a partir del método descriptivo, fue necesario contemplar las dos variables principales de este tipo de investigación, en primer lugar, el conocimiento que se ha adquirido sobre el tema durante años de trabajo y por otro lado la perspectiva que se busca dar al proyecto.

Lo descrito a lo largo del documento, da fe del conocimiento que se tiene sobre el tema de investigación, el cual puede ser aplicado para sustentar y fortalecer la investigación. Adicionalmente, se relacionan variados estudios y documentos que describen experiencias sustentadas de aspectos generales que permiten hacer investigación descriptiva (Hernández-Sampieri & Mendoza, 2018)

También, se encuentran teorías que se aplican al problema de investigación, lo que la lleva a contar con elementos exploratorios (Hernández-Sampieri & Mendoza, 2018, págs. 104-121).

Como parte del método cualitativo se desarrollan los elementos fundamentales que la componen, tales como los objetivos, la pregunta de investigación, la justificación del proyecto, así como la viabilidad de este, todo descrito en la parte inicial del documento (Hernández-Sampieri & Mendoza, 2018, pág. 388)**.**

6.2 Proceso de investigación

Las etapas en el proceso de investigación “son en realidad acciones para adentrarnos más en el problema de investigación y la tarea de recolectar y analizar datos es permanente” a lo largo del desarrollo de la investigación, una vez contaba con problema

planteado se hace imperativo realizar acciones que permitan familiarizarse con el tema, y no exclusivamente con el objetivo central del mismo, sino adicionalmente con aquellos conceptos relacionados exógenamente, que generan impacto y se deben tener en cuenta en la concepción general del problema. (Hernández-Sampieri & Mendoza, 2018, pág. 356)

Otro de los pasos fundamentales dentro del proceso investigativo es la validación juiciosa del marco teórico, teniendo en cuenta que toda la literatura alrededor de esta es la fuente más útil para recolectar ideas e información para luego ser analizada, análisis que será la fuente de conceptos clave que permitirán sustentar aún más los resultados obtenidos logrando así ampliar la capacidad de profundizar en las interpretaciones de los datos recolectados.

“El planteamiento se fundamenta en las investigaciones previas, pero también en el proceso mismo de inmersión en el contexto, la recolección de los primeros datos y su análisis.” (Hernández-Sampieri & Mendoza, 2018, pág. 365).

“Las hipótesis de trabajo van surgiendo durante el proceso y en ocasiones, incluso, no solo se pulen poco a poco, sino que surgen a medida que se obtienen más datos o al final terminan siendo un resultado del estudio” (Henderson, 2009). “Las hipótesis: en raras ocasiones se establecen antes de ingresar en el ambiente o contexto y comenzar la recolección de los datos” (Williams, Unrau y Grinnell, 2005) (Hernández-Sampieri & Mendoza, 2018, pág. 365).

Cuando se analizan datos usando el método cualitativo, es de vital importancia, el proceso utilizado para su recolección, aquí, a diferencia del método cuantitativo, el objetivo de esta obtención no es medir variables y realizar análisis estadísticos, aquí se apropian esos datos y se transforman en información relevante y útil para soportar y

fortalecer la investigación o para obtener la respuesta al cuestionamiento de investigación. (Hernández-Sampieri & Mendoza, 2018).

6.3 Procedimientos y técnicas aplicadas para recoger y analizar la información

El método cualitativo usa como principal fuente de recolección de información al mismo desarrollador de la investigación ya que es este quien obtiene información a partir de la cuidadosa revisión documental, así como usando la observación. El método cualitativo se sirve de diversas fuentes como entrevistas, observaciones directas, documentos, material audiovisual, etc., de cualquier forma, lo que se quiere obtener al final del ejercicio es un entendimiento profundo del tema de estudio. (Hernández-Sampieri & Mendoza, 2018, pág. 397)

En esta parte del proceso se debe identificar, validar y referencias bibliográficas y fuentes adicionales de información que aporten de manera relevantes a cumplir con los objetivos planteados, es necesario tener claridad sobre cuáles pueden ser las posibles fuentes para obtener las referencias requeridas, tales como bases de datos de universidades, que cuentan con proyectos de grado, libros, páginas web, videos, entrevistas, revistas académicas, bases de datos, leyes, periódicos, artículos,

La recopilación de información es realizada haciendo revisión documental y análisis de datos valiéndose de diferentes fuentes como revistas académicas, periódicos, libros, bases de datos, tesis, sitios web, normas, entre otros (Hernández-Sampieri & Mendoza, 2018, pág. 98).

Para el estudio de las fuentes de información se analiza que tal útil resulta basado en cercanía o similitud con respecto al caso de estudio presentado, la semejanza al método de investigación, así como el rigor y calidad del estudio (Hernández-Sampieri & Mendoza, 2018, pág. 78).

La búsqueda de fuentes de información adicional a que se basa en información académica sobre temáticas directamente ancladas a la pregunta de investigación. también cuenta con la recolección, consulta y análisis de marcos de gobernabilidad de TI que apalancan la implementación de la Ley dando más valor a las estrategias o recomendaciones planteadas, así como a la futura aplicación de estás por parte de diferentes empresas.

Se estudia en su gran mayoría literatura extranjera que permiten analizar contextos y situaciones de empresas de otros países que se ven enfrentadas a los mismos retos que las empresas colombianas y pueden guiar el enfoque y tratamiento que se le dará al problema de investigación y orientar respecto de los diversos elementos que intervienen en la problemática planteada.

El desarrollo del proyecto se realizó siguiendo los pasos relacionados a continuación:

1. Obtención e identificación con base en la documentación fuente los requerimientos tecnológicos exigidos para implementar la ley SOX
2. Obtención con base en el marco conceptual de la información del marco COBIT para la identificación de los requerimientos tecnológicos de la ley SOX.
3. Elaboración de una matriz en la herramienta Excel donde se incluyen las preguntas basadas en el detalle de cada objetivo de control basado en los requerimientos y en el marco COBIT, preguntas que serán sujetas a una calificación para obtener una ponderación de resultados.

7. Trabajo de Campo

La investigación realizada se centra en desarrollar tres actividades para obtener datos que permitan identificar los principales retos y las mejores prácticas a ser implementadas desde la perspectiva tecnológica al implementar la Ley SOX.

En primer lugar, se realiza un análisis de la Ley SOX y sus requerimientos tecnológicos el cual se complementa con una validación de como el marco de COBIT los cubre, en segundo lugar se realiza una evaluación del nivel de madurez tecnológico de las empresas para cumplir la ley SOX basado en un instrumento de indagación elaborado según los lineamientos del marco de referencia COBIT, finalmente basado en lo analizado en la primera actividad y en los resultados obtenidos en la segunda se definen estrategias para fortalecer el entorno de TI teniendo como marco de referencia COBIT.

7.1 Análisis de la Ley SOX y sus requerimientos para el cumplimiento en materia de control para la gestión de TI.

El análisis de la ley SOX inicia con la revisión de los requerimientos tecnológicos que deben cumplir las empresas que planean implementar la Ley SOX, la cual se complementa con el análisis del marco de gobernabilidad de tecnología COBIT como base para el cumplimiento de estos requerimientos.

El análisis de los requisitos tecnológicos se hace basado en la norma AS 5 de la PCAOB que satisface las secciones 302 y 404 de la Ley Sarbanes-Oxley (2002), centrada en las implicaciones de la tecnología de la información (TI) en la auditoría del cumplimiento de la SOX; es importante comprender estos requisitos y su importancia para el diseño y la aplicación de los controles internos.

Con base en el marco teórico los requerimientos tecnológicos de la ley SOX resultan ser una de las partes más retadoras al momento de implementarla, teniendo en cuenta

que además de su impacto en la gestión financiera, el procesamiento y la presentación de informes, la Ley SOX está afectando a las organizaciones de TI, ya que intentan desarrollar infraestructuras de TI más rentables para cumplir con los requisitos. (Sarctoni, 2005)

Los directores generales y los directores financieros esperan que la organización de TI implemente soluciones tecnológicas y de software adecuadas que controlen y automaticen los procesos y sistemas empresariales dentro de las directrices de cumplimiento de la Ley SOX.

Para empresas muy grandes, se tiene la duda de cómo saber si la aplicación entra o no a alcance SOX, por principio, por seguridad, todas deben administrarse con los mismos lineamientos, todas deben cumplir con los mismos controles, esta situación es un reto gigante por la descentralización en la administración para aplicaciones con tecnologías muy antiguas.

El área de IT no solo debe operar la tecnología si no debe administrarla. Cuando el gobierno es centralizado se busca que todas las aplicaciones cumplan con todos los controles generales.

Se deben controlar todas las aplicaciones que se ven involucradas en el proceso, porque el input de uno puede afectar la otra y si una de las dos no cumple pone en riesgo la integridad de la información; sobre todo, garantizar que todo lo que está conectado al ERP, así como al sistema CORE de la compañía cumpla con los controles generales de tecnología.

Dentro de los requerimientos de cumplimiento de la Ley SOX que las empresas desde sus áreas de control interno en trabajo conjunto con las áreas de tecnología deben cumplir está la implementación de controles a nivel de entidad (ELC – por sus siglas en inglés). El entorno de control a nivel de entidad crea la base para un control interno

eficaz, establece el *"Tone at the top"* y representa la cúspide de la estructura de gobierno corporativo. Las cuestiones planteadas en el componente de entorno de control se aplican a toda una organización de TI y a la hora de establecer el marco para la interacción de TI con sus partes interesadas.

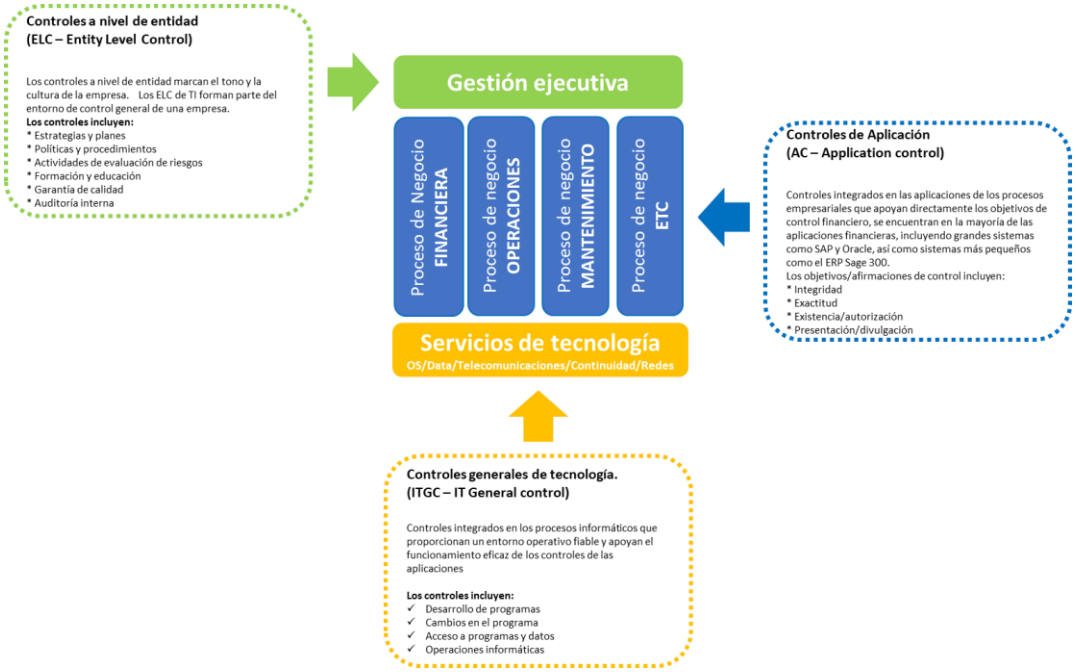
Otro de los requerimientos tecnológicos de la ley SOX son los controles generales de tecnología (ITGC por sus siglas en inglés *information Technology General controls)* los cuales aplican a todos los sistemas, componentes, procesos y datos del entorno de TI de una organización. (Udemy Business, 2022)

Otro de los requerimientos que tiene la ley SOX es la identificación y definición de controles de aplicación, los cuales se refieren a los controles sobre el procesamiento de las transacciones y los datos dentro de una aplicación y, por lo tanto, son específicos de cada aplicación.

Los objetivos de los controles de aplicación, que pueden ser manuales o automatizados y buscan garantizar la exactitud, la integridad, la fiabilidad y la confidencialidad de los registros y la validez de las entradas que se realicen en ellos, resultantes tanto del tratamiento manual como del programa, los cuales son ejecutados directamente por las aplicaciones y que deben ser monitoreados para garantizar que los procesos se ejecuten de manera correcta y oportuna.

El resumen de los requerimientos tecnológicos para la implementación de la ley SOX se observa en la ilustración 5.

Ilustración 5. Requerimientos tecnológicos de la ley SOX



Fuente: Elaboración propia basada en (ISACA, 2014)

1. **Controles a nivel de entidad – IT ELC**

Controles internos que contribuyen a garantizar que las directrices de la dirección relativas a la toda la entidad se lleva a cabo. Son el segundo nivel de un enfoque descendente para de la comprensión del riesgo de una empresa. En general, la entidad se refiere a toda la empresa. (ISACA, 2014)

Los ejemplos incluyen:

- Controles para supervisar otros controles, incluidas las actividades de la función de auditoría interna, el comité de auditoría y los programas de autoevaluación

- Políticas que abordan el control empresarial significativo y las prácticas de gestión de riesgos.

La norma AS 5 de la PCAOB hace mucho hincapié en los controles a nivel de entidad. La norma señala lo siguiente:

El auditor hace una evaluación de los controles a nivel de entidad que generan relevancia al momento de determinar si la empresa cuenta con un control interno eficaz sobre su información financiera. (ISACA, 2014)

Algunos controles a nivel de la entidad, como ciertos controles del entorno de control, tienen un efecto importante, pero indirecto, sobre la probabilidad de que una incorrección sea detectarse o evitarse a tiempo. Estos controles pueden afectar a los demás controles que el auditor selecciona para su comprobación y la naturaleza, el momento y el alcance de los procedimientos que el auditor lleva a cabo en otros controles. (ISACA, 2014)

Algunos controles a nivel de la entidad supervisan la eficacia de otros controles. Dichos controles pueden estar diseñados para para identificar posibles fallos en los controles de nivel inferior, pero no a un nivel de precisión que permita, por sí mismo, abordar suficientemente el riesgo evaluado de que se eviten o detecten a tiempo las incorrecciones en una afirmación relevante. a tiempo. Estos controles, cuando funcionan eficazmente, pueden permitir al auditor reducir las pruebas de otros controles. (ISACA, 2014).

Los controles a nivel de entidad definidos por el PCAOB AS 5, están relacionados con el entorno de control informático, este entorno incluye el proceso de gobierno de TI, la supervisión y la presentación de informes. El proceso de gobierno de TI incluye la planificación estratégica de los sistemas de información; el proceso de gestión de riesgos de TI; la gestión del cumplimiento y la gestión de la normativa; y las políticas, procedimientos y normas de TI. La supervisión y los informes son necesarios para alinear a TI con los requisitos del negocio. (ISACA, 2014)

La estructura de gobierno de TI debe diseñarse de manera que la TI añada valor al negocio y Los factores de riesgo de TI se abordan. Esta estructura de gobierno también

incluye una estructura de organización de TI que apoye y promueva la consecución de los objetivos de la empresa. (ISACA, 2014)

a. Identificando los controles a nivel de entidad

Los controles a nivel de entidad incluyen, entre otros, los siguientes:

- Control del entorno de control general

- Control de la gestión

- Evaluación de los riesgos de la empresa

- Controles y procesamientos centralizados, incluidos los entornos de servicios compartidos

- Supervisión de los resultados de las operaciones

- Controles para supervisar otros controles, incluidas las actividades de la función de auditoría interna, el comité de auditoría y los programas de autoevaluación

- Controles sobre el proceso de presentación de informes financieros al final del período

- Políticas que abordan las prácticas significativas de control y gestión de riesgos de la empresa (ISACA, 2014).

Muchos de los controles a nivel de entidad tienen implicaciones informáticas. Por ejemplo, el proceso APO02 de COBIT 5 Gestión de la estrategia de TI puede ser un control a nivel de entidad y requiere que TI proporcione una visión holística del negocio y del entorno de TI, la dirección futura y las iniciativas que se requieren para migrar al entorno futuro, que aprovecha la arquitectura de la empresa (incluidos los servicios proporcionados externamente y las capacidades relacionadas) para permitir respuestas ágiles, fiables y eficientes a los objetivos estratégicos (ISACA, 2014).

2. Controles generales de tecnología - ITGC

Los ITGCs (*Information Technology General controls*) engloban los controles mínimos que deben tener las aplicaciones utilizadas en una empresa que incluye la administración de accesos, la administración de cambios relacionados con el ciclo de vida del desarrollo del software (SDLC), la administración de operaciones y la administración de incidentes como se observa en la Ilustración 6 Controles generales de tecnología – ITGCs.

Para entender con mayor claridad cada uno de esos controles a continuación se dará una definición de cada uno de estos y se listarán los requerimientos que se tienen para lograr su cumplimiento.

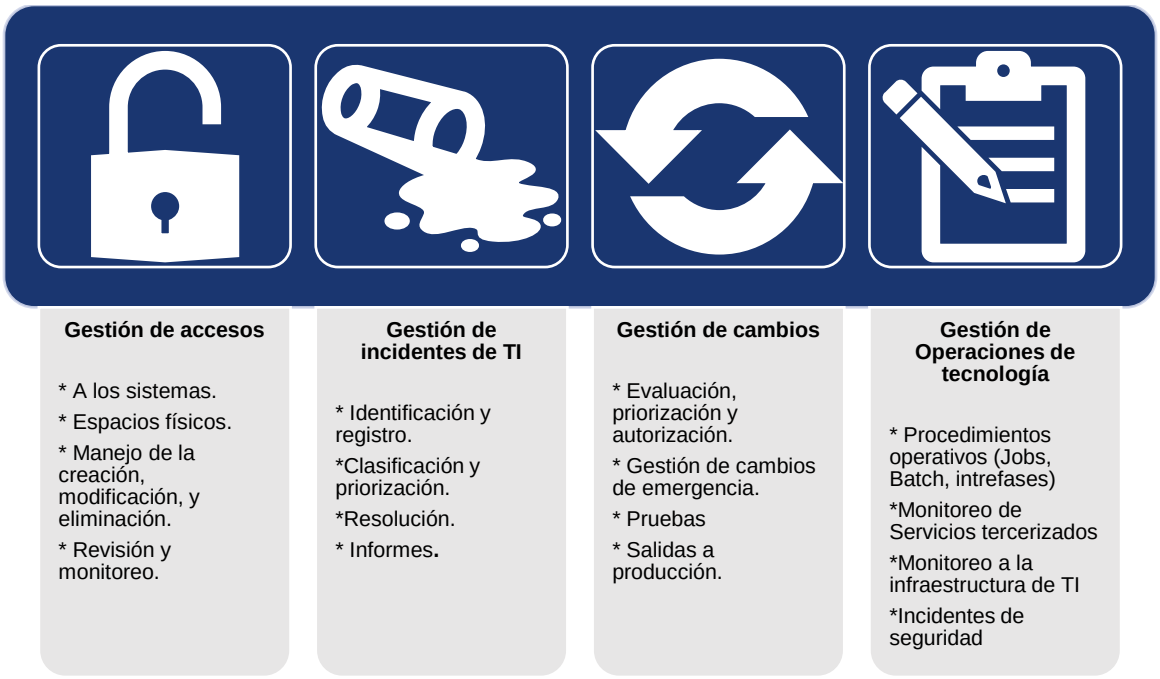
a. Gestión de accesos.

El control de acceso a la información, a los sistemas, es decir acceso lógico, así como a los lugares físicos donde se almacena la información debe ser garantizado por los equipos de tecnología a partir de la implementación de controles que aseguren quién en su organización tiene acceso a qué sistemas y datos, basado en las funciones de cada cargo; esto teniendo en cuenta que los empleados de su organización tienen más conocimientos sobre los procesos, sistemas y controles internos implementados, con este conocimiento, pueden hacer más daño a los sistemas y datos que alguien de fuera de su organización.

Tradicionalmente, las empresas se basan en controles genéricos de aprovisionamiento y des provisionamiento de usuarios, y en revisiones periódicas de alto nivel de los usuarios para mitigar los riesgos relacionados con el acceso no autorizado a datos financieros sensibles. Las mejores prácticas han sugerido que las áreas de control interno que gestionan el cumplimiento de la Ley SOX identifiquen los datos maestros clave, identifiquen a los propietarios de los datos y desarrollen controles sobre la concesión, eliminación y recertificación periódica del acceso a estos datos (Chiu, 2015).

El control de acceso también incluye la seguridad física donde el acceso al centro de datos sea solo a través de un sistema de tarjetas y que este asignado a un número limitado de empleados.

Ilustración 6. Controles Generales de Tecnología (ITGC's)



Fuente: Elaboración propia basada en IT Compliance Training – Sarbanes Oxley (SOX) ITGC, Audit Concepts and Coordination.

La administración de accesos debe contemplar como mínimo los controles relacionados en la Tabla 10.

Tabla 9. Controles para la gestión de accesos

Proceso	Riesgo	Control a implementar
Gestión de accesos	Personas no autorizadas tienen acceso a los sistemas y datos clave de la empresa	1. Documentación de la administración de los accesos.
		2. Procedimiento para asignar, retirar o modificar accesos.
		3. Monitoreo de Logs de actividad de usuarios.
		4. Configuración de contraseñas en aplicaciones.
		5. Acceso de super usuarios.
		6. Validación periódica de accesos.
		7. Asignación de nuevos roles.
		8. Acceso físico al centro de datos.

Fuente: Elaboración propia basada en Sarbanes-Oxley (SOX) ITGC Audit Concepts and Coordination (Udemy Business, 2022)

El gran reto del control de accesos es evitar que existan accesos de forma inadecuada a los sistemas de la empresa, se debe asegurar que la creación, la modificación, las bajas y cuentas especiales se realice adecuadamente. El control de acceso está basado en roles con la regla del menor privilegio, donde cada usuario este limitado a hacer lo que le corresponde, más allá de eso puede poner en riesgo la información.

De igual forma se debe controlar que los usuarios administradores en ninguna circunstancia sean utilizados para temas transaccionales.

b. **Gestión de Operaciones de tecnología.**

El objetivo del ITGC de operaciones es “coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados, así como incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas” (ISACA, 2019).

Dentro de las actividades realizadas para garantizar la entrega del servicio se encuentra el monitoreo de Jobs, la definición de *backups,* la gestión de incidentes de seguridad, así como el monitoreo del ambiente de control de los proveedores de servicios tercerizados.

Dentro de la gestión de *backups* se deben considerar los controles para realizar pruebas a estos con el fin de garantizar que cuando se vaya a utilizar la información se encuentre disponible, esto debido a que son eventos aislados incrementa la posibilidad que cuando se requiera no sea posible utilizarlo, por diferentes razones, por lo que se debe validar que la información que se tendrá disponible es la que se necesita.

La gestión de las operaciones de tecnología debe contemplar como mínimo los controles relacionados en la tabla 11.

Tabla 10. Controles para la gestión de operaciones de tecnología

Proceso	Riesgo	Control a implementar
Gestión de las operaciones de tecnología	Pérdida de integridad y/o exactitud de los datos financieros por fallas no identificadas o no resueltas durante la ejecución de tareas programadas.	Copias de respaldo sobre plataforma tecnológica
		Pruebas de restauración de copias de respaldo
		Monitoreo de procesos automáticos (*Batch, jobs)*
		Monitoreo de cumplimiento SLA con Terceros.
		Gestión con proveedores de TI (Certificación control interno TI- SOC1 tipo 2)
		Gestión de incidentes de seguridad de la información / ciberseguridad

Fuente: Elaboración propia basada (Udemy Business, 2022).

Otro de los puntos más importantes contemplados en este ITGC es la revisión del ambiente de control de los proveedores tercerizados, monitoreando que se cuenten con los reportes SOC que lo aseguran.

El monitoreo a los servicios de terceros se encuentra relacionado en el ITGC de operaciones, no obstante, teniendo en cuenta la relevancia de este debido a la creciente demanda de servicios de tercerización, que obliga a las empresas a asegurarse de que sus proveedores de soluciones tienen controles fiables, se hace una contextualización más profunda al respecto.

Los informes de controles de sistemas y organizaciones (SOC – *System and Organization Controls)* son la pieza clave para conocer y evaluar que tan robusto o confiables son los entornos de control interno de los proveedores de software (Booth, 2021)

Incluso si una organización no está comprando una nueva aplicación alojada en la nube, los informes SOC continúan teniendo importancia para el ambiente de control interno, ya que las aplicaciones de software están en continua evolución. Se requiere entonces asegurarse que las modificaciones o actualizaciones del ambiente de control de los servicios tercerizados sean probados y correctamente documentados en los reportes

SOC. Realizar actualizaciones al ambiente de control es una situación permanente, por lo que las empresas deben asegurarse de cada modificación o actualización se documente y pruebe de manera adecuada, ya que los fallos de control pueden, de manera inevitable, dar lugar a errores o inefectividades en el ambiente de control interno en los estados financieros de una empresa (Booth, 2021)

Teniendo todo esto en cuenta, a continuación, se mencionan los tipos de informes SOC que suelen emitirse para los productos de software, cómo entenderlos y qué buscar.

Desarrollado por el Instituto Americano de Contadores Públicos, “un informe SOC es un informe de auditoría emitido por una empresa de contadores públicos que presenta una opinión sobre los controles de una organización de servicios” (Booth, 2021)

Los informes SOC son una herramienta fundamental para evaluar a los proveedores de SaaS *(Software as a Services),* tenido en cuenta que quienes contratan sus servicios no pueden controlar ni tienen visibilidad del código que tienen configurado los sistemas.

Tanto los clientes, los auditores como los inversores necesitan saber que cuentan con servicios de proveedores de software con un ambiente de control seguro y confiable, por lo que se basan en el informe SOC para asegurarse de esto. (Booth, 2021)

Actualmente se reconocen tres tipos de informes SOC, como se observa en la tabla 12, cada uno con alcances diferentes.

Tabla 11. Tipos de reportes SOC.

SOC1		SOC2		SOC3
Tipo 1	**Tipo 2**	**Tipo 1**	**Tipo 2**	
Evaluación de los controles financieros de una	Mismo cubrimiento del Tipo1, en este las pruebas se realizan por un periodo de tiempo (6 meses o 1 año), por esta	Es una evaluación de la existencia	Es una evaluación de la eficacia de	Con detalles menos específicos, puede notificarse a un grupo más amplio. No cuenta con una

organización a partir de una fecha concreta	razón el tipo 2 es más riguroso y consta de más información sobre la eficacia de los controles del proveedor	de controles	los controles	el detalle de las pruebas de los controles ni de los resultados del auditor de servicios

Fuente: Elaboración propia basado en (Booth, 2021)

El informe SOC 1 tiene el Tipo 1 y Tipo 2, el tipo 1 contiene el resultado de la evaluación del ambiente de control financiero desde una fecha específica; por su lado el tipo 2, que, aunque también abarca los controles internos sobre la información financiera, la prueba es realizado durante un periodo de tiempo (como seis meses o un año). (Booth, 2021); al abarcar un periodo de tiempo frente a un momento determinado, este informe es más riguroso y relaciona información más detallada de la eficacia del ambiente de control del proveedor.

Para una empresa que confía en los controles del proveedor el reporte SOC 1 tipo 2 resulta más conveniente ya que confirma que los controles están definidos y funcionan eficazmente en su organización durante todo el periodo completo (Booth, 2021)

Confiar en los reportes SOC de los terceros permite a los usuarios tener claridad sobre al ambiente de control del tercero y usar este para replicarlo en los controles a ejecutar internamente (Booth, 2021)

Lo anterior puede ser considerado como una disminución de costos en la empresa, si en vez de realizar una documentación por parte de una persona, se puede confiar en los controles probados y que son reportados en el informe SOC. (Booth, 2021).

Los otros dos reportes el SOC 2 y el SOC 3 se enfocan en los controles del tercero proveedor del servicio relacionados con la seguridad, la disponibilidad, la integridad del procesamiento, y la confidencialidad o privacidad. Existen 2 tipos, el 1, que consiste en una valoración de los controles definidos, el tipo 2, es una evaluación del correcto funcionamiento de los controles definidos.

Los reportes SOC 2 y SOC 3 centran su diferencia en que los SOC 3 contienen menos detalle, son distribuidos a un público más extenso y no cuentan con la especificidad de las pruebas de los controles ni de la conclusión del auditor de servicios (Booth, 2021).

Para las aplicaciones tecnológicas, el reporte SOC 1tipo 2 es excelente ya que se enfoca en los controles sobre la información financiera durante un periodo de tiempo, no obstante, los informes SOC 2 o 3 se pueden considerar completos para los sistemas utilizados para funciones aparte de la información financiera (Booth, 2021).

Tanto si recibe un informe SOC como parte de la evaluación de un nuevo proveedor, como si obtiene el último informe de su proveedor actual, hay tres elementos importantes que debe buscar en el informe:

¿Quién emitió el informe? Para cumplir con los criterios del AICPA (Instituto Americano de Contables Públicos Certificados), los reportes SOC requieren ser generados por contadores públicos registrados y autorizados. Con el fin de asegurar la imparcialidad de su informe, los contadores deben ser auditores sin relación de ningún tipo con el tercero prestador del servicio (Rodríguez, 2021).

Las compañías contratantes del servicio de terceros deben validar y asegurarse que el reporte SOC entregado ha sido generado por una firma certificada como Auditor Certificado de Sistemas de Información o Certificado en Control de Riesgos y Sistemas de Información, estas certificaciones, unida con la asignación del contador público autorizado, reúnen el nivel de conocimiento suficiente para realizar una evaluación eficaz al proveedor (Rodríguez, 2021)

¿Cuál es la opinión del auditor? La auditoría independiente y sus reportes darán uno de los tres tipos de las conclusiones de auditoría: sin reservas, con reservas o adversa; difícilmente, las firmas auditorias entregarán una opinión con descargo de responsabilidad.

Lo ideal es que el reporte SOC del prestador de servicios, tenga una revisión y conclusión sin reservas, es decir, que el proveedor logra cumplir o sobrepasa las características de la evaluación sin alteración alguna, en algunos casos existirán excepciones, que no deberían ser lo suficientemente importantes como para que se dé una opinión con algún grado de reservas, cuando se tiene una conclusión sin reservas se entiende que se tiene una opinión de auditoría "limpia" (Rodríguez, 2021).

¿Cuáles eran los objetivos de control? El reporte SOC del tercero debe relacionar un detalle específico de cada uno de los objetivos de control, de las actividades de control que fueron evaluadas y la conclusión del auditor sobre su eficacia (Rodríguez, 2021)

Otros procedimientos para evaluar. Entre otros informes valiosos, un compromiso de procedimientos acordados es otra capa de informes y procedimientos que se debe pedir a un proveedor para garantizar el valor y el cumplimiento de una solución. Un compromiso de procedimientos acordados se realiza de acuerdo con las normas del AICPA.

Un CPA cualificado realiza procedimientos específicos e informa de los resultados sin proporcionar una opinión o conclusión. Dado que la parte del encargo es la que mejor conoce sus propias necesidades, está de acuerdo con los procedimientos y reconoce su idoneidad para el objetivo previsto del encargo.

Los usuarios previstos evalúan los procedimientos y resultados comunicados por el contador público y extraen sus propias conclusiones del trabajo realizado. (Rodríguez, 2021)

El resultado final. La revisión de los informes SOC y otros procedimientos de los posibles proveedores debería ser una parte estándar de cualquier proceso de compra de software de contabilidad. Y como muchos siguen trabajando desde casa, es más

importante ahora que nunca confirmar que nada de lo que figura en el informe SOC de un proveedor ha fallado en el entorno de control.

Aunque los cambios en los controles son bastante inevitables y está perfectamente bien que se produzcan, las organizaciones de servicios deben documentar todos los cambios y comprobar los nuevos controles (Rodríguez, 2021)

Como las soluciones SaaS (Software as a Services) son cada vez más importantes para los departamentos de contabilidad de hoy en día, mantenerse alerta y asegurarse de que los proveedores comunican y comparten de forma proactiva sus informes SOC, cartas puente, compromisos AUP y otros datos relevantes establece aún más su fiabilidad a largo plazo.

a. Gestión de Cambios

Los controles de cambio de la aplicación implican procesos para realizar cambios en el código actualizando o instalando nuevo software, o realizando cambios a las bases de datos u otros componentes de la arquitectura de la información.

El ciclo de vida de desarrollo de software (SDLC – por sus siglas en inglés) debe ser debidamente documentado, aprobado, testeado y documentado antes de pasar a ambiente de producción para garantizar que los cambios a implementar tendrán los resultados esperados y no afectarán la continuidad del negocio.

De igual forma, es posible que por diferentes razones la implementación no salga como se planeó es mandatorio tener un plan para realizar un *rollback,* es decir volver al lugar donde se estaba y estabilizar el proceso.

Cualquier actualización significativa del sistema o una nueva implementación que afecte a los procesos de negocio críticos que soportan los elementos financieros debe tener en cuenta el control más allá de los controles de cambio de la aplicación (Udemy Business, 2022).

Otro de los aspectos que se encuentran incluidos en la gestión de cambios son los proyectos de migración de datos de un sistema antiguo a un sistema nuevo, proceso que debe ser documentado y asegurándose de mantener toda la información sobre la estrategia de migración.

El control de cambios buscar asegurar que no se altere la configuración de forma inapropiada, garantizando que no se haga ningún cambio de paso a producción, sin que se haga un análisis del riesgo.

Tener un registro de lo que se ha cambiado, además de cuándo se ha cambiado, quién lo ha cambiado, cómo se ha probado y quién lo ha aprobado, simplifica una auditoría SOX ITGC y facilita la corrección de los problemas cuando llegan.

La gestión de los cambios debe contemplar como mínimo los controles relacionados en la tabla 13.

Tabla 12. Controles para la Gestión de cambios

Proceso	Riesgo	Control a implementar
Gestión de cambios	Pérdida de disponibilidad, integridad y/o exactitud de los estados financieros debido a cambios no autorizados o no controlados en los componentes de TI.	Administración de cambios (Pruebas, *rollback,* aprobación, documentación
		Segregación de Ambientes de TI
		Cambios de emergencia
		Migración de datos

Fuente: Elaboración propia basada en Sarbanes-Oxley (SOX) ITGC Audit Concepts and Coordination (Udemy Business, 2022)

b. Gestión de incidentes.

El objetivo de este ITGC es que los incidentes que se presenten estén bien administrados y gestionados, teniendo en cuenta que cuando estos se presentan provocan interrupciones, indisponibilidades o retrasos en los sistemas, servicios o procesos.

La administración de los incidentes consiste en detectarlos y resolverlos a tiempo, siguiendo el proceso definido en la política correspondiente creada por la compañía para dicho fin.

Al final del ejercicio el ITGC de incidentes busca tener la menor afectación posible en la operación de las empresas lo cual la puede darse a nivel operacional, económico y/o reputacional.

La gestión de los cambios debe contemplar como mínimo los controles relacionados en la tabla 14.

Tabla 13. Controles para la Gestión de Incidentes

Proceso	Riesgo	Control a implementar
Gestión de incidentes	Pérdida de disponibilidad de los sistemas o datos financieros, debido a incidentes no gestionados efectiva y oportunamente.	Administración de incidentes (Registrados, priorizados, escalados, documentados y resueltos)

2. Controles de aplicación

El otro de los requerimientos de la ley SOX para el ambiente tecnológico es la definición de los controles de aplicación que son un subconjunto de controles internos que se refieren a un sistema de aplicación y la información que gestiona dicha aplicación, es decir, aquellas tareas manuales y/o automáticas que garantizan que la información reúne ciertas características que demuestran la completitud, exactitud, precisión, validez e integridad de la data al realizar las transacciones a través de las aplicaciones

informáticas durante las etapas de entrada, procesamiento y salida de sistemas de información (ISACA, 2014).

Los controles de aplicación son todas las políticas, procedimientos y actividades que se crean para asegurar el logro de los objetivos para determinadas soluciones automatizadas (ISACA, 2014).

Las organizaciones dependen en gran medida del tratamiento automatizado de la información por parte de una serie de aplicaciones que son la fuente para la creación y generación de los estados financieros. Prácticamente cada aspecto de la transaccionalidad empresarial diaria tiene una gran dependencia de datos oportunos, precisos y fiables, datos que son generados, procesados, acumulados, almacenados y comunicados por aplicaciones informáticas automatizados (ISACA, 2014)

Los clientes, los proveedores, los empleados, los directivos, los mandos intermedios, los directivos, los accionistas y todas las demás partes interesadas toman decisiones basadas en la información que reciben, una información cuya integridad y fiabilidad dependen casi exclusivamente de los sistemas de aplicación y los procesos de control que se utilizan para procesar la información (ISACA, 2014).

Estas decisiones sólo pueden ser tan buenas como la eficacia de los datos y de la información que sustenta las decisiones de las directivas. Unos controles inadecuados integrados en una aplicación provocarían con toda probabilidad una declaración errónea de los resultados financieros (ISACA, 2014)

Los controles de las aplicaciones son los que permiten alcanzar los objetivos empresariales de información oportuna, precisa y fiable, sirviéndose de transacciones o actividades manuales y/o automáticas que garantizan que la información este alineada con las características de la información que el marco COBIT llama “requisitos de negocio” tales como efectividad, eficiencia, confidencialidad, integridad, disponibilidad,

cumplimiento y confiabilidad y que se relacionan directamente con las aserciones de los estados financieros.

De esta forma los controles de aplicación son aquellos controles que se extienden a los sistemas y los procesos empresariales que contribuyen a las aserciones de los estados financieros, incluyendo la integridad, la exactitud controles de valoración y autorización, en la tabla 15 se resumen las definiciones y algunos ejemplos de estas aserciones de los estados financieros.

Tabla 14. Definiciones y ejemplos de afirmaciones de estados financieros

Afirmaciones de los estados financieros	Definición	Ejemplo
Existencia	"Las afirmaciones sobre la existencia o la ocurrencia se refieren a si los activos o pasivos de la entidad existen en una fecha determinada y si las transacciones registradas han ocurrido durante un período determinado" (ISACA, 2014)	"La dirección afirma que las existencias de las existencias de productos terminados en el balance están disponibles para la venta. Del mismo modo, la dirección afirma que las ventas en la cuenta de resultados representan el intercambio de bienes o servicios con clientes a cambio de dinero en efectivo u otra contraprestación" (ISACA, 2014).
Completitud	"Las afirmaciones sobre la integridad abordan si todas las transacciones y cuentas que deben ser que deben presentarse en los estados en los estados financieros" (ISACA, 2014).	"La dirección afirma que todas las compras de bienes y servicios se registran y se incluyen en los estados financieros estados financieros. Del mismo modo, la dirección afirma que los efectos a pagar en el balance de cuentas incluyen todas las obligaciones de la entidad" (ISACA, 2014).
Valuación	"Las afirmaciones sobre la valoración o asignación abordan si el activo, pasivo, patrimonio, ingresos y componentes de los gastos se han incluidos en los estados financieros en las cantidades adecuadas" (ISACA, 2014)	"La dirección afirma que los bienes se registran al coste histórico y que dicho coste se asigna sistemáticamente a los períodos contables adecuados. Del mismo modo, la dirección afirma que los créditos comerciales incluidos en el balance se contabilizan por su valor neto de realización. Los estados financieros están correctamente clasificados y descritos" (ISACA, 2014).

Fuente: (ISACA, 2014)

Si bien es cierto los controles generales de tecnología y los controles de aplicación están estrechamente relacionados, es importante indicar que, aunque puede ser que los controles generales de tecnología trabajen correctamente, esto no da seguridad que los controles de aplicación sean adecuados, por el contrario, si los controles generales tienen evaluaciones negativas, lo más seguro es que los controles de aplicación también lo serán. (ISACA, 2014).

Los controles automáticos están integrados en las aplicaciones de los procesos empresariales que apoyan directamente los objetivos de control financiero. Pueden encontrarse en la mayoría de las aplicaciones financieras, incluyendo grandes sistemas como SAP y Oracle, así como sistemas más pequeños como el ERP Sage 300.

Se establecen para proporcionar una seguridad razonable del logro de los objetivos que la gerencia define sobre las aplicaciones a través de actividades manuales y/o automatizadas que aseguran que la información cumple con ciertos criterios, los que COBIT refiere como requerimientos de negocio para la información tales como efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

7.1.1 Análisis del Marco de gobernabilidad de tecnología COBIT como base para el cumplimiento de los requerimientos tecnológicos de la ley SOX.

COBIT 2019 y la Ley SOX

COBIT 2019 permite gobernar y gestionar las TI de forma general para toda la empresa, teniendo en cuenta todas las áreas donde tienen responsabilidad negocio y el área de TI.

El marco de referencia COBIT para la gobernabilidad de la tecnología, como se explicó en el marco conceptual, está conformado por 40 principios que contemplan la gobernabilidad y la gestión de los procesos, de los cuales para cumplimiento del objetivo

de este numeral se analizarán aquellos que impactan directamente con los requerimientos de la ley SOX vistos en el numeral anterior.

El objetivo es establecer una hoja de ruta para el cumplimiento de los objetivos y responsabilidades de TI en apoyo del ICFR (Control interno para el reporte financiero). Entender cómo se aplica el cumplimiento de la SOX a una empresa, basándose en sus características comerciales, ayuda a desarrollar el programa de control interno de la empresa. Muchas unidades funcionales dentro de TI entran en juego a la hora de garantizar el adecuado cumplimiento de la SOX.

Las empresas más grandes se enfrentan a retos en la aplicación de la ley SOX que son distintos de los de las empresas más pequeñas. Además, en la medida en que ya se ha establecido un marco de control interno sólido tiene una influencia significativa en las actividades de información financiera.

El análisis se realiza para cada uno de los dos objetivos y sus cincos dominios donde se identifican si existen o no objetivos que vayan directamente relacionados con cada uno de los requisitos de cumplimiento de la ley SOX a saber, ELC o controles a nivel de entidad, ITGC o controles generales de tecnología, ambientes de control de los servicios tercerizas y los controles de aplicación.

1. **Análisis del Marco de gobernabilidad de tecnología COBIT relacionado con los controles a nivel de entidad ELC.**

El marco de referencia COBIT contempla de manera muy amplia la administración de los controles a nivel de entidad (ELC por sus siglas en inglés).

Los ELC se encuentran referenciados en tres de los dominios. El primero de ellos es el EDM – Evaluar, Orientar y Supervisar como se observa en tabla 16.

Tabla 15. COBIT y los controles a nivel de entidad – Dominio EDM

Controles a Nivel de Entidad (ELC)

Principios COBIT	EDM - Evaluar, Orientar y Supervisar EDM01 - Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno EDM03 - Asegurar la Optimización del Riesgo EDM05 - Asegurar la Transparencia hacia las Partes Interesadas
Control	**Actividad**
EDM01.01 Evaluar el sistema de gobierno.	"Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y evaluar el diseño actual y futuro del gobierno de I&T empresarial". (ISACA, 2019)
EDM03.01 Evaluar la gestión de riesgos	"Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado" (ISACA, 2019).
EDM03.02 Orientar la gestión de riesgos	"Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo" (ISACA, 2019).
EDM03.03 Supervisar la gestión de riesgos	"Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución" (ISACA, 2019).
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes	"Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas" (ISACA, 2019).
EDM05.03 Supervisar la comunicación con las partes interesadas	"Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles a nivel de entidad tomado de (ISACA, 2019).

En la tabla 17, se relaciona el otro de los dominios que contempla los ELC que es el APO – Alinear, Planificar y Organizar

Tabla 16. COBIT y los controles a nivel de entidad - Dominio APO

Controles a Nivel de Entidad (ELC)	
Principios COBIT	**APO- Alinear, Planificar y Organizar**
	APO01- Gestionar el Marco de Gestión de TI
	APO02 - Gestionar la Estrategia

	APO07 - Gestionar los Recursos Humanos
	APO11 - Gestionar la Calidad
	APO12 - Gestionar el Riesgo
APO01.02 Establecer roles y responsabilidades	“Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante” (ISACA, 2019).
APO01.03 Mantener los elementos catalizadores del sistema de gestión	“Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos)” (ISACA, 2019).
APO01.04 Comunicar los objetivos y la dirección de gestión	“Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa” (ISACA, 2019).
APO01.06 Definir la propiedad de la información (datos) y del sistema.	“Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación” (ISACA, 2019).
APO01.08 Mantener el cumplimiento con las políticas y procedimientos.	“Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control” (ISACA, 2019).
APO02.01 Comprender la dirección de la empresa	“Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia)” (ISACA, 2019).
APO02.05 Definir el plan estratégico y la hoja de ruta	“Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel” (ISACA, 2019).
APO02.06 Comunicar la estrategia y la dirección de TI	“Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa” (ISACA, 2019).
APO07.01 Mantener la dotación de personal suficiente y adecuada.	“Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos” (ISACA, 2019).

APO07.03 Mantener las habilidades y competencias del personal	"Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales" (ISACA, 2019).
APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	"Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI" (ISACA, 2019).
APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor	"Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y tratar las incidencias identificadas" (ISACA, 2019).
APO11.01 Establecer un sistema de gestión de calidad (SGC)	"Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo" (ISACA, 2019).
APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	"Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Este debería estar en consonancia con los requisitos del marco de control TI. Considerar la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave" (ISACA, 2019).
APO11.03 Enfocar la gestión de la calidad en los clientes	"Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad" (ISACA, 2019).
APO11.06 Mantener una mejora continua	"Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Esto debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de mejora continua de la calidad" (ISACA, 2019).
APO12.01 Recopilar datos	"Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI" (ISACA, 2019).
APO12.02 Analizar el riesgo	"Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo" (ISACA, 2019).
APO12.03 Mantener un perfil de riesgo	"Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados" (ISACA, 2019).
APO12.04 Expresar el riesgo	"Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las

	partes interesadas necesarias para una respuesta apropiada" (ISACA, 2019).
APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	"Gestionar las oportunidades para reducir el riesgo aun nivel aceptable como un portafolio" (ISACA, 2019).
APO12.06 Responder al riesgo	"Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles a nivel de entidad tomado de (ISACA, 2019).

El último de los dominios que contempla el marco para referenciar los ELC como se relaciona en la tabla 18 es el dominio MEA – Supervisar, Evaluar y Valorar.

Tabla 17. COBIT y los Controles a nivel de entidad - Dominio MEA

Controles a Nivel de Entidad (ELC)	
Principios COBIT	**MEA - Supervisar, Evaluar y Valorar**
	MEA01 - Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad
	MEA02 - Supervisar, Evaluar y Valorar el Sistema de Control Interno
	MEA03 - Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos
Control	**Actividad**
MEA01.01 Establecer un enfoque de la supervisión.	"Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía" (ISACA, 2019).
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento.	"Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento" (ISACA, 2019).
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento	"Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio" (ISACA, 2019).
MEA01.04 Analizar e informar sobre el rendimiento	"Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión" (ISACA, 2019).
MEA01.05 Asegurar la implantación de medidas correctivas	"Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías" (ISACA, 2019).

MEA02.01 Supervisar el control interno.	"Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos" (ISACA, 2019).
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.	"Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias" (ISACA, 2019).
MEA02.04 Identificar y comunicar las deficiencias de control.	"Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas" (ISACA, 2019).
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados	"Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales" (ISACA, 2019).
MEA02.06 Planificar iniciativas de aseguramiento	"Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía" (ISACA, 2019).
MEA02.07 Estudiar las iniciativas de aseguramiento.	"Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento" (ISACA, 2019).
MEA02.08 Ejecutar las iniciativas de aseguramiento	"Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno" (ISACA, 2019).
MEA03.01 Identificar requisitos externos de cumplimiento.	"Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI" (ISACA, 2019).
MEA03.02 Optimizar la respuesta a requisitos externos.	"Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles a nivel de entidad tomado de (ISACA, 2019).

2. Análisis del Marco de gobernabilidad de tecnología COBIT relacionado con los controles generales de tecnología ITGCs.

Desde los controles generales de tecnología se busca abordar y dar cumplimiento a cuatro frentes, la gestión de accesos, la gestión de cambios, la gestión de las operaciones de TI y la gestión de incidentes, en ese sentido a continuación se relaciona como el marco COBIT abarca cada uno de estos.

- **COBIT y la administración de accesos.**

La administración de accesos se contempla dentro del marco de referencia COBIT y se encuentra presente en tres de sus principios.

Se encuentra presente en los principios de entrega de Alinear, Planificar y Organizar (APO), Construir, adquirir e implementar (BAI) y Entregar, Dar Servicio y Soporte (DSS), como se muestra en la tabla 19.

Siguiendo el hilo conductor de COBIT, en primera instancia en el principio APO, se gestiona el personal contratado y se establecen roles y responsabilidades desde el momento de su contratación para asegurar que se conocen los riesgos de un uso incorrecto del acceso otorgado. (ISACA, 2019)

El segundo principio que se relaciona con la administración de accesos tiene que ver con la gestión de la construcción de soluciones que es el ciclo de desarrollo de software, donde se deben segregar las funciones para que existan procesos que se ejecuten siguiendo los niveles de aprobación requeridos por el personal autorizado para quienes cuyos accesos se encuentran limitados de acuerdo con los niveles asignados.

Por último, se encuentra el principio de la entrega de servicio y soporte, donde se gestionan los accesos físicos y lógicos, así como el acceso a documentos sensibles.

Con base en lo anterior COBIT logra a través de sus principios abarcar los principales requerimientos para la administración de accesos que sugiere SOX.

Tabla 18. COBIT y la administración de accesos

Administración de accesos	
Principios COBIT	**APO: Alinear, Planear y Organizar**
	APO07 - Gestionar los Recursos Humanos **APO01 - Gestionar el Marco de Gestión de TI**
	BAI: Construir, adquirir e implementar
	BAI03 - Gestionar la Identificación y Construcción de Soluciones
	DSS: Entrega, Servicio y Soporte
	DSS05 - Gestionar Servicios de Seguridad **DSS06 - Gestionar Controles de Proceso de Negocio**
Control	**Actividad**
APO07.06 Gestionar el personal contratado.	"Al inicio del contrato, obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de I&T empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación" (ISACA, 2019).
	"Implementar las políticas y procedimientos del personal contratado" (ISACA, 2019).
	"Como parte de sus contratos, proporcionar a los contratistas una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados" (ISACA, 2019).
APO01.05 Establecer roles y responsabilidades.	"Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa. Delinear claramente las responsabilidades y la rendición de cuentas, especialmente para la toma de decisiones y aprobaciones" (ISACA, 2019).
	"Incluir requisitos específicos en las descripciones de roles y responsabilidades relativos al cumplimiento de las políticas y procedimientos de gestión, el código ético y las prácticas profesionales" (ISACA, 2019).
	"Implementar las prácticas de supervisión adecuadas para asegurar que los roles y responsabilidades se ejerzan adecuadamente, para asegurar que todo el personal tiene la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades, y de forma general, para revisar el rendimiento. El nivel de supervisión debe alinearse con la sensibilidad del puesto y la extensión de las responsabilidades asignadas" (ISACA, 2019)
	"Estructurar roles y responsabilidades para reducir la posibilidad de que un único rol comprometa un proceso crítico" (ISACA, 2019).
	"Asegurar que se defina la rendición de cuentas a través de roles y responsabilidades" (ISACA, 2019).
	"Proporcionar información al proceso de continuidad de servicios de I&T, manteniendo la información de contacto y las descripciones de roles de la empresa actualizados" (ISACA, 2019).
BAI03.03 Desarrollar los componentes de la solución.	"Garantizar que las responsabilidades de usar componentes de infraestructura de alta seguridad o de acceso restringido estén claramente definidas y sean comprendidas por aquellos que desarrollan e integran los

	componentes de infraestructura. Es necesario monitorizar e informar sobre su uso" (ISACA, 2019).
DSS05.04 Gestionar la identidad del usuario y el acceso lógico	"Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer" (ISACA, 2019).
	"Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección" (ISACA, 2019).
	"Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas. Asegurar la supervisión de todas las actividades en estas cuentas" (ISACA, 2019).
	"Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio" (ISACA, 2019).
	"Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente" (ISACA, 2019).
	"Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca" (ISACA, 2019).
	"Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios" (ISACA, 2019).
	"Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados" (ISACA, 2019)
DSS05.05 Gestionar el acceso físico a los activos de TI	"Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores" (ISACA, 2019).
	"Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento" (ISACA, 2019).
	"Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones" (ISACA, 2019).
	"Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores" (ISACA, 2019).
	"Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo" (ISACA, 2019).
	"Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades" (ISACA, 2019).
	"Realizar formación sobre concienciación de la seguridad de la información física de forma regular" (ISACA, 2019).

DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	“Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio” (ISACA, 2019).
	“Asignar niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados” (ISACA, 2019).
	“Asignar roles para actividades sensibles para que haya una clara segregación de funciones” (ISACA, 2019).
	“Asignar derechos de acceso y privilegios basado en lo mínimo requerido para realizar las actividades laborales, conforme a roles de trabajo predefinidos. Eliminar o revisar derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso sea adecuado para las amenazas, riesgo, tecnología y necesidades empresariales actuales” (ISACA, 2019).
	“Concienciar y formar regularmente sobre los roles y responsabilidades, para que todos entiendan sus responsabilidades; la importancia de los controles; y la seguridad, integridad, confidencialidad y privacidad de la información de la compañía en todas sus formas” (ISACA, 2019).
	“Garantizar que los privilegios administrativos están asegurados, rastreados y controlados de forma suficiente y eficaz para prevenir el mal uso” (ISACA, 2019).
	“Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción. Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados” (ISACA, 2019).

Fuente: Elaboración propia basada en (ISACA, 2019) Fuente: Relación de las actividades de los dominios de COBIT aplicable a gestión de accesos tomado de (ISACA, 2019).

- **COBIT y la administración de cambios**

La administración de cambios se contempla dentro del marco de referencia COBIT y se encuentra presente en el principio BAI - Construir, adquirir e implementar a través de dos de sus prácticas de gestión, como se muestra en la tabla No. 20.

Este principio está enfocado específicamente en la gestión y el manejo de los cambios, tal como lo definen los controles generales de tecnología ITGC, la gestión de cambios está asociada al ciclo de vida del desarrollo del software con los pasos que lo componen como se observa en la ilustración 9.

Ilustración 7. COBIT 2019 y la administración de cambios

Fuente: Elaboración propia

Tabla 19. COBIT y la administración de cambios

Administración de cambios	
Principios COBIT	**BAI: Construir, adquirir e implementar**
Prácticas de Gestión	**BAI06- Gestionar los Cambios** **BAI07- Gestionar la Aceptación del Cambio y la Transición**
Control	**Actividad**
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio	"Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio" (ISACA, 2019).
	"Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados" (ISACA, 2019).
	"Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio" (ISACA, 2019).
	"Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados. Evaluar la probabilidad de que afecten negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, legales, contractuales, y de cumplimiento normativo del cambio solicitado. Considerar además todas las inter-dependencias entre cambios. Involucrar a los propietarios de procesos de negocio en el proceso de evaluación, de forma apropiada" (ISACA, 2019).
	"Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser preaprobados como cambios estándar" (ISACA, 2019).
	"Planificar y programar todos los cambios aprobados" (ISACA, 2019).

	“Considerar el impacto en los proveedores de servicios contratados (ej. procesamiento de negocio externalizado, infraestructuras, desarrollo de aplicaciones y servicios compartidos) en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANSs” (ISACA, 2019).
BAI06.02 Gestionar cambios de emergencia.	“Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia” (ISACA, 2019).
	“Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio” (ISACA, 2019).
	“Supervisar todos los cambios de emergencia y realizar revisiones post-implementación involucrando a todas las partes interesadas. La revisión debería considerar e iniciar acciones correctivas basadas en causas raíz tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos” (ISACA, 2019).
	“Definir qué constituye un cambio de emergencia” (ISACA, 2019).
BAI06.03 Hacer seguimiento e informar de cambios de estado.	“Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados, pero aún no iniciados, aprobados y en proceso y cerrados)” (ISACA, 2019).
	“Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre” (ISACA, 2019).
	“Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo con su prioridad” (ISACA, 2019).
	“Mantener un sistema de seguimiento e informe para todas las peticiones de cambio” (ISACA, 2019).
BAI06.04 Cerrar y documentar los cambios	“Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio” (ISACA, 2019).
	“Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario” (ISACA, 2019).
	“Someter a la documentación a la misma revisión que al cambio en sí mismo” (ISACA, 2019).
BAI07.01 Establecer un plan de implementación.	“Crear un plan de implantación que refleje la estrategia global de implantación, la secuencia de acciones de implantación, recursos necesarios, interdependencias, criterios para la aceptación por parte de la Dirección de la implantación en producción, requisitos para verificar la instalación, estrategia de transición para el soporte en producción, y la actualización de los planes de continuidad de negocio (BCPs)” (ISACA, 2019).
	“Identificar y documentar el proceso de marcha atrás y recuperación” (ISACA, 2019).

BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos	"Definir un plan de migración de procesos de negocio, datos, servicios e infraestructura de TI. Considerar, por ejemplo, hardware, redes, sistemas operativos, software, datos transaccionales, ficheros maestros, copias de seguridad y archivadas, interfaces con otros sistemas (tanto internos como externos), posibles requisitos de cumplimiento y documentación del sistema en el desarrollo del plan.
	Planificar el respaldo de todos los sistemas y datos tomados hasta el instante anterior a la conversión. Mantener registros de auditoría para posibilitar que pueda seguirse la traza de la conversión y asegurar que hay un plan de recuperación que cubra la marcha atrás de la migración y la vuelta al procesamiento anterior, en caso de que la migración fallara" (ISACA, 2019).
BAI07.03 Planificar pruebas de aceptación	"Desarrollar y documentar el plan de pruebas, que esté alineado con el programa, el plan de calidad del proyecto y los estándares organizativos relevantes. Comunicar y consultar con los dueños del proceso de negocio y las partes interesadas de TI apropiadas" (ISACA, 2019).
	"Asegurar que el plan de pruebas refleja la evaluación del riesgo del proyecto y que se prueban todos los requisitos funcionales y técnicos. Con base en la evaluación del riesgo de fallo del sistema y los fallos en la implementación, incluir en el plan requisitos de rendimiento, estrés, usabilidad, piloto, pruebas de seguridad y privacidad" (ISACA, 2019).
	"Confirmar que todos los planes de pruebas cuentan con la aprobación de las partes interesadas, incluidos los dueños del proceso de negocio y de TI, como corresponda. Las partes interesadas podrían incluir a los gestores del desarrollo de aplicaciones, gestores de proyecto y usuarios finales del proceso de negocio" (ISACA, 2019).
BAI07.05 Realizar pruebas de aceptación.	"Garantizar que se llevan a cabo pruebas de los cambios conforme al plan de pruebas. Asegurar que las pruebas han sido diseñadas y ejecutadas por un grupo de pruebas, independiente del equipo de desarrollo. Considerar hasta qué punto están incluidos los dueños de los procesos de negocio y los usuarios finales en el grupo de pruebas. Asegurar que las pruebas se realicen solo dentro del entorno de pruebas" (ISACA, 2019).
	"Cuando se lleven a cabo las pruebas, garantizar que se han considerado los elementos de *fallback* y *rollback* del plan de pruebas" (ISACA, 2019).
BAI07.06 Promover a producción y gestionar las liberaciones *(releases).*	"Prepararse para la transferencia de procedimientos del negocio y servicios de soporte, aplicaciones e infraestructura desde el entorno de pruebas al entorno de producción conforme a los estándares de gestión de cambios organizativos" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles para la gestión de cambios tomado de (ISACA, 2019).

- **COBIT y las operaciones de tecnología**

Dentro del marco COBIT se contempla la gestión de las operaciones en el dominio DSS – Entregar, Dar servicio y Soporte en tres de sus prácticas de gestión, dentro de la cuales se tiene como objetivo "coordinar y ejecutar las actividades y los procedimientos

operativos requeridos para entregar los servicios de I&T, internos y externalizados, así como incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas" (ISACA, 2019).

En la tabla 21, se relacionan cada una de las actividades mencionadas en el marco COBIT y que dan alcance al ITGC de operaciones.

Tabla 20. COBIT y la administración de operaciones

Administración de Operaciones	
Principios COBIT	**DSS - Entregar, Dar Servicio y Soporte**
	DSS01 - Gestionar Operaciones
	DSS04 - Gestionar la continuidad
	DSS05 - Gestionar Servicios de Seguridad
Control	**Actividad**
DSS01.01 Ejecutar procedimientos operativos	"Desarrollar y mantener los procedimientos operativos y las actividades relacionadas para respaldar todos los servicios prestados" (ISACA, 2019).
	"Mantener un calendario de las actividades operativas y ejecutar las actividades" (ISACA, 2019).
	"Comprobar que todos los datos esperados para su procesamiento se reciban y procesen de forma completa, precisa y en el plazo debido. Entregar el producto conforme a los requisitos de la empresa. Soportar las necesidades de reinicios y reprocesamientos. Asegurar que los usuarios reciban los productos adecuados de forma segura y en el plazo debido" (ISACA, 2019).
	"Gestionar el rendimiento y *throughput* de las actividades programadas" (ISACA, 2019).
	"Monitorizar los incidentes y problemas relacionados con los procedimientos operativos y realizar las acciones adecuadas para mejorar la confiabilidad de las tareas operativas ejecutadas" (ISACA, 2019).
DSS01.02 Gestionar servicios tercerizados de I&T.	"Asegurar que los requisitos de los procesos de seguridad de la información de la empresa cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios" (ISACA, 2019).
	"Asegurar que los requisitos de procesamiento operacional del negocio y de TI de la empresa y las prioridades para la prestación de servicios cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios" (ISACA, 2019).
	"Integrar los procesos de gestión de TI internos críticos con los de los proveedores de servicios externalizados. Esto debería cubrir, por ejemplo, la planificación de rendimiento y capacidad, gestión del cambio, gestión de la configuración, solicitud de servicios y gestión de incidentes, gestión de problemas, gestión de la seguridad, continuidad del negocio y monitorización del rendimiento y reporte del proceso" (ISACA, 2019).
	"Planificar una auditoría independiente y el aseguramiento de los entornos operacionales de proveedores que proporcionen servicios externalizados para confirmar que se han abordado de forma adecuada los requisitos acordados" (ISACA, 2019).

	"Asegurar que los requisitos de los procesos de seguridad de la información de la empresa cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios" (ISACA, 2019).
DSS01.03 Monitorizar la infraestructura de I&T.	"Registrar los eventos. Identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento" (ISACA, 2019).
	"Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos" (ISACA, 2019).
	"Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos. Encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria" (ISACA, 2019).
	"Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones" (ISACA, 2019).
	"Garantizar que se creen *tickets* de incidentes en el plazo debido a la hora de monitorizar desviaciones identificadas en los umbrales definidos" (ISACA, 2019).
	"Establecer procedimientos para monitorizar los registros de eventos. Llevar a cabo revisiones regulares" (ISACA, 2019).
DSS04.07 Gestionar acuerdos de respaldo.	"Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido. Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., *disk mirroring* para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios. Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación" (ISACA, 2019).
	"Definir requisitos para el almacenamiento en las instalaciones (*on-site*) y fuera de ellas (off-site) de copias de seguridad de datos, conforme a los requisitos de negocio. Considerar el acceso requerido para hacer copias de seguridad de los datos" (ISACA, 2019).
	"Probar y refrescar de forma periódica los datos archivados y las copias de seguridad de los datos" (ISACA, 2019).
	"Garantizar que se haga una copia de seguridad o se aseguren de forma adecuada los sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros. Considerar que se requiera que los terceros devuelvan las copias de seguridad. Considerar la opción de mantenimiento en fiducia (*escrow*, por su término en inglés) o acuerdos de depósitos" (ISACA, 2019).
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	"Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla por un periodo apropiado para asistir en futuras investigaciones" (ISACA, 2019).
	"Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada" (ISACA, 2019).
	"Revisar regularmente los registros de eventos para detectar incidentes potenciales" (ISACA, 2019).
	"Mantener un procedimiento para la recopilación de evidencias en línea con los procedimientos de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos" (ISACA, 2019).

	“Hay que asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales” (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles para la gestión de operaciones tomado de (ISACA, 2019).

Adicionalmente, el ITGC de operaciones incluye las prácticas y los controles relacionados con la gestión de proveedores donde se incluyen las políticas y procedimientos relacionados con la obtención del soporte que asegure su control interno, conocido como reporte SOC. Los objetivos de control son definidos por el tercero que presta el servicio y deben alinearse con las necesidades de la empresa basado en las tareas ejecutados por el sistema contratado. La referencia de COBIT para los servicios tercerizados se relaciona en la tabla 24.

Tabla 21. COBIT y el control a los servicios tercerizados

Aseguramiento del control interno de los servicios tercerizados	
Principios COBIT	**DSS - Entrega, Servicio y Soporte**
	DSS01 - Gestionar Operaciones
	MEA - Supervisar, Evaluar y Valorar
	MEA02 - Supervisar, Evaluar y Valorar el Sistema de Control Interno
	MEA03 - Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.
Control	**Actividad**
DSS01.02 Gestionar servicios externalizados de TI	“Asegurar que los procesos de información se adhieren a los requerimientos de seguridad de la empresa y conformes con los contratos y ANSs con terceros que alojan o proveen servicios” (ISACA, 2019).
	“Asegurar que los requerimientos operativos del negocio y de procesamiento de TI, así como a las prioridades en la entrega del servicio se adhieren y son conformes a los contratos y ANSs con terceros que alojan o proveen servicios” (ISACA, 2019).
	“Integrar los procesos críticos de gestión interna de TI con los de los proveedores de servicios externalizados cubriendo, por ejemplo, la planificación de la capacidad y el rendimiento, la gestión del cambio, la gestión de la configuración, la gestión de peticiones de servicio y de incidentes, la gestión de problemas, la gestión de la seguridad, la continuidad del negocio y la monitorización y notificación del desempeño de los procesos” (ISACA, 2019).
	“Planificar la realización de auditorías y aseguramientos independiente de los entonos operativos de los proveedores de externalización (outsourcing) para confirmar que los requerimientos acordados están recibiendo el tratamiento adecuado” (ISACA, 2019).
MEA02.01	“Identificar los límites del sistema de control interno de TI (p. ej., considerar cómo los controles internos organizativos de TI toman en consideración las

Supervisar el control interno.	actividades de producción o desarrollo externalizadas y/o deslocalizadas)" (ISACA, 2019).
	"Evaluar el estado de los controles internos de los proveedores externos de servicios y confirmar que dichos proveedores cumplen con los requisitos legales y regulatorios, así como las obligaciones contractuales" (ISACA, 2019).
MEA02.07 Estudiar las iniciativas de aseguramiento.	"Definir el alcance actual mediante la identificación de los objetivos empresariales y de TI para el entorno bajo estudio, el conjunto de procesos y recursos de TI y todas las entidades auditables relevantes dentro de la compañía y externas a la compañía (p. ej. proveedores de servicios), si aplica" (ISACA, 2019).
MEA03.01 Identificar requisitos externos de cumplimiento.	"Valorar el impacto de los requisitos legales y regulatorios relacionados con TI sobre los contractos con terceros que afecten a las operaciones de TI, los proveedores de servicio y los socios de negocio" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a la gestión de operaciones – administración de servicios tercerizados tomado de (ISACA, 2019).

- **COBIT y el manejo de incidentes**

La administración de incidentes tiene como objetivo llevar a cabo todo el flujo de manejo de estos como se relaciona a continuación:

- Identificación
- Registro
- Clasificación y priorización.
- Resolución.
- Informes de gestión

Según lo descrito en la tabla 22, el marco COBIT contempla la gestión de incidentes en el dominio de DSS – Entregar, Dar Servicio y Soporte

Tabla 22. COBIT y la administración de incidentes

Administración de Incidentes	
Principios COBIT	**DSS – Entregar, Dar Servicio y Soporte**
Prácticas de Gestión	**DSS02: Gestionar las Peticiones y los Incidentes del Servicio**
Control	**Actividad**
DSS02.01	"Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas. Usar esta información para

Definir esquemas de clasificación de incidentes y peticiones de servicio	garantizar estrategias constantes a fin de gestionar e informar a los usuarios sobre los problemas y llevar a cabo análisis de tendencias" (ISACA, 2019).
	"Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz" (ISACA, 2019).
	"Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente para solicitudes estándar" (ISACA, 2019).
	"Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad" (ISACA, 2019).
	"Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas" (ISACA, 2019).
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	"Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo" (ISACA, 2019).
	"Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría" (ISACA, 2019).
	"Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio" (ISACA, 2019).
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	"Completar las peticiones siguiendo el procedimiento de petición seleccionado, utilizando, cuando sea posible, menús automáticos de autoayuda y modelos de petición predefinidos para los elementos solicitados frecuentemente" (ISACA, 2019).
DSS02.04 Investigar, diagnosticar y localizar incidentes	"Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referenciar los recursos de conocimientos disponibles (incluidos errores y problemas conocido) para identificar posibles resoluciones de incidentes (soluciones temporales y/o permanentes)" (ISACA, 2019).
	"Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de problemas, registrarlo como un problema nuevo" (ISACA, 2019).
	"Asignar incidentes a funciones de especialista si se necesita una mayor habilidad. Contar con el nivel directivo adecuado, donde y si se necesita" (ISACA, 2019).
DSS02.05 Resolver y recuperarse ante incidentes	"Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución *workaround* y/o solución permanente)" (ISACA, 2019).
	"Registrar, si se usaron, *workarounds* para la resolución de incidentes" (ISACA, 2019).
	"Aplicar medidas correctivas, si se requieren" (ISACA, 2019).
	"Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura" (ISACA, 2019).
DSS02.06 Cerrar peticiones de servicio e incidentes	"Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable" (ISACA, 2019).
	"Cerrar las peticiones e incidentes de servicio" (ISACA, 2019)
DSS02.07 Hacer seguimiento al estado y producir informes.	"Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar hacia la resolución o finalización de estos.
	Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar frecuencia y medio de elaboración de los reportes" (ISACA, 2019).

	“Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea” (ISACA, 2019).
	“Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA” (ISACA, 2019).
	“Usar la información como un insumo a la planificación de la mejora continua” (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles para la gestión de incidentes tomado de (ISACA, 2019).

3. Análisis del Marco de gobernabilidad de tecnología COBIT relacionado con los controles de aplicación.

Los controles de aplicación tienen como objetivo principal asegurar la completitud, exactitud, precisión, validez e integridad de los datos al procesar transacciones usando las aplicaciones informáticas y su diseño se centra en evitar que entre al sistema información errónea; adicionalmente, permiten identificar y dar solución a errores que se ingresaron al sistema previamente.

Aunque la responsabilidad del diseño e implementación de los controles de aplicación recae en TI, es importante indicar que la responsabilidad operativa de administrar y controlar los controles de aplicación no es de TI, sino del dueño del proceso de negocio.

Por lo tanto, la responsabilidad de los controles de aplicación es una responsabilidad conjunta, fin a fin, entre el negocio y TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

- La empresa es responsable de:
    - Definir apropiadamente los requisitos funcionales y de control
    - Uso adecuadamente los servicios automatizados
- TI es responsable de:
    - Automatizar e implementar los requisitos de las funciones de negocio y de control.

- Establecer controles para mantener la integridad de controles de aplicación.

Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero sólo los aspectos de desarrollo de los controles de aplicación; la responsabilidad de definir y el uso operativo es de la empresa.

Cada uno de los controles de aplicación establecidos por COBIT están relacionados en el principio **DSS – Entregar, Dar servicio y soporte** como se observa en la tabla 23.

Tabla 23. COBIT y los controles de aplicación

Controles de aplicación	
Dominio COBIT	**DSS - Entrega, Servicio y Soporte**
Proceso de gobierno	**DSS06 - Gestionar Controles de Proceso de Negocio**
Práctica de gobierno	**DSS06.01** - Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales. **DSS06.02** - Controlar el procesamiento de la información. **DSS06.03** - Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización **DSS06.04** - Gestionar errores y excepciones. **DSS06.05** - Asegurar la trazabilidad y la rendición de cuentas de los eventos de información **DSS06.06** - Asegurar los activos de información
Control	**Actividad**
DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos	“Evaluar y supervisar continuamente la ejecución de las actividades del proceso de negocio y los controles relacionados, basados en el riesgo de la empresa, para garantizar que los controles de los procesos alineados con las necesidades del negocio” (ISACA, 2019).
DSS06.02 Controlar el procesamiento de la información	“Operar la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo de la empresa, para garantizar que el procesamiento de la información es válido, completo, preciso oportuno y seguro (es decir, refleja el uso legítimo y autorizado uso empresarial)” (ISACA, 2019).

DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	"Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre" (ISACA, 2019).
DSS06.04 Gestionar errores y excepciones	"Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio" (ISACA, 2019).
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.	"Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos" (ISACA, 2019).
DSS06.06 Asegurar los activos de información	"Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin" (ISACA, 2019).

Fuente: Relación de las actividades de los dominios de COBIT aplicable a los controles de aplicación tomado de (ISACA, 2019).

7.2 Evaluación del nivel de madurez tecnológico de las empresas para cumplir la ley SOX basado en un instrumento elaborado según los lineamientos del marco de referencia COBIT.

Después de analizar como el marco COBIT incluye dentro de sus dominios, los requerimientos que facilitarán la correcta implementación y cumplimiento de la Ley SOX, a través de un instrumento se realiza la evaluación para diagnosticar el nivel de madurez tecnológica que tiene la empresa e identificar los retos a los que deberá enfrentarse para implementar la Ley SOX.

El instrumento se realizó basado en lo siguiente:

1. Su estructura está basada, primero, en los requerimientos de la ley SOX estudiados, que incluyen, los controles a nivel de entidad (ELC), los controles generales de tecnología (ITGC) y los controles de aplicación.
2. Las preguntas definidas se basan en lo definido en cada uno de los dominios de COBIT identificados como marco de referencia para cumplir con estos requerimientos.
3. Antes de iniciar la implementación del instrumento se requiere como paso fundamental, la identificación de las personas clave a ser entrevistadas, es importante tener claro que la eficacia y efectividad del resultado de la encuesta dependerá de las personas que la desarrollen, las cuales deben conocer sobre cada uno de los temas. Dentro de los perfiles clave se encuentran los líderes de tecnología a cargo del departamento de desarrollo, manejo de incidentes, gestión de accesos y manejo de incidentes de seguridad, desde la perspectiva de riesgo es importante involucrar a los encargados de la gestión del riesgo y del control interno.
4. El instrumento está desarrollado como una matriz en excel donde se definieron las preguntas referentes a cada uno de los dominios que se estudiaron para dar cumplimiento a los requerimientos de la ley SOX.
5. Cada una de las respuestas dadas a las preguntas elaboradas tiene una ponderación basada en el nivel de madurez el cual fue asignado de acuerdo con lo indicado por COBIT, como se muestra en la tabla 25.

Tabla 24. Niveles para evaluar la madurez de los procesos según COBIT

Niveles para evaluar la capacidad de los procesos basado en COBIT		
Nivel de capacidad		**Logro**
Nivel 5	Optimización	El proceso se mejora continuamente para cumplir con los objetivos relevantes actuales y proyectados.
Nivel 4	Predecible (Administrado cuantitativamente)	El proceso se ejecuta consistentemente dentro de los límites definidos.

Nivel 3	Establecido (Bien definido)	Se define y utiliza un proceso estándar en toda la organización.
Nivel 2	Administrado (Planificado y Monitoreado)	Se gestiona el proceso y se especifican, controlan y mantienen los resultados.
Nivel 1	Realizado (Informado)	El proceso implementado logra su propósito de proceso.
Nivel 0	Incompleto	El proceso no se implementa o no logra su propósito de proceso.

Fuente: Elaboración propia basado en (ISACA, 2019).

6. El promedio del puntaje dado a cada pregunta arroja el nivel de madurez del ambiente de control interno desde la perspectiva tecnológica.
7. El instrumento de evaluación se debe aplicar a cada uno de los requerimientos identificados con el fin de obtener un puntaje general. Cada uno de los cuestionarios se encuentra relacionado a continuación.
8. Con base en el resultado se establecen estrategias que permitan eliminar los GAPS existentes, mitigar los riesgos a los que se está expuesto y alienar los requerimientos tecnológicos para lograr el cumplimiento de la ley SOX.

A continuación, se desarrolla para cada uno de los requerimientos identificados.

7.2.1 Diagnostico nivel de maduración del proceso para la gestión de incidentes de tecnología

Tabla 25. Diagnostico nivel de maduración del proceso para la gestión de incidentes de tecnología

DOMINIO COBIT	PRACTICA DE GESTION	ITGC - GESTION DE INCIDENTES		DIAGNOSTICO	
		OBJETIVO	PREGUNTAS DE EVALUACION	Puntaje	Nivel de madurez
Entregar, Dar Servicio y Soporte	DSS02 Gestionar las peticiones y los	**DSS02.01** Definir esquemas de clasificación para incidentes y peticiones de servicio.	¿Se tienen definidos esquemas de priorización y clasificación de solicitudes de servicios e incidentes y los criterios para el registro de problemas? (ISACA, 2019).	2	Realizado
			¿Se definen modelos de incidentes sobre errores conocidos para permitir resolución eficiente y eficaz? (ISACA, 2019).	2	
			¿Se tienen definidos modelos de solicitud de servicios conforme a su tipo que permita la autogestión? (ISACA, 2019).	1	

			¿Se tienen definidas reglas y procedimientos de escalamiento de incidentes, especialmente para aquellos incidentes más importantes o de seguridad?	0	
			¿Se tienen definidas las fuentes de conocimiento sobre incidentes y solicitudes con una descripción de cómo usarlas? (ISACA, 2019).	1	
		DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	¿Se tiene establecido un mecanismo para el registro de solicitudes e incidentes de servicio que garantice su gestión de forma eficaz y la conservación de su registro histórico? (ISACA, 2019).	2	
			¿Se tienen establecidos KPIs que permitan analizar las tendencias de los incidentes? (ISACA, 2019).	2	
			¿Se priorizan las solicitudes e incidentes de servicios basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio? (ISACA, 2019).	2	
		DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	¿Se cumple con las solicitudes realizando el proceso seleccionado? (ISACA, 2019).	2	
		DSS02.04 Investigar, diagnosticar y asignar incidentes.	¿Se identifican y describen síntomas relevantes para establecer las causas más probables de los incidentes? (ISACA, 2019).	2	
			¿Si un problema o error identificado no existe todavía y si este se clasifica como incidente se registra como un problema nuevo? (ISACA, 2019).	1	
			¿Los incidentes son asignados a un especialista en caso se requiera una mayor habilidad para su análisis y resolución? (ISACA, 2019).	2	
		DSS02.05 Resolver y recuperarse de los incidentes.	¿Se asegura que se selecciona y aplique la resolución de incidentes más adecuada? (ISACA, 2019).	2	
			¿Se registra, cuando son usados los *workarounds* en la solución del incidente? (ISACA, 2019).	2	
			¿Si se requiere se aplican medidas correctivas? (ISACA, 2019).	1	
			¿Se gestiona el conocimiento a través de la documentación del incidente y la resolución de este? (ISACA, 2019).	1	
		DSS02.06 Cerrar las peticiones de servicio y los incidentes.	¿Se valida con los usuarios afectados si la solución ha cumplido de forma satisfactoria dentro del plazo de tiempo acordado/aceptable? (ISACA, 2019).	1	
			¿Se asegura de cerrarse todas las peticiones e incidentes de servicio? (ISACA, 2019).	1	
		DSS02.07 Hacer seguimiento al estado y producir informes.	¿Se hace monitoreo a los incidentes para progresar hacia la solución o finalización de estos? (ISACA, 2019).	2	
			¿Se tienen identificadas las partes interesadas en la información, así la frecuencia y medio de elaboración de los reportes? (ISACA, 2019).	1	
			¿Se producen y distribuyen o se da acceso controlado a los informes en el plazo debido? (ISACA, 2019).	0	
			¿Se realiza un análisis de los incidentes para establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA? (ISACA, 2019).	1	

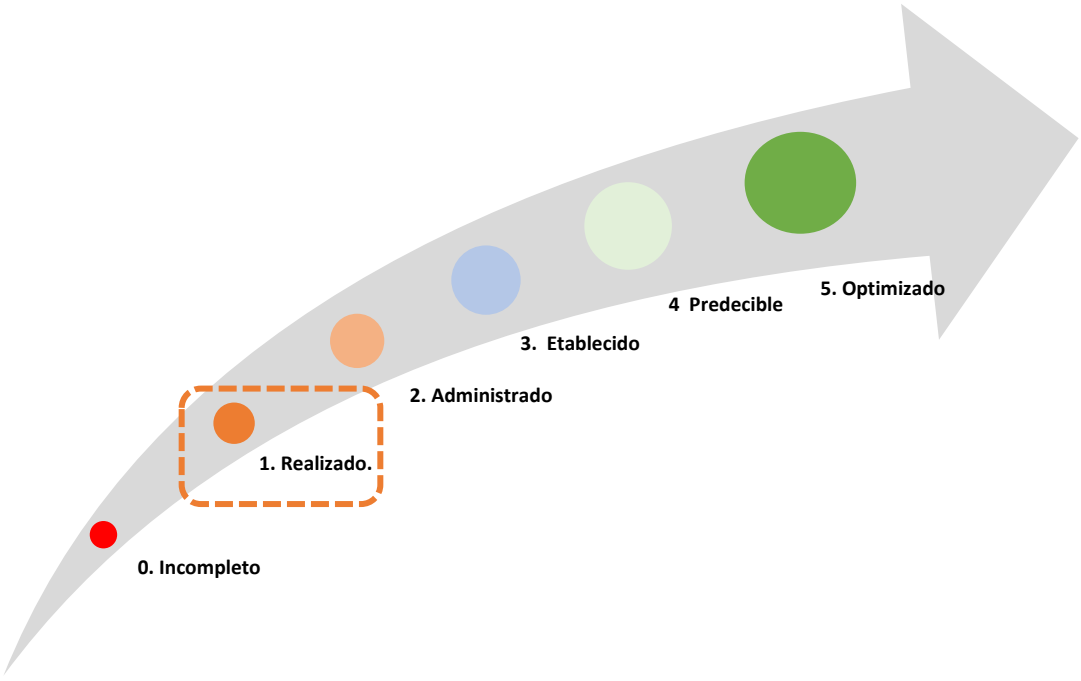
			¿Se utiliza la información de los reportes y análisis como insumo para la planificación de la mejora continua? (ISACA, 2019).	1	
TOTAL				**1,39**	

Fuente: Elaboración propia basada en (ISACA, 2019)

De acuerdo con la tabla 26, se identifica que el ITGC (Control general de tecnología) de incidentes, tiene un puntaje de **1,39** lo que lo ubica dentro del nivel de **REALIZADO,** es decir que el proceso implementado logra su propósito de proceso.

En este caso, si bien es cierto el proceso logra su propósito básico, al analizarlo según la escala definida, se encuentra en un nivel muy inmaduro que no permite cumplir con los requerimientos tecnológicos exigidos por la ley SOX. En este sentido, la gestión de incidentes se encuentra en sus etapas iniciales tal como se muestra en la ilustración 8.

Ilustración 8. Diagnóstico nivel de maduración del proceso de gestión de incidentes basado en escala COBIT 2019.



Fuente: Elaboración propia basado en (ISACA, 2019).

En general se identifica que si bien es cierto se tiene establecido un procedimiento para el manejo de incidentes en general es una acción más reactiva que se limita a atender las situaciones cuando estas se presentan, por lo que se requiere que se implementen actividades adicionales que permitan tener un proceso enfocado más en la gestión que lleva a la mejora continua a través de las siguientes actividades:

1. Establecer criterios de clasificación y priorización, que permita identificar, registrar y documentar problemas nuevos.
2. Robustecer las fuentes de conocimiento que permitan a través de históricos llegar a nivel de autogestión para los casos que así lo permitan.
3. Implementar KPIs para el seguimiento tanto de la gestión como del cumplimiento de los SLAs.
4. Implementar procedimientos que logren llevar al proceso a la implementación de medidas correctivas que evite estar atendiendo los mismos incidentes recurrentemente
5. Elaborar informes que permitan identificar tendencias, ineficiencias, errores recurrentes que lleven a la implementación de acciones de mejora.

7.2.2 Diagnostico nivel de maduración del proceso para la gestión del cambio

De acuerdo con la tabla 27, se identifica que el ITGC (Control general de tecnología) de gestión del cambio, tiene un puntaje de **4,76** lo que lo ubica dentro del nivel de OPTIMIZADO, es decir que el proceso se mejora continuamente para cumplir con los objetivos relevantes actuales y proyectados.

En este sentido, la gestión del cambio es un proceso maduro tal como se muestra en la ilustración 13 y su estado actual le permitiría cumplir con los requerimientos tecnológicos exigidos por la ley SOX.

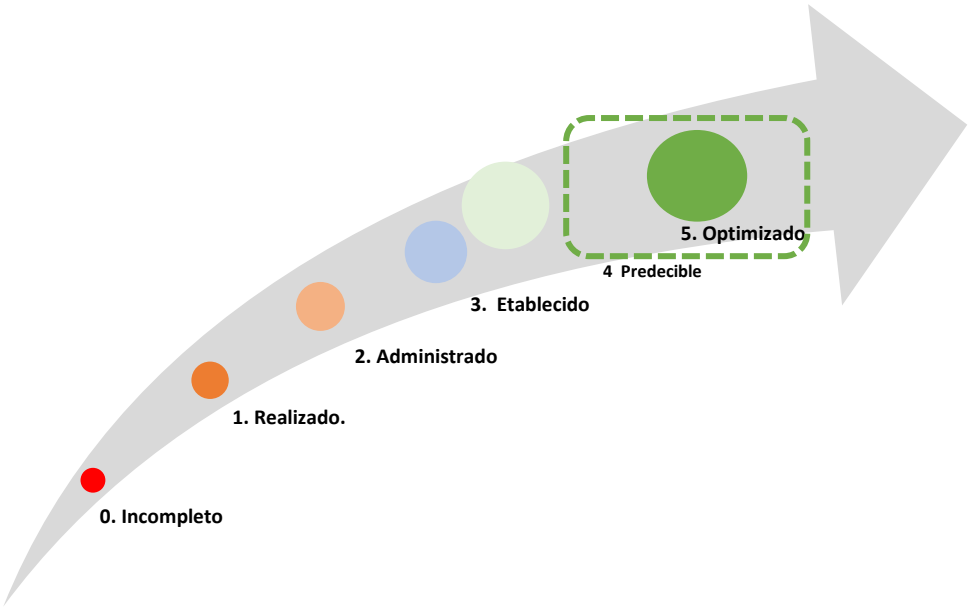
Tabla 26. Diagnóstico nivel de maduración del proceso de gestión del cambio

DOMINIO COBIT	PRACTICA DE GESTION	ITGC GESTION DE CAMBIOS		DIAGNOSTICO	
		OBJETIVO	PREGUNTAS	Puntaje	Nivel de madurez
Construir, Adquirir e Implementar (BAI)	**BAI06 -** Gestionar los cambios de TI	**BAI06.01** Evaluar, priorizar y autorizar solicitudes de cambio.	¿Todas las solicitudes de cambios de negocio, infraestructura, sistemas o aplicaciones se realizan a través de peticiones formales? (ISACA, 2019).	5	**Optimizado**
			¿Todas las solicitudes de cambios son categorizadas (Proceso, infraestructura, sistemas operativos, redes, aplicaciones, software eterno) y relacionadas con el elemento de configuración afectado? (ISACA, 2019).	5	
			¿Todos los cambios son analizados basado en la razón del cambio tales como requisitos técnicos de negocio, recursos necesarios, requerimientos contractuales, legales o de regulación? (ISACA, 2019).	5	
			¿Se planifican y evalúan todas las peticiones de manera estructurada incluyendo impacto, planes de continuidad de negocio, afectación negativa en el entorno operativo y el riesgo de la implementación del cambio? (ISACA, 2019).	4	
			¿Los cambios son aprobados por las personas autorizadas? (ISACA, 2019).	4	
			¿Los cambios aprobados son planificados y programados? (ISACA, 2019).	5	
			¿Se considera el impacto en los proveedores de servicios contratados en el proceso de gestión de cambio? (ISACA, 2019).	5	
		BAI06.02 Gestionar cambios de emergencia.	¿Existe un procedimiento documentado para declarar, evaluar, aprobar, autorizar y registrar el cambio de emergencia? (ISACA, 2019).	5	
			¿Se autorizan debidamente los accesos para realizar los cambios de emergencia y son revocados una vez se ha aplicado al cambio? (ISACA, 2019).	5	
			¿Todos los cambios de emergencia son supervisados y se realizan revisiones post-implementación para identificar acciones correctivas? (ISACA, 2019).	5	
			¿Está definido claramente que es un cambio de emergencia? (ISACA, 2019).	5	
		BAI06.03 Hacer seguimiento e informar sobre cambios de estado.	¿Se categorizan todas las peticiones de cambios en el proceso de seguimiento (Rechazados, aprobados, pero no iniciados, aprobados en proceso y cerrado) (ISACA, 2019).	5	
			¿Se tienen definidas métricas de rendimiento para la gestión de los cambios? (ISACA, 2019).	5	
			¿Se supervisan los cambios abiertos para asegurar que los cambios aprobados se cierran en los plazos previstos, de acuerdo con su prioridad? (ISACA, 2019).	4	
		BAI06.04 Cerrar y documentar los cambios.	¿Se incluyen los cambios en la documentación (Ej. Procedimientos existentes o nuevos) en el proceso de gestión del cambio como parte integral del cambio?) (ISACA, 2019).	4	
			¿Se tienen definidos periodos de conservación de la documentación del cambio? (ISACA, 2019).	4	
			¿Se revisa la documentación de la misma forma en la que se revisa el cambio? (ISACA, 2019).	4	

	BAI07 Gestionar la aceptación y la transición de los cambios de TI	**BAI07.01** Establecer un plan de implementación.	¿Se tiene establecido un plan de implementación que refleje la estrategia global de la implantación (criterios de pruebas de aceptación, comunicación, formación, preparación de puestas en producción, paso a producción, soporte temprano en producción) (ISACA, 2019).	5	
			¿Se tiene identificado y documentado un proceso de *fallaback* y recuperación? (ISACA, 2019).	5	
			¿Todos los planes de implementación cuentan con la aprobación de las partes interesadas técnicas y de negocio? (ISACA, 2019).	5	
			¿Se revisa, se considera y se aborda formalmente el riesgo técnico y de negocio en el proceso de planificación? (ISACA, 2019).	5	
		BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.	¿Se tiene definido un plan de migración de procesos de negocio, datos servicios e infraestructura de TI? (ISACA, 2019).	5	
			¿Se tiene respaldo de todos los sistemas y datos hasta el instante anterior a la conversión? ¿Se mantienen registros de auditoría que permita asegurar la traza de la conversión? ¿Existe un plan de recuperación que cubra la marcha atrás de la migración y la vuelta al procesamiento anterior en caso de que la migración fallara? (ISACA, 2019).	5	
		BAI07.03 Plan de pruebas de aceptación.	¿Se desarrolla y documenta el plan de pruebas alineado con el programa, el plan de calidad del proyecto y los estándares organizativos relevantes? (ISACA, 2019).	5	
			¿Se asegura que el plan de pruebas refleja la evaluación del riesgo del proyecto y que se pruebas todos los requisitos funcionales y técnicos? (ISACA, 2019).	5	
			¿Todos los planes de prueba cuentan con la aprobación de las partes interesadas técnicas y de negocio? (ISACA, 2019).	5	
		BAI07.05 Realizar pruebas de aceptación.	¿El plan de pruebas es diseñado y ejecutado por un grupo de pruebas independiente del equipo de desarrollo? (ISACA, 2019).	5	
			¿Se garantizan que se han considerado los elementos de *fallback* y *rollback* del plan de pruebas? (ISACA, 2019).	5	
		BAI07.06 Promover a producción y gestionar las liberaciones (*releases).*	¿El paso de pruebas a producción se realiza conforme a los estándares de gestión de cambios organizativos? (ISACA, 2019).	4	
TOTAL				**4,76**	

Fuente: Elaboración propia basada en **(ISACA, 2019)**.

Ilustración 9. Nivel de maduración del proceso de gestión del cambio basado en escala COBIT 2019.



Fuente: Elaboración propia basado en **(ISACA, 2019)**

En este caso, cuando un proceso se encuentren el nivel de Optimización, quiere decir que es un proceso maduro que busca la mejora continua.

El reto cuando un proceso se encuentra en este nivel es lograr mantenerlo a través del tiempo y sin importar la rotación de personal que pueda presentarse o lo cambios que, desde la perspectiva organizacional, operacional, tecnológica o estratégica surjan, ya que su definición permite que cualquiera de estas circunstancias no afecte el proceso que se ejecuta si no que por el contrario se ajuste según sea requerido.

7.2.3 Diagnostico nivel de maduración del proceso de gestión de operaciones.

De acuerdo con la tabla 28, se identifica que el ITGC (Control general de tecnología) de gestión de operaciones, tiene un puntaje de **4,27** lo que lo ubica dentro del nivel de **PREDECIBLE**, es decir que el proceso se realiza de forma consistente dentro de los límites definidos.

Tabla 27. Diagnóstico nivel de maduración del proceso de gestión de operaciones

DOMINIO COBIT	PRACTICA DE GESTION	ITGC GESTION DE OPERACIONES OBJETIVO	PREGUNTAS DE EVALUACION	DIAGNÓSTICO Puntaje	 Nivel de madurez
Entregar, Dar Servicio y Soporte (DSS)	**DSS01 Gestionar las operaciones**	**DSS01.01** Ejecutar procedimientos operativos.	¿Se desarrollan y mantienen los procedimientos operativos para respaldar los servicios prestados? (ISACA, 2019).	5	**Predecible**
			¿Se mantiene un calendario de las actividades operativas? (ISACA, 2019).	4	
			¿Se monitorea que los procedimientos operativos se hayan ejecutado de forma completa, precisa y en el tiempo indicado? (ISACA, 2019).	3	
			¿Se gestiona el rendimiento de las actividades programadas? (ISACA, 2019).	3	
			¿Se monitorean los incidentes y problemas de los procedimientos operativos y se realizan acciones para mejorar su confiabilidad? (ISACA, 2019).	5	
		DSS01.02 Gestionar servicios tercerizados de I&T.	¿Se asegura que los requisitos de los procesos de seguridad de la información cumplan con los contratos y *SLA's* de terceros o proveedores de servicios? (ISACA, 2019).	5	
			¿Se asegura que los requisitos de procesamiento operacional del negocio y de TI de la empresa cumplan con los contratos y *SLA* de *hosting* de terceros o proveedores de servicios? (ISACA, 2019).	4	
			¿Se integran los procesos de gestión de TI internos críticos con los de los proveedores de servicios externalizados? (ISACA, 2019).	5	
			¿Se realiza una auditoría independiente para revisar el aseguramiento de los entornos operaciones de proveedores que proporcionan servicios externalizados? (ISACA, 2019).	5	
		DSS01.03 Monitorizar la infraestructura de I&T.	¿Se tiene registro de los eventos conforme a una consideración de riesgo y rendimiento?	4	
			¿Se identifica y mantiene una lista de activos de infraestructura que deben ser monitorizados de acuerdo con la criticidad del servicio? (ISACA, 2019).	5	
			¿Se definen e implementan reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos? (ISACA, 2019).	4	
			¿Se mantiene registro de eventos durante un periodo de tiempo adecuado? (ISACA, 2019).	5	
			¿Se crean *tickets* de incidentes en el plazo adecuado para monitorizar desviaciones de los umbrales? (ISACA, 2019).	5	
			¿Se tienen establecidos procedimientos para monitorizar los registros de eventos y se revisan regularmente? (ISACA, 2019).	4	
		DSS04.07 Administrar los acuerdos de respaldo.	¿Se realizan copias de seguridad de los sistemas, aplicaciones, datos y documentación basado en un calendario definido, incluyendo frecuencia, modo de la copia y tipo de copia? (ISACA, 2019).	4	
			¿Se tienen definidos los requisitos para el almacenamiento en instalaciones y fuera de ella de	5	

			copias de seguridad de datos según los requisitos de negocio? (ISACA, 2019).		
			¿Se prueban y refrescan de manera periódica los datos archivados y las copias de seguridad de los datos? (ISACA, 2019).	4	
			¿Se garantizar una copia de seguridad para los datos, aplicaciones y documentación mantenida o procesada por terceros? (ISACA, 2019).	5	
		DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	¿Se usa de forma continua un portafolio de tecnologías, servicios y activos soportados para identificar vulnerabilidades de seguridad de la información? (ISACA, 2019).	4	
			¿Se revisan regularmente los logs de eventos para detectar posibles incidentes? (ISACA, 2019).	3	
			¿Se garantiza la creación de *tickets* relativos a incidentes de seguridad de forma oportuna? (ISACA, 2019).	4	
			¿Se registran los eventos relacionados con la seguridad y se conservan registros durante el periodo de tiempo apropiado? (ISACA, 2019).	4	
MEA (Monitorizar, Evaluar y Valorar)	**MEA02** Supervisar, Evaluar y Valorar el Sistema de Control Interno	**MEA02.01** Supervisar el control interno.	¿Se evalúa el estado de los controles internos de los proveedores externos y se confirman que cumplan con los requisitos exigidos? (ISACA, 2019).	4	
		MEA02.07 Estudiar las iniciativas de aseguramiento.	¿Se contempla dentro del alcance de los objetivos empresariales y de TI la auditabilidad de las entidades externas? (ISACA, 2019).	4	
	MEA03.01 Identificar requisitos externos de cumplimiento.	**MEA03.01** Identificar requisitos externos de cumplimiento.	¿Se valora el impacto de los requisitos legales y regulatorios relacionados con los contratos con terceros que afecten las operaciones de TI? (ISACA, 2019).	4	
TOTAL				**4,27**	

Fuente: Elaboración propia basada en (ISACA, 2019)

En este sentido, la gestión de operaciones es un proceso maduro tal como se muestra en la ilustración 14, con este resultado se identifica que el proceso es administrado cuantitativamente, es decir se lleva a cabo de acuerdo con los límites establecidos.

Ilustración 10. Nivel de maduración del proceso de gestión de operaciones basado en escala COBIT 2019.

Fuente: Elaboración propia basada en (ISACA, 2019)

La mayoría de las actividades evaluadas se ubican dentro del rango superior, se identifican algunas oportunidades de mejora que llevarían al proceso a un nivel máximo de maduración lo que le permitiría mejorar continuamente, dentro de las cuales se identifican las siguientes:

1. Se hace necesario establecer un procedimiento de monitoreo para asegurar que las tareas programadas se hayan ejecutado de manera adecuada y oportuna

2. Aunque se tienen identificadas las actividades programas, no existe una gestión que permita revisar el rendimiento de las actividades programadas, lo que no permite validar si las actividades gestionadas están generando el rendimiento que se espera, o se deben hacer cambios para mejorar los tiempos.

7.2.3.1 Diagnostico nivel de maduración del proceso para la gestión de accesos.

Tabla 28. Diagnóstico nivel de maduración del proceso de gestión de accesos.

DOMINIO COBIT	PRACTICA DE GESTION	ITGC GESTION DE ACCESOS		DIAGNOSTICO	
		OBJETIVO	PREGUNTAS	Puntaje	Nivel de maduración
Alinear, Planificar y Organizar (APO)	**APO01** Gestionar el marco de gestión de I&T	**APO01.05** Establecer roles y responsabilidades	¿Al asignar roles y responsabilidades se comunican y se incluyen los niveles de autoridad, responsabilidad y rendición de cuentas? (ISACA, 2019).	0	Incompleto
			¿Se estructuran los roles y las responsabilidades para reducir la posibilidad de que la concentración de funciones comprometa un acceso crítico? (ISACA, 2019).	0	
			¿El nivel de supervisión de los roles y responsabilidades está alineada y realizada de acuerdo con la sensibilidad del puesto y la extensión de las responsabilidades asignadas? (ISACA, 2019).	0	
	APO07 Gestionar los recursos humanos	**APO07.06** Gestionar al personal contratado.	¿Al asignar roles y responsabilidades al personal por contrato, así como a los consultores se asegura que conozcan y cumplan con las políticas de acceso existentes en la compañía? (ISACA, 2019).	0	
Construir, Adquirir e	**BAI03** Gestionar la identificación y construcción	**BAI03.03** Desarrollar los componentes de la solución.	¿Se monitorea e informa las responsabilidades de usar componentes de infraestructura de alta seguridad o de acceso restringido estén claramente definidas por aquellos que desarrollan e integran los componentes de infraestructura? (ISACA, 2019).	1	
Entregar, Dar Servicio y Soporte (DSS)	**DSS05** Gestionar los servicios de seguridad	**DSS05.02** Gestionar la seguridad de la conectividad y de la red.	¿Todos los dispositivos autorizados para acceso a la información están configurados para forzar a la introducción de contraseña? (ISACA, 2019).	2	
		DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	¿Los derechos de accesos son asignados de acuerdo con la función del negocio y con base en los requisitos del proceso y las políticas de seguridad basándose en los principios de menor privilegio? (ISACA, 2019).	1	
			¿Los cambios en los derechos de acceso (Creación, modificación y eliminación) se administran de manera oportuna y garantizando que hayan sido documentadas y aprobadas por el personal autorizado?	0	
			¿Se realiza supervisión de todas las cuentas de usuario privilegiadas? (ISACA, 2019).	0	
			¿Se asegura que todos los roles se definen y se coordinan con las unidades de negocio, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de proceso de este? (ISACA, 2019).	0	
			¿Se autentican todos los accesos a los activos de información de acuerdo con el rol del colaborador o a las reglas de negocio, se hace monitoreo que la autenticación haya sido administrada adecuadamente? (ISACA, 2019).	0	

			¿La autenticación de los usuarios (Internos, externos, temporales) así como su actividad en los sistemas de TI se pueden identificar de manera unívoca? (ISACA, 2019).	1	
			¿Se realiza de manera periódica revisiones gerenciales de todas las cuentas y sus privilegios relacionados? (ISACA, 2019).	0	
		DSS05.05 Gestionar el acceso físico a los activos de I&T.	¿Se tiene establecido un procedimiento para el otorgamiento de acceso, registro y monitoreo de visitantes al centro de cómputo? (ISACA, 2019).	1	
			¿Se restringe y monitoriza el acceso a las instalaciones sensibles de TI? (ISACA, 2019).	1	
			¿Los perfiles de acceso a los centros de cómputo se basan en el cargo y las responsabilidades y se garantiza que se mantengan actualizados? (ISACA, 2019).	0	
	DSS06 Gestionar los controles de procesos de negocio	**DSS06.03** Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	¿Los roles y responsabilidades son asignados conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio? (ISACA, 2019).	0	
			¿Se asignan niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados? (ISACA, 2019).	0	
			¿Se asignan roles para actividades sensibles para que haya una clara segregación de funciones? (ISACA, 2019).	1	
			¿Se eliminan o revisan los derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de negocio? (ISACA, 2019).	1	
			¿Se revisa periódicamente la correcta actualización de los derechos de acceso? (ISACA, 2019).	0	
			¿Los privilegios otorgados a los usuarios administradores son asegurados, rastreados y controlados para prevenir su mal uso? (ISACA, 2019).	1	
			¿Se revisa periódicamente los accesos para asegurar que todos son válidos y están alineados con los miembros actuales del personal y sus roles asignados? (ISACA, 2019).	0	
TOTAL				**0,43**	

Fuente: Elaboración propia basada en **(ISACA, 2019)**.

Tal como se evidencia en la tabla 29, la gestión de accesos se encuentra en su nivel más bajo, por lo que sin lugar a duda se requiere del establecimiento y definición de planes de acción para llevarla a un nivel más maduro.

Mejorar un proceso partiendo de un nivel inmaduro requiere inversión de tiempo, esfuerzo y dinero y dependerá fuertemente del tamaño de la empresa.

Al haber identificado el estado actual de los accesos, es importante entonces determinar las actividades a implementar para iniciar el proceso.

1. Hacer un listado de las aplicaciones usadas en la compañía
2. Hacer un listado de los roles y perfiles tiene configurada cada aplicación
3. Hacer un listado de los usuarios de cada una de las aplicaciones
4. Identificar las características y permisos asignados a cada uno de los roles y perfiles identificados
5. Identificar los usuarios asignados a cada uno de los roles y perfiles
6. Determinar cuáles de los usuarios tienen incorrectamente asignados los roles y perfiles de acuerdo con el cargo asignado
7. Eliminar los permisos mal asignados a los usuarios correspondientes
8. Identificar, n las responsabilidades de su cargo, aquellos roles que requieren permisos especiales.
9. Establecer procedimientos de monitoreo de actividades para roles y perfiles críticos.
10. Establecer un procedimiento para la administración de accesos que contemple como mínimo:

- ✓ Actualización
- ✓ Monitoreo
- ✓ Monitoreo a roles críticos
- ✓ Accesos a terceros
- ✓ Accesos a los centros de cómputo

Ilustración 11. Nivel de maduración del proceso de gestión de accesos basado en escala COBIT 2019.

Fuente: Elaboración propia basada en (ISACA, 2019).

7.2.4 Diagnostico nivel de maduración de los controles a nivel de entidad ELC (Entity level controls)

Al hacer el ejercicio para evaluar el nivel de madurez de los controles a nivel de entidad obtiene un puntaje de 2,21 como se muestra en la tabla 30, lo que indica que es un proceso **ADMINISTRADO** (Ilustración 14) es decir que se gestionan, especifican, controlan y mantienen los resultados.

Según lo evaluado el proceso debe fortalecer el establecimiento y mantenimiento del marco de referencia de gobierno de IT documentando la comprensión de los requerimientos y realizando una estimación del actual y futuro diseño del gobierno de TI de la empresa.

Otro de los aspectos que deben ser revisados es la alineación del entorno de control de TI se con los marcos y políticas de tecnología para garantizar que lo definido a nivel normativo cuenta con los controles que permitan una gestión adecuada.

Tabla 29. Diagnostico nivel de maduración del proceso para la gestión de los ELC

DOMINIO COBIT	PRACTICA DE GESTION	Controles a Nivel de Entidad (ELC)		DIAGNOSTICO	
		OBJETIVO	PREGUNTAS	Puntaje	Nivel de madurez
EDM - Evaluar, Orientar y Supervisar	**EDM01** Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	**EDM01.01** Evaluar el sistema de gobierno.	¿Se identifican y compromete continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa?	**1**	**Administrado**
	EDM03 Asegurar la Optimización del Riesgo	**EDM03.01** Evaluar la gestión de riesgos	¿Se examina y evalúa continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa, considerando si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado?	**2**	
		EDM03.02 Orientar la gestión de riesgos	¿Se orienta el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo?	**2**	
		EDM03.03 Supervisar la gestión de riesgos	¿Se supervisan los objetivos y las métricas clave de los procesos de gestión de riesgo y se establece cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución?	**3**	
	EDM05 Asegurar la Transparencia hacia las Partes Interesadas	**EDM05.02** Orientar la comunicación con las partes interesadas y la elaboración de informes	¿Se garantiza el establecimiento de la comunicación y la elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, ¿vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas?	**4**	
		EDM05.03 Supervisar la comunicación con las partes interesadas	¿Se supervisa la eficacia de la comunicación con las partes interesadas y se evalúan los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados?	**2**	
APO- Alinear, Planificar y Organizar	**APO01** Gestionar el Marco de Gestión de TI	**APO01.02** Establecer roles y responsabilidades	¿e establecen, acuerdan y comunican roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante?	**2**	

		APO01.03 Mantener los elementos catalizadores del sistema de gestión	¿Está alineado el entorno de control de TI con el entorno de políticas de TI, los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control y se evalúan las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda?	**1**	
		APO01.04 Comunicar los objetivos y la dirección de gestión	¿Se comunica la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa	**1**	
		APO01.06 Definir la propiedad de la información (datos) y del sistema.	¿Se definen y mantienen las responsabilidades de la propiedad de la información (datos) y los sistemas de información? y se asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación?	**2**	
		APO01.08 Mantener el cumplimiento con las políticas y procedimientos.	¿Se ponen en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia y se hacen cumplir las consecuencias del no cumplimiento o del desempeño inadecuado? ¿Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control?	**2**	
	APO02 Gestionar la Estrategia	**APO02.01** Comprender la dirección de la empresa	¿Se considera el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía y se toman también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia)?	**2**	
		APO02.05 Definir el plan estratégico y la hoja de ruta	¿Se crea un plan estratégico que define, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa que Incluya cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI?	**3**	
		APO02.06 Comunicar la estrategia y la dirección de TI	¿Se crea conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa?	**3**	
	APO07 Gestionar los Recursos Humanos	**APO07.01** Mantener la dotación de personal suficiente y adecuada.	¿Se evalúan las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales, e incluye recursos tanto internos como externos?	**4**	
		APO07.03 Mantener las habilidades y competencias del personal	¿Se definen las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos?	**4**	

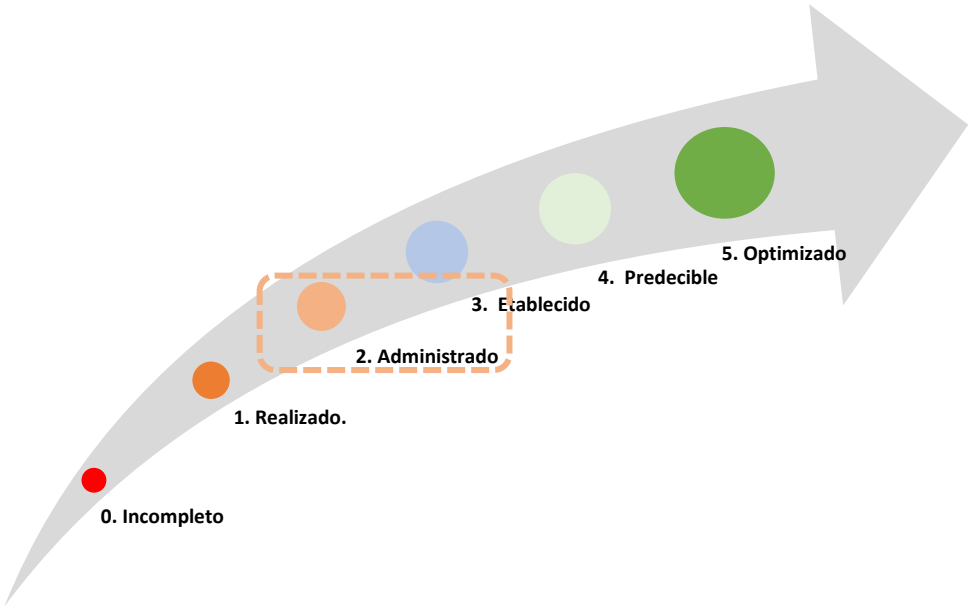
		APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	¿Se crea y mantiene un inventario de recursos humanos de negocio y de TI?	**3**	
			¿Se tiene definida la demanda actual de recursos humanos para apoyar el logro de los objetivos de TI?	**2**	
			¿Se identifican las carencias y se tienen planes de aprovisionamiento de personal de TI?	**2**	
	APO11 Gestionar la Calidad	**APO10.05** Supervisar el cumplimiento y el rendimiento del proveedor	¿Se revisa periódicamente el rendimiento general y el cumplimiento de los requisitos contractuales de los proveedores de TI?	**2**	
		APO11.01 Establecer un sistema de gestión de calidad (SGC)	¿Se tiene y se establece un SGC (sistema de gestión de calidad) que permita gestionar la calidad de la tecnología?	**1**	
		APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	¿Se tienen definidas las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI?	**1**	
		APO11.03 Enfocar la gestión de la calidad en los clientes	¿Está enfocada la gestión de la calidad en los clientes, mediante la determinación de los requisitos de los clientes externos e internos y asegurando su alineamiento con las normas y prácticas de TI?	**4**	
		APO11.06 Mantener una mejora continua	¿Se mantiene y comunica regularmente un plan de calidad global que promueva la mejora continua?	**4**	
	APO12 Gestionar el Riesgo	**APO12.01** Recopilar datos	¿Se identifican y recopilan datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI?	**2**	
		APO12.02 Analizar el riesgo	¿Se construyen y actualizan regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta?	**2**	
			¿Se estima la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI, teniendo en cuenta todos los factores de riesgo que apliquen, evaluando controles operacionales conocidos y estimando niveles de riesgo residual?	**1**	
		APO12.03 Mantener un perfil de riesgo	¿Se cuenta con un inventario de los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y se documenta la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI?	**1**	
		APO12.04 Expresar el riesgo	¿Se proporciona información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada?	**1**	

		APO12.05 Definir un portafolio de acciones para la gestión de riesgos.	¿Se clasifican las actividades de control y se mapean con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.	**1**	
		APO12.06 Responder al riesgo	¿Se responde de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI?	**1**	
MEA - Supervisar, Evaluar y Valorar	**MEA01** Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	**MEA01.04** Analizar e informar sobre el rendimiento	¿Se revisar e informa de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión?	**2**	
	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	**MEA02.01** Supervisar el control interno.	¿Se realizan, de forma continua, supervisión a los estudios comparativos y la mejora del entorno de control de TI y del marco de control para alcanzar los objetivos organizativos?	**2**	
		MEA02.04 Identificar y comunicar las deficiencias de control.	¿Se comunican los procedimientos de escalamiento de las excepciones de control, análisis de causas raíz e información a los propietarios del proceso y grupos de interés de TI?	**2**	
		MEA02.06 Planificar iniciativas de aseguramiento	¿Se realiza una evaluación del riesgo a alto nivel y/o se evalúa la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI?	**1**	
		MEA02.07 Estudiar las iniciativas de aseguramiento.	¿Se define el alcance actual mediante la identificación de los objetivos empresariales y de TI para el entorno bajo estudio, el conjunto de procesos y recursos de TI y todas las entidades auditables relevantes dentro de la compañía y externas a la compañía (p. ej. proveedores de servicios), si aplica?	**3**	
		MEA02.08 Ejecutar las iniciativas de aseguramiento	¿Se refina la comprensión en materia de aseguramiento de TI y el alcance de los objetivos de control clave en materia de aseguramiento de TI?	**4**	
	MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	**MEA03.01** Identificar requisitos externos de cumplimiento.	¿Se identifican y supervisan, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI?	**4**	
TOTAL				**2,21**	

Fuente: Elaboración propia basada en (ISACA, 2019).

En general y muy alineado con los objetivos de los controles a nivel de entidad, el proceso debe asegurarse de definir, administrar y mantener un sistema de gestión de calidad que permita asegurar los procesos de tecnología.

Ilustración 12. Nivel de maduración del proceso para la gestión de accesos.



Fuente: Elaboración propia basada en (ISACA, 2019).

7.2.5 Diagnostico nivel de maduración de los controles de aplicación

Una vez aplicado el instrumento de evaluación se obtiene un puntaje de 2,0 según se evidencia en la tabla 31, lo que ubica a este proceso en el nivel 3 es decir se encuentra **ESTABLECIDO** (Ilustración 13) es decir que se define y utiliza un proceso estándar en toda la organización.

En este caso, se observa como este proceso se ve afectado por una mala administración de accesos que se evidencia de igual forma en la evaluación correspondiente a este tema, por consiguiente, se deben establecer planes que permitan asegurar y garantizar que los accesos otorgados son lo suficientemente seguros que permiten una correcta administración de la información.

Tabla 30. Diagnóstico nivel de maduración de los controles de aplicación

DOMINIO COBIT	PRACTICA DE GESTION	Controles de aplicación		DIAGNOSTICO	
		OBJETIVO	PREGUNTAS	Puntaje	Nivel de madurez
DSS - Entrega, Servicio y Soporte	DSS06 - Gestionar Controles de Proceso de Negocio	**DSS06.01** Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos	¿Se evalúan y supervisan continuamente la ejecución de las actividades del proceso de negocio y los controles relacionados, basados en el riesgo de la empresa, para garantizar que los controles de los procesos estén alineados con las necesidades del negocio? (ISACA, 2019).	4	Establecido
		DSS06.02 Controlar el procesamiento de la información	¿Se controla el procesamiento de la información a través de la ejecución de actividades de los procesos de negocio y controles relacionados basados en el riesgo de la empresa para garantizar que su uso es válido, completo, preciso, oportuno y seguro? (ISACA, 2019).	3	
		DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	¿Existe una gestión de roles, responsabilidades, privilegios de acceso y niveles de autorización para asegurar que el negocio sepa dónde están los datos y quién los está manejando? (ISACA, 2019).	2	
		DSS06.04 Gestionar errores y excepciones	¿Se gestionan las excepciones y errores de los procesos de negocio y se facilita su corrección, incluyendo el escalamiento de errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas? (ISACA, 2019).	3	
		DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.	¿Se asegura que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan? (ISACA, 2019).	2	
		DSS06.06 Asegurar los activos de información	¿Se aseguran los activos de información accesibles por el negocio a través de los métodos aprobados e información en tránsito? (ISACA, 2019).	2	
TOTAL				**2,7**	

Fuente: Elaboración propia basada en (ISACA, 2019).

Adicionalmente y con base en la importancia y el impacto que tienen los controles de aplicación es requerido establecer los planes de acción que aseguren la trazabilidad de los eventos y responsabilidades y de información, dentro de las cuales se pueden referir las siguientes:

1. Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.
2. Proporcionar concienciación y formación de un uso aceptable.
3. Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación.

4. Identificar e implementar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento.
5. Informar al negocio y a los grupos de interés acerca de violaciones y desviaciones

Ilustración 13. Nivel de maduración de los controles de aplicación

Fuente: Elaboración propia basada en (ISACA, 2019)

7.3 Definición de estrategias para fortalecer el entorno de TI teniendo como marco de referencia COBIT 2019.

Hasta el momento se ha realizado un estudio de los requerimientos tecnológicos exigidos por la ley SOX para las empresas colombianas emisoras de valores en la bolsa de valores de Estados Unidos; de igual forma se ha identificado como a través del marco de referencia COBIT se puede dar cumplimiento a estos requerimientos.

Tomando como base de referencia el marco COBIT se elabora un instrumento de medición que permite identificar el nivel de madurez que tiene la empresa para cada uno de los requerimientos de estudio, la cual permitirá definir las estrategias y pasos a seguir para lograr la implementación de SOX de manera exitosa.

La sección 404 de la Ley SOX indica que los niveles gerenciales de las compañías que presentan informes anuales ante la SEC, en virtud de la sección 13(a) o 15(d) de la Ley de Intercambio de Valores de 1934 (la “Ley de Bolsa”), incluidos los emisores privados extranjeros, deben llevar a cabo una evaluación anual del control interno de la entidad sobre los informes financieros.

Por tanto, se debe emitir un informe de control interno que contenga las afirmaciones de la gerencia, con respecto a la efectividad de la estructura y los procedimientos de control interno de la entidad sobre los informes financieros. Asimismo, la Sección 404 requiere que el contador público, independiente de la entidad, certifique la efectividad del control interno sobre los informes financieros de la entidad, de acuerdo con las normas establecidas por la PCAOB.

La realización de esta evaluación implica un trabajo interno en el cual se debe realizar un análisis de brecha, que permita establecer el estado actual del ambiente de control interno de la empresa (instrumento de evaluación) el principal objetivo es identificar que se tiene en referente a controles implementados, parcialmente implementados o aquellos

que no cumplen con su objetivo o no existen y requieren ser implementados como nuevos o ser replanteados.

Para cualquiera de los escenarios se deben crear planes de acción estructurados que puedan ser monitoreados de manera oportuna según lo que se haya definido.

Basado en lo anterior, el marco teórico ha permitido identificar factores de éxito o estrategias para la implementación de la norma y que pueden aplicar aquellas empresas que inician su viaje de adopción SOX.

Tabla 31. Estrategias para el cumplimiento de los requerimientos tecnológicos de la ley SOX

Estrategias para el cumplimiento de los requerimientos tecnológicos de la Ley SOX.	
Estrategia 1	Establecer el proyecto tecnológico de implementación SOX.
Estrategia 2	Seleccionar un equipo de proyecto eficaz para el desarrollo del proyecto tecnológico.
Estrategia 3	Realizar un *pre-assessment* del estado actual de la empresa en materia de control interno para tecnología basado en el marco de administración de tecnología-COBIT.
Estrategia 4	Definir e implementar los planes de acción con base en el resultado del *pre-assessment.*
Estrategia 5	Implementar la hoja de ruta que permita mantener el cumplimiento del control interno de las herramientas tecnológicas en alcance.

Fuente: Elaboración propia

Estrategia 1. **Establecer el proyecto tecnológico de implementación SOX**

Con esta estrategia se busca que el líder del proyecto por lo general el director de control interno, de manera formal de a conocer el proyecto a las altas directivas, así como socializarlo de manera general en toda la empresa. Los hitos más relevantes de esta primera estrategia son:

1. Establecer la alienación del proyecto con los objetivos estratégicos de la compañía; para las altas directivas, cualquier proyecto a implementar en la empresa debe

apuntar al cumplimiento de la estrategia que ha sido definida. Involucrar y comprometer a la alta dirección en la implementación del proyecto, en el cumplimiento en la ejecución de los planes de acción definidos y en el monitoreo de manera periódica a las áreas permitirá asegurar el correcto funcionamiento de los controles SOX- IT implementados.

2. Definir y comunicar el costo-beneficio de la implementación del proyecto; muchas empresas consideran la implementación de la ley meramente como un costo que permite cumplir con las exigencias, si bien es cierto, que esta tiene un costo considerable, implementar controles generales de TI para SOX va más allá y puede dar a la empresa la oportunidad de tomar mejores decisiones de negocio basadas en una información de mayor calidad y más oportuna gracias a la correcta administración y aseguramiento de los componentes tecnológicos que la procesan.
3. Involucrar al departamento de TI desde el inicio del proyecto; las inversiones en tecnología serán erróneas si se deja al departamento de TI al margen de la planificación estratégica y se le hace intervenir sólo a posteriori para averiguar cómo aplicar el plan establecido por los directores de negocio y los auditores, como aliado estratégico, actor importante.

Estrategia 2. Seleccionar un equipo de proyecto eficaz para el desarrollo del proyecto tecnológico.

La determinación del equipo de trabajo es definitiva para el correcto desarrollo del proyecto; es probable que la organización no esté preparada para dar cumplimiento a la ley SOX en un primer año, debido a esto se hace necesario contar con el apoyo de profesionales especializados para realizar un ejercicio de SOX – *Pre assessment* para después pensar en una certificación formal.

Para la definición del equipo de trabajo interno dependerá en gran medida del tamaño de la empresa y del estado de madurez de sus procesos de TI asociados a los controles requeridos por SOX; no obstante, para dar inicio al proyecto, es importante contar con un Gerente de proyecto, profesional en ingeniería de sistemas con experiencia en auditoria de sistemas e implementación de SOX, un contador experto en auditoria SOX (Controles automáticos) y un ingeniero de sistema especializado en auditoria de sistemas y con experiencia en implementación de COBIT, quienes estarán a cargo de realizar el *pre-assessment* y determinar el grado de madurez de control interno de TI de la empresa y la definición de los planes de acciones a ser implementados.

Por último, y para las fases posteriores, se deben contar con el acompañamiento de los equipos de auditoría interna y auditoría externa, quienes vigilarán que se cumpla adecuadamente con los controles mediante la ejecución periódica de pruebas, emisión de resultados y recomendaciones y acompañamiento permanente.

Estrategia 3. Realizar un *pre-assessment* del estado actual de la empresa en materia de control interno para tecnología basado en el marco de administración de tecnología-COBIT.

Esta estrategia permite determinar el nivel de madurez de cada una de las herramientas tecnológicas que componen el ambiente de control de TI de los procesos en alcance.

El pre-assessment debe basarse en primera instancia en lo que SOX exige y segundo en la herramienta que permita cumplir esta exigencia, por lo que definir un marco de referencia de administración de tecnología como COBIT (hoy por hoy el más utilizado) es el punto de partida para evaluar el ambiente de TI, en la medida que COBIT 2019 da los lineamientos, así como los aspectos a ser evaluados para determinar la madurez del ambiente de control interno de TI.

SOX IT y COBIT están estrechamente relacionados toda vez que COBIT abarca dentro de sus 40 componentes los tres principales requerimientos tecnológicos necesarios para implementar la ley SOX, la cual, de manera general busca garantizar la correcta administración de la tecnología para asegurar la razonabilidad de la información financiera, tarea para la que COBIT resulta ser una de las mejores opciones disponibles.

La aplicación del instrumento es una de las estrategias más relevantes ya que será el insumo principal para la definición de los planes de acción para ejecutar el proyecto.

Estrategia 4. Definir e implementar los planes de acción con base en el resultado del pre-assessment.

Esta estrategia del proyecto busca que la definición de los planes de acción esté sustentada en datos reales sobre el estado actual del ambiente de TI lo que asegura que se está atacando la necesidad de manera adecuada para llegar al estado mínimo deseado.

La definición de los planes de acción a ejecutar deberá ser un informe donde se indique:

- Nivel de madurez general del ambiente de TI -SOX de la empresa.
- Planes de acción a ejecutar por cada uno de los frentes (ITGC's, ELC y controles automáticos).
- Cronograma para la ejecución de cada uno de los planes de acción.
- Recurso humano y financiero requerido.
- Relación de los beneficios (crecimiento, objetivos estratégicos, cumplimiento, ingresos, inversiones, estandarización) que tiene para la compañía implementar los planes de acción y mejorar el nivel de madurez del ambiente de control interno de TI.

- Entregables por fases.

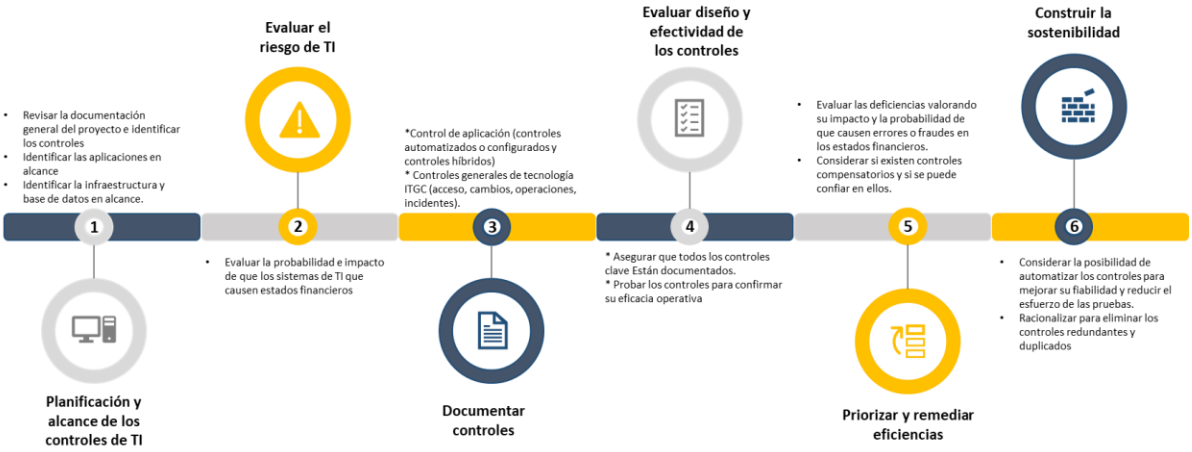
Esta estrategia se convierte en el centro del proyecto ya que es aquí donde se definen los controles a implementar para cada una de las herramientas tecnológicas en alcance.

Estrategia 5. Implementar una hoja de ruta que permita mantener el cumplimiento del control interno de tecnología de las herramientas tecnológicas en alcance.

El éxito de cualquier proyecto implementado se mide con base en la sostenibilidad de este a través del tiempo y como este logra mejorarse continuamente según sea requerido de acuerdo con las necesidades que surjan, en este sentido, esta estrategia, permitiría garantizar que lo definido atiende los requerimientos tecnológicos de SOX IT de manera continua.

Los resultados de la implementación de la hoja de ruta se convertirán en el input de las siguientes evaluaciones del ambiente de control interno de TI y permitirá definir si la empresa está preparada para enlistarse en la bolsa de valores, atender la rigurosa evaluación de la SEC y obtener un resultado favorable que maximice el valor de la compañía, asegurando la información de los estados financieros que se procesan a través de las herramientas bajo control. Una hoja de ruta a seguir se observa en la ilustración 14.

Ilustración 14. Hoja de ruta para el cumplimiento de SOX en TI



Fuente: Elaboración propia.

Cada una de las estrategias definidas se basan en el marco teórico que sustenta la monografía atendiendo a la necesidad identificada y que puede ser utilizado por empresas de cualquier línea de negocio, no obstante, es importante mencionar que cada empresa es diferente y será con el resultado de la aplicación del instrumento de evaluación como se podrá determinar el tiempo, los recursos y los planes de acción a ejecutar para cumplir con los requerimientos de la ley SOX.

Discusión

La presente investigación se desarrolla con el fin de recomendar a las empresas colombiana que cotizan en la bolsa de valores de New York la definición de estrategias para dar cumplimiento de los requisitos tecnológicos al implementar la Ley SOX.

De acuerdo con el marco teórico, las exigencias tecnológicas de la ley SOX se convierten en uno de los grandes retos al implementar el marco en cualquier empresa, esto se debe en primera instancia al desconocimiento sobre el impacto que la ley puede tener sobre el ambiente tecnológico de la compañía y segundo, porque consideran que solo la ley requiere controlar los procesos financieros y contables.

Este desconocimiento se debe a que por ser una ley que busca controlar la información financiera pero no se tiene en cuenta que cualquier dato financiero hoy por hoy tiene interacción con cualquier sistema de información por consiguiente si se quiere asegurar el dato contable, primero se debe asegurar que la aplicación por donde esta se procesa este controlado y sea seguro, de lo contrario no será posible garantizar la fiabilidad de la información financiera.

Una de las primeras evidencias al estudiar el marco teórico es que “la tecnología es imprescindible para el cumplimiento de los objetivos y la prestación de servicios de las entidades a sus diferentes grupos de interés, en condiciones de seguridad, calidad y cumplimiento. Por lo tanto, se tiene que velar porque el diseño del sistema de control interno para la gestión de la tecnología responda a las políticas, necesidades y expectativas de la entidad, así como a las exigencias normativas sobre la materia” (Superintendencia Financiera de Colombia, 2014).

De otra parte, el sistema debe ser objeto de evaluación y de mejoramiento continuo con el propósito de contribuir al logro de los objetivos institucionales y a la prestación de

los servicios en las condiciones señaladas. (Superintendencia Financiera de Colombia, 2014)

En este sentido, las empresas tendrán que establecer, desarrollar, documentar y comunicar los lineamientos de tecnología y asignar los recursos, procesos, procedimientos, metodologías y controles necesarios para lograr su cumplimiento. (Superintendencia Financiera de Colombia, 2014).

Por otro lado, sin que sea un punto apartado de la administración de la tecnología, se evidencia la imperante necesidad del involucramiento de CIO dentro del comité de líderes, quien tendrá la responsabilidad de dar a conocer la estrecha relación y la importancia del área de tecnología para lograr una exitosa implementación de la ley SOX.

La implementación de la ley SOX es una tarea que involucra todas las áreas de la compañía y se requiere que el equipo encargado de la implementación establezca la hoja de ruta y la comunique a todos los *steakeholders* su papel dentro de esta y el impacto que tendría para la empresa y los objetivos desde la perspectiva SOX el no ejecutar lo definido.

Con base en lo anterior se recomienda a las empresas implementar la hoja de ruta sugerida, que contempla todos los aspectos que deben tenerse en cuenta para lograr una implementación controlada y que se acerca a cumplir de manera precisa los requerimientos tecnológicos de la ley SOX.

Conclusiones.

A muchas empresas, particularmente a los emisores extranjeros, les ha resultado bastante difícil y han tenido problemas para hacer frente a la gran cantidad de requisitos tecnológicos de la Ley Sarbanes Oxley - SOX, lo anterior sucede porque la mayoría se centran en atender las implicaciones que esta tiene desde la perspectiva financiera desconociendo los requerimientos y exigencias de cumplimiento desde el ambiente tecnológico.

Las empresas que buscan cotizar en bolsa de valores de New York deben asegurar que a las aplicaciones que soportan todos sus procesos financieros, así como aquellos que puedan afectar estos datos les sean implementados los mínimos controles de tecnología para poder iniciar de manera adecuada el proceso y cumplir con lo exigido por la ley SOX.

Para dar respuesta al cumplimiento de los requerimientos tecnológicos de la Ley SOX las empresas deben partir de un diagnóstico inicial que les permita identificar el estado actual de su ambiente de control interno de las tecnologías de la información que las lleve a definir los planes de acción requeridos definir si la empresa está preparada para enlistarse en la bolsa de valores y atender la rigurosa evaluación de la SEC.

Para realizar el diagnóstico del estado actual del ambiente de control interno, la empresa debe basarse en un marco de administración de la tecnología que le provea los lineamientos para poder ejecutar la evaluación y tener un punto de partida y referencia que permita medir el estado actual, así como el estado futuro o esperado una vez se implementen los planes de acción.

Referencias

Aaccoullum, T. (2006). Bridging the Great Divide. *Internal Audit*, 49-53.

Bone, J. (2009). Managing IT Controls for SOX Compliance. *Compliance Week*, 51, 62.

Booth, J. (4 de 12 de 2021). *What to look for in SOC reports for accounting software?* Obtenido de Accounting Today: Accountingtoday.com

Chan, S. (2004). *Sarbanes-Oxley: The IT Dimension.* TIM MCCOLLUM COMPUTERS & AUDITING.

Chiu, G. (2015). The Evolution of ITGC. *Informationtech*, 18-19.

Cifuentes, A. (2006). *LA LEY SARBANES-OXLEY DE 2002.* Bogotá: Universidad Externado de Colombia.

Cohen, A. F. (2005). *The US Sarbanes–Oxley Act of 2002: Summary and update for non-US issuers.* London: HENRY STEWART PUBLICATIONS, 2005.

Colombia, Superintendencia financiera de. (19 de Mayo de 2009). Circular 029 de 2009. Bogotá, Colombia.

Commission, S. -S. (30 de Julio de 2002). *SEC - Security and Exchange Commission.* Obtenido de https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Control interno - Marco integrado - Resumen Ejecutivo .*

Damianides, M. (15 de Oct de 2004). How does SOX change IT? *The Journal of Corporate Accounting & Finance*, pág. 35.

Dziak, M. (2019). *COBIT (Control Objectives for Information and Related Technologies).* Salem Press Encyclopedia.

Escuela Pública digital Universidad de la Punta. (s.f.). Teoría y gestión de las organizaciones. San Luis, San Luis, Argentina.

García, V. (Julio de 2005). Discovering Business Value in IT investments for Sarbanes-Oxley Compliance. *Wall Street & Technology*, pág. S3.

Hernández-Sampieri, R., & Mendoza, P. (2018). *Metodología de la investigación : las rutas cuantitativa, cualitativa y mixta.* México: McGraw-Hill.

ISACA. (2012). *COBIT 5, Procesos Catalizadores.* Rolling Meadows, IL.

ISACA. (2014). *IT Control Objectives for Sarbanes-Oxley.* Rolling Meadows, IL: ISACA.

ISACA. (2019). *COBIT 2019 MARCO DE REFERENCIA, Objetivos de gobierno y gestión.* Schaumburg, IL: ISACA.

ISACA. (08 de 2022). *Isaca*. Obtenido de www.isaca.org

IT Governance Institute. (2007). *COBIT 4.1 Marco de Trabajo, Objetivos de Control, Directrices Generales, Modelos de Madurez.* Illinois: IT Governance Institute.

Jaques, R. (2005). IT implications of Sarbanes-Oxley. *Financial Director*, 53.

Karanja, E., & Zaveri, J. (2013). *Ramifications of the Sarbanes.* Emerald Group Publishing Limited.

Kecskés, A. (2017). *REFORMING CORPORATE GOVERNANCE VIA LEGISLATION IN THE UNITED STATES – THE CASE OF THE SARBANES-OXLEY ACT*.* Hungary: University of Pécs. .

Lahti, C. B. (2005). *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools.* Elsevier Inc.

Lanto Ningrayati Amali, M. R. (1 de February de 2020). The measurement of maturity level of information technology service based on COBIT 5 framework. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, pág. 133~139.

Marta Blahova, V. M. (2019). *THE INFORMATION SECURITY TO SOFTWARE.* Viena, Austria: Annals of DAAAM & Proceedings.

McCausaland, R. (2004). *SOX and the IT risk factor.* Accounting Technology.

Morales, J. D. (Septiembre de 2005). *La Ley Sarbanes-Oxley y la auditoría.* Obtenido de Partida Doble: www.partidadoble.es

Muñoz, I. U. (2011). Gobierno de TI – Estado del arte. *Revista S&T*, 53.

Murphy, G. (2016). Los controles generales de tecnología y el líder de contabilidad. *Techology Workbook*, 3.

Nathoo, F. (Nov de 2007). Finding the Synergies in SOX and IT Risk. *The RMA Journal*.

PCAOB. (31 de Diciembre de 2016). *PCAOB Public Company Accounting Oversight Board*. Obtenido de PCAOBPublic Company Accounting Oversight Board Web site: https://pcaobus.org/

PCAOB. (2020). *PCAOB*. Obtenido de https://pcaobus.org/

Rodríguez, I. (2 de Mayo de 2021). *Auditool, Red global de conocimientos de auditoria y control interno*. Obtenido de https://www.auditool.org/blog/auditoria-externa/7759-la-utilidad-de-los-informes-soc

Sally, C., & Lepeak, S. (2004). *IT and Sarbanes OXley.* Toronto: CMA Management.

Samuel, S. (2021). Securities and Exchange Commission (SEC).

Sarctoni, K. (03 de July de 2005). Sarbanes-Oxley Act impacts IT Systems. *Focus*, pág. 2.

SEC, S. a. (2020). *The Laws That Govern the Securities Industry - Sarbanes-Oxley Act of 2002.*

SEC, U.S. SECURITIES AND EXCHANGE COMMISSION. (2020). *Cybersecurity and Resiliency Observations.* Washington, DC: SEC, US SECURITIES AND EXCHANGE COMMISSION.

Superintendencia Financiera de Colombia. (03 de Octubre de 2014). *CIRCULAR EXTERNA 29 DE 2014.* Bogotá. Obtenido de https://www.superfinanciera.gov.co/

Thibodeau, P. (24 de Oct de 2005). Sarbanes-Oxley Adds to IT Costs But Pushes Companies to Prepare. *Computerworld*, pág. 1.

Udemy Business. (Abril de 2022). Sarbanes-Oxley (SOX) ITGC Audit Concepts and Coordination. Estados Unidos.