El modelo COBIT 5 para auditoría y el control de los sistemas de información

Autores:

Ing. Julio Ernesto Mora Aristega (jmora@utb.edu.ec)

Ing. Joffre Vicente León Acurio (jvleon@utb.edu.ec)

Ing. Magdalena Rosario Huilcapi Masacon (mhuilcapi@utb.edu.ec)

Ing. Diana Carolina Escobar Mayorga (descobar@utb.edu.ec)

Institución: Universidad Técnica de Babahoyo

Sistemas: Tecnologías de la información y comunicación

Resumen

El desarrollo informático de las organizaciones representa el progreso en el logro de las metas de las organizaciones. El COBIT 5, es un modelo para auditar la gestión y el control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de las tecnologías de información (TI), usuarios y, por supuesto, a los auditores involucrados en el proceso.

Por tal razón, el objetivo de esta investigación es conocer cómo se ha utilizado en modelo COBIT en la auditoría de los sistemas informáticos de las organizaciones, se aplicó una encuesta de la cual se obtuvo la información pertinente que permite concluir que los sistemas de información representan la oportunidad para el logro de los objetivos organizacionales en congruencia con sus metas corporativas, metas de tecnologías de la información y las metas de los catalizadores, por ende, es prioridad de los administradores de sistemas informáticos y del gobierno corporativo realizar todas las acciones necesarias para lograrlas y que el modelo COBIT 5 proporciona una visión integral y sistémica del gobierno, y la gestión de la empresa TI basada en varios catalizadores, así como que la gestión de la información de la empresa y la TI relacionada, incluyen las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

Palabras claves: Auditoría, sistemas, control, información.

Abstract

The organizational development of organizations represents progress in achieving the goals of organizations. COBIT 5 is a model for auditing the management and control of information and technology systems, aimed at all sectors of an organization, ie information technology (IT) managers, users and, of course, to the auditors involved in the process.

For this reason, the objective of this research is to know how has been used in the COBIT model in the audit of the information systems of the organizations, a survey was applied from which the relevant information was obtained that allows to conclude that the information systems represent the opportunity to achieve organizational objectives in

line with corporate goals, information technology goals and catalyst goals is therefore a priority for IT administrators and corporate governance to take all necessary actions to and that the COBIT 5 model provides a comprehensive and systemic view of governance, and the management of the IT company based on various catalysts, as well as the management of company information and related IT, including the activities and responsibilities both of IT functions as well as business
Keywords: Audit, systems, control, information.

Introducción

El desarrollo de sistemas informáticos ha sido clave en el desarrollo empresarial, los sistemas han pasado por un sinnúmero de transformaciones que cada vez han implementado beneficios, y las formas de auditar han sido modificadas en función de las necesidades que se van presentando una a continuación de otra.

En tal sentido, el Cobit es un aporte a través de un modelo que permite revisar cuidadosamente el trabajo realizado por los sistemas informáticos en relación a las necesidades empresariales. Con lo cual, la información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

Como resultado, hoy más que nunca, las empresas y sus ejecutivos se esfuerzan en:

- ✓ Mantener información de alta calidad para soportar las decisiones del negocio.
- ✓ Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI eficaz e innovador.
- ✓ Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- ✓ Mantener los riesgos relacionados con TI en un nivel aceptable.
- ✓ Optimizar el coste de los servicios y tecnologías de TI.

- ✓ Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Durante la pasada década, el término “gobierno” ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

Al respecto, la empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión. Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad.

En tal sentido, COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. Por lo tanto, COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

El problema fundamental es que las empresas poseen un capital activo muy valioso: información y tecnología. Con lo cual, cada vez en mayor medida, el éxito de una empresa depende de la comprensión de ambos componentes. Las buenas prácticas concentradas en el marco de referencia COBIT, permiten que los negocios se alineen con la tecnología de la información para así alcanzar los mejores resultados.

La información y la tecnología que la soporta representan los activos más valiosos de muchas empresas, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, es decir, el aumento en los requerimientos regulatorios, así como también una gran dependencia de muchos de los procesos de negocio en TI. Pero todos estos elementos son clave para el gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos agrupados en el consejo de directores de la empresa y, para ello, es necesario el liderazgo y una buena base de estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas.

Los Objetivos de Control para la Información y la Tecnología relacionada (CobiT®), brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de CobiT, están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudan a optimizar las inversiones facilitadas por la TI, asegura la entrega del servicio y brindan un patrón de medición, con el cual, se puede calificar cuando las cosas no vayan bien. Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección empresarial debe implantar un sistema de control interno o un marco de trabajo. El marco de trabajo de control CobiT contribuye a estas necesidades de la siguiente manera:

- ✓ Estableciendo un vínculo con los requerimientos del negocio.
- ✓ Organizando las actividades de TI en un modelo de procesos.

- ✓ Identificando los principales recursos de TI.
- ✓ Definiendo los objetivos de control gerenciales.

La orientación al negocio que realiza CobiT, consiste en vincular las metas del negocio con las metas de TI, brindando métricas y modelos de madurez para medir los logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las responsabilidades de planear, construir, ejecutar y monitorear; de esta manera, se ofrece una visión de punta a punta de la TI.

En tal sentido, el concepto de arquitectura empresarial ayuda a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas. En resumen, para proporcionar la información que la empresa necesita de acuerdo a sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Una respuesta al requerimiento de determinar y monitorear el nivel apropiado de control y desempeño de TI, son los conceptos que *CobiT* define específicamente:

- ✓ Benchmarking de la capacidad de los procesos de TI. Son modelos de madurez derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software.
- ✓ Metas y métricas de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de *balanced business Scorecard* de Robert Kaplan y David Norton.
- ✓ Objetivos de las actividades para controlar estos procesos, con base en los objetivos de control detallados de COBIT.

La evaluación de la capacidad de los procesos basada en los modelos de madurez de CobiT, es una parte clave de la implementación del gobierno de TI. Después de

identificar los procesos y controles críticos de TI, el modelado de la madurez permite identificar y demostrar a la dirección las brechas en la capacidad.

CobiT, es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. CobiT, permite el desarrollo de políticas claras y de buenas prácticas para el control de TI por parte de las empresas. CobiT constantemente se actualiza y armoniza con otros estándares, por lo tanto, CobiT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. Con lo cual, la estructura de procesos de CobiT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar.

De tal manera, que el objetivo de la investigación es conocer cómo se ha utilizado en modelo COBIT en la auditoría de los sistemas informáticos de las organizaciones.

Desarrollo

Estado del Arte

Electronic Data Processing (EDP) Auditor´s Association, fue creada en 1967 y con el tiempo sería el antecedente del grupo profesional que se encargaría de elaborar el marco de referencia del COBIT. Esta organización, estuvo integrada por Auditores Internos que consideraban que podrían brindar mayor importancia a los temas relacionados con la tecnología de información, dado que la asociación profesional a la que pertenecían no lo hacía. El COBIT ha sido diseñado por dos organizaciones: IT *Governance Institute e Information System Audit and Control Foundation* – ISACA. Según sus mentores, el proceso de evolución del COBIT ha pasado por las siguientes etapas: (Fonseca Luna, 2011, pág. 26).

- ✓ Primera 1996: Herramienta de auditoría para la Tecnolgía de Información (TI).
- ✓ Segunda 1998: Orientada al control de la TI en las compañías.
- ✓ Tercera 2000: Orientada a la gestión de la TI en las compañías.

- ✓ Cuarta 2005: Orientada al gobierno corporativo de la TI.
- ✓ 2007: Fue divulgada la versión 4.1

El modelo COBIT, es un modelo de evaluación que permite verificar y llevar un control de los sistemas de información de los negocios y la seguridad. Mediante este modelo, se vincula la tecnología, orientado a todos los sectores de una organización, es decir: dirigentes, beneficiarios y los auditores responsables del proceso.

El modelo posee una estructura con marco de acción donde se ajustan los razonamientos de investigación, por ejemplo la seguridad y eficacia, se verifican los recursos que perciben la tecnología de información, mediante recurso humano, instalaciones técnicas, entre otras y, al final, una valoración sobre los métodos involucrados en la organización (Figueroa Morán , Paladines Morán, Paladines Morán , Caicedo Plúa, & Romero Castro , 2017, pág. 37).

El modelo COBIT, es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de las tecnologías de información (TI), usuarios y por supuesto, los auditores involucrados en el proceso (Baud, 2016, pág. 43).

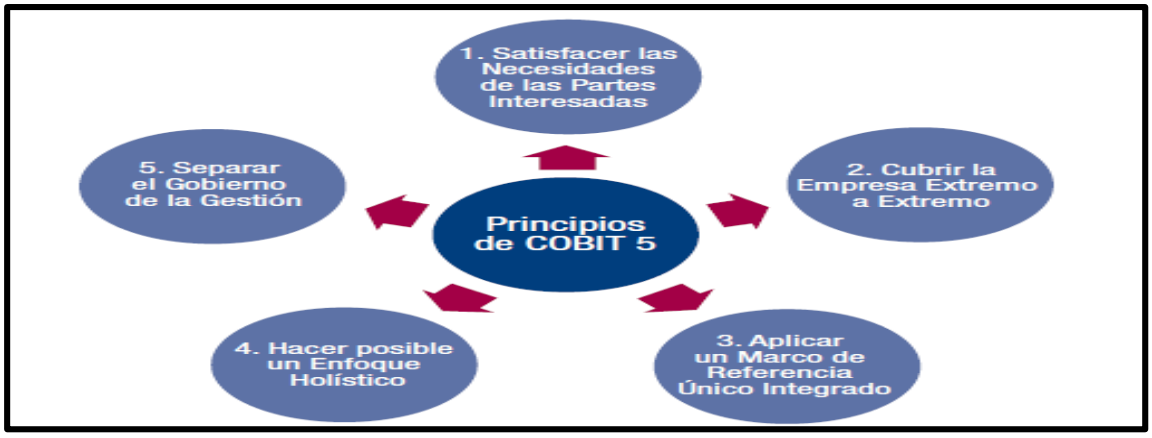
COBIT, se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado, en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT propone un marco de acción, donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros; y, finalmente, se realiza una evaluación sobre los procesos involucrados en la organización.

Este modelo define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios principales, a saber:

- ✓ Planificación y organización
- ✓ Adquisición e implantación
- ✓ Soporte y servicio
- ✓ Monitoreo

Figura 1. Principios del COBIT 5



Fuente: tomado de COBIT 5

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor, significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales (Fonseca Luna, 2011, pág. 28).

Figura 2. Necesidades de las partes interesadas

Fuente: tomado de COBIT 5

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT, es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y, por supuesto, a los auditores involucrados en el proceso.

O sea, es un conjunto de mejores prácticas para el manejo de información creado o desarrollado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA, en inglés: Information Systems Audit and Control Association), conformada por expertos de varios países, y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés:IT Governance Institute) en 1992. (Solares Soto , Baca Urbina, & Acosta Gonzaga, 2014, pág. 75).

Las siglas COBIT, significan Objetivos de Control para Información y Tecnologías relacionadas (Control Objectives for Information and related Technology). La estructura del modelo COBIT, propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, entre los que destacan: el recurso humano,

instalaciones, sistemas, entre otros; y, finalmente, se realiza una evaluación sobre los procesos involucrados en la organización.

Por lo tanto, el COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca control específicos de IT desde una perspectiva de negocios.

La adecuada implementación de un modelo COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado".

Asimismo, señaló un informe de ETEK.COBIT, que es una herramienta de gobierno de TI, que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

De esta manera, COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Con lo cual, estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Los mismos, que facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

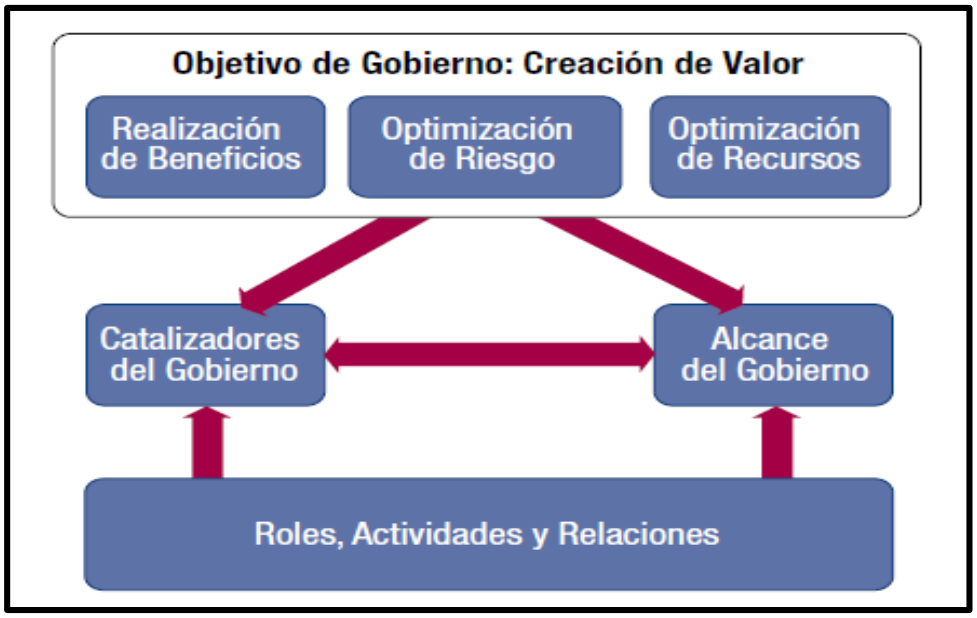
La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores". En tal sentido, los gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información), y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información (Muñoz Razo, 2014, pág. 54).

Cualquier tipo de empresa, puede adoptar una metodología COBIT como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos IT y, consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos, finalizó el informe de ETEK.

La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición on-line estuvo disponible en 2003); y la cuarta edición en diciembre de 2005. Asimismo, la versión 4.1 está disponible desde mayo de 2007. En su cuarta edición, COBIT como un conjunto de lineamientos y estándares internacionales tiene 34 objetivos de alto nivel que cubren 210 objetivos de control (específicos o detallados), define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, a saber : Planificación y Organización, Adquisición e Implementación, Entrega o Servicios y Soporte, y, Supervisión o Monitoreo y Evaluación. En inglés: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

El enfoque de gobierno extremo a extremo que es la base de COBIT 5, está representado en la figura 3, mostrando los componentes clave de un sistema de gobierno.

Figura 3. Objetivo del Gobierno – Creación de Valor



Fuente: tomado de COBIT 5

En el desarrollo de la investigación se ha utilizado una encuesta aplicada a las organizaciones sobre como evalúan los sistemas de información en las organizaciones, a continuación se detallan los aspectos más relevantes:

Tabla 1. Frecuencia de práctica de auditoría

Criterio	Frecuencia	Impacto Porcentual
Siempre	16	27%
Frecuentemente	32	53%
A veces	12	20%
Rara vez	0	0%
Nunca	0	0%
Total	**60**	**100%**

Fuente: tomado de encuesta aplicada al personal responsable de la administración de sistemas

Según la tabla 1, la mayoría de las empresas realizan la revisión de sus sistemas informáticos a fin de conocer sus debilidades y superarlas a futuro, para lo cual, deben implementar acciones que se encaminen al logro de los objetivos organizacionales planteados por la gerencia.

Tabla 2. Nivel de definición de objetivos

Criterio	Frecuencia	Impacto Porcentual
Alto	15	25%
Medio	40	67%
Bajo	5	8%
Total	**60**	**100%**

Fuente: tomado de encuesta aplicada al personal responsable de la administración de sistemas

Según la tabla 2, un alto porcentaje de empresas tiene un nivel medio respecto a la definición de los objetivos, por tal razón, deben empezar por reforzar esta debilidad, para poder fortalecer los sistemas informáticos y alinearlos a los objetivos empresariales correctamente definidos.

Tabla 3. Consideración de las partes interesadas en la toma de decisiones

Criterio	Frecuencia	Impacto Porcentual
Alto	12	20%
Medio	45	75%
Bajo	3	5%
Total	**60**	**100%**

Fuente: *tomado de encuesta aplicada al personal responsable de la administración de sistemas*

La tabla 3, indica que las empresas toman en consideración a sus partes interesadas al momento de tomar decisiones respecto a beneficios, evaluación de riesgos y recursos que se necesitan para el correcto desarrollo de las actividades empresariales.

Tabla 4. Factores que influyen en el desarrollo empresarial

Criterio	Frecuencia	Impacto Porcentual
Mercado	3	5%
Industria	10	17%
Geopolítica	5	8%
Cultura	5	8%
Organización	17	28%
Umbral de riesgos	13	22%
Otros	7	12%
Total	**60**	**100%**

Fuente: tomado de encuesta aplicada al personal responsable de la administración de sistemas

La tabla 4, revela que las empresas consideran que uno de los factores más importantes en el desarrollo empresarial está reflejado en los riesgos, teniendo que la organización debe tomar las acciones pertinentes para superarlos.

Tabla 5. Metas de la organización

Criterio	Frecuencia	Impacto Porcentual
Metas corporativas	15	25%
Metas relacionadas con las TI	32	53%
Metas de los catalizadores	13	22%
Total	**60**	**100%**

Fuente: tomado de encuesta aplicada al personal responsable de la administración de sistemas

De acuerdo con la tabla 5, las metas más importantes de las organizaciones son las metas relacionadas con las tecnologías de información, las mismas que están estrictamente relacionadas con las corporativas y las de los catalizadores y todas estas coadyuvan a conseguir las metas de las empresas.

Conclusiones

Los sistemas de información representan la oportunidad para el logro de los objetivos organizaciones en congruencia con sus metas corporativas, metas de tecnologías de la información y las metas de los catalizadores, es prioridad de los administradores de sistemas informáticos y del gobierno corporativo realizar todas las acciones necesarias para lograrlas.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo a extremo, es decir, todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

Referencias bibliográficas

Baud, J.-L. (2016). ITIL - V3: Entender el Enfoque y Adoptar las Buenas Prácticas. Barcelona: Eni Ediciones.

Figueroa Morán , G. L., Paladines Morán, J. P., Paladines Morán , J. N., Caicedo Plúa, C. R., & Romero Castro , M. I. (2017). Modelo de Plan Estratégico de los Sistemas para la Gestión y Organización a través de una Plataforma Informática. Alicante: 3 Ciencias.

Fonseca Luna, O. (2011). Sistema de Control Interno para Organizaciones. Lima: IICO.

Muñoz Razo, C. (2014). Auditoría de Sistemas Computacionales. México: Pearson.

Solares Soto , P., Baca Urbina, G., & Acosta Gonzaga, E. (2014). Administración Informática I: Análisis y Evaluación de Tecnologías de Información. México: Patria.