UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS ECONÓMICAS Y FINACIERAS

CARRERA DE CONTADURÍA PÚBLICA

UNIDAD DE POSTGRADO

AUDITORÍA INFORMÁTICA DEL SISTEMA CONTABLE FINANCIERO DE LA EMPRESA M & F Ltda.

(Estudio de Caso)

Materia: Taller de Investigación II

Docente: Mg. Sc. Elizabeth Salazar Ballesteros

Maestrante: Olesia Dalenkevitch

Fecha: Agosto 2017

TABLA DE CONTENIDOS

AUDITORÍA INFORMÁTICA DEL SISTEMA CONTABLE FINANCIERO

Estudio de Caso: Empresa M & F Ltda.

1. MARCO TEÓRICO

1.1. INFORMÁTICA

Se define que (ENCICLOPEDIA DE DEFINICIONES (DEFINICION DE:), 2008-2016): El término informática proviene del francés informatique, implementado por el ingeniero Philippe Dreyfus a comienzos de la década del ’60 como combinación de las palabras information y automatique. Es el procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales. Los sistemas informáticos deben contar con la capacidad de cumplir tres tareas básicas: entrada (captación de la información), procesamiento y salida (transmisión de los resultados). El conjunto de estas tres tareas se conoce como algoritmo.

La informática reúne a muchas de las técnicas que el hombre ha desarrollado con el objetivo de potenciar sus capacidades de pensamiento, memoria y comunicación. Su área de aplicación no tiene límites: la informática se utiliza en la gestión de negocios, en el almacenamiento de información, en el control de procesos, en las comunicaciones, en los transportes, en la medicina y en muchos otros sectores.

La informática abarca también los principales fundamentos de las ciencias de la computación, como la programación para el desarrollo de software, la arquitectura de las computadoras y del hardware, las redes como Internet y la inteligencia artificial. Incluso se aplica en varios temas de la electrónica.

1.2. SISTEMA DE INFORMACIÓN

Según los autores LAUDON Y LAUDON (2012), profesores de Administración de Empresas, un sistema de información es un organismo que recolecta, procesa, almacena y distribuye información. Son indispensables para ayudar a los gerentes a mantener ordenada su compañía, a analizar todo lo que por ella pasa y a crear nuevos productos que coloquen en un buen lugar a la organización. Esta definición es una de las únicas que manifiesta la exigencia de que un sistema de información tenga componentes, aunque no especifica cuáles deban ser, posiblemente porque intenta englobar todas las posibles variantes de este concepto.

1.3. SISTEMA DE INFORMACIÓN CONTABLE

El propósito básico del sistema de información contable (ELIZONDO LÓPEZ, 2004) de una organización es proveer información útil acerca de una entidad económica, para facilitar la toma de decisiones de sus diferentes usuarios tales como: accionistas, acreedores, inversionistas, administradores o las mismas autoridades gubernamentales. Como consecuencia que el sistema de información contable de una empresa sirve a un conjunto de diversos usuarios, se originan diferentes ramas o subsistemas.

- El subsistema de información financiera: contabilidad financiera.
- El subsistema de información fiscal: contabilidad fiscal.
- El subsistema de información administrativa: contabilidad administrativa.

1.3.1. Subsistema de información financiera

Está conformado por una serie de elementos tales como las normas de registro, criterios de contabilización y formas de representación de información de usuarios externos. A este tipo de sistema de información se le conoce debido a que expresa en términos cuantitativos y monetarios las transacciones que realiza una entidad así como ciertos acontecimientos económicos que le afectan, con el fin de proporcionar información útil y confiable a los diferentes usuarios externos para su toma de decisiones.

Los usuarios de la contabilidad financiera: La información financiera es útil para los accionistas, acreedores, analistas e intermediarios financieros, el público inversionista, los organismos reguladores y para todos aquellos usuarios externos de la información contable de una organización económica.

1.3.2. Subsistema de información fiscal

Está diseñado para dar cumplimiento a las obligaciones tributarias de las organizaciones respecto de usuario específico: el fisco. A las autoridades gubernamentales les interesa contar con la información de las diferentes organizaciones económicas para cuantificar el monto de la utilidad que haya obtenido de acuerdo con las leyes fiscales en vigor como producto de sus actividades y así poder determinar la cantidad del impuesto que le corresponde a pagar.

Los usuarios de la contabilidad fiscal: La información generada por el subsistema de información fiscal es útil para las autoridades gubernamentales.

1.3.3. Subsistema de información administrativa

La contabilidad administrativa es un sistema de información al servicio de las necesidades internas de la administración orientado a facilitar las funciones administrativas de planeación y control así como la toma de decisiones. Entre las aplicaciones se encuentran la elaboración de presupuestos, la determinación de costos de producción y la evaluación de la eficiencia de las diferentes áreas operativas de la organización, así como el desempeño de los diferentes ejecutivos de la misma.

Los usuarios de la contabilidad administrativa: La información generada por este subsistema, es útil solo para los usuarios internos de la organización representados por los directivitos de la misma, especialmente por los directores generales, gerentes de área, jefes de departamento, entre otros.

1.4. AUDITORÍA

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto, con el objeto de emitir una opinión independiente y competente.

Aunque hay muchos tipos de auditoría, la expresión se utiliza generalmente para designar a la «auditoría externa de estados financieros», que es una auditoría realizada por un profesional experto en contabilidad, de los libros y registros contables de una entidad, para opinar sobre la razonabilidad de la información contenida en ellos y sobre el cumplimiento de las normas contables.

Según Adriana AMADO: “La auditoría es una serie de métodos de investigación y análisis con el objetivo de producir la revisión y evaluación profunda de la gestión efectuada”. (2008)

El requisito básico para la realización de una auditoría es la independencia, que comprende los siguientes puntos:

- Independencia mental: El estado mental que permite proporcionar una opinión sin ser afectados por influencias que comprometan el juicio profesional y su dirección, permitiendo a una persona actuar con integridad, y ejercer objetividad y escepticismo profesional.
- Independencia aparente: Cuando se evitan hechos y circunstancias que sean tan importantes que un tercero juicioso e informado, con conocimiento de toda la información relevante, incluyendo

cualesquiera salvaguardas que se apliquen, concluiría de manera razonable que la integridad, objetividad o escepticismo profesional del equipo auditor para atestiguar hubieran sido comprometidos.

1.4.1. Tipos de Auditoría

De acuerdo al criterio de Antonio LATTUCA, Cayetano MORA et al (1991), los tipos de auditoría son:

- Auditoría contable, la realizada por un profesional, experto en contabilidad, sobre los estados contables de una entidad.
- Auditoría administrativa, es la técnica de control administrativo que examina -sistemática e integralmente- el grado de eficiencia en la aplicación del proceso administrativo a las distintas funciones de una entidad, así como la manera en que esta eficiencia influye en la efectividad de las mismas.
- Auditoría energética, una inspección, estudio y análisis de los flujos de energía en un edificio, proceso o sistema con el objetivo de comprender la energía dinámica del sistema bajo estudio.
- Auditoría jurídica, la efectuada por un profesional del derecho, con capacidad y experiencia en derecho civil que realiza la revisión, examen y evaluación de los resultados de una gestión específica o general de una institución o cuerpo, con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño.
- Auditoría informática, proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
- Auditoría medioambiental, cuantificación de los logros y la posición medioambiental de una organización.
- Auditoría social, proceso que una empresa u organización realiza con ánimo de presentar balance de su acción social y su comportamiento ético.
- Auditoría de seguridad de sistemas de información, análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.
- Auditoría de innovación, proceso de obtención información sobre la situación actual de la empresa frente a la innovación.
- Auditoría política, revisión sistemática de los procesos y actividades, orientadas ideológicamente, de toma de decisiones

de un grupo para la consecución de unos objetivos, en beneficio de todos.

- Auditoría electoral, la realizada a sistemas electorales de los diferentes países con sistema democrático y se realizan para darle confiabilidad y transparencia al sistema.
- Auditoría de accesibilidad, revisión de la accesibilidad de un sitio web por parte de un experto.
- Auditoría de marca, metodología para medir el valor de una marca.
- Auditoría de código de aplicaciones, proceso de revisar el código de una aplicación para encontrar errores en tiempo de diseño.
- Auditoría científico-técnica, realizada a instituciones encargadas de la investigación científica y técnica en las diferentes áreas del trabajo humano.
- Auditoría forense, cuando se revisan datos y documentos históricos de empresas y se comparan con el fin de detectar principalmente fraudes, robos, trucos fiscales, trucos contables o cualquier otra situación anómala en la que se investiga a los involucrados intelectuales y materiales del hecho; regularmente se hacen estimaciones en dinero de las cifras malversadas.

1.5. AUDITORÍA INFORMÁTICA

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. (PIATTINI, DEL PESO, & Et Al, 2001)

Los objetivos de la auditoría Informática son:

- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos

Sus beneficios son:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Desempeño
- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad.

Se ejecuta usualmente en alguna o combinación de las siguientes áreas:

- Gobierno corporativo
- Administración del Ciclo de vida de los sistemas
- Servicios de Entrega y Soporte
- Protección y Seguridad
- Planes de continuidad y Recuperación de desastres

1.5.1. Tipos de Auditoría Informática

Se destacan los siguientes tipos (entre otros):

- Auditoría de la gestión: la contratación de bienes y servicios, documentación de los programas, etc.
- Auditoría legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por la normativa legal específica en la materia.
- Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

- Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- Auditoría de la seguridad física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- Auditoría de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.
- Auditoría de las comunicaciones. Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes. (PIATTINI, DEL PESO, & Et Al, 2001)

1.5.2. Importancia de la Auditoría Informática

La auditoría permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización. Se hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma.

1.5.3. Principales pruebas y herramientas para efectuar una auditoría informática

En la ejecución de una auditoría informática, el auditor puede realizar las siguientes pruebas:

- Pruebas sustantivas: Verifican el grado de confiabilidad del Sistema de Información del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

- Pruebas de cumplimiento: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente (PIATTINI, DEL PESO, & Et Al, 2001).

1.5.4. Áreas dónde aplicar la Auditoría Informática

Son:

- A toda la entidad
- A un departamento
- A un área
- A una función
- A una subfunción

Se pueden aplicar los siguientes tipos de auditoría:

- Auditoría al ciclo de vida del desarrollo de un sistema
- Auditoría a un sistema en operación
- Auditoría a controles generales (gestión)
- Auditoría a la administración de la función informática
- Auditoría a microcomputadoras aisladas
- Auditoría a redes (PIATTINI, DEL PESO, & Et Al, 2001)

1.5.5. Herramientas de un Auditor Informático

Los métodos y técnicas aplicadas son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujogramas
- Listas de chequeo
- Mapas conceptuales (PIATTINI, DEL PESO, & Et Al, 2001)

1.5.6. Metodologías para una Auditoría Informática

La auditoría informática es una parte fundamental de la Seguridad Computacional que permite medir y controlar riesgos informáticos que pueden ser aprovechados por personas o sistemas ajenos a cualquier organización o que no deben tener acceso a los datos.

La identificación oportuna de los riesgos ayudará a implementar de manera preventiva, las medidas de seguridad. Para facilitar esta actividad, existen diferentes metodologías que ayudan en el proceso

de revisión de riesgos informáticos. Dos de las más utilizadas son Octave y Magerit.

1.5.6.1. Octave

La metodología Octave es una evaluación que se basa en riesgos y planeación técnica de seguridad computacional. Es un proceso interno de la organización, significa que las personas de la empresa tienen la responsabilidad de establecer la estrategia de seguridad una vez que se realice dicha evaluación, esta metodología permite que la evaluación se base en el conocimiento del personal de la empresa para capturar el estado actual de la seguridad. De tal manera es simple determinar los riesgos críticos.

A diferencia de las evaluaciones típicas enfocadas en la tecnología, OCTAVE está dirigida a riesgos organizacionales y está enfocada en temas estratégicos relacionados con la práctica, es flexible y puede aplicarse a la medida para la mayoría de las organizaciones.

En esta revisión es necesario que las empresas manejen el proceso de la evaluación y tomen las decisiones para proteger la información. El equipo de análisis, integrado por personas de los departamentos de sistemas, de ventas, etc., lleva a cabo la evaluación, debido a que todas las perspectivas son cruciales para controlar los riesgos de seguridad computacional. (GÓMEZ RAMÍREZ, 2014)

1.5.6.2. Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

La metodología Magerit fue desarrollada en España debido al rápido crecimiento de las tecnologías de información con la finalidad de hacerle frente a los diversos riesgos relacionados con la seguridad informática.

La CSAE (Consejo Superior de Administración Electrónica) promueve la utilización de esta metodología como respuesta a la creciente dependencia de las empresas para lograr sus objetivos de servicio.

“Las fases que contempla el modelo MAGERIT son:

1. Planificación del Proyecto.- establece el marco general de referencia para el proyecto.

2. Análisis de Riesgos.- permite determinar cómo es, cuánto vale y cómo están protegidos los activos.

3. Gestión de Riesgos.- permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados".

Al aplicar esta metodología se conocerá el nivel de riesgo actual de los activos, y por lo tanto se podrá mejorar las aplicaciones de salvaguardas y se podrá conocer el riesgo reducido o residual.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos, pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza cuando se utilicen tales medios. (LUCERO GÓMEZ, 2012)

1.6. PROCESO DE LA AUDITORÍA INFORMÁTICA

La siguiente tabla resume los procesos que se deben operativizar para la ejecución de una Auditoría de Sistemas Informáticos:

ETAPAS	PASOS A REALIZAR
Planeación de la Auditoria de Sistemas	1. Identificar el origen de la auditoría. 2. Realizar una visita preliminar al área que será evaluada. 3. Establecer los objetivos de la auditoría. 4. Determinar los puntos que serán evaluados en la auditoría. 5. Elaborar planes, programas y presupuestos para realizar la auditoría. 6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. 7. Asignar los recursos y sistemas computacionales para la auditoría.
Ejecución de la Auditoria de Sistemas	1. Realizar las acciones programadas para la auditoría. 2. Aplicar los instrumentos y herramientas para la auditoría. 3. Identificar y elaborar los documentos de oportunidades de

	mejoramiento encontradas. 4. Elaborar el dictamen preliminar y presentarlo a discusión. 5. Integrar el legajo de papeles de trabajo de la auditoría
Dictamen de la Auditoria de Sistemas	1. Analizar la información y elaborar un informe de situaciones detectadas. 2. Elaborar el Dictamen final. 3. Presentar el informe de auditoría.

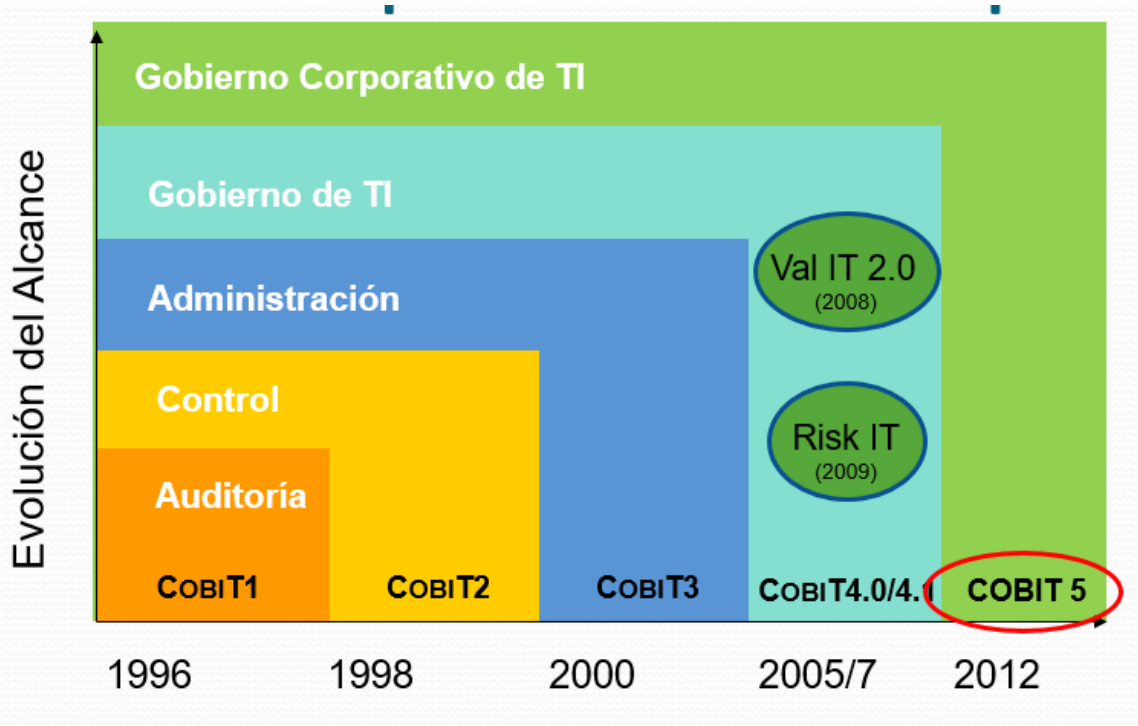
Este criterio es expresado por Francisco Nicolás Javier Solarte en su Guía Didáctica de docencia de Riesgos y Control Informático (SOLARTE SOLARTE, 2014).

1.7. MODELO Y METODOLOGÍA COBIT

La metodología COBIT (**C**ontrol **O**bjectives for **B**usiness and **I**nformation **T**echnologies, cuyo significado es Objetivos de Control para los Negocios y las Tecnologías de Información relacionadas), tiene la misión, según el criterio de sus autores (INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;, 2000), de investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores en más de 180 países, entre los que se incluye Bolivia, comprendiendo todos los niveles de tecnologías de información en: Dirección ejecutiva, gerencia media y participantes para armonizar los estándares de las prácticas de control de TI a nivel mundial, con alianzas estratégicas con otros grupos dentro del ámbito profesional financiero, contable, de auditoría y de TI, asegurando a los dueños del proceso del negocio un nivel sin paralelo de integración y compromiso (INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;, 2000).

Esta asociación cuenta con servicios de: a) programa de certificación para el control y auditoría de TI mediante el Auditor de Sistemas de Información Certificado; y b) Actividades estándar que establecen la base de calidad mediante la cual otras tareas de control y auditoría se miden.

Esta metodología ha sido desarrollada en versiones, desde la 1 hasta la 5, entre los años 1996 hasta 2012, donde el marco empresarial de alcance ha ido incrementando con cada versión: la Auditoría en COBIT 1, el Control en COBIT 2, la Administración en COBIT 3, el Gobierno de TI en COBIT 4 que incluyó Seguridad contra Riesgos y Valor Agregado y todo el Gobierno Corporativo de TI en COBIT 5.



Alcance de COBIT a todo el marco empresarial

Fuente: Asociación de Auditoría y Control de Sistemas de Información (ISACA, 2012)

«Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) Relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- «- La creciente dependencia en información y en los sistemas que proporcionan dicha información
- «- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información
- «- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y
- «- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

«Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la Gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Por lo tanto, la Administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega; al tiempo que demanda que esto se realice a un costo más bajo.» (INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;, 2000)

El criterio anterior es una de las justificaciones que se pueden establecer para utilizar las herramientas que provee la Metodología COBIT.

Como parte de dicha metodología se encuentra el Modelo COBIT, que resultan ser los estándares internacionales generalmente aceptados para la planificación y el proceso de Auditorías Informáticas, a falta de otras normas legales que regulen estas actividades, que inclusive son tomadas en cuenta por las Normas Gubernamentales de Auditoría de Tecnologías de Información y Comunicación emitidas por la Contraloría General del Estado boliviano en 2012 (CONTRALORÍA GENERAL DEL ESTADO DE BOLIVIA, 2012) que permiten asegurar la uniformidad y calidad de la auditoría gubernamental en Bolivia.

El 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 los auditores involucrados en el proceso.

1.7.1. ESTRUCTURA DE LA AUDITORÍA BASADA EN COBIT

El objetivo es la secuencia de pasos a seguir en la planificación, proceso y resultados de la auditoría, siguiendo las guías de acción del modelo COBIT, que debe ser:

1) Situación actual de la Empresa: Misión, visión, entorno general.

2) Selección de Recursos de Tecnologías de Información: Recursos de Hardware, Recursos de Software (Aplicaciones y Software en general). Recursos de Comunicaciones, Recursos de Infraestructura y Recursos Humanos.

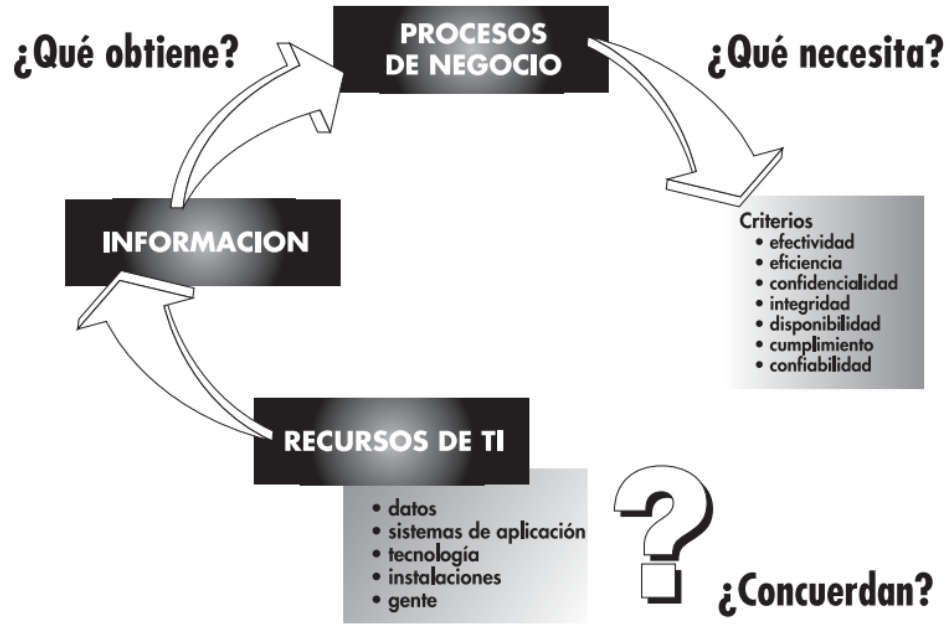
3) Análisis de Riesgos de las Tecnologías de Información: Construcción de una matriz de evaluación de riesgos.

4) Plan de Auditoría: Alcance de la Auditoría, Objetivos de la Auditoría, Identificación de los Dominios, Procesos y Objetivos de Control COBIT aplicables. Matriz de criterios y recursos afectados. Descripción de herramientas, documentos, estándares, directrices, etc.

5) Puesta en Marcha de la Auditoría: Por cada objetivo de control de COBIT, identificar los factores de riesgo. Elaboración de una matriz de pruebas para cada objetivo de control. Recolección de documentación: manuales, procedimientos, funciones.

6) Resultados de la aplicación de la Auditoría: Cuadros de evaluación para cada uno de los objetivos de COBIT. Análisis de Resultados.

7) Informe Final de Auditoría: Carta de entrega de informe. Alcance. Objetivos. Listado de objetivos de control con: Observación, Riesgo, Recomendación. (INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;, 2000)



Identificación de Objetivos de Control auditados utilizando COBIT

Fuente: Instituto de Gobernanza de Tecnologías de Información (INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;, 2000)

2. BIBLIOGRAFÍA

AMADO SUÁREZ, A. (2008). *Auditoría de Comunicación.* La Crujía.

COHEN, L., & MANION, L. (1990). *Métodos de Investigación Educativa.* Madrid: La Muralla.

CONTRALORÍA GENERAL DEL ESTADO DE BOLIVIA. (2012). *Normas de Auditoría de Tecnologías de Información y Comunicación NE/CE-017 .* La Paz - Bolivia: CGE.

ELIZONDO LÓPEZ, A. (2004). *Proceso Contable 3.* México D.F.: International Thomson Editores.

ENCICLOPEDIA DE DEFINICIONES (DEFINICION DE:). (2008-2016). *definicion.de*. Recuperado el 25 de 04 de 2016, de http://definicion.de/informatica/

FLICK, U. (2007). *Introducción a la investigación cualitativa.* Madrid - España: Ediciones Morata S.L.

GÓMEZ RAMÍREZ, V. (2014). *Evaluación de la seguridad de la información con la metodología Octave.* Medellín: Institución Universitaria Pascual Bravo.

INFORMATION SYSTEMS AUDIT AND CONTROL, Asociation; IT GOBERNANCE, Institute;. (2000). (Trad.: Asociación de Auditoría y Control de Sistemas de Información; Instituto de Gobernanza de Tecnologías de Información) *COBIT Objetivos de Control.* Illinois, U.S.A.: ISACA / ITGI.

ISACA. (2012). *Metodología COBIT.* U.S.A.: ISACA. Recuperado el 27 de 09 de 2016, de http://www.isaca.org/cobit

LATTUCA, A., MORA, C., & Et Al. (1991). *Manual de Auditoría.* Buenos Aires: Federación Argentina de Consejos Profesionales de Ciencias Económicas.

LAUDON, K. C., & LAUDON, J. P. (2012). *Sistemas de Información Gerencial.* México D.F.: Pearson.

LUCERO GÓMEZ, A. (2012). *Análisis y Gestión de Riesgos utilizando la metodología Magerit.* Cuenca, Ecuador: Universidad de Cuenca.

MARTÍNEZ BONAFÉ, J. (1988). El estudio de casos en la investigación educativa. *Revista Investigación en la Escuela*(6).

PÉREZ SERRANO, G. (1998). *Investigación Cualitativa: Retos e Interrogantes. I. Métodos.* Madrid: La Muralla.

PIATTINI, M., DEL PESO, E., & Et Al. (2001). *Auditoría Informática, un enfoque práctico.* México D.F.: AlfaOmega Grupo Editor.

SOLARTE SOLARTE, F. N. (2014). *Riesgos y Control Informático.* San Juán del Pasto, Nariño, Colombia: Universidad Nacional Abierta y a Distancia UNAD.

TAYLOR, S., & BOGDAN, R. (1986). *Introducción a los métodos cualitativos de investigación.* Buenos Aires: PAIDOS.