Visionario Digital
www.visionariodigital.org

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Recibido: 05-04-2019 /Aceptado: 08-05-2019/ Publicado: 07-06-2019

Aplicación del sistema COBIT en los procesos de auditoría informática para las cooperativas de ahorro y crédito del segmento 5

Application of the COBIT system in the computer audit processes for the savings and credit cooperatives of segment 5

Jonnathan Oswaldo Campos Pacurucu.[1], Cecilia Ivonne Narváez Zurita.[2] Juan Carlos Eràzo Álvarez.[3], & Yanice Licenia Ordoñez Parra.[4]

DOI: https://doi.org/10.33262/visionariodigital.v3i2.1.584

Abstract.

In Latin America, Ecuador represents the second country with the largest number of savings and credit cooperatives, which has led the control body to create a supervision model aimed at safeguarding the citizens interests especially in the current context, where the creation of strategic alliances has been promoted, through the use of a technological infrastructure to ensure the information transparency and to integrate to the entire popular and solidary financial sector.

In this sense, the computing audit performs an essential role, since it allows to have a deep knowledge about the information technology (IT) management processes, about the existing risks in the computer applications, the procedures and operating rules, the physical security of information and the data and programs backup controls; especially, nowadays where there is a great dependence on computerization in order to warrant the accountant information. This implies enormous transformations in the savings and credit cooperatives internal control and financial evaluation processes, since it requires of exams that allow to establish the compliance

[1] Universidad Católica de Cuenca, Posgradista Maestría en Contabilidad y Auditoría, Cuenca, Ecuador, jocamposp017@psg.ucacue.edu.ec
[2] Universidad Católica de Cuenca, Subdirección de Posgrado, Cuenca, Ecuador, inarvaez@ucacue.edu.ec
[3] Universidad Católica de Cuenca, Subdirección de Posgrado, Cuenca, Ecuador, jcerazo@ucacue.edu.ec

[4] Universidad Católica de Cuenca, Subdirección de Posgrado, Cuenca, Ecuador, jordonezp@ucacue.edu.ec

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

degree about the controls associated with the computer systems, as well as the protection degree about its assets.

Keywords: Computing audit, savings and credit cooperatives, information system, risks, information technology.

Resumen.

En América Latina, Ecuador representa el segundo país con el mayor número de cooperativas de ahorro y crédito, lo que ha conllevado a que el organismo de control genere un modelo de supervisión encaminado a salvaguardar los intereses de la ciudadanía sobre todo en el entorno actual, donde se ha promovido la creación de alianzas estratégicas, mediante el uso de una infraestructura tecnológica que busca transparentar la información e integrar a todo el sector financiero popular y solidario.

En este sentido, la auditoría informática desempeña un rol fundamental, ya que permite tener un conocimiento profundo de los procesos de gestión de las tecnologías de información (TI), de los riesgos existentes en las aplicaciones informáticas, de los procedimientos y normas operativas, de la seguridad física de la información y de los controles de respaldo de los datos y programas; sobre todo hoy en día donde existe una gran dependencia de la informatización a fin de garantizar la información contable. Esto implica enormes transformaciones en los procesos de control interno y en la evaluación financiera de las cooperativas de ahorro y crédito, ya que se requiere de exámenes que permitan establecer el grado de cumplimiento de los controles asociados a los sistemas informáticos, así como el grado de protección de sus activos.

Palabras claves: auditoría informática, cooperativas de ahorro y crédito, sistemas de información, riesgos, tecnologías de información.

Introducción.

En el Ecuador las cooperativas de ahorro y crédito (COAC), son reconocidas por el importante papel que desempeñan para lograr un desarrollo social y económico, permitiendo que el cooperativismo genere factores positivos, son instituciones que se dedican a realizar intermediación financiera para los socios por lo que su principal actividad es captar recursos económicos y otorgar préstamos a corto y mediano plazo. Sin embargo, las COAC del segmento 5 enfrentan muchas dificultades para la colocación y recuperación de cartera, ya que no cuentan con personal capacitado, instalaciones adecuadas y equipo tecnológico de vanguardia que les permitan un desempeño eficaz, lo que da como resultado altos riesgos operativos, financieros, tecnológicos y de mercado, que repercuten sobre su liquidez, solvencia y credibilidad.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

La información que generan las COAC es de uso privado por lo que debe ser manejada con mayor seguridad. Los sistemas informáticos utilizados deben ser seguros de manera que garanticen que los procesos se desarrollen sin contratiempos y que los resultados sean los esperados garantizando el inicio del proceso financiero. Un punto importante para lograrlo es el registro y análisis de las acciones ejecutadas y los eventos desencadenados por cada una de ellas. La estructura de gestión de la información se basa en: a) la planificación de recursos empresariales (ERP) y, b) administración basada en la relación con los clientes (CRM).

La especialización de las tecnologías de información y su aplicación en las actividades computacionales, genera la necesidad de controlar los procesos a través de una auditoría. Este control permite tomar medidas correctivas, asegurando la funcionalidad y productividad de los sistemas de información encaminando a guiar al buen desarrollo y funcionamiento de los mismos.

Auditoría informática

La auditoría informática se la define como el proceso en el cual se recolecta y evalúa la evidencia determinando si los sistemas de información son eficientes en cuanto al uso de recursos para mantener la integridad de los activos y la accesibilidad a los datos. (ISACA, 2011). Para realizar una auditoría, se debe tener presente el objetivo del mismo; dentro del cual se establece la acción que se va a desarrollar con la con el fin de emitir una opinión que refleje con criterio acertado la situación en la que se encuentra la entidad. Es preciso recordar que una auditoría debe ser profesionalmente elaborada con un enfoque neutral sobre los diferentes eventos que se presenten en su desarrollo.

Las etapas de la auditoría informática se resumen en las fases que se muestran en la figura 1.

Figura 1. Etapas de la auditoría informática

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Fase 1: Planificación

En esta fase se adquiere un entendimiento y obtención de información de la entidad que se encuentra auditando considerando prácticas apropiadas para realizar las evaluaciones iniciales. De esta planificación dependerá la eficiencia y efectividad para el logro de los objetivos, siendo realizada por los miembros más experimentados del equipo de trabajo.

Al ser un proceso inicial, debe considerar y seleccionar los métodos más apropiados para realizar las tareas, ya que pueden modificarse durante el proceso de auditoría, por lo que esta se constituye en una ventaja para que el trabajo quede correctamente sustentado. Para iniciar este proceso, el auditor líder emitirá el contrato de trabajo que incluirá entre el objetivo, alcance, lista de personal, tiempo estimado y las instrucciones de la auditoría, siendo este el documento principal para dar inicio a la auditoría. Así, la fase de planeación contará con los puntos que se detallan a continuación.

a) Planificación preliminar. - es entendida como la fase en la que se tiene un conocimiento general de la organización, para lo cual se deben analizar varios elementos como conocimiento de actividades, políticas, prácticas, determinación de la confiabilidad de la información, comprensión global de la dependencia de las TI, determinación de unidades operativas, determinación de riesgos inherentes (Venegas, Esparza, Guerrón, 2017). Para tener el conocimiento sobre estos elementos se debe realizar una evaluación del control interno, aplicando diferentes modelos, que permitan identificar la necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática promoviendo la creación y desarrollo de mejores prácticas como son el COBIT y COSO.

   Como resultado se obtiene el esquema de la planificación en el cuál se detallan: a) antecedentes, b) objetivo, c) alcance de la auditoría, d) bases legales, e) sistemas de información computarizado, f) resultados de auditorías anteriores, g) componentes importantes a ser evaluados en la siguiente etapa y a su vez se elabora una matriz de riesgos.

b) Planificación específica. – de acuerdo a la información obtenida en la planificación preliminar, en esta fase se realiza la evaluación de control interno, determinando los componentes de alto riesgo o que han sido afectados por cambios en los sistemas de información, e incluso permite tener una visión general de la situación de la empresa. Como resultado que se obtiene: a) programas de auditoría, b) plan de muestreo, c) requerimiento de personal técnico, d) cronograma de trabajo, y e) papeles de trabajo (Contraloría General del Estado [CGE], 2015).

Para la evaluación del riesgo de una empresa se verifica si cuenta con procesos de control interno, con el fin de proporcionar seguridad razonable e identificar posibles eventos negativos que se dan como resultado del análisis de la probabilidad de ocurrencia y el impacto

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

que este puede tener si llega a materializarse, Buendía y Campos (1995). De esta evaluación se genera el programa de trabajo que contiene pruebas analíticas, sustantivas y de cumplimiento.

En cuanto a las técnicas de muestreo, Levin y Rubin (2004) las definen como la estratificación de un conjunto de información o datos denominado universo con la finalidad de inferir conclusiones a base de los resultados que se obtengan. El muestreo es aplicable para pruebas sustantivas y de control, considerando siempre la cantidad de información que se maneja. Al establecer el método de muestreo se debe considerar que el mismo se encuentre alineado con los objetivos de la auditoría, al mismo tiempo sea práctico y útil para el trabajo.

Control interno informático

Es un control diario de las actividades de los sistemas de información verificando que cumplan los procedimientos, estándares y normas establecidas por la organización. Su misión según ISACA (2012) consiste en asegurar que las medidas que se obtengan de cada responsable sean correctas y válidas, generando los siguientes objetivos:

- ✓ Controlar las actividades y verificar que cumplan los procedimientos y normas establecidas.
- ✓ Asesorar sobre el conocimiento de las normas implantadas.
- ✓ Colaborar en el trabajo de auditoría informática, así como las externas al grupo.
- ✓ Definir e incorporar mecanismos y controles para comprobar los niveles de confianza adecuados a los sistemas informáticos

El objetivo de control interno es alcanzar los resultados deseados con la implementación de actividades de control; entre estas actividades se encuentran el cumplimiento de las políticas corporativas, confiabilidad de los procesos o servicios de tecnologías de información (TI), como son: a) salvaguarda de activos (información), b) eficacia y eficiencia de operaciones, c) integridad de la información financiera y, d) autorización de las transacciones.

Las categorías de control interno informático se clasifican en:

Preventivas. – son controles que tratan de evitar que un evento negativo se materialice, como por ejemplo un software que verifique los accesos no autorizados al sistema, monitoreando las acciones de ingreso, modificación y eliminación de información. En otras palabras, se puede decir que segregan funciones, controlan el acceso a instalaciones, y establecen procedimientos adecuados para la autorización de transacciones.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Detectivos. - utilizan controles que detectan e informan la ocurrencia de un error, omisión o acto fraudulento como, por ejemplo, la revisión de logs [5]de seguridad o transacciones para detectar intentos de acceso no autorizado, revisión de logs transaccionales para identificar transacciones inusuales. Cuando el control preventivo no es el adecuado, se aplican los controles detectivos.

Correctivos. - cuando se han generado incidencias estos controles facilitan la normalización de los procesos. Entre sus funciones están minimizar el impacto de una amenaza, remediar errores descubiertos por controles detectivos, identificar la causa de un problema, corregir errores y modificar los sistemas de procesamiento para minimizar futuras ocurrencias del problema, mediante planes de contingencia y procedimientos de respaldo.

La inversión en sistemas de TI busca agilizar funciones y procesos específicos que desarrollan las organizaciones haciendo que la administración de información, se vuelva un factor crítico para el éxito de las empresas. Las TI generan cambios en las organizaciones y en las prácticas de negocio, con el fin de obtener nuevas oportunidades y reducción de costos. Por lo que se desarrolla como método de control el COBIT.

El COBIT es un marco de trabajo que permite comprender la gestión de las TI de una organización, así como evaluar el estado en que se encuentran en la empresa. También se lo puede definir como un conjunto de instrumentos de soporte empleados por los auditores para reducir la brecha entre los requerimientos de control y los riesgos del negocio (Ibídem),

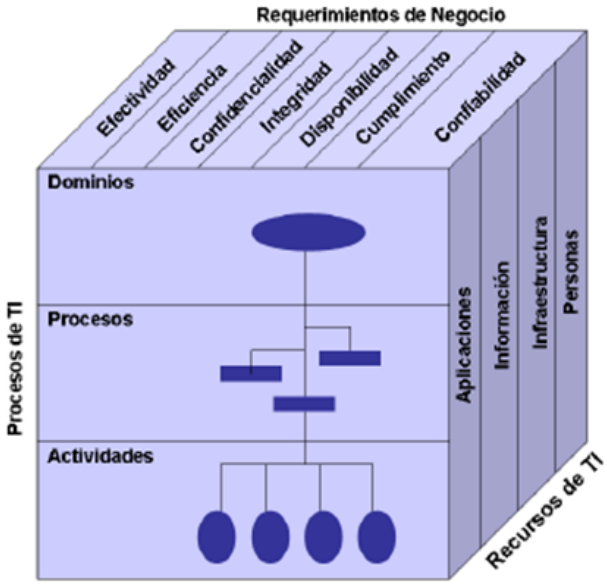
La estructura conceptual se puede enfocar desde tres puntos de vista entre los cuales existen criterios empresariales que deben satisfacer los requerimientos del negocio como la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información; a su vez identificar los recursos de las TI como aplicaciones, información, infraestructura y personas, que son necesarias para alcanzar los objetivos de negocio.

COBIT se divide en tres niveles: dominios, procesos y actividades, las cuales se identifican en la siguiente figura:

[5] Los logs representan los registros que ocurren internamente en los sistemas y redes de toda organización, sistema o aplicación. La entrada a estos archivos contiene datos e información relacionados a eventos específicos que acontecen en las redes o sistemas.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Figura 2. Cubo de COBIT 5



Para llevar a cabo los requerimientos de negocio y recursos de TI es necesario identificar los procesos de TI que se detallan a continuación:

Dominios. – son agrupaciones de procesos que corresponden a una responsabilidad personal (ISACA, 2012).

Procesos. – son una serie de actividades unidas con delimitación o cortes de control (ibídem).

Actividades. – objetivos de control requeridas para lograr un resultado medible (ibídem).

COBIT define las actividades de TI en un modelo genérico de procesos organizados en cuatro dominios:

1) Planear y organizar (PO). - identifica la forma en que las TI pueden contribuir de mejor manera al logro de los objetivos de negocio.

2) Adquirir e implementar (AI). - las estrategias de TI deben estar identificadas, desarrolladas, así como implementadas e integradas dentro del proceso del negocio.

3) Entregar y dar soporte (DS). - hace referencia a la entrega de los servicios requeridos, que se componen desde las operaciones cotidianas, pasando por seguridad y aspectos de continuidad.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

4) Monitorear y evaluar (ME). - deben ser evaluados constantemente para verificar la calidad y cumplimiento en cuanto a los requerimientos de control, integridad y confidencialidad.

Mediante el COBIT se puede desarrollar una política que permite el control de las TI e incide en el cumplimiento e incrementa el valor asociado al área de TI. Ha evolucionado desde su uso para la auditoría de TI, para luego continuar con el control, la gestión de TI, y el gobierno de TI, demostrando un enfoque holístico de gobierno corporativo de TI. COBIT cuenta con cinco principios que una organización debe seguir para adoptar la gestión de TI (figura 3).

Figura 3. Principios de COBIT 5

Para entender los principios del COBIT se debe considerar que el **gobierno corporativo** asegura que se evalúen las necesidades, condiciones y opciones de las partes interesadas para alcanzar las metas; define la dirección a través de la cual realiza la toma de decisiones; mide el rendimiento y cumplimiento respecto a la dirección y metas acordadas; así como establece la **gestión corporativa,** planifica, construye, ejecuta y controla las actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Principio 1. Satisfacer las necesidades de las partes interesadas. - las empresas existen para crear valor manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT provee todos los procesos necesarios para permitir la creación de valor del negocio mediante el uso de TI.

Principio 2. Cubrir la empresa extrema a extremo. - integra el gobierno y la gestión de TI, cubre las funciones y procesos en la empresa; no se enfoca en la "función de TI", sino en la

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa

Principio 3. Aplicar un marco de referencia único integrado. - se alinea con estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de TI de la empresa (ibídem).

Principio 4: Hacer posible un enfoque holístico. - COBIT define un conjunto de catalizadores para apoyar la implementación de un sistema de gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier objeto que puede ayudar a conseguir las metas de la empresa (ibídem).

Principio 5: Separar el gobierno de la gestión. - el marco de trabajo COBIT establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos (ibídem).

La administración de riesgo es un proceso estructurado, consistente y continúo a través del cual la organización identifica, evalúa, mide y, reporta amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos; por lo que se ha desarrollado una estructura conceptual para su administración denominada Enterprise risk management (ERM) para el entendimiento de la formulación y seguimiento de un proceso básico como apoyo al buen gobierno corporativo y mejores medidas de control.

- ✓ Proceso de administración de riesgos. - Morán (2015) señala que es un proceso basado en la comprensión, administración de riesgos y sus impactos, es ajustable a las situaciones donde un resultado no esperado puede ser significativo el mismo que, permite la identificación de nuevas oportunidades.

- ✓ Establecer marco general. - para definir la dependencia entre la organización y el área en el que se desenvuelve, podrá instaurar el argumento organizacional proporcionando a la organización capacidades y habilidades mediante el conocimiento de sus objetivos, estrategias, y recursos humanos. Así mismo, identificar áreas críticas sobre la cual pueda efectuar una gestión de riesgos.

- ✓ Análisis de riesgos. - el uso de TI se ve inmerso en cada actividad que se realiza, sean de carácter económico o aquellas que no tienen una relación directa con el movimiento de dinero, como datos personales almacenados en bases de dominio público o privado (Oxman, 2013).

  Para determinar el riesgo inherente se requiere que se defina una escala de valoración: a) cualitativa: alto, medio, bajo, b) cuantitativa: escala numérica y, c) semicuantitativa: asigna categorías numéricas a las características. La determinación se puede hacer

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

mediante el uso de datos históricos para los métodos cuantitativos, utilizando la siguiente fórmula: Riesgo= Impacto X Probabilidad

Del resultado obtenido se pueden aplicar las siguientes técnicas para administrar el riesgo:

Tabla 1. Técnicas de procedimiento

Técnica	Descripción
Evitar:	Reduce la probabilidad de pérdida al mínimo; deja de ejercer la actividad o proceso.
Reducir:	Mediante la optimización de los procedimientos y la implementación de controles tendientes a disminuir la probabilidad de ocurrencia o el impacto.
Transferir:	Transferir el riesgo de un lugar a otro, esta técnica no reduce la probabilidad ni el impacto, involucra a otro en la responsabilidad.
Asumir:	Acepta la pérdida residual probable, con la aceptación del riesgo las estrategias de prevención se vuelven esenciales.

Fuente: (Kuong, 1997)

- ✓ Riesgos de administración de datos. - la información es un recurso que, como el resto de activos tiene valor para la organización y debe ser protegida garantizando que sea accesible solo a quienes están autorizados; entre sus principales características se encuentran la integridad, que hace referencia a la salvaguarda de la totalidad de la información y los métodos de procesamiento; la disponibilidad que avala el acceso a la información por parte de los usuarios autorizados y de igual manera a los recursos relacionados que se requieran, Coronel (2012).

- ✓ Ciberseguridad. – consiste en la administración de ataques cibernéticos, control de ruptura de privacidad de datos y análisis de impacto de eventos de riesgo, García (2007).

Para evaluar el riesgo informático se elabora la matriz de probabilidad de ocurrencia e impacto de un proceso mal ejecutado, el mismo que permite identificar los riesgos establecidos en el método de evaluación COBIT y, clasificarlos según la relevancia del proceso a fin de tener un entendimiento posterior, tal como se puede apreciar en la tabla 2.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 2. Matriz de probabilidad de ocurrencia e impacto

Probabilidad	Impacto		
	Bajo	**Moderado**	**Alto**
Alto (61% - 100%)	Riesgo Moderado	Riesgo Significativo	Riesgo Inaceptable
Medio (31% - 60%)	Riesgo Tolerable	Riesgo Moderado	Riesgo Significativo
Bajo (0% - 30%)	Riesgo Aceptable	Riesgo Tolerable	Riesgo Moderado

A continuación, la tabla de riesgos identifica la probabilidad de ocurrencia según el periodo en el que se materializa la amenaza y permite conocer el impacto de un proceso según las consecuencias relevantes que generó la materialización de dicha amenaza, logrando determinar criterios de aceptación del riesgo obtenido.

Tabla 3. Tabla de riesgos

Probabilidad (materialización)	Impacto (consecuencias relevantes derivado de la materialización)		
	Bajo 1 (no tiene)	**Moderado 2 (son relevantes)**	**Alto 3 (son graves)**
Alto 3 (cada semana)	3	6	9
Medio 2 (cada mes)	2	4	6
Bajo 1 (cada año)	1	2	3

Documentación de los programas de auditoría informática

Los programas de auditoría son un esquema que sirve para alcanzar los objetivos determinados en la auditoría, identificando las tareas que se van a realizar en los tiempos establecidos y quien las ejecuta (Marketing and web, 2019). Se debe considerar que cuando se elaboran los programas de trabajo estos deben estar alineados a los objetivos de la auditoría

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

garantizando los resultados que se van a obtener en la ejecución, para ello, se debe: establecer el desarrollo de las actividades y procesos a auditar por cada uno de los miembros del equipo; determinar el método que se va a aplicar en la auditoría; y, asignar las tareas a cada uno de ellos.

Para ejecutar los programas de auditoría informática se utilizará el método más conveniente para evaluar el uso de TI, donde se especifica el proceso que se debe trabajar con el objetivo y alcance. Los programas de auditoría identificaran: a) objetivos de auditoría, b) riesgos de auditoría, c) aseveraciones, d) programa de evaluación de pruebas sustantivas y de cumplimiento.

En este sentido, el auditor obtiene conocimiento sobre el examen que se ejecuta, determina el tiempo que se requiere para cada procedimiento y aprovecha la información obtenida considerándola como punto de partida para las próximas auditorías. Por otra parte, el programa de auditoría permite conocer el estado del trabajo e identificar las actividades pendientes a realizar. El bosquejo de un programa de auditoría incluye lo siguiente:

- ✓ Tema. - identifica el área a ser auditada.
- ✓ Objetivo. - el propósito del trabajo a realizar.
- ✓ Alcance. - los sistemas que se incluye en la revisión.
- ✓ Planificación. - recursos y destrezas que necesitan para ejecutar el trabajo, fuentes de información para revisión y lugares donde se va auditar.
- ✓ Procedimientos de auditoría para: a) recopilación de datos, b) personas a entrevistar, c) identificación del enfoque de trabajo, d) políticas, normas y directivas, e) metodología para verificar controles existentes, f) ejecución de pruebas, g) comunicación con la gerencia y, h) Procedimientos de seguimiento.

El programa de auditoría se convierte en una guía para documentar las fases de auditoría y tiene la siguiente estructura:

Tabla 4. Estructura de programa de auditoría.

Programa de Auditoría						
Cliente:		Auditoría a:				
No.	Operación	Horas estimadas	Horas ejecutadas	Realizado por	Ref. P/t	Fecha
	Introducción					
	Objetivo de la auditoría					
	Procedimientos aplicables a la fase 1					
	Procedimientos aplicables a la fase 2					
	Procedimientos aplicables a la fase 3					

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Fase 2: Ejecución

La ejecución de los programas de auditoría previamente establecidos en la planificación específica, permiten evaluar el uso de las TI; como resultado se identifican hallazgos, los mismos que deben estar sustentados con sus respectivos papeles de trabajo, además, las conclusiones que se pueden obtener de los componentes analizados permiten recomendar medidas de control para que la entidad las ponga en ejecución, Los programas de auditoría incluso llevan un registro de todas las pruebas que se aplican para su desarrollo, garantizando así que todos los aspectos a examinar sean cubiertos.

Para la ejecución se necesitan realizar procedimientos de control, que son las que permiten verificar la existencia de controles a través de la indagación u observación directa de los hechos. De estos procedimientos se derivan las pruebas de observación y pruebas de cumplimiento, las cuales tienden a verificar que las actividades se realicen de acuerdo a los controles establecidos; o pruebas sustantivas que proporcionan veracidad y validez de la información que se está estudiando a través de la verificación física mediante la observación (Maldonado, 2001).

Las técnicas que usa el auditor para la verificación de información son automatizadas, sin embargo, estas técnicas deben permitir realizar el análisis de registros, determinación de elementos duplicados, verificación de secuencias y saltos, exportación de información a otro formato, comparaciones de archivos y operaciones con la información, estratificación de archivos, generación y extracción de información y, realización de pruebas de simulación del sistema, Arens (2007). Para realizar estas pruebas, generalmente se basa en una muestra debido a la magnitud de información que se utiliza.

Para la aplicación de estas técnicas se elaboran los papeles de trabajo que son el conjunto de documentos que se obtienen por la elaboración de la auditoría, y estos se van generando de acuerdo al avance del trabajo desde la etapa de la planificación hasta la fase de ejecución, siendo los respaldos para el informe de auditoría. Estos documentos de respaldo deben ser precisos en su elaboración para facilitar la evaluación general y son de responsabilidad propia del área examinada al que corresponda, las cuales deben garantizar su seguridad y custodia.

Los hallazgos son eventos, irregularidades o deficiencias que se encuentran después de aplicar los procedimientos de auditoría en cada programa de trabajo, los cuáles deben ser comunicados únicamente con las personas involucradas en los mismos. Estas evidencias se deben basar en la suficiencia, competencia y confiabilidad de la información. Pueden originarse a partir de observaciones en cuanto al uso de las políticas o por la omisión e incluso distorsión de la información que contienen. Estos hallazgos deben ser evaluados ya sea por componente o en su totalidad, determinando su importancia y su grado de significatividad,

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

es decir, la capacidad de que estos hallazgos pueden o no afectar directamente la veracidad de la información.

Fase 3: Informe

El informe es la comunicación que se realiza sobre el trabajo realizado, el cual contempla todos los resultados positivos o negativos obtenidos en el examen. La comunicación de resultados debe contener: a) título del informe, b) introducción, c) alcance, d) resumen (hallazgos) y, e) opinión.

La opinión del informe se establece de acuerdo a la experticia y juicio del auditor teniendo presente que ante una conclusión siempre se tiene expuesta la responsabilidad del profesional que emite su comentario.

Metodologia.

La presente investigación se desarrolló bajo el enfoque cuali-cuantitativo ya que se consideraron las características y especificaciones propias de las variables de estudio para la elaboración del marco teórico y se combinaron con métodos estadísticos en el tratamiento de la información levantada en la fase de diagnóstico. El estudio se realizó con un alcance descriptivo - explicativo, puesto que se enfocó en la descripción de las actividades que se desarrollan en los distintos departamentos de las COAC del segmento 5 de la provincia del Azuay, para posteriormente de forma detallada explicar la metodología a utilizar por estas instituciones en sus procesos de control sobre el uso de las TI.

En cuanto a los métodos científicos y empíricos se emplearon los siguientes: el método inductivo - deductivo permitió el estudio de casos y teorías generales para llegar a conclusiones particulares sobre instituciones del sector financiero de economía popular y solidaria y el control del uso de las tecnologías de información en las mismas. El método analítico - sintético permitió el estudio en cada una de sus partes de la auditoría informática y de las TI, para luego reestructurarlas, presentarlas y analizarlas de forma integral; el método de observación permitió valorar el manejo, administración y control de las TI en las unidades de análisis. Finalmente, en la investigación se consideraron como unidad de análisis las COAC rurales de la provincia del Azuay, pertenecientes al segmento 5[6], localizadas en los cantones Nabón y Sigsig pertenecientes a la provincia del Azuay, Ecuador. Los tipos de muestreo aplicados correspondieron a técnicas probabilísticas y no probabilísticas sustentadas en el juicio del auditor.

[6] La Junta de Política y Regulación Monetaria y Financiera ubica en el segmento 5 a las COAC que poseen activos hasta 1’000.000,00 dólares de los Estados Unidos de América y a las instituciones financieras constituidas como cajas de ahorro, bancos comunales y cajas comunales (Asamble Nacional de la República del Ecuador, 2014)

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Resultados.

De acuerdo a la información obtenida en la fase de diagnóstico, a continuación, se presentan los resultados:

Disponibilidad. – se identificó que las COAC no tienen claramente identificadas a las personas que deben manejar los activos de información, por ende, no cuentan con responsables de los distintos tipos de información que gestionen la misma con exactitud, accesibilidad, integridad, consistencia, actualización y disponibilidad.

Integridad. – se evidenció que los sistemas informáticos no cuentan con buenas medidas de seguridad, por lo que no se mantiene a salvo la información y los datos importantes de la cuenta ahorristas, esto ocurre a consecuencia de que al sistema acceden usuarios no autorizados a registrar operaciones fuera de tiempo.

Confidencialidad. – el personal tiene acceso total a los sistemas, debido a la falta de limitaciones y jerarquización de los grupos de usuarios. No existe la segregación de funciones en las cuentas personales de cada empleado.

Autenticidad. – los sistemas poseen campos necesarios para el registro de información, permitiendo evaluar que su procedencia sea veraz y autentica.

Trazabilidad. – la transferencia de información se ve interrumpida debido a que los proveedores del servicio de redes no garantizan la velocidad de transmisión de datos por la ubicación geográfica de estas entidades.

A partir de estos resultados y considerando la necesidad de mejorar el manejo de las bases de datos de los sistemas contables de las cooperativas de ahorro y crédito del segmento 5, se propone a continuación una guía de auditoría informática, con la finalidad de que los auditores cuenten con una herramienta que permita evaluar de una manera más ágil y segura el uso de las TI.

Guía de auditoría informática

1. Origen de la auditoría:
   Aquí se determina el por qué surge la necesidad de realizar una auditoría informática. Contestando las preguntas ¿Por qué?, ¿Quién? o ¿Para qué? Se quiere hacer la evaluación de los sistemas de información de la empresa.
2. Visita preliminar:
   Luego de conocer el origen y con la finalidad de tener un contacto con el personal asignado, distribución de los sistemas y donde se localizan los servidores y equipos de cómputo, características, medidas de seguridad y aspectos sobre la problemática

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

que se presenta. Aquí se debe considerar aspectos tales como: distribución de los equipos, servidores que existen, características generales de los sistemas que serán auditados, instalaciones y conexiones físicas existentes, medidas de seguridad física existentes, y limitaciones para realizar la auditoría.

3. Objetivos:
   General. – identificar el fin de lo que se pretenden alcanzar con el desarrollo de la auditoría informática, en él se plantean los aspectos a evaluar.
   Específicos. - son los fines individuales que se proyectan para el logro del objetivo general.
4. Puntos a ser evaluados:
   Se consideran aspectos específicos del área informática y de los sistemas a ser examinados como: la gestión administrativa y el centro de cómputo, el cumplimiento de funciones del personal, operación de los sistemas, programas de capacitación, protección de bases de datos, datos confidenciales y accesos a las mismas, protección de las copias de seguridad y la restauración de la información.
5. Conocimiento de la entidad:

- Antecedentes.
- Base legal de creación.
- Disposiciones legales: normativa externa, normativa interna.
- Estructura orgánica.
- Misión, visión, objetivos institucionales y funciones.

6. Recursos analizados:

Tabla 5. Recursos analizados

Activos	Amenazas
Servidor 1 (contabilidad)	Accesos no autorizados
Servidor 1 (contabilidad)	Alteración de la información
Servidor 1 (contabilidad)	Desaprobación del servicio
Servidor 2 (TI)	Fuga de información
Servidor 2 (TI)	Alteración de la información
Servidor 2 (TI)	Condiciones inadecuadas

7. Trabajadores responsables

Tabla 6. Registro de responsables

Nombres	Apellidos	Título académico	Cédula de ciudadanía	Cargo	Periodo de actuación	
					Desde	Hasta

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

8. Sistemas de información automatizados

Tabla 7. Sistemas de información.

Programas	Descripción	Unidad	Fecha de vigencia
SAAC Full		Contabilidad	
Workflow Team		Sistemas	
Core bancario		Crédito	

9. Plan de muestreo

Considerando los activos más propensos a materializar la amenaza, se debe identificar los riesgos de una manera sencilla en base a una escala de probabilidad e impacto: a) determinar el riesgo aceptable, b) identificar los activos, c) identificar las amenazas de cada activo, 4) establecer la probabilidad y el impacto de que dicha amenaza se materialice; y, 5) establecer medidas para los riesgos que sobrepasen el riesgo aceptable.

Tabla 8. Probabilidad de materialización

Probabilidad (materialización)	**Impacto (consecuencias relevantes derivado de la materialización)**		
	Bajo 1 (no tiene)	**Moderado 2 (son relevantes)**	**Alto 3 (son graves)**
Alto 3 (cada semana)			
Medio 2 (cada mes)			
Bajo 1 (cada año)			

10. Evaluación y calificación de los riesgos de auditoría en base al método COBIT.

COBIT define las actividades de TI en un modelo de 34 procesos genéricos agrupados en 4 dominios:

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 9. Estructura de programa de auditoría.

Dominios	Procesos
Planear y Organizar (PO): cubre las estrategias y las tácticas que identifican como TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Cubriendo los cuestionamientos típicos de la gerencia como: a) ¿Las estrategias de TI están alineadas al negocio?, b) ¿Se optimiza el uso de sus recursos?, c) ¿La calidad de los sistemas de TI es apropiada para las necesidades del negocio?	PO1 Definir un plan estratégico de TI. PO2 Definir la arquitectura de la información PO3 Determinar la dirección tecnológica PO4 Definir la organización y relaciones de TI PO5 Manejar la inversión en TI PO6 Comunicar las directrices y aspiraciones gerenciales PO7 Administrar recursos humanos PO8 Asegurar el cumplir requerimientos externos PO9 Evaluar riesgos PO10 Administrar proyectos PO11 Administrar calidad
Adquirir e Implementar (AI): identifica las posibles soluciones de TI, así como implementa e integra los procesos del negocio. El mantenimiento de los sistemas está cubierto por este dominio. Cubre los siguientes cuestionamientos de la gerencia: a) ¿Los proyectos generan soluciones que satisfacen las necesidades del negocio?, b) ¿Los proyectos son entregados a tiempo?, c) ¿Los sistemas trabajarán adecuadamente una vez sean implementados?, y d) ¿Los cambios afectarán las operaciones del negocio?	AI1 Identificar soluciones. AI2 Adquirir y mantener software de aplicación. AI3 Adquirir y mantener arquitectura de TI. AI4 Desarrollar y mantener procedimientos relacionados con TI. AI5 Instalar y acreditar sistemas. AI6 Administrar cambios.
Entregar y Dar Soporte (DS): cubre la entrega de los servicios requeridos, administración de la seguridad, el soporte del servicio a los usuarios. Cubre los siguientes cuestionamientos de la gerencia: a) ¿Los servicios de TI Se están de acuerdo a las metas del negocio?, b) ¿Optimiza los	DS1 Definir niveles de servicio. DS2 Administrar servicios de terceros. DS3 Administrar desempeño y calidad. DS4 Asegurar servicio continuo. DS5 Garantizar la seguridad de sistemas. DS6 Identificar y asignar costos DS7 Capacitar usuarios. DS8 Asistir a los clientes de TI. DS9 Administrar la configuración. DS10 Administrar problemas e incidentes.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

costos de TI?, c) ¿Los sistemas de TI se manejan de manera productiva y segura?	DS11 Administrar datos. DS12 Administrar instalaciones. DS13 Administrar operaciones.
Monitorear y Evaluar (ME): incluye la administración del desempeño, monitoreo del control interno, el cumplimiento y aplicación del gobierno corporativo; y abarca las siguientes preguntas de la gerencia: a) ¿Mide el desempeño de TI para detectar los problemas antes de que se materialicen?, b) ¿Los controles son efectivos y eficientes?, c) ¿Mide y reporta el riesgo, cumplimiento y el desempeño?	M1 Monitorear los procesos. M2 Evaluar lo adecuado del control interno. M3 Obtener aseguramiento independiente. M4 Proveer auditoría independiente.

Tabla 10. Matriz de evaluación de riesgo

Evaluación de Control Interno

Examen: _____

Período: _____

No	Normativa	Descripción	Ref. P/T	Respuestas			Calificación			Controles Claves	Observaciones
				Si	No	N/A	P	C	%		
1							10		0%		
2							10		0%		
3							10		0%		
4							10		0%		
5							10		0%		
6							10		0%		
7							10		0%		
8							10		0%		
9							10		0%		
10							10		0%		
			Total	0	0	0	100	0	0%		

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

NC = ——— = 0% 100	BAJO

RC = 100%	ALTO

Nivel de confianza (NC)	Bajo	15%-50%	Alto	76%-95%	Riesgo de control (RC)
	Moderado	51%-75%	Moderado	51%-75%	
	Alto	76%-95%	Bajo	15%-50%	

Conclusiones:	

Elaborado por: _____
Fecha: _____

Tabla 11. Matriz de confianza

		riesgo		
		Bajo	**Moderado**	**Alto**
Confianza	**Alto (61% - 100%)**	Moderado	Significativo	Inaceptable
	Moderado (31% - 60%)	Tolerable	Moderado	Significativo
	Bajo (0% - 30%)	Aceptable	Tolerable	Moderado

11. Programas de auditoría

Para llevar a cabo los programas de auditoria, se debe delimitar las etapas, actividades que se van a realizar, estimación de los recursos humanos responsable de realizar la auditoria, recursos materiales e informáticos que serán utilizados y tiempos de ejecución estimados para actividades y para la auditoria. Además, se debe identificar y seleccionar los métodos, y procedimientos necesarios para la auditoria de acuerdo a los planes, presupuestos y programas establecidos en la auditoria.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 12. Programa de Auditoria

Programa de auditoría						
Cliente:		Auditoría a:				
No.	Operación	Horas estimadas	Horas ejecutadas	Realizado por	Ref. P/t	Fecha
	Introducción					
	Objetivo de la auditoría					
	Procedimientos aplicables a la fase 1					
	Procedimientos aplicables a la fase 2					
	Procedimientos aplicables a la fase 3					

12. Programa de actividades: tiempo asignado

Tabla 13. Cronograma de actividades

Días programados y fechas de intervención				
		Días Calendario	Desde	Hasta
I	Planificación y programación:			
	Programado 30%			
II	Trabajo de Campo:			
	Programado 50%			
III	Comunicación de Resultados:			
	Programado 20%			
	Notificación a Comunicación Institucional			
	Entrega de borrador de informe y convocatoria			
	Conferencia Final			

13. Distribución del trabajo: se debe considerar que la auditoria informática se ejecutará cumpliendo lo siguiente:

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 14. Asignación de responsables

Responsable	Actividad	Días calendario	Días programados	
			Desde	Hasta
Auditor Líder	Revisión de la planificación			
	Supervisión de campo			
	Revisión de comunicación provisional de resultados			
	Revisión del borrador del informe			
	Lectura borrador de informe			
Jefe de equipo	Notificación Inicial			
	Conocimiento preliminar de la Entidad			
	Planificación			
	Evaluación del Control Interno			
	Elaborar de comentarios, conclusiones y recomendaciones sobre los hallazgos determinados en el análisis.			
	Elaboración del borrador del informe			
	Conferencia Final			
Operativo	Notificación Inicial			
	Conocimiento preliminar de la entidad			
	Planificación			
	Evaluación del control interno			
	Elaboración de comentarios, conclusiones y recomendaciones sobre los hallazgos identificados en el análisis.			
	Elaboración del borrador del informe			

14. Metodología

La evaluación de la dirección de informática se ejecutará de acuerdo a las siguientes actividades:

- Solicitud de los manuales, estándares y programas de trabajo.
- Cuestionario para la evaluación de la dirección al personal.
- Entrevistas y evaluación de la información
- Elaboración del informe

Los sistemas evaluados se llevarán a cabo según los siguientes procedimientos:

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

- ✓ Análisis de los sistemas, como manuales de operación y del usuario.
- ✓ Recopilación y análisis de procedimientos de cada sistema (flujo de información, reportes y consultas).
- ✓ Entrevista con los usuarios del sistema.
- ✓ Evaluación de la información obtenida ante las necesidades y requerimientos del usuario.
- ✓ Análisis de la estructura y flujo de los programas
- ✓ Análisis y evaluación de la información obtenida
- ✓ Elaboración del informe

Los equipos de cómputo se evalúan según lo siguiente:

- ✓ Características de los equipos actuales
- ✓ Contratos de mantenimiento de equipo y sistemas
- ✓ Contratos de seguros
- ✓ Cuestionario de utilización de equipos informáticos, archivos y seguridad
- ✓ Evaluación de la información recopilada, obtención de gráficas, y su justificación
- ✓ Elaboración del informe.

Es necesario diseñar formatos para la recolección de información y presentación de los resultados, estos documentos denominados papeles de trabajo son elaborados en cada proceso evaluado donde se presenta el dictamen e informe de resultados.

Formato fuentes de conocimiento. - son usados para especificar quien tiene la información, que documentos la poseen, y que pruebas se ejecutan en cada proceso.

Tabla 15. Fuentes de conocimiento

Cuadro de fuentes de conocimiento			Ref. ____
Entidad auditada:		Página	
Proceso auditado:		___ de ___	
Responsable:			
Material de soporte:	COBIT		
Dominio:			
Proceso:			
Fuentes de conocimiento	Pruebas aplicables		
	De análisis	De ejecución	
		Auditor responsable	

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 16. Guía para la evaluación del sistema de control interno.

Entidad:							
Área o rubro evaluado:							
Período:		Del			Al		
Norma técnica de control interno aplicada:							
No.	Preguntas						
		Incipiente	Básico	Confiable	Muy confiable	Optimo	Total factor
		5,0	10,0	15,0	20,0	25,0	0,00
1							
2							
3							
4							

Tabla 17. Identificación de procesos y riesgos asociados.

Descripción del proceso			
Macroproceso	Proceso	Subproceso	Descripción del riesgo
Gestión de TI	Adquisición e implementación	Equipos de computo	
Gestión de TI	Adquisición e implementación	Licencias	
Gestión de TI	Entregar y dar soporte	Respaldos	
Gestión de TI	Entregar y dar soporte	Bases de datos	
Gestión de TI	Planeación y organización	Plan operativo anual	
Gestión de TI	Planeación y organización	Estructura de redes	
Gestión de TI	Monitoreo y evaluación	Control interno	

Formato de cuestionario. - tiene dos objetivos: a) confirmación de riesgos detectados y, b) descubrir nuevos riesgos que no se han detectado, por lo que se aplica solamente al personal que posee la información para responderlo. Las preguntas son de dos tipos, primero sobre la existencia de controles o riesgos, y segundo la complejidad por saber si está aplicando los controles de manera general o parcial.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Tabla 18. Cuestionario

Cuestionario						
Entidad auditada:						
Proceso auditado:					Página	
Responsable:					___ de ___	
Material de soporte:	COBIT					
Dominio:		Proceso:				
Pregunta		Si	No	N/A	Ref.	Fuente
1. ¿ ?						
2. ¿ ?						
Totales						
Conclusiones:		Auditor Responsable				

Formato de hallazgos. - son de importancia ya que llevan la información del proceso realizado y una descripción de cómo se presenta el riesgo y sus consecuencias para la valoración de los riesgos. Además, se puede encontrar información de las recomendaciones para establecer los posibles controles para mitigar los riesgos en el uso de las TI.

Tabla 19. Hallazgo

Hallazgo			Ref. ____
Proceso auditado:		Página	
Responsable:		___ de ___	
Material de soporte:	COBIT		
Dominio:	Proceso:		
Periodo:			
Ref. P/T:			
Condición:			
Criterio:			
Causa:			
Efecto:			
Conclusión:			
Recomendaciones:			

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

15. Informe de auditoria

- Identificación del informe: auditoria informática.
- Identificación del cliente
- Identificación de la entidad auditada
- Objetivos.
- Hallazgos potenciales
- Alcance de la auditoria.
- Conclusiones.
- Recomendaciones
- Fecha del informe
- Identificación y firma del auditor

Conclusiones.

- ✓ La auditoría informática permite identificar la metodología del uso de recursos de TI para la generación de información logrando el cumplimiento de los objetivos para los cuales fue establecido, además da a conocer vulnerabilidades e inconvenientes que obstaculizan el flujo de información.
- ✓ La aplicación de COBIT en la auditoria informática optimiza la utilización de las TI, ya que permite armonizar los beneficios, el manejo de los recursos y los niveles de riesgo, mediante una gestión integral en la organización.
- ✓ La Auditoría informática permite el manejo adecuado de TI y automatización de controles de riesgos, a través de la identificación de: vulnerabilidades de los sistemas de información, riesgos de mayor importancia en el área auditada y toma de medidas preventivas o correctivas para la minimización y materialización de los riesgos.
- ✓ El uso de COBIT en las auditorias informáticas que se lleven a cabo en las cooperativas de ahorro y crédito del sector financiero popular y solidario, permitirá a estas organizaciones contar con una herramienta de buenas prácticas para el manejo de la información, ya que la gerencia y los directivos podrán estrechar la brecha entre los requerimientos de control, problemas de carácter técnico y los riesgos tecnológicos y operativos propios del giro del negocio.

Referencias bibliográficas.

Aldana, S., Vereda, F., Hidalgo-Alvarez, R., & de Vicente, J. (2016). Facile synthesis of magnetic agarose microfibers by directed selfassembly. *Polymer, 93*, 61-64.

Alles, M. A. (2000). *Dirección estratégica de RRHH. Gestión por competencias. Management Master.* Granica .

Álvarez, J. (2010). *Apuntes Auditoría Administrativa.* México: FCA.

Arens, A. (2007). *Auditoría: un enfoque integral.* México: Pearson Prentice Hall.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Arter, D. (2004). *Auditorías de la calidad para mejorar su comportamiento.* Madrid: Díaz de Santos S.A.

Asamble Nacional de la República del Ecuador. (2014). *Código Orgánico Monetario y Financiero.* Quito: Tribunal Constitucional de la República del Ecuador.

Baker, K. (2012). *Administración de riesgo.* México: Trillas.

Bhat, S., Tripathi, A., & Kumar, A. (2010). Supermacroprous chitosan-agarose-gelatin cryogels. in vitro characterization and in vivo assesment for cartilage tissue engineering. *Journal of the Royal Society Interface*, 1-15.

Blanco, Y. (2012). *Auditoría Integral: normas y procedimientos.* Bogotá: D.C: Ecoe.

Bossis, G., Marins, J., Kuzhir, P., Volkova, O., & Zubarev, A. (2015). Functionalized microfibers for field-responsive materials and biological applications. *Journal of Intelligent Material Systems and Structures*, 1-9.

Buendía, M., & Campos, E. (1995). *Tratado de Auditoría Informatica.*

Contraloría General del Estado. (1999). *http://www.contraloria.gob.ec.* Recuperado el 3 de Junio de 2018, de http://www.contraloria.gob.ec: http://www.contraloria.gob.ec/documentos/normatividad/NAFG-Cap-III-1.pdf

Contraloria General del Estado. (2015). Normas Ecuatorianas de Auditoria Gubernamental. En C. G. Estado. Quito, Pichincha, Ecuador.

Coronel, K. (2012). *Auditoría Informatica orientada a los procesos de credito generados en la Cooperativa de Ahorro y Credito "Fortuna" aplicando el marco de trabajo COBIT.*

Cortés, J., Puig, J., Morales , J., & Mendizábal, E. (2011). Hidrogeles nanoestructurados termosensibles sintetizados mediante polimerización en microemulsión inversa. *Revista Mexicana de Ingeniería Química., 10*(3), 513-520.

Davara, M. (2000). *Manual de Derecho Informatico.* Madrid: Editorial Aranzadi.

Derrien, Y. (1995). *Técnicas de la Auditoria Informática.* ALfaomega.

Dias, A., Hussain, A., Marcos, A., & Roque, A. (2011). A biotechnological perspective on the application of iron oxide magnetic colloids modified with polysaccharides. *Biotechnology Advances 29 , 29*, 142–155.

Echenique, J. (1988). *Auditoria de Sistemas.*

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Estrada Guerrero, R., Lemus Torres, D., Mendoza Anaya, D., & Rodriguez Lugo, V. (2010). Hidrogeles poliméricos potencialmente aplicables en Agricultura. *Revista Iberoamericana de Polímeros, 12*(2), 76-87.

Franklin, E. (2007). *Auditoría administrativa: gestión estratégica del cambio.* México: Pearson Prentice Hall.

García Pagan, J. (2007). *Seguridad en redes corporativas.*

García-Cerda, L., Rodríguez-Fernández, O., Betancourt-Galindo, R., Saldívar-Guerrero, R., & Torres-Torres, M. (2003). Síntesis y propiedades de ferrofluidos de magnetita. *Superficies y Vacío., 16*(1), 28-31.

Gomez, A. (2014). *Auditoría de Seguridad Informática.* Madrid: RA-MA, S.A. Editorial y Publicaciones.

Gómez, Estrada, Bauta y García. (2012). Modelo de gestión de log para la auditoría de información.

Haffes, G., Holguín, F., & Galán, A. (1994). *Auditoría de los Estados Financieros.*

Ilg, P. (2013). Stimuli-responsive hydrogels cross-linked by magnetic nanoparticles. *Soft Matter, 9*, 3465-3468.

Imbaquingo Esparza, D. E. (2015). *EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL.* (U. d. ESPE, Ed.)

Imbquingo Daisy, Pusdá Marco, Jácome José. (2016). *FUNDAMENTOS DE AUDITORIA INFORMÁTICA.* Ibarra, Ecuador: Editorial UTN.

Koontz, H. &. (1994). *Una perspectiva global.* Editorial McGraw-Hill.

Kuong, J. (1997). *Seguridad, Control y Auditoria de las Tecnologías de Información.* MASP.

Levin, Rubin. (2004). *Estadística para administración y economía.*

Lewitus, D., Branch, J., Smith, K., Callegari, G., Kohn, J., & Neimark, A. (2011). Biohybrid carbon nanotube/agarose fibers for neural tissue engineering. *Advanced Functional Materials, 21*, 2624-2632.

Lin, Y.-S., Huang, K.-S., Yang, C.-H., Wang, C.-Y., Yang, Y.-S., Hsu, H.-C., . . . Tsai, C.-W. (2012). Microfluidic synthesis of microfibers for magnetic-responsive controlled drug release and cell culture. *PLoS ONE, 7*(3), 1-8.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Maldonado, M. (2001). *Auditoría de Gestión.* Quito, Ecuador.

Marketing and web. (15 de january de 2019). Obtenido de https://www.marketingandweb.es/emprendedores-2/plan-de-trabajo/

Mendivil, V. (2010). *Elementos de auditoría.* México: Cengage Learning.

Morán, D. (2015). *Auditoria Informatica Administracion de Riesgos.*

Piattini Mario G., Del Peso Emilio. (2001). *Auditoría Informática Un Enfoque Práctico.* ALFAOMEGA GRUPO EDITOR.

Piattini, M. (2001). *Auditoría Informatica Un Enfoque Práctico* (2da Edición ed.). Mexico: ALFAOMEGA GRUPO EDITOR .

Piattini, M., & Del Peso, E. (1998). *Auditoría Informática, Un enfoque práctico.*

Piattini, M., & Del Peso, E. (2001). *Auditoría Informática Un enfoque práctico* (Segunda edición ed.).

Ruiz Estrada, G. (2004). *Desarrollo de un Sistema de liberación de fármacos basado en nanopartículas magnéticas recubiertas con Polietilénglicol para el tratamiento de diferentes enfermedades.* Madrid: Universidad Autónoma de Madrid. Departamento de Física Aplicada.

Shim, J. (2000). *Respuestas rápidas para Sistemas de Información.* Editorial PEARSON.

Solis, G. (2002). *Reingeniería de la Auditoria Informática.* México: Trillas.

Song , J., King, S., Yoon , S., Cho, D., & Jeong, Y. (2014). Enhanced spinnability of narbon nanotube fibers by surfactant addition. *Fiberes and Polymers, 15*(4), 762-766.

Tartaj, P., Morales, M., González-Carreño, T., Veintemillas-Verdaguer, S., & Serna, C. (2005). Advances in magnetic nanoparticles for biotechnology applications. *Journal of Magnetism and Magnetic Materials, 290*, 28-34.

Venegas L, Esparza F, Guerrón D. (2017). *Evaluación y Auditoría de Sistemas Tecnológicos.*

Wulff-Pérez , M., Martín-Rodriguez, A., Gálvez-Ruiz, M., & de Vicente, J. (2013). The effect of polymer surfactant on the rheological properties of nanoemulsions. *Colloid and Polymer Science, 291*, 709–716.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

Zamora Mora, V., Soares, P., Echeverria, C., Hernández , R., & Mijangos, C. (2015). Composite chitosan/Agarose ferrogels for potential applications in magnetic hyperethermia. *Gels.*, *1*, 69-80.

ISSN: 2602-8506
Vol. 3, N°2.1., p. 445-475, junio, 2019

PARA CITAR EL ARTÍCULO INDEXADO.

Campos Pacurucu, J., Narváez Zurita, C., Eràzo Álvarez, J., & Ordoñez Parra, Y. (2019). Aplicación del sistema COBIT en los procesos de auditoría informática para las cooperativas de ahorro y crédito del segmento 5. *Visionario Digital*, *3*(2.1.), 445-475. https://doi.org/10.33262/visionariodigital.v3i2.1.584